First Impression: 2012

Recent Trends in IT and Green Computing
(ETIT – 2012)

24th & 25th February 2012

Editor

Dr. Rupa Hiremath
Director MCA

© Indira Institute of Management (MCA) Pune, —SARATHYA
3rd National Conference on Emerging Trends in Information Technology

No part of this publication may be reproduced or transmitted in any form by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the copyright owners.

DISCLAIMER

The author solely responsible for the contents of the papers compiled in this volume. The publishers or editors do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future.

ISBN: 978-81-910244-0-1
# Content

## Guest Section:

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Title</th>
<th>Author</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Academia to Industry: how to stay ahead Of the Game</td>
<td>Mahesh Baxi Managing Director, ThoughtWorks</td>
<td>01-03</td>
</tr>
<tr>
<td>2</td>
<td>Emerging Trends – Big Data Space</td>
<td>Hemant Joshi Sr. Consultant, TCS System Research Lab</td>
<td>04-07</td>
</tr>
<tr>
<td>3</td>
<td>Be Sure from Cyber Crime</td>
<td>Malle Malikarjun Project Manager &amp; Consultant Cyber Crime Branch</td>
<td>08-10</td>
</tr>
<tr>
<td>4</td>
<td>Distributed Defense Against DDoS Attacks</td>
<td>Maitreya Natu Sr. Scientist TRDDC Pune</td>
<td>11-19</td>
</tr>
<tr>
<td>5</td>
<td>IT for Green: Road Transportation Sector</td>
<td>Dnyaneshwar Kamble CMC Ltd.</td>
<td>20-25</td>
</tr>
<tr>
<td>6</td>
<td>Embedded System – Trend and Career Opportunities</td>
<td>Abhay Arvind Phansikar &amp; Ashok Dhanji Jagatia</td>
<td>26-30</td>
</tr>
<tr>
<td>7</td>
<td>Innovation in Information Technology</td>
<td>Allalkathan K. Group Project Manager Infosys</td>
<td>31-36</td>
</tr>
<tr>
<td>8</td>
<td>Meeting of the need of Mobile User!</td>
<td>Werner Egipsy Souza Technology Consultant</td>
<td>37-41</td>
</tr>
<tr>
<td>9</td>
<td>Trends in Mobility</td>
<td>Mr. Vivek Mohile Persistent System Ltd.</td>
<td>42-47</td>
</tr>
</tbody>
</table>

## Faculty & Student Section:

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Title</th>
<th>Author</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Android Operating System</td>
<td>Vaishali Manoj Dardige IIMP-MCA</td>
<td>48-55</td>
</tr>
<tr>
<td>11</td>
<td>Popularity &amp; Growth of Android Operating System for Mobile Phones</td>
<td>More Laxman JSPM</td>
<td>56-58</td>
</tr>
<tr>
<td>12</td>
<td>Android</td>
<td>Varsharani B. Budde &amp; Sominath P. Pathare IIMP-MCA</td>
<td>59-65</td>
</tr>
<tr>
<td>13</td>
<td>Channel Allocation for Cellular Mobile Network</td>
<td>Shobha Mishra Asst. Prof. Navasahyadri</td>
<td>66-70</td>
</tr>
<tr>
<td>14</td>
<td>Android</td>
<td>Digamber Dilip Dhole IIMP-MCA*</td>
<td>71-79</td>
</tr>
</tbody>
</table>

## Android

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Title</th>
<th>Author</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Android Operating System</td>
<td>Vaishali Manoj Dardige IIMP-MCA</td>
<td>48-55</td>
</tr>
<tr>
<td>11</td>
<td>Popularity &amp; Growth of Android Operating System for Mobile Phones</td>
<td>More Laxman JSPM</td>
<td>56-58</td>
</tr>
<tr>
<td>12</td>
<td>Android</td>
<td>Varsharani B. Budde &amp; Sominath P. Pathare IIMP-MCA</td>
<td>59-65</td>
</tr>
<tr>
<td>13</td>
<td>Channel Allocation for Cellular Mobile Network</td>
<td>Shobha Mishra Asst. Prof. Navasahyadri</td>
<td>66-70</td>
</tr>
<tr>
<td>14</td>
<td>Android</td>
<td>Digamber Dilip Dhole IIMP-MCA*</td>
<td>71-79</td>
</tr>
</tbody>
</table>

## Green Computing

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Title</th>
<th>Author</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Cloud Computing Services, Techniques, Security Issues and Their Resolution</td>
<td>Mane Dnyaneshwar JSPM</td>
<td>80-83</td>
</tr>
<tr>
<td></td>
<td>Title</td>
<td>Author(s)</td>
<td>Pages</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>16</td>
<td>Green Computing</td>
<td>Anna G Pol IIMP-MCA</td>
<td>84-90</td>
</tr>
<tr>
<td>17</td>
<td>Green Computing</td>
<td>Mitesh Agarwal IIMP-MCA</td>
<td>91-97</td>
</tr>
<tr>
<td>18</td>
<td>Green Computing: A way to Sustainable Development</td>
<td>Prof. Mrs. Pallavi N. Shintare MCE</td>
<td>98-99</td>
</tr>
<tr>
<td>19</td>
<td>Green Computing: A Waste Minimization Procedure</td>
<td>Sumit O Sharma Asst. Prof. DMS Sevagram</td>
<td>100-102</td>
</tr>
<tr>
<td>20</td>
<td>Modify Green IT</td>
<td>Vijai A Tathe CSIT Chichawad</td>
<td>103-108</td>
</tr>
<tr>
<td>21</td>
<td>Understanding the Cloud Computing</td>
<td>Akash Sangamnerkar PCCE</td>
<td>109-112</td>
</tr>
<tr>
<td>22</td>
<td>Cloud Computing</td>
<td>Swapnil Gaikwad JSPM</td>
<td>113-116</td>
</tr>
<tr>
<td></td>
<td><strong>Information Technology</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Context Aware Application</td>
<td>Sanket Kene IIMP-MCA</td>
<td>117-121</td>
</tr>
<tr>
<td>24</td>
<td>Virtual Reality Technology</td>
<td>Partha Sardar IIMP-MCA</td>
<td>122-128</td>
</tr>
<tr>
<td></td>
<td><strong>Network Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Network Security</td>
<td>Abhijit B. Kulkarni &amp; Kranti B. Yadav JSPM</td>
<td>140-146</td>
</tr>
<tr>
<td>27</td>
<td>Network Security</td>
<td>Nikhil Sonakamble IIMP-MCA</td>
<td>147-151</td>
</tr>
<tr>
<td>28</td>
<td>Using Wireless Technology</td>
<td>Sharad S Salve IIMP-MCA</td>
<td>152-158</td>
</tr>
<tr>
<td></td>
<td><strong>General</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>E-commerce as a Recent Trends in IT</td>
<td>Sagar Rajendra Kulkarni PITMSR</td>
<td>159-166</td>
</tr>
<tr>
<td>30</td>
<td>Ethical Hacking</td>
<td>Deepak B Kadave &amp; Reshma P Mavakar</td>
<td>167-177</td>
</tr>
<tr>
<td>31</td>
<td>Growth of Blue-Ray Disc</td>
<td>Birajdar Bhaurao D Y Patil</td>
<td>178-180</td>
</tr>
<tr>
<td>32</td>
<td>World of Inventory</td>
<td>Manisha Manoj Upadhyay</td>
<td>181-183</td>
</tr>
<tr>
<td>33</td>
<td>The Impact of Social Media on Online Marketing of Financial Services</td>
<td>Gajanan P Mudholkar SRTM University Nanded</td>
<td>184-187</td>
</tr>
</tbody>
</table>
Guest Section:

1. Academia to the Industry – How to stay ahead of the game?

Mr. Mahesh Baxi Managing Director, ThoughtWorks

I happened to watch a Hindi movie called ‘Aarakshan’ the other day and was shocked to see how the education ‘industry’ is portrayed. I am not saying that the movie reflects the absolute reality, but it does bring some disturbing facts to light. In the last couple of decades, the education system has undergone unprecedented commercialization including large number of universities opening up across India. However, it feels like the gap between academia and industry has widened especially in fast moving fields like IT industry. Currently, as of 2011, approximately 350,000 engineering students graduate each year in India with over 2.5 million university graduates. As per the study conducted by McKinsey recently, an alarming 25% of these engineering graduates remain unemployed. In a separate report, NASSCOM projected a shortage of about 500,000 knowledge workers in the IT industry. These two contrasting reports are one of the many indicators of a deep incongruence between the demands of the industry and the quality desired OF its work force.

UN is predicting that if developed economies and developing economies doesn’t come up with coordinated strategy for jobs and growth, world will be pushed towards global recession (http://www.un.org/en/development/desa/policy/wesp/index.shtml). UN is predicting that developed economies will have negative growth in 2012 and about 1.1% in 2013 while developing economies like China, India & Brazil will drive growth of developing world at around 4% which is still lower than original prediction.

What does this mean for fresh graduates? Will the job opportunities drop? Will companies not hire new blood? Will there be no exciting startup initiatives? Will the VC’s stop funding new cutting edge ideas? No, these and other new avenues that create jobs will continue to open up but the rules of the game are going to be more stringent. The competition in the field will get fierce
and intense. The good news is that there are things that you can focus on which will help you not only survive but thrive in any market conditions. This article focuses on three key elements, which will help you differentiate yourself from the ‘crowd’.

1. Be Innovative

As vague as the definition of ‘innovation’ might be – it does get recognized when something different happens in the market or when you come across a product that ‘wows’ you. I think we all can agree that Innovation has led to many of the products that we now use in our day to-day life and curiosity has fueled human being to be innovative. Many of the companies we see today have thrived in the global market because of their innovation such as Salesforce.com through their Software as a Service Approach, Apple through many of the products such as iPad, iPhone but primarily about bringing that entire experience together, Flipkart for bringing Amazon.com like buying experience to India with an amazing site. However, the ones, which managed to fetch my attention, were companies like Tata. They have been innovating which is also known as ‘Frugal’ innovation where you not only develop products for the masses and needy people but to make sure that it can reach to rural places. Tata Nano is one such example that everyone is aware. They also have invested water purifier, which costs only $21, doesn’t use any electricity and filter lasts for up to 200 days. What is more fascinating is recent tie-up of Tata with SunCatalytix who have invested a way to generate electricity with just a jar of water.

While companies who are innovative thrive in any market condition, if you are creative in your approach (irrespective of what you do) and if you bring ideas which are relevant to ever changing market place - you are sure to be noticed and put you in a different comparison bucket.

2. Be Passionate

“Passion alone determines what one should or should not be doing because it enables one to overcome all obstacles” (unknown source). I think this statement sums it all up as t should not be doing because it
enables one to overcome all obstacles” (unknown source). I think this statement sums it all up as to why following your passion is so important. A great example is Henri Ford who was born to a farmer. At 15, he dismantled and reassembled the timepieces of friends many times and was very passionate about machines. After his mother dies in 1876, his father expected him to take over the family farm but he was absolutely not into farming at all. He argued, fought with father and finally, left home to work as an apprentice machinist in the city of Detroit. From then on – he worked several different jobs and founded Ford Motors. He was one of the most successful people of that time

While being passionate is important, knowing what you are passionate about is equally important. Also, it is important to understand what big problem of the world serve as your passion such as climate change, sustainability, poverty, education, health care, emerging markets etc. You have to experiment with some, you may have to develop more awareness, travel with your eyes & ears open, look into your past to see what personal issues you have faced which you would like to solve. If you find your passion and make that your profession – you will always be ahead in any competition.

3. Learnability and Adaptability

If you have chosen to be in the IT field, you are in one of the most non-static field in the industry. If you or your organization don’t have or maintain learn-ability, you will very quickly lose competitive advantage that you may have. Gone are the days when companies used to make really long-term strategy and execution plans. In the current global market place, what you need is an ability to learn, quickly experience and adapt to changing global and emerging markets.

So remember – know your passion, be innovative in whatever you do and keep your eyes and ears open to quickly learn what’s happening around you and adapt to changing situations quickly.

If you do this – you will help yourself by changing your ‘comparison parameters’ and automatically put you ahead in the game.
2. Emerging Trend – Big Data Space

By Hemant Joshi, Senior consultant, TCS System Research Lab

Introduction

Data has always played a critical role in business. Organizations have always mined internal and external data for increasing the efficiency of their operations or gaining a competitive advantage in the market. And the rules for success have always been the same; those who can obtain and exploit that extra bit of knowledge, gains handsomely. What is happening around us today is erringly similar, and yet different. And the difference lies in the quantum and complexity of data used for analysis – it’s “Big Data”.

Big Data refers to data sets whose **volume, variety, velocity** and complexity make it extremely difficult for current databases and architectures to Store, Manage and Process to gain business insights. The overwhelming digitization of information; viral spread of sensors, smartphones and other connected devices; and the increasing use of social media as a communication channel provides a varied source of data to tap into for business analytics. This data however is extremely huge in volume and growing rapidly, and is made up of a lot of free form text, voice and pictures along with structured data from the enterprise. The traditional database technologies and analytical engines are unable to deal with this volume and variety. The advent of a new technology in the form of Hadoop and its stack is providing the ability to manage and process this data in ways and at speeds not thought of being possible before.

Big data analytics is changing the way companies of all sizes, in all industries, go about their business. From the way they understand their markets, to how they mine information about their own operations; big data is unlocking insight at every turn. The real value from ‘Big Data’ is expected to be in the form of “deep insights” derived predominantly using data mining, statistical, optimization and forecasting
techniques. Businesses would be able to gain significant benefits only when they convert these “insights” into products and offerings that their end customers would love and thus increase customer retention and product sales and hence revenue; and / or use the “insights” to streamline operations and save costs.

**The Technology behind Big Data**

The exponential growth in the volume, velocity and variety of data is increasingly demanding for more storage, compute, integration and analytics platforms to effective use of data in business. Big data technologies include distributed file system (DFS), massively parallel processing (MPP) databases, mining techniques, high speed internet and scalable storage solutions.

Agile analytics and powerful processing technology rank high on investment priorities for the financial services firm. They are investigating next generation technologies for data analytics. One of the most promising technologies is the open source Apache Hadoop software and MapReduce framework for dealing with “big data” challenge. Big names like Yahoo, Google, Facebook, twitter etc. are the early adaptors of Hadoop framework.

Following diagram depicts the typical Hadoop stack across different layers:

![Figure 1: Hadoop Technology Stack](image-url)
The core components of Hadoop, viz., the distributed file system and the distributed programming (i.e. MapReduce) come from Google. Google published its papers on Google File System and the MapReduce framework in 2003 and 2004, based on which the Hadoop DFS and MapReduce framework were first created in 2005. Since then it has been significantly enhanced and a number of tools and frameworks have been developed to tackle the varied problems.

While Hadoop has been the poster boy for Big Data Technologies, other developments that have also boosted the processing power are

a) NoSQL Databases
b) Cheaper and faster disks. Larger Flash drives.
c) Faster and multi-core chips.
d) Open sourcing of statistical and graph algorithms.

**Industry Trends**

The advent of Big Data processing capabilities is a game changer for many industries. The possibilities for analyzing the data and gaining insights are immense, and therefore this ability would give the organizations real business advantages over their competition.

The timing couldn’t have been any better. We now stay in an increasingly digital world; with over 95% of all information produced in the digital format. Both humans and “things” are more connected than ever and getting smarter day-by-day. There is a lot of voluntary data / information sharing via Facebook, Twitter, Blogs, etc. All of this produce terabytes of data daily which when combined with the data from an enterprise can become a goldmine.

The supporting technology however is in its early days. Many components are still being developed around Hadoop to address different gaps and / or create various new features. The first versions of commercial tools are just getting released, and none of them seem to have all the various features that are available in the open source.

From the business side, organizations are just beginning to realize the various ways in which this Big Data can be used to create a differentiaation and get into an advantageous position with respect to the competition. The applications known today are the proverbial tip of the iceberg, with lots of new
possibilities still under the covers. While there are a large number of problems that can be addressed by Big Data solutions, some of the following key analytics would help organizations differentiate themselves in a very crowded market place today:

- **Consumer Sentiment analysis**
- Recommendation Engines based on **predictive analysis**
- **Event analytics** - events led to a desired outcome considering customer portfolio and goals
- Fraud detection and **security analytics** based on transaction
- **Risk Analytics** Identify, measure, monitor and control risk
- **Context Aware Services** for improved user experiences based on personal interests, intentions, connections and so on.

The key to success in this new and fast developing world of big data lies in:

a) Identifying the right scenarios that would make a difference.
b) Applying the right techniques to the problem
c) Collaborating across organizational boundaries to create a unique solution

The Web based companies with marketing as their primary revenue stream (Facebook, Google, Twitter, etc) have been at the forefront of using Big Data to their advantage. The large financial services firms and retail companies have been busy creating customized solutions. However there are a number of other sectors like Power / Utilities, Government, Healthcare, Education etc where the use of this technology can make a world of difference.
3. Be secure from cyber criminals

By Malle Mallikarjun

cybercrime@consultant.com

The rising cyber crime is an indication of an enormous threat to national security law makers and law enforcement agencies to give immediate attention to the matter in today’s age when everything from, small gadgets to nuclear plants is being operated through computers, cyber crime has assumed threatening ramifications.

What is cyber crime?

“Any criminal activity that use a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.” Various kinds of cyber crimes are prevailing in the world today. Hacking, bombing, diddling, spoofing, botnet attacks, Salami attacks and Viruses are capable of breaching the security in the information systems of vital installations. The first recorded cyber crime dates back to 1820.

“For hackers, it is no longer a matter of disrepute. Now the game is all about money. The players can now be identified, their roles are identified and they can enjoy the returns on their investments. A cyber criminal is no longer the nerd who loves to stay indoors but is now the nerd who loves to stay indoors but is now an organized gangster closely associated with drug-trafficking, extortion and money laundering.” People with comparatively low technical skills can also steal thousands of pounds a day in the world of cyberspace. It is like giving a loaded gum in the hands of a small child. Cybercrime flaunts a large international market for skills, tools and finished products. It even has its own currency. Unlike conventional communities, there are no policemen patrolling the cyber freeways that are open to all kinds of grime including Trojans, love bugs, cyber stalking and cyber terrorism. Website, fake advertise in media, online data entry jobs like this….

“There is huge potential for damage to national security through cyber attacks. The internet is a means for money laundering and funding terrorist attacks in an organized manner. Online child pornography, trafficking in contrabands and e-commerce frauds are on the rise.” Dos attacks
may favor the assailant, but skilled it professionals can counter them. There are no simple ways to prevent the World Wide Web from becoming a zone where powerful criminals operate unfettered and large players can push around small ones. Software makers can work to make systems more secure, but many computers are compromised by user error rather than technical flaws. The public can better educated in computer security. But I think human nature is imperfect.

Setting international standards to counter cybercrime, while still protecting civil liberties, will be a continuing challenge. Gaining control of a bank account is increasingly accomplished through phishing. Add phishing to the other cyber-criminal activities driven by hacking and virus technologies such as carding, adware/spyware planting, online extortion. On top of viruses, worms bots and Trojan attack organizations in particular are contending with social engineering deception and traffic masquerading as legitimate applications on the network. In a reactive approach to this onslaught, companies have been layering their networks with stand alone firewalls intrusion prevention devices, anti-virus and anti-spyware solutions in a desperate attempt to plug holes in the armoury

Internet users using unsecured WiFi connections are the next victims after Cyber Café owners, whose connections have been found to be used by Terrorists Outfits clamming responsibility for various blasts in the country. In view of such threats, TRAI has issued various instructions to the ISPs to be followed by WiFi users to make sure there is connection is fully secured and there is no possibility of misuse. “Cyber crime is omnipresent and although cyber crime cells have been set up in major cities, most cases remain unreported due to lack of awareness.” Cyber crime is an issue that needs to be addressed without further delay. If technology takes over an entire race the consequences can be alarming. The entire world is living in the shadow of the constant threat imposed by organized cyber crime. It is high time we do something about it- before it is too late...

**Indian Government wants to know where you are!**
The government is looking to track all mobile phone users. Our govt wants to know where you are on real time basis and has made amendments in the law which would force mobile operators to share details of users’ longitude and latitude at real time basis.

As per amendments made to operators’ licenses, beginning May 31, operators would have to provide the Department of Telecommunications real-time details of users’ locations in latitudes and longitudes.

Documents obtained by The Indian Express show that details shall initially be provided for mobile numbers specified by the government. Within three years, service providers will have to provide information on locations of all users.

The will have some margin of error at first. But by 2013, at least 60 per cent of the calls in urban areas would have to be accurately tracked when made 100 meters away from the nearest cell tower. By 2014, the government will seek to increase the proportion to 75 per cent in cities and 50 per cent in suburban and rural areas.

For calls made 300 meters from the nearest cell tower, accurate coordinates will be required for 95 per cent in cities and 60 per cent in towns and villages at the end of two years.

The changes in license terms also include making service providers completely responsible for the security of their networks. License holders would pay a fine of Rs 50 crore for any breach of security. The government can also start criminal proceedings for a breach.
4. Distributed Defense Against DDoS Attacks

Rohan Patil and Maitreya Natu
Tata Research Development and Design Centre, Pune, India.
Email: rohanpatil.id@gmail.com, maitreya.natu@tcs.com

Abstract—In this paper we discuss the need for a paradigm shift from single-point defense to a distributed defense against DDoS attacks. Defense nodes need to be deployed at strategic locations in the client, core, and victim networks. The strengths of different network locations need to be exploited to build a robust framework in order to mitigate the ever-increasing threat posed by DDoS attacks. This paper presents a discussion of the defense capabilities required for DDoS defense and the best locations to deploy these capabilities.

I. INTRODUCTION

Distributed denial of service (DDoS) attacks remain an unmitigated threat to today’s networks in spite of various academic and commercial attempts to build an effective defense. This unmitigated threat can be attributed to various factors such as the large number of potential attackers, continuously evolving types of attacks, ability of the attackers to hide their identity through techniques such as spoofing, reflector attacks, zombie attacks, etc. Previous attempts on DDoS defense provide two main insights: (a) Wide deployment is a necessary condition for a DDoS defense. Many smart defenses, when deployed sparsely, can be defeated by the attacker by either being too diffused to bypass unnoticed, or being too large to overwhelm the defense itself [2], [4]. (b) There is a critical need for a sophisticated mechanism to differentiate legitimate traffic from attack traffic. However, the wide variety of attacks, the large scale of attacks, together with limited resources at the defense node, etc. make it very difficult to accurately differentiate legitimate traffic from attack traffic.

In this paper, we survey the existing techniques and identify opportunities and challenges in order to develop a defense against DDoS attacks using the above two insights.
II. DEFENSE FUNCTIONALITIES

A DDoS defense requires three vital functionalities namely (a) Attack detection: quickly detecting the presence of an attack; (b) Traffic differentiation: differentiating legitimate traffic from the attack traffic; and (c) Rate limiting: providing preferential treatment of the shared resource to the legitimate traffic.

A. Attack detection

It is essential to correctly detect all malicious attacks that can potentially damage the system. Detection of an attack triggers an alert that in-turn causes other defense functionalities to turn on the defense mechanisms. Missing the detection of a genuine attack can make all other operations futile. On the other hand, incorrectly detecting an attack can lead to additional effort by defense mechanism and also potential collateral damage. While detecting a DDoS attack it is very important to differentiate a legitimate increase in traffic from an attack. Attack detection needs to be done at locations close to victim network where maximum traffic can be observed. However such locations observe large traffic volumes. Hence, attack detection needs to be computationally light-weight. Attack detection has been done in various ways in the past such as – by observing traffic signatures, checking for anomalies, profiling user-traffic patterns.

B. Traffic differentiation

One of the most vital functionalities of a DDoS defense is to differentiate legitimate traffic from attack traffic. The traffic must be classified into categories of legitimate, attack, and unknown classes. Different classification mechanisms support different levels of classification. Some solutions only provide binary classification of legitimate and attack traffic. A binary classification carries the risk of high collateral damage in case of incorrect classification. Hence, some solutions classify senders into different levels of legitimate and attack nodes. This classification needs to be communicated to other defense nodes to ensure preferential treatment to legitimate traffic over attack traffic. Incorrect traffic differentiation can lead to high collateral damage. Because of possibility of IP spoofing, the IP address cannot be used to classify
legitimate from attack clients. Hence, there is a need to provide another unique identification of legitimate client traffic that can enable defense to differentiate legitimate client from attackers even in the presence of IP spoofing. A lot of work on capability based traffic differentiation has been done in the past. Mechanisms such as IP Easypass [6] provide dynamically changing identifiers in the header extensions. Mechanisms such as PI and StackPI [7] use the intermediate routers to stamp packets to provide such identifiers. The mechanism used to insert these capabilities also decides the level to which the attackers can be localized. By using the routers techniques such as traceback [5] and pushback [1] are able to trace the attack nodes close to the source networks. On the other hand, techniques such as IP Easypass [6] only use source and victim nodes to enable capabilities. Such techniques can differentiate legitimate traffic from attack traffic but cannot localize the attack nodes.

C. Rate limiting

The traffic classification information is used to provide preferential treatment to legitimate traffic

Fig. 1. Example network showing different potential defense locations.

Over the unknown and attack traffic. The classification mechanism needs to ensure that incorrect classification does not lead to heavy collateral damage. Hence, the unknown and potential attack traffic is not completely dropped but is given a limited bandwidth. Typically a priority queuing mechanism is deployed for ratelimiting where different queues are allocated different share of bandwidth. Traffic from different clients is mapped to different priority queues based on the traffic classification inputs. Deploying rate limiting at victim network can prevent the victim
node’s resources but cannot prevent exploitation of various network resources on the way to the victim network. Traffic classification can have maximum impact when deployed away from victim network there by preventing attack traffic from affecting both the victim network and the network resources on the path to the victim network.

III. DEFENSE LOCATIONS

A distributed denial of service attack originates from source networks, gets forwarded through the intermediate core routers, and finally converges at the defense node. As the attack is visible at all three network locations, defense can be deployed at each of these locations. In this section, we present different approaches that have been proposed in the past to develop defense at these locations. Each of these locations have different strengths in supporting various defense functionalities. We discuss the level of defense that can be provided by these locations.

A. Client networks

Client networks, as the name suggests, are closest to the traffic source, hence also termed as source-end networks. Being closest to the source has the biggest advantage of thwarting attacks before they enter the Internet core thus causing minimum collateral damage. As client networks are furthest from the victim server, they are highly distributed and thus relay small amount of traffic. This enables the client networks to deploy sophisticated compute-intensive defense solutions and easier trace back to investigate the attack.

The client network sounds like the best location to place the DDoS defense. But client networks have their own share of disadvantages. Each client network hosts a small number of the DDoS attackers. These attackers from different client networks send attack traffic too diffused to get noticed at the client (source-end) network. But this low-degree of traffic aggregation together converges downstream to form high impact DDoS attack traffic. In Figure 1 [1], node R1 is a source-end defense location, where the attack traffic passes undetected but congests the bandwidth downstream. This makes it very difficult for the client network to detect an attack. Client networks require that many routers at different network entry points each independently
run the defense system to police data flows originating from its own network thus rendering them economically expensive due to the high cost of deployment.

Various client-based defense solutions have been proposed in the past. An example of defense deployed at client networks is D-WARD [3] which is a self-regulating reverse-feedback system installed at the source router to periodically compare the observed values of the two-way traffic statistics for each peer against a predefined model of normal traffic and respond by imposing a rate limit on the suspicious outgoing flow for this peer.

**B. Intermediate networks**

Intermediate networks consisting of core routers relay large volumes of traffic. Being not too close to the source or the victim, the strategic location of the intermediate networks coupled with better infrastructure availability prove extremely resourceful for DDoS defense. As most of the traffic passes through a limited number of core internet routers, intermediate networks can provide maximum impact with minimal deployment. Intermediate networks are also a good location for handling traffic coming from legacy networks.

However, these nodes cannot dedicate compute resources for complex defense mechanism. Defense at these locations need to be light-weight in terms of computation and memory requirements. Core internet routers being extremely busy routing large volumes of traffic, can barely spare resources and hence sophisticated DDoS solutions cannot be implanted. The stakes are high due to strategic location of intermediate networks. Because of the large volumes of highly aggregated traffic, the defense at intermediate networks carries the risk of high collateral damage in case of incorrect traffic differentiation.

Intermediate networks play a very important role in detecting of attackers. Various techniques have been proposed in the past where intermediate nodes stamp the ongoing packets with unique identifiers that can then be used to trace the attacker backwards from victim to the source of attack.

An example of defenses deployed at intermediate networks is StackPI [7] marking scheme where the forwarding nodes mark the packet with their node identifier. The nodes traveling on a path
thus form a path identifier. This identifier is then used by the victim to differentiate legitimate and attack traffic. Another example is Traceback [5] which is based on probabilistic packet marking in the network, for tracing anonymous packet flooding attacks in the Internet back towards their source. Pushback [1] is another example of defense deployed at intermediate networks that detects attacks characterized by an attack/congestion signature.

<table>
<thead>
<tr>
<th>Client-Side Network</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Observe very limited attack traffic | • More computational resources can be spared for rate-limiting and traffic filtering activities.  
• Rate limiting at the source itself enables limited collateral damage. | • Low degree of traffic aggregation may converge downstream to create highly aggregated attack traffic. Too early for attack detection. |
| Distributed deployment points | • Easier traceback and investigation of the attack. | • Difficult to deploy at multiple locations.  
• Expensive |

<table>
<thead>
<tr>
<th>Intermediate Network</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Observe highly aggregated traffic | Better infrastructure availability and strategic location to:  
• Detect attacks.  
• Perform rate-limiting | • Sophisticated computationally intensive solutions cannot be implemented as routers are busy routing traffic.  
• Light-weight algorithms required for traffic filtering and rate-limiting.  
• Risk of collateral damage |
| Limited deployment points | • Easy to deploy and monitor.  
• Less expensive. | |

<table>
<thead>
<tr>
<th>Victim Network</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observe highly aggregated traffic</td>
<td>• Attack detection very easy.</td>
<td>• Rate limiting is too late as the network is already congested and the users are denied service</td>
</tr>
</tbody>
</table>
| Single-point deployment | • Easy to deploy and monitor.  
• Least expensive | • Unrestrained aggregated attack traffic converging at one point makes traffic-filtering difficult |

Fig. 2. Comparison of the three network locations for defense deployment.

and preferentially drops packets that belong to the attack. Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the routers resources be used to route legitimate traffic. Secure Overlay Services [2] used a combination of secure overlay tunneling, routing via consistent hashing and filtering. It introduces randomness and anonymity into the architecture, making it difficult for an attacker to target nodes along the path to a specific SOS-protected destination.

C. Victim networks
Victim network consists of the server or server network that is being attacked. Victim networks are the best locations for detecting attacks as the entire traffic reaching the victim is visible at this point. This location can best judge attack and non-attack mode of operation for defense mechanism. Victim networks are good to take proactive actions on detecting anomalous behavior and predicting the likely possibility of attack. Needing only a single-point deployment, this location has the highest economic incentive to deploy defense.

However, when under an attack, victim will be flooded with huge volumes of traffic and hence compute-intensive solutions are not suitable at this location. Also, tracing the attacker location is difficult from the victim-end due to highly aggregated and unrestrained traffic volumes reaching the victim. Victim locations are not good for reactive solutions as it might be too late to take corrective actions at the victim end after under attack. In Figure 1, R8 can be termed as a victim network. Dropping packets at R8 will not help the congestion at links between R1 and R5, R2 and R5, R3 and R6. Although attack is detected and packets will be dropped at R8, the mentioned links will still be congested and the DDoS attack will be successful as the users will be denied service.

As victim location has highest economic incentive to deploy a defense, several victim-based solution have been proposed in the past. IP Easy-pass is an example of defense deployed at victim end. IP Easy-pass is a fast and light-weight IP network-edge resource access control mechanism to prevent unauthorized access to reserved network resources at edge devices, which attaches a unique pass to each legitimate real-time packet so that an ISP edge router can validate the legitimacy of the incoming IP packet very quickly and simply by checking its pass.

IV. NEED FOR DISTRIBUTED DEPLOYMENT

The three vital functionalities of attack detection, traffic differentiation, and rate-limiting are very different in nature and need to be placed at different network locations to their most effective operation (Figure 2). The victim network can best detect when under attack. The victim network together with the down-stream routers can proactively trigger alerts to activate the other
defense locations for any potential attack. Attack detection mechanism needs to be kept computationally light-weight as these locations will be observing very high traffic volumes.

Traffic differentiation is the most compute intensive operation of all three defense operations. This needs profiling client behavior, generating encrypted stamps, etc. This operation can be done at client network where the number of clients and traffic volumes are significantly lower as compared to other locations.

Rate-limiting requires wide deployment to ensure all traffic gets rate-limited. This operation needs to be done at locations that observe most of the network traffic. Rate limiting can be performed at the core routers where large amount of traffic can be rate-limited by deployment at very few nodes.

V. CONCLUSION

With the large scale of DDoS attacks and the continuously evolving nature of these attacks, it is important to do a paradigm shift from single-point defense to an distributed defense. Single-point defense can lead to inaccuracy in traffic differentiation causing high collateral damage and single point of failure. On the other hand, the other extreme of deployeverywhere is discouraged due to economic concerns and lack of deployment incentive at locations away from victim network. The selection of defense nodes should be done such that defense nodes are evenly distributed throughout the network and none of the defense nodes is overwhelmed with traffic from a large number of nodes. Furthermore, a hierarchical deployment of defense nodes is required such that defense nodes are deployed at strategic locations in the client, core, and victim networks. The strengths of different network locations need to be exploited to build a robust framework to mitigate the ever-increasing threat posed by DDoS attacks.

REFERENCES


5. IT for Green: Road Transportation Sector

By Dnyaneshwar Kamble CMC Ltd.

Greenhouse gas emissions from transport sector: a global challenge

The transport sector in most of the developing countries is experiencing an increased share of personal motorized traffic, which has impacts in terms of growing traffic congestion, travel time, road accidents, pollution and most of all high dependence on fossil energy. According to IPCC (2007), 95% of the total energy used in transport sector globally comes from a single fossil resource, petroleum. The sector was responsible for 23% of the world’s energy-related GHG emissions (6.3 Gt) in 2004, about three quarters of which came from on-road vehicles. Sector’s GHG emissions have increased at a faster rate than any other energy using sector during the last one decade. According to the World Energy Outlook 2009, global energy-related CO2 emissions are expected to increase to over 40Gt by 2030, of which emissions from transport sector would be around 9Gt (more than one-fifth) despite significant mitigation policies built into the reference scenario. Transport sector will continue being the second largest energy consuming sector after industry and will be responsible for 60% of the world’s liquids consumption by 2035. As per the estimates of the International Energy Agency (IEA), emerging economies like China and India will drive this growth in transport sector’s energy consumption.

The Indian scenario:

The transport sector in India is facing trends similar to the other developing countries. Witnessing a growth rate of 7.3% and 5.8% per annum between 1980-81 and 2004-05 in the consumption of petrol and diesel, respectively, the sector meets 98% of its energy requirements from petroleum products. Within the transport sector, the road sector is the largest consumer of commercial fuel energy; it accounts for nearly 35% of the total liquid commercial fuel consumption by all sectors. This has primarily happened due to emergence of the road sector as the most dominant means of surface transport, both in terms of passenger and freight traffic.
(Figures 1 and 2). On-road passenger transport activities in just 23 million-plus cities in India had a share of about 25% in country’s total on-road passenger transport activities in 2001

ICT applications for road transport sector: a key enabler for reducing energy consumption from the sector
As stated, ICT has a tremendous potential in terms of improving the road transport operations and hence can lead to reduction in the energy consumption. Specifically, in large urban centers where the road transportation activities are concentrated, ICT has a huge potential to improve the existing inefficiencies.

Households and Transportation:

In 2008, the Eco home diagnosis council, made up of representatives from industry, government, academia and citizen, was established towards achieving a low carbon society with the aim for a substantial CO2 reduction in households. The ‘Eco-Home Diagnosis Project’ scheme, a project that performs consultation with tailor made measure based on analysis of factors influencing household’s CO2 emission, was created and a trial project was conducted.
The breakdown of CO2 emission from participating households is shown in fig 5

Figure 5: Breakdown of CO2 Emission from Household

**ICT application for intelligent/sm art public transport**

Intelligent Public Transport Management (IPTM) uses ICT applications to make public transport operations more efficient and customer-friendly. The ICT systems enhance the efficiency by optimizing the delivery of transit services; applications include computerized timetabling, dispatch and rostering, fleet monitoring, and intelligent control systems. It also targets disseminating real-time/comprehensive information of public transport operations to the users, which help them to make modal choices and trip decisions 4 (Button & Hensher, 2001). Some of the key ICT interventions used in IPTM to improve public transport service levels are discussed below 5 (CII-DESC, 2010):

**Public transport fleet management:**

It involves managing the public transit fleet with the help of AVLS and Surveillance by CCTV cameras. AVLS employs one or more technologies to track vehicle location (Casey, 1998) (Figure 7). Surveillance helps in anticipating/detecting violence and ensuring security of commuters. It can also help in collecting real-time data on traffic situation (NTDPC, 2011). The information collected with the help of mentioned technologies is received by control centers, which disseminate the estimated arrival/departure time of the public transit fleet at various locations. The various mediums used for information dissemination include internet, display screens, SMS or WAP services.
Electronic ticketing:

It involves developing advanced and easy ways of collecting public transit fares by payment services like common mobility card and smart cards. Smart cards are contactless cards used for automatic fare collection. It is cash-less transaction with complete security, which also reduces the waiting time for ticket collection. These cards offer passenger convenience as they need not buy tickets everyday for mass transit services. Smart cards that can be used across different public/ para transit modes make inter-modal transfers even more convenient for commuters and help in making these modes attractive to commuters. Use of ICT applications in public transport systems as discussed above, leads to improvement in overall efficiency while also making the systems more commuter-friendly and attractive for users. It may be difficult to attribute the benefits of a well-designed public transport system to its components (better buses, use of smart technologies, fare policies, rationalized routes etc.), it is to be understood that all such elements including ICT use are critical for success of the public transport systems.

Conclusion:
There is a need for a multi-pronged strategy to promote the use of ICT applications in road transport sector; the strategy should target addressing all barriers that effect large scale deployment of ICT. Figure 8 depicts the keys elements of such a strategy.

![Figure 8: Strategy to promote the use of ICT applications in road transport sector](image)

**References:**

1) Report ‘‘Sustainable Tomorrow: Harnessing ICT Potential’ by Business Council for Sustainable Development (TERI-BCSD) and National Association of Software & Services Companies (NASSCOM).
2) Environmentally sustainable transport( EST) as a basis for NAMAs – By Akshima Ghate ands Sundar (TERI).
3) Promotion of CO2 Reduction measures in household by cooperation among government, industry, and research institute

4) http://www.calgary.ca/portal/server.pt/gateway/PTARGS_6_0_771_217_0_43/http%3B/content.calgary.ca/CCA/City+Hall/Business+Units/Transportation+Planning/Transportation+optimization/What+makes+up+Intelligent+Transportation+Systems.htm (Last Accessed on August 5, 2011)


6) Delhi Government is planning to install CCTV cameras in DTC buses to check harassment of women and petty crimes and also to collect real-time data on traffic situation.

Abhay Arvind Phansikar Advisor (abhay@acevin.com) &
Ashok Dhanji Jagatia President & CTO (ashok@acevin.com)

Acevin Emtechnology Pvt Ltd. 104-I Marwah Complex, Saki Vihar Road,
Andheri (E) Mumbai – 4015415

Embedded Systems is gaining prominence and is considered to become the next sunrise sector in the Indian Technology Scenario. This article provides an introduction to the eco-system around the Embedded Technologies, the currents technology, trends and the career opportunities in that space, both for the technologists as well as the business management personnel.

Introduction

Embedded systems are devices or systems that are built to handle one or more pre-established tasks; the computing and controlling elements are 'embedded' within the devices / systems. It is used extensively in all areas – consumer, telecom, automotive, aerospace, energy, manufacturing, security, home automation etc. Complexity is involved in embedded design and solutions which offers both challenge and opportunity.

Embedded Systems are commonly seen and felt in all walks of life. An automobile today can contain about 50 embedded electronic boards as against a couple few years back. While in early days electronics was limited to ignition and door locking systems, today the various elements in a smart car are found handling cruise control parking assist, driving assist, navigation, smart gate control and cellular phone interfaces.

Today Embedded Solutions are seen right from mobile bus ticket vending machine, washing machines to complex solutions, like a completely unmanned public rail system like Docklands Light Rail.
Embedded Ecosystem

Students today are familiar with Embedded Electronics as having Printed Circuit board with some electronics and basic software for device control. The technologies commonly known are micro-controllers, RTOS, RFID, Short Range Wireless and GPS. Off the shelf bread boards are used to build a solution using these technologies. Embedded Ecosystem however is a very vast area consisting of various players in that domain like IC Design Houses, Board Design Houses, Embedded Software Providers, Application Software Providers, Test houses, Software Tool Providers, Electronic Design Automation tool vendors, IC Manufacturers, Board / System Manufacturers, System Integrators.

Some trends

Micro-Controllers: Increased processing power, large size on-chip Flash/RAM/EEPROM memories, support of vast variety of interfaces and communication protocols, more integration of analog functions, increased energy efficiency for longer battery life, smaller foot prints, high density packages. This leads to increase in complexity for design, implementation, testing.

System-On-Chip(SOC): Integration of many computer components on a single chip, Most of the new ASICs include a embedded processor, omnipresent everywhere from mobile phones to portable media players, feature CPU running at above 500MHz, heterogeneous multi-processor SoC (programmable processors e.g. DSPs and microcontrollers). All of this requires developing complex software.

Embedded Database: Embedded and tightly coupled with the application

Network on Chip (NoC): Emerging paradigm for communications within large VLSI systems implemented on a single silicon chip, constructed from multiple point-to-point data links interconnected by switches, internal modules such as processor cores, memories and specialized IP blocks exchange data using a internal “network”. NoC links can reduce the complexity of designing wires for predictable speed, power, noise, reliability.

Convergence: Multimedia convergence (voice, video & data), Network convergence (GSM, CDMA, GPRS, WLAN), Device convergence.
Components: Fine pitch QFPs, BGAs, Micro BGAs upto 2000 pins, Buried components, Miniature (0.5mm x 0.25mm) size, Dense hybrid modules.

Programmable Devices: FPGAs over 6 million gates, Cores for DSP/Processors, Serial transceivers on device pins up to 6.5Gbps, Core voltages – up to 0.9V

PCB/Board Speeds: Layer Count: from 20 to 50 layers, Trace width / spacing - 2 mil, <6 Mils hole size, Board Data Rates 2.5 to 40 GB, Memory – DDR3 (12.8GBps), Processor -1333MHz

Considerations of SoC applications: To contain with ASIC designers have a hardware-centric view of the system design problem and Software designers have a software-centric view.

Hardware and Software Co-Design is now an important consideration in developing an embedded solution. Abstract models of both software and hardware components are required, and HW/SW interface design very difficult and time-consuming as design requires knowledge of both software and hardware and their interactions. In SoC designs, hardware and software are more tightly coupled than in general-purpose processor designs and System designers (HW/SW) are required

The Market Trends

All of the above is now leading to a shift from fixed function to multi function devices, Analog to Digital, 8/16 bit to 32/64 bit processors. Proprietary to commercial software with standalone to integration between embedded devices and web is now the key. Convergence of functions in single device with need for wireless devices in embedded systems is increasing phenomenally.

Systems are becoming more sophisticated, Software workload is increasing in computational size as well as complexity, Move towards small form factor designs and Low power battery powered designs. Integration of diverse and unrelated technologies and Development of IP blocks is on the rise.

The Indian Scenario

Embedded software is becoming the next sunrise sector in India with a number of multinationals have started new design entities in India. India is moving towards becoming a hub for embedded
technologies and solutions and Fivefold increase in professionals is expected by 2015 in embedded systems industry. Embedded systems market is evolving rapidly with complete Embedded Ecosystem being in place in India now. India is also emerging as a big market for consumer electronics and telecom products. Currently, major embedded activities in India pertain to products developed for foreign markets, and today Indian companies are more of system solution / product implementers. The scene is changing to motivation seen in Indian companies to become true contributors to innovation and moving up the value chain by conceiving and specifying products.

According to a market research, semiconductor and embedded design industry in India, generated revenues of $3.25 billion in 2005 and targeting $19 billion in 2012. It is expected to reach $43 billion in 2015, thus growing at CAGR of 30%.

**The India Advantage**

Large pool of talented professionals, Embedded expertise, Low product development cost, Established working models, Large domestic market, Reliable Manufacturing Sector, Quality Conscious Systems, Hugely Untapped Market of Buyers as well as Solution Providers.

In recent years, India has developed expertise in High-speed, complex, high performance board / system designs, Advanced real time embedded software. More and more MNCs are setting up large centers in the country. India is moving towards becoming a major R&D center for global companies. There is a Large increase in outsourcing of design and development related projects to India. Increasing number of expatriates are setting up their own firms in the country.

Increase in indigenous demand from defense agencies and increase in local demand has given rise to more domestic companies involved in product development. There are Equal opportunities in small Towns/Cities. Manufacturing activities by the EMS players in India have increased the scope of embedded design.

Last few years have seen a huge growth in number of small and innovative companies doing complete design of innovative embedded products. Indian companies are migrating from being
resource augmentation to product innovation and design centers. More and more Mass Manufacturing is shifting from China to India now.

**Embedded Career Opportunities in the Embedded Eco-system**

Embedded eco-system is wide open field; some career opportunities are:

- Employment for Engineers in Embedded Space
- Entrepreneurs to create start-ups and innovate
- Setting up of Design Centres
- Setting up of Test Labs
- Distribution Channels for Electronic Components
- Sales Channels for Electronic Products
- Training Centres for Creation of Talent Pool
- Ancillary Industry to Feed Manufacturing Setup

In and around Pune are Companies that supply systems which allow European Trains to run at lightning speeds, Airlines to fly securely and safely, Washing Machines to run reliably lifelong, Luxury Cars to be driven safely, Consumer devices to be efficient and cheaper, devices with complex functionality in small form factor, Improvise Medical Diagnosis Equipment etc

…. AND BETTER STILL that none of these companies are a part of Global R&D centre nor India Manufacturing Plant nor Setup by Multinationals.
7. Innovation in Information Technology

Allalkathan K. Group Project Manager Infosys

I am trying to introduce the concept of Innovation by showing “Visuals” and imprint the message deeply so that communication will be effective to all and connect the subject with audience.

Following areas are covered in this session of Innovation

- What is Innovation?
  - *Innovation is the profitable implementation of ideas.*
  - Think of invention as the laying of an egg, innovation as the laying, incubation and hatching.
  - There is no shortage of ideas and inventions in the world. The challenge is to introduce these successfully to a market.

- Means of Innovation
  - Innovation can be of any different forms which will be used for generating commercial value and market competition
    - Product
    - Process
    - Service
    - Business model
    - Value
    - Market

- A special breed of Innovation
  - This is “Disruptive Innovation,” a term first coined by Clayton Christensen. Disruptive innovation refers to a firm’s strategy relative to other firms. Often, low-cost business models and “good enough” solutions/products for low-end and/or non-consumers

- The Degree of Innovation
• The degree of innovation is nothing but the degree of change required by the innovating firm and/or the market
  • Incremental (sometimes called “continuous” or “evolutionary” or “small”)
  • Semi Radical
  • Radical (sometimes called “Discontinuous” or revolutionary or big)
• Innovation Tech Trends – 2012

• The new form of the second screen – TV
  o The TV will gain new momentum with advanced features like brilliant OLED screen displays, ultra-thin bezels, Internet connectivity, 3D display, and a multitude of sensors, including voice and motion

• Windows platform come back with new Avatar
  o At a time where iOS and Android have become the dominant mobile platforms and Apple is gaining an increasing amount of market share in the PC and laptop markets, we predict that Windows platforms will have a strong showing in 2012, driven by significant traction in the mobile space through the re-emerging Nokia brand and the release of touch-focused, Windows 8 for PCs and laptops.
  o Windows 8 will be the first OS that has been specifically designed for touch screen PCs.

• Recruitment takes a new form through Social Networking
  o Today, active Facebook users alone account for over 38 percent of the world’s Internet population. Additionally, there are nearly 150m users on LinkedIn and 100m active
users on Twitter. Driven by their massive membership and demographic super-status, social networks will become the go-to avenue for talent acquisitions in 2012.

- **Software + Hardware + Content – Hatrick to record a new Trends in IT Market place**
  - Stand alone hardware or content propositions will find it increasingly difficult to compete as the trend of closely integrated hardware and content solutions accelerates.

- **Recommendation Engine becomes so Personal by Social mapping**
  - Recommendation engines have employed a breadth of tools to identify individual consumer preferences. Some engines require users to take a short quiz to associate them with a targeted preference category, and others, for example BeachMint (fashion), focus on celebrity endorsement, under the assumption that individuals who associate with a celebrity will also associate with their lifestyle preferences.

- **Five Innovations – that Change our Life within Five Years**
  - Create our Own Energy
    - Created energy comes in all shapes and forms and from anything around us. We will be able to power our home with energy we create ourselves.
  - Biometric Security
    - Our biological makeup is the key to our individual identity, and soon, it will become the key to safeguarding it
  - Just Think it
    - Mind Reading is no more Science Fiction
  - Information Access Global
- Growing communities will be able to use mobile technology to provide access to essential information and better serve people with new solutions and business models such as mobile commerce and remote health care.
  - Spam may be History
    - Technology to make sense and integrate data from across all the forms of our life such as social networks and online preferences to present and recommend information that is only useful to us

- What is Innovation Mantra?
  - Don’t Look for Needs to fill them
  - Create a need that only you can fill

- The Process of Innovation – 3 simple steps to follow

- 9 Tips for Innovators
  - Be Investigative
  - Exploit Science Fiction
  - Be Courageous
  - Be Optimistic
  - Be Multifunctional
  - Think Global
  - Be Cooperative
  - Be Farsighted
  - Be Open Minded

- Final Take Away for Audience
  - The bulk of Future Innovation – less likely driven by Technologies and Apps from Labs but from their Applications outside the laboratory
We, People as Providers and Consumers play a Great Role Inducing for Impetus Innovation
References:-

http://www.symposion.de/?cmslesen/q0002050_25720101
http://www.nouve.eu
http://www.itbusinessedge.com/
Gordon@westportwire.com
www.thefifthconference.com
http://www.thefifthconference.com/council
www.thefifthconference.com
http://www.facebook.com/thefifthconference
8. Meeting the needs of the mobile user!

Werner Egipsy Souza

Mobile Consultant, hephail@gmail.com

+919833295454

Gipsy Cove, Sauntavaddo, Baga, Calangute, Bardez, Goa, India - 403516

Our objective here is to first understand the typical mobile user. Once we achieve this, we then look at the typical client trying to woo the mobile user. Based on this, we can then draw up a typical process for wooing the mobile user.

**Target User - Connected**

This kind of user, is someone who is more connected to his mobile, than to the outside world. More comfortable with checking his email four times a day, rather than checking his post box. Six times more likely to be chatting/texting(SMS) with his friends on the phone, rather than in real life. Five times more likely to Foursquare every restaurant around him, rather than actually eat there.

Hence, this person would appreciate:

a) More privacy, with suitable options to be able to turn off certain individuals with a simple Block button.
b) Easy segregation between work and personal life, ensuring that neither does personal life intrude into work, nor should work intrude into personal life.
c) Security of data and connection, hence security of identity.

**Target User - Living**

This user would give the mobile phone a second priority to life. Hence email checking would typically occur once a week, usually on a desktop or a laptop. Three times more likely to call,
rather than text/chat. More likely to eat home food rather than eating out, during which time mobile access is limited.

Hence this person would appreciate:

a) More integration with email, since email frequency is low, hence importance is high.
   b) Easy alerts for important calendar events.

**Client Interests**

Next, we take a look, at the interests of a typical client out to woo this mobile user:

a) Creation of a unique identity(brand) which target users identify with.
   b) Generation and storage of a database of target users.
   c) Creation of awareness of unique identity(brand) among target users.
   d) Awareness of product and services within and outside related geography.

Hence, to create the brand, the client first tries to create a mobile experience which falls within the brand environment.

The generation and storage of the database, involves use of analytics which first categories, then analyses the target user.

Actual awareness of the brand, means actual involvement of the user with the brand. This means that the user should use the service provided on a regular basis, with the sweet spot being once a day.

Hence, this should involve in growth of the target user base, through passionate involvement of new users, by existing users.

For regular usage of the brand service, we need constant updates of content and service, at least on a monthly basis, in line with the Wow! experience created by the brand.

A typical target for ideal number of users could be established at 50,000 users, depending on the brand.
The more the population of target users, greater should be the content base.

**Client Metrics**

1) Campaigns developed, have to be different for each brand.
2) No single tool, works “off-the-shelf”

Hence, metrics are established based on actual needs of the brand, which develop to required goals.

Examples of Goals:

1) To be the number one youth application!
2) To get one million downloads, from youth in the 18-23 age group!

Goals may be defined based on past campaign results, or on comparative industry campaign results (but note Metric no. 1, Campaigns developed have to be different for each brand).

The key, is incremental learning, versus setting benchmarks on loose assumptions.

**Team Architecture**

In order to achieve a goal which requires:

a) High usability and aesthetics quotient.
b) Stable execution and operation.

We need to organize a team which has to execute the following modules:

- Web Backend
- Web Frontend
- Mobile Website User Architecture design
- Mobile Application User Architecture design
- Mobile Application Content (Graphics and Text) Architecture design
How it works

A concept is built, around the kind of experience the user should have with the mobile medium. This concept is owned by the Brand Custodian (usually an experienced copywriter), who directly handles the design manager and the content (mostly text) manager.

A Planner after working on the scope of the project, with the Project Manager, then plans out the entire framework for exposing the campaign to the user.

A moderation panel, then evaluates the content and design, to qualify whether the experience matches the experience planned.

Examples:

Smirnoff: Generating leads

Alcohol is a tricky subject. In India, for example, the legal drinking age is listed as 25, and all print and TV advertisements showing the bottle are banned.

With respect to the vodka segment, another major issue, is that the life of a vodka drinker, is shortlived, hemmed in from one end by beer as the starting drink, and whisky, as the drink which most seasoned drinkers eventually turn to. Hence, the focus on vodka as a party drink.

Notice how Caipiroska is featured, instead of Mojito, which is a white rum based drink.
The innovation here, is how Smirnoff uses this application to ensure that vodka is an essential part of every cocktail served at a party.

A very slickly made application.

**Aston Martin: Keeping the brand alive through sound**

Aston Martin is the world’s most coveted British supercar. With prices typically above INR 1 Crore, it is a marqué, very few will actually own.

Hence, the main aim of this application, is to keep the experience of owning an Aston Martin alive in the hearts of the user.

The application begins with the actual start stop button used in all Aston Martin cars.

Upon touching it, the button lights up first with red, then blue showing the typical ignition, along with the ignition sound of the DBS.

The application actually has a layout of the Aston Martin factory in Gaydon, Warwickshire, where you are treated to short video clips of the various processes which go into making an Aston Martin, such as chassis build, the VIP area, etc.

There is a special accelerator section, where the user has to shake the phone, to hear the acceleration sound. Hence, the more vigorous the shake, the faster the acceleration. The interface is the typical RPM counter on the Aston Martin, which lights up when initiated.
The application also has direct links to Facebook, Twitter and Youtube, so that you may quickly register as a fan.

This application fully utilizes the media capabilities of the phone, as well as the accelerometer in the accelerator application.
9. Trends in Mobility

-Vivek Mohile, Persistent Systems Limited

This article provides an overview of some aspects of the current and emerging scenario in ‘mobile computing’; referred to in short as mobility. Mobility is a familiar concept today, with a wide variety of smart cell-phones, tablets, and similar compact devices used to access information on the fly, and to run an increasingly complex set of applications. Various salient features and benefits of mobility for the individual and businesses are described, along with the technology drivers, challenges and success factors, and some speculation about future developments expected.

1.0 A quick overview of what’s been happening in mobility

It is clear that mobility is a powerful force not just in computing, but to an extent in our social framework as well. Here are a few of my observations that will serve to demonstrate this.

1. In terms of sheer numbers, the number of mobile devices, including basic cell-phones, smart phones, tablets, readers etc. manufactured so far already exceeds the number of people on the planet. It does not as yet mean that every human being now has at least one mobile device; a lot of the devices manufactured earlier have been replaced or scrapped, and most who can afford it have multiple devices today. However, given the trend of cheap mobiles reaching hitherto untouched sections of society, and the corresponding development in technology and reduction in cost, it is clear that in the near future most adults will own at least one connected device. This makes cell-phones very different in terms of social impact from computers, where the penetration has been slower to reach the uneducated and poor sections of society.
2. Smart phones are increasingly ‘smarter’, cheaper and user friendly. There are a large number of start-ups developing a huge number of applications catering to different domains, use-cases etc. and many of them have free versions, or at a reasonable price.

3. Media companies are realizing they have to contend with mobility as a given, and a game changer in the way people use content. So the smart companies are figuring out the best way they can leverage this trend and use that to generate new business avenues.

4. Most businesses today, whether they are in the IT space, or they are the brick and mortar variety, realize the need to leverage this force. Equipment manufacturers and ISVs are focused on developing products and applications, whereas the brick and mortar companies are reaching out to their customers.

2.0 What are the drivers behind the emergence of mobility

Some of the technology advancements and innovations that have supported the development of power mobile computing are:

• Smarter processors and cheaper and smaller memories: Moore’s law has been as applicable for device electronics as for mainstream computing. Today’s emerging smart-phones boast of multi-core processors with clock speeds greater than a GHz making complex applications possible

• Technical advances in other components: Apart from processors, advances in displays like AMOLED, capacitive touch screens, CMOS cameras, higher capacity batteries, sensors like GPS / accelerometers have played a role.

• Faster cellular networks: 3G, UMTS, LTE etc. have allowed applications to access data at very fast rates making possible high data consuming applications like maps, real time media playback etc. possible.
• New codecs: The wide use of real time and stored media through mobile devices was facilitated by codecs such as MPEG4 and H.264. Built-in hardware acceleration for running these codecs is a key part of most smart-phone chips today.

• New paradigms of interaction: Intuitive touch based, and gesture based UIs, voice commands have made it easy to use mobile applications conveniently.

• Software: There is plethora of useful applications, easily down-loaded over the air on app stores.

• Back-end integration: While many applications are stand alone, the real power of mobile computing could be unleashed only through the support of a robust and secure integration with back-end application servers and databases.

3.0 Challenges and success factors for deriving the most from mobility

In order for developers, and businesses wanting to use mobility, to derive full advantage from the potential of mobile computing, it is necessary to get out of the mindset that a mobility application is just a stripped down, or ‘reduced screen resolution’ version of a desktop application or a web interface. While it is true that in some cases, creating an uncluttered version of a web-page may be all that is necessary to give a convenient access to the user, developing a really nifty application means understanding the features and context unique to a smart-phone or a tablet. These can be both challenges and opportunities and a proper attention to these enables the success factors differentiating an application or interaction model. Some of these are listed below:

• Think differently about your User Interaction model: A mobile application is typically used on the go, e.g. while traveling in a bus, train, walking around a marketplace, checking something during a chat over coffee and so on. This allows the user convenience in getting what he wants done immediately when it occurs to him, rather than wait to reach a desktop. Yet this also imposes constraint that the UI has to be simple, easy to use, intuitive and convenient to operate in difficult conditions like standing in a
queue etc. Some of the very simple yet addictive games like Angry Birds, Moron Test etc. demonstrate how a very simple UI can be very appealing.

- Leverage accessories like camera, accelerometer, location in innovative ways: Location based information on restaurants, scene recognition, QR codes, use of tilt and shake as a user interaction model point to a lot more that can be done with mobile devices than simply using the touch screen. Leverage this to the fullest

- Catering to the diversity of devices and platforms: Traditional applications today for the most part are either through the Web interface to the service or run on a Windows OS. True, there is also Linux, but mainstream consumers are all hooked to Windows. In mobile devices however there are so many variants of form factors, Operating Systems, touch screens versus keyboards that catering to all and yet meeting some of the other success factors outlined above is a challenge. In this context, HTML5 appears very interesting as a game changer in making it easier for developers to ‘develop once, run anywhere’.

- Reducing power consumption and working with low bandwidth and flaky connections: Although I have mentioned above that there has been a significant improvement in these factors, the large power required by new devices and the no of connected devices, means that there is also an increase on the demand side, making it important to have applications that do their work efficiently. Using connectionless protocols for server communication, or maintaining sessions in some way is important.

4.0 Enterprise mobility

As individual consumers, we have already been well exposed to mobility. Therefore I thought it is pertinent to list out some ways in which businesses can leverage mobility for catering better to their customers, or for improving productivity internally. Some of the emerging trends in this area are:

For the businesses’ customers
• Simplified apps for smart-phones and tablets: If the web is the place where customers interact with the business and its services a lot, it is obvious that customers will increasingly come in on mobile devices as well. Simplified, custom apps and SMS integration is a key to enable customers to conveniently get the information or service they need.

• Location and context based marketing for retail: Addressing a customer’s needs immediately can drive dividends for retail. As an example targeted ads and instant coupons for discounts based on a user’s location and what he is searching for, can help grab a customer the moment a purchasing idea emerges in his mind.

Internal to the enterprise
• Sales force automation: Enabling sales persons to quickly log call details, CRM and stock information while in the field will greatly improve sales productivity and accurate information about prospects and orders.
• Connecting to enterprise apps and workflows: Mobile devices can be another convenient access mechanism
  • Simplify work-flows for low importance tasks: e.g. leave and travel approval

5.0 What the future holds

There will of course be continued improvement along the technology and software dimensions in the years to come. Besides these, some of the aspects of mobility that I expect will emerge, or will develop further and be adopted fully are:

• Increased use for payment settlement: NFC, e-Wallets will gradually replace separate plastic cards and smart cards
• Much more powerful voice engines and gesture recognition technology
• Innovation in education: e-Learning, immersive education concepts will be greatly strengthened.
• Increased use for tele-medicine: We will see many intelligent sensor systems being developed to be used with mobile phones, that leverage the computing power and
connectivity of the mobile to make it easier for medical practitioners and even patients themselves to quickly and cheaply carry out diagnoses. The recent development of a low cost portable ECG based around a mobile phone is a case in point.

- Projector phones/tablets could ease the small screen constraints: Watching a movie or sharing an app with friends would be far easier with more powerful projectors being integrated.

- New paradigms in gaming: Making use of cameras, accelerometers and connectivity innovatively will result in a different breed of games will emerge leveraging these accessories.

- Mobility could be the key game changer for social development and e-governance: The wide spread of mobile devices, and the acceptability in all strata of society could help in easy access by citizens to government information, workflows etc. This will need UIs to be even simpler, mostly icon or voice based and government enterprise systems need to be opened up with connectors for mobile access.

In conclusion, we can say that ‘mobile computing’ is here to stay and we can expect many delightful surprises going forward. It has to be approached as an independent domain to leverage the maximum from this emerging technology.

**Note:** This article is based on a presentation made by the author at the event “Emerging Trends in IT, 2012” held at the Indira Institute of Management, Wakad, Pune on 24th February 2012, but is not an exact transcription, and has been adapted for the written form.
What is Android?

Android is an Operating system which includes Software Applications for mobile devices. The Android SDK provides the tools and APIs necessary to begin developing applications on the Android platform using the Java programming language. Android is a software stack for mobile devices that includes an operating system, middleware and key applications. Google Inc. purchased the initial developer of the software, Android Inc., in 2005. Android’s mobile operating system is based on the Linux kernel. Google and other members of the Open Handset Alliance collaborated on Android’s development and release. The Android Open Source Project (AOSP) is tasked with the maintenance and further development of Android. Android was listed as the best-selling smartphone platform world-wide in Q4 2010 by Canalys (wikipedia.org)

History of Android

Android is a Linux-based operating system for mobile devices such as smartphones and tablet computers. It is developed by the Open Handset Alliance led by Google. Google purchased the initial developer of the software, Android Inc., in 2005 the unveiling of the Android distribution in 2007 was announced with the founding of the Open Handset Alliance, a consortium of 86 hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. Google releases the Android code as open-source, under the Apache License. The Android Open Source Project (AOSP) is tasked with the maintenance and further
development of Android. Android has a large community of developers writing applications ("apps") that extend the functionality of the devices. Developers write primarily in a customized version of Java. Apps can be downloaded from third-party sites or through online stores such as Android Market, the app store run by Google. As of October 2011 there were more than 400,000 apps available for Android, and the estimated number of applications downloaded from the Android Market as of December 2011 exceeded 10 billion. Android was listed as the best-selling smartphone platform worldwide in Q4 2010 by Canalys with over 200 million Android devices in use by November 2011. According to Google's Andy Rubin, as of December 2011 there are over 700,000 Android devices activated.

**Foundation of Android**

Android, Inc. was founded in Palo Alto, California, United States in October, 2003 by Andy Rubin (co-founder of Danger), Rich Miner (co-founder of Wildfire Communications, Inc.), Nick Sears (once VP at T-Mobile), and Chris White (headed design and interface development at WebTV) to develop, in Rubin's words "...smarter mobile devices that are more aware of its owner's location and preferences". Despite the obvious past accomplishments of the founders and early employees, Android Inc. operated secretly, revealing only that it was working on software for mobile phones. That same year, Rubin ran out of money. Steve Perlman, a close friend of Rubin, brought him $10,000 in cash in an envelope and refused a stake in the company.

**Architecture of Androids**

Android consists of a kernel based on the Linux kernel, with middleware, libraries and APIs written in C and application software running on an application framework which includes Java-compatible libraries based on Apache Harmony. Android uses the Dalvik virtual machine with just-in-time compilation to run Dalvik dex-code (Dalvik Executable), which is usually translated from Java byte code. The main hardware platform for Android is the ARM architecture. There is support for x86 from the Android x 86 projects, and Google TV uses a special x86 version of Android.

The following diagram shows the major components of the Android operating system.
What is Features of Android?

Application framework enabling reuse and replacement of components

Dalvik virtual machine optimized for mobile devices

Integrated browser based on the open source Web Kit engine

Optimized graphics powered by a custom 2D graphics library; 3D graphics based on the OpenGL ES 1.0 specification (hardware acceleration optional)

SQLite for structured data storage

Media support for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, and GIF)

GSM Telephony (hardware dependent)

Bluetooth, EDGE, 3G, and Wi-Fi (hardware dependent)

Camera, GPS, compass, and accelerometer (hardware dependent)

Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE

Which Applications used in Android?

Applications are usually developed in the Java language using the Android Software Development Kit, but other development tools are available, including a Native Development Kit for applications or extensions in C or C++, Google App Inventor, a visual environment for
novice programmers and various cross platform mobile web applications frameworks. Android will ship with a set of core applications including an email client, SMS program, calendar, maps, browser, contacts, and others. All applications are written using the Java programming language.

**What is Use of Android?**

While Android is designed primarily for smartphones and tablets, the open and customizable nature of the operating system allows it to be used on other electronics, including laptops and

![Google TV Home Screen](image)

Galaxy Nexus, the latest "Google phone"

Netbooks, smart books,—and eBook readers. Further, Google intends to bring Android to televisions with Google TV, and the OS has seen niche applications on wristwatches, headphones, car CD and DVD players, digital cameras, portable media players and landlines.

The first commercially available phone to run Android was the HTC Dream; released on 22 October 2008 in early 2010 Google collaborated with HTC to launch its flagship Android device, the Nexus One. This was followed later in 2010 with the Samsung-made Nexus S and in 2011 with the Galaxy Nexus. IOS and Android 2.3.3 'Gingerbread' may be set up to dual boot on a jail broken iPhone or iPod Touch with the help of OpeniBoot and droid. In December 2011 it was announced the Pentagon has officially approved Android for use by its personnel.

**What are the Benefits of Google’s Open Social and Android?**

Google's vision of creating open platforms for both Open Social (using a single API) and Android (Open Handset Alliance) is absolutely genius. Not
only does it help Google competitively but it also helps create a stronger user experience and a strong support community. Here are some of the major benefits to open platforms such as Open Social and Android:

**User Experience:** Allowing developers to design applications on top of your platform provides the ability for users to have unique experiences tailored specifically for them. From a mobile perspective there will now potentially be a thousand different versions of the same operating system each tweaked slightly so that it fits the owner’s needs. Furthermore it will allow people to share the coolest parts of their user experience across all networks.

**Standardization:** With numerous partners involved in both Open Social and Android, developers have a standardized way of creating applications for users without having to worry about platform. The standard platform also helps define documentation, procedures and application sharing.

**Cost:** Open platforms always tend to be far less expensive than mainstream/off the shelf products. With platforms such as Android in place, users will notice a cut in cost compared to handhelds operating systems like Windows Mobile and Palm OS.

**Innovation:** Giving developers the access to such powerful and flexible platforms will encourage increased innovation as they compete to develop the next killer application.

**Support:** Open Platforms (common base) equals Thousands of Developers which equals the amount of support available for applications and configuration that are built on top of the platform.

"Android does not differentiate between the phone's core applications and third-party applications. They can all be built to have equal access to a phone's capabilities providing users with a broad spectrum of applications and services. With devices built on the Android Platform, users will be able to fully tailor the phone to their interests. They can swap out the phone's home screen, the style of the dialer, or any of the applications. They can even instruct their phones to use their favorite photo viewing application to handle the viewing of all photos."

"Open Social provides a common set of APIs for social applications across multiple websites. With standard JavaScript and HTML, developers can create apps that access a social network's friends and update feeds. Common APIs mean you have less to learn to build for multiple
websites. Open Social is currently being developed by Google in conjunction with members of the web community."

Comments to “What are the Benefits of Google’s Open Social and Android?”

Open Social, Google and Red Tape « The Whole Enchilada

First Look: The ‘Social Web Browser’ Flock Hits Primetime

What are the Benefits of Google™s Open Social and Android?

Mcahornsirup

Open Social + Android seem to be a good idea. But, pure web apps are often slow. Of course, they are calling a server for resources. With e.g. phone gap, it is possible to store resources locally. I am not sure, how to run an open social gadget without an open social container. Maybe, the solution could look like this:

Local: (PhoneGapOpenSocial API + OpenSocialGadget)

Remote: (OpenSocialContainer)

We outsourced our OpenSocialContainer But we run locally.

What is Advantages of Androids?

Biggest advantages of Android are an open platform and free. So many manufacturers that can design a variety of software are loaded on the Android system. Android display system can be changed to horizontal or vertical, making it easier for the user in finding an adequate picture you want. If you have a phone with Android consistently then you can download and install several free programs for Android. You can see in the Android Market through applications based on Android, Google Chrome. With Google Chrome you can open many windows at once. Many Android applications have been, until April 2011 has reached 250,000 applications for Android. With the support of many applications, the user can change the screen display. Android phones can also function as a router to share Internet.
What is Disadvantages of Androids?

Android Linux-based system, so as to modify Ander, the user must know the commands on the Linux system, and should log on as administrator. Not only is the installation of Program, each phone has a different way. The lack of compatibility all users of Android phones, we must learn again if Android phones to replace with other brands. Even to show any recovery mode, an Android phone has a different way. So in conclusion, if you are a person who likes to tinker with the phone, then you should not use mobile phones for Android.

What is Scope of Android in Future?

Google is developing applications for mobile phones Android stocks, small company in Palo Alto, began after a dispute over Google in the mobile arena to speculate. Some people do nothing about Android by end of 2007 handeeotjiman giant Internet Company Google Maps and Google Calendar with the original, such as enhanced mobile phones, aim their online applications, and say he wants. Now the is open-source Android software, mobile computing is whether to be in the future. Android is definitely the future of mobile computing has great potential. Android SDK release is just another symptom. Android ™ s strength lies in the opening. This open-source software, operating systems and can be completely customized with the hardware manufacturer can also, to extend the capabilities of mobile computing by.

This open-source software for mobile devices, including the choice of. That is far more users of Apple’s return policy is not satisfied ™ s iPhone and other smartphones can be an important area. The new Android mobile operating system, in the Linux kernel phone. It is basically to provide a cell phone and instant messaging, Web surfing, e-mail at other times, to desktop. Open-source software, and it is this background that the application is running, can be accessed by users with support for multi-tasking on social networking sites. Meanwhile, the user can listen
to music and talking on the phone at the same time, create an e-mail. Opportunities Android OS as a desktop operating system that allows multiple applications to run, Android will be limited by the imagination.

Google, Motorola and HTC, LG Electronics, Dell, and with the new Android smart phone market penetration. It is a promise of innovation. The Android system in order to light speed by the user, the idea that to work like a robot.

In addition, the new version 2.0 of the Android Market, the Android system, the newest of the line, he said. Appointment as soon as possible for release 2.0.1 ready to realize. There are all the person on the phone most of the work is still PC-sharing systems feature is a new trend. The technique has to be more to come has just begun. And promised to change the world, expert’s mobile operating system Android, it’s worth it. New edition is whether the future of the Android mobile computing, the ideal response “can be safe.” Android’s open nature, they can imagine, hardware developers can use the new device. Wants SDK, developers can easily require the user to explore the functions. Have Android phones are very useful reulwihan for a turnkey solution for the Android OS to go. Before outsourcing an Android application developer, your application is scalable and can be adapted to the use of the best sports technology, to choose the companies.
11. Popularity & Growth Of Android Operating System For Mobile Phones

(Mr. More Laxman , JSPM’s Jayawant Institute of Computer Applications,Pune.

E-Mail:- Morelaxman_docs@rediffmail.com , Mob: +91-9970962518 )

Android is a software platform and operating system for mobile devices, based on the Linux kernel and developed by Google and later the Open Handset Alliance. It allows developers to write managed code in the Java language, controlling the device via Google-developed Java libraries Android as an OS which runs the powerful applications and gives the users a choice to select their applications and their carriers. The Android platform is made by keeping in mind various sets of users who can use the available capacity within Android at different levels. Android is gaining strength both in the mobile industry and in other industries with different hardware architectures. The increasing interest from the industry arises from two core aspects: its open-source nature and its architectural model. Android is available as open source. Open Handset Alliance (OHA) is a collaboration of different companies as following: In July 2005, Google acquired Android Inc., a small startup company based in Palo Alto, CA. Android’s co-founders who went to work at Google included Andy Rubin (co-founder of Danger), Rich Miner (co-founder of Wildfire Communications, Inc), Nick Sears (once VP at T-Mobile), and Chris White (one of the first engineers at WebTV). At the time, little was known about the functions of Android Inc. other than they made software for mobile phones. First phone with Android was G1 phone which is developed by HTC in November 2008.

Following are the features of Android:-

**Handset Layouts** Android can adapt to traditional smart phone layouts, as well other VGA, 2D, and 3D graphics libraries.

**Java Support** Software written in Java can be compiled into Dalvik bytecodes and executed in the Dalvik virtual machine, which is a specialized VM implementation designed for mobile device use, although not technically a standard Java Virtual Machine.
Connectivity  Android supports a wide variety of technologies, including Bluetooth, WiFi, GSM/EDGE, and EV-DO.

Messaging  MMS and SMS are available for Android, as well as threaded text messaging. So you can send as many texties as you like

Web Browser  Android comes pre-loaded with the Web Kit application

Media Support  Android will support advanced audio/video/still media formats such as MPEG-4, H.264, MP3, and AAC, AMR, JPEG, PNG, GIF.

Optimized Graphics  It support for 2D & 3D graphics based on OpenGL.

Data Storage  SQLite is extremely small relational database management system, which is integrated in Android.

Dalvik Virtual Machine  It is extremely low-memory based virtual machine, which was designed especially for Android to run on embedded systems and work well in low power situations. It is also tuned to the CPU attributes. The Dalvik VM creates a special file format (.DEX) that is created through build time post processing. Conversion between Java classes and .DEX format is done by included dx tool.

All of Android’s software is written in Java, which is interpreted by the Dalvik virtual machine. Even the most core features such as the phone and the contacts application reside in this layer. This layer contains software written by the Android team as well as any third-party software that is installed on the device.

The Android Market  an online software store is developed by Google for Android devices. Most of the Android devices come with preinstalled “Market” application which allows users to browse, buy, download, and rate different available applications and other content for mobile phones equipped with the open-source operating system. Android Market follows a 70/30 revenue-sharing model for applications developed by developers. The developers of priced applications receive 70% of the application price and remaining 30% distributes. As of May 04, 2010, Android apps hit around 49,000 applications which were around 12,500 in August 2009 and 20,000 in December 2009. The global smart phone sell in second quarter of 2009, 2010 & 2011 is shown in section of survey of android.

Android is a multi-process system  in which each application (and parts of the system) runs in its own process. Most security between applications and the system is enforced at the process
level through standard Linux facilities, such as user and group IDs that are assigned to applications. Additional finer-grained security features are provided through a "permission" mechanism that enforces restrictions on the specific operations that a particular process can perform, and per-URI permissions for granting ad-hoc access to specific pieces of data.

Comparison is based on main criteria as follows.

1) Portability: Symbian mostly runs on Nokia cell phones and that it is not Java based lets it fall behind Android. Unfortunately Windows Mobile also has several applications that are specific to certain hardware platforms and therefore are not portable. The Android Mobile platform is a Linux & Java based which allow us to use it on many different platforms unlike Symbian & Win Mobile.

2) Reliability: Reliability is very much dependent on user experience. Symbian OS and Windows Mobile, are reliable enough for all kinds of users and applications which are available at the moment. It doesn’t mean that both systems run perfectly well but problems with the systems will not result in major difficulties. The Linux kernel used by Android has existed for long period which has proven that it is stable and fail-proof. Therefore it is useful for mobile applications. Because Symbian OS and Windows Mobile control the biggest part of the market and Android is Linux based.

3) Open Platform: An Android is “open mobile platform” software. All these functionalities have to be free of charge. The only operating system which really fits to these criteria is the Android mobile platform. Which is based on a free available operating system? Another fact is that publishing your own developed applications is free which not the case for Symbian OS and Windows Mobile.

4) Kernel Size: An often used assessment factor for comparing the kernel size is the “Memory footprint” which is the amount of memory used by the operating system. Symbian OS require 200 Kb. The Windows Mobile platform requires 300Kb for a typical installation. The Android OS which is using Linux kernel will need about 250 kb of memory.

5) Special Features: The new integrated browser based on the open source WebKit engine, the virtual machine Dalvik optimized for mobile devices, is a feature which enables every application runs in its own process. Windows Mobile has, due to its outstanding position in
the computer market, the advantage that the synchronization between the PC and the cell phone is very easy. Symbian OS however has no special features which must be mentioned.
12. Android

Varsharani B. Budde & Sominath P. Pathare
Indira Institute of Management (MCA) Pune

What is Android?
- Android is an open source operating system, created by Google specifically for use on mobile devices (cell phones mostly).
- Linux based (2.6 kernel).
- Can be programmed in C/C++ but most app development is done in Java (Java access to C Libraries via JNI (Java Native Interface)).

Android history timeline:

- July 2005 Google purchased a little known company called Android Inc.
- November 5th, 2007 Open Handset Alliance announces Android
- November 12th, 2007 Early look SDK released
- April 17th, 2008 Android Developer Challenge I. $5 million in total awarded to developers for great Android applications
- August 28th, 2008 Android Market announced
- September 23rd, 2008 Android 1.0 SDK release. Developers have access to first 1.0 compatible SDK.
- September 23rd, 2008 T-Mobile G1 World’s first Android-powered phone announced.
- October 21st, 2008 Android Open Source Project Source code is released

Android Platform Highlights

The Android platform introduces many features for users and developers. Below is a list of the new features which will make Android even better!
Performance Improvements

- Smoother page scrolling in Browser.
- Speedier GMail conversation list scrolling.

New Features

On-screen soft keyboard

- Works in both portrait and landscape orientation.
- Support for user installation of 3rd party keyboards.

Home screen

- Widgets.
- Bundled home screen widgets include: analog clock, calendar, music player, picture frame, and search.
- Live folders.

Camera & Gallery

- Video recording.
- Video playback (MPEG-4 & 3GP formats).

Bluetooth

- Open wireless technology.
- Developed by ericsson(1994).
- Originally supposed to replace wired rs-232.
- Allows creation of personal area networks.
- Mostly to connect wireless peripheral devices to host computer (mice headset microphones keyboard).

Wi fi.

Wi fi used to brand certified products that belong to a class of wireless local area network based on IEE Standard 802.11. Currently there are 3 versions of 802.11 in common use:
-B, about 150 feet indoors, 300 ft outdoors.

3G (3rd Generation Network):-
Must allow simultaneous use of speech and data services and provide peak data rate of 200 kbits/sec

4G:-

- Peak data rate of 100 Mbit for high mobility devices and 1 Gbit for low mobility devices.

Browser:

- Updated with latest Webkit browser JavaScript engines..
- User-selectable text-encoding.
- UI changes include:
  - Unified Go and Search box.

System:

- New Linux kernel.
- SD card file system auto-checking and repair.
- SIM Application Toolkit 1.0.

Google applications (Android SDK):

View Google Talk friends’ status in Contacts, SMS, MMS, GMail, and Email applications.
Batch actions such as archive, delete, and label on Gmail messages.
Upload videos to YouTube.
Upload photos on Picasa.

Getting Started with Android Apps:

Android uses the java programming language and for anyone who has learned Java the Hello World example is a good reminder of that very first class or online tutoring session. First you will need to download the Android SDK kit and if you are using Eclipse install the ADT Plug-in, this is very easy and all of the information you need to do this can be found at http://developer.android.com/sdk/index.html.

Below is an example of the Hello World program. You will see that the coding is similar to that of java but not exactly the same. You can also see that it is fairly simple and this makes everyone happy 😊.

```java
package com.example.helloandroid;
import android.app.Activity;
```
import android.os.Bundle;
public class HelloAndroid extends Activity {
    /** Called when the activity is first created. */
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }
}

Running your application:

Asing Eclipse (probably your best choice) the ADT plug-in that you install makes it very easy and simple to run your applications.
Select run -> run
Select Android Application
The Eclipse ADT will automatically create a new run configuration for your project and the Android Emulator will automatically launch. Once the emulator is booted up, your application will appear and should look like this:

What is the Open Handset Alliance (OHA)?

→ It's a consortium of several companies.

1. Architecture of android:-
2. Platform:

2.1 Hardware

Android is not a single piece of hardware; it's a complete, end-to-end software platform that can be adapted to work on any number of hardware configurations. Everything is there, from the bootloader all the way up to the applications.

2.2 Operating System(s)

Android uses Linux for its device drivers, memory management, process management, and networking.

The next level up contains the Android native libraries. They are all written in C/C++ internally, but you’ll be calling them through Java interfaces. In this layer you can find the Surface Manager, 2D and 3D graphics, Media codecs, the SQL database (SQLite), and a native web browser engine (WebKit).

Dalvik Virtual Machine. Dalvik runs dex files, which are converted at compile time from standard class and jar files.

Security

Android is a multi-process system, in which each application (and parts of the system) runs in its own process. Most security between applications and the system is enforced at the
process level through standard Linux facilities, such as user and group IDs that are assigned to applications.

Additional finer-grained security features are provided through a "permission" mechanism that enforces restrictions on the specific operations that a particular process can perform, and per-URI permissions for granting ad-hoc access to specific pieces of data.

2.6 Future possibilities

Google Android Sales to Overtake iPhone in 2012. The OHA is committed to make their vision a reality: to deploy the Android platform for every mobile operator, handset manufacturers and developers to build innovative devices. Intel doesn’t want to lose ownership of the netbook market, so they need to prepare for anything, including Android. Fujitsu launched an initiative to offer consulting and engineering expertise to help run Android on embedded hardware, which aside from cellphones, mobile internet devices, and portable media players, could include GPS devices, thin-client computers and set-top boxes.

3.1 Development requirements

- Android SDK
- Eclipse IDE (optional)
- Software development (2)
  - IDE and Tools

Android SDK

- Class Library
- Developer Tools
  - dx – Dalvik Cross-Assembler
  - aapt – Android Asset Packaging Tool
  - adb – Android Debug Bridge
  - ddms – Dalvik Debug Monitor Service
- Emulator and System Images
- Documentation and Sample Code

Is android Linux?

- NO, android is not linux!
  
  Android is based on the Linux kernel 2.6
but it's not GNU/Linux.
No native windowing system.
No glibc support.

**Why Linux kernel for Android?**
- Great memory and process management
- Great permissions based security model
- Proven driver model
- Support for shared libraries
- It’s already open source

**So is android java?**

NO, android is not java! Android is not an implementation of any of the Java variants.
- Uses the java language
- Implements part of the Java5 SE specification
- Runs on a dalvik virtual machine instead of JVM
13. Channel Allocation for Cellular Mobile Network

Shobha Mishra (M.Tech computer) Asst. Professor, Deptt of M.C.A.
Navsahyadri Group of Institutions,

tiwari.shobha82@gmail.com 09823481926, Pune -India

ARTICLES

The demand for Cellular mobile Services is increasing at a very high rate every years and in a lot of metropolitan areas the demand has already far exceeded the capacity. In the field of the mobile communication and by the FCC still very limited frequency spectrum allocated to this service, the efficient management and sharing of the spectrum among numerous users become important issues. This limitation means that the frequency channels have to be reused as much as possible in order to support the many thousands of simultaneous calls that may arise in any typical mobile communication environment. Thus, evolved the concept of cellular architecture, which is conceived as a collection of geometric areas called cells (typically hexagonal-shaped), each serviced by a base station (BS). Referred as mobile service station (MSS) and numbers of mobile hosts (MH) are present in the cell. Mobile service stations are connected to each other via fixed wire network and communication between MSS and MH is through wireless network. The bandwidth is the limited resource in cellular mobile system. The proper utilization of limited bandwidth is key factor to improve the performance of cellular system. The total bandwidth is divided into a set of carriers is further divided into a number of channels for communication. In cellular communication mainly two types of channels are available between MH and MSS: communication channel and control channel. Establishing a communication session between MSS and MS in a cell, communication channel is used while control channel is the set-up channel used to send messages that are generated by the channel allocation algorithm. In cellular/wireless system two cells can use the same channel if the distance between these cells have the minimum reuse distance.

The channel allocation schemes can be classified in three categories,
Fixed channel allocation (FCA)

Dynamic channel allocation (DCA)

And Hybrid channel allocation (HCA).

In fixed channel allocation, a set of channel is permanently allocated to each cell of the system. When user requests a channel for communication, it search the free channel in its own cell, if the free channel is available assigned to the user otherwise the request will be blocked in fixed channel allocation, a set of channel is permanently allocated to each cell of the system. When user requests a channel for communication, it search the free channel in its own cell, if the free channel is available assigned to the user otherwise the request will be blocked. In the fixed assignment (FA) schemes, a set of channels are permanently allocated to each cell, which can be reused in another cell, sufficiently distant, such that the co-channel interference is tolerable. Such a pair of cells is called co-channel cells. In one type of FA scheme, clusters of cells, called compact pattern (CP), are formed by finding the shortest distance between two co-channel cells, such that each cell within a compact pattern is assigned a different set of frequencies.

The advantage of an FA scheme is its simplicity, which is the primary reason why it is adopted in most of the existing systems. But the disadvantage is that if the number of calls exceeds the number of channels assigned to a cell, the excess calls are blocked. This problem can be partially alleviated by channel borrowing methods, in which a channel is borrowed from one of the neighboring cells in case of blocked calls, provided that it does not interfere with the existing calls. The disadvantage of channel borrowing is that the borrowed channel has to be locked in those co-channel cells of the lender, which are non-co-channel cells of the borrower in order to avoid interference.

In dynamic channel allocation implies that channels are allocated dynamically as new calls arrive in the system and is achieved by keeping all free channels in a central pool. This means when a call is completed, the channel currently being used is returned to the central pool. The dynamic channel allocation schemes are divided into two types centralized and distributed.
In Centralized dynamic channel allocation (CDCA) schemes, a channel is selected for a new call from a central pool of free channels, and a specific characterizing function is used to select one among available free channels. The simplest scheme is to select the first available free channel that can satisfy the reuse distance. Also, that free channel can be picked which can minimize the further blocking probability in the neighborhood of the cell that needs an additional channel. Centralized schemes can theoretically provide near optimal performance, but the amount of computation and communication among the BSs (base stations) lead to excessive system latencies and make them impractical. Therefore, distributed dynamic channel allocation (DDCA) schemes have been proposed that involve scattering of channels across a network. A channel is selected for a new call from its cell or interfering neighboring cells.

A channel allocation algorithm consists of two phases: a channel acquisition phase and channel selection phase. The task of channel acquisition phase is to collect the information of free available channels from the interference cells and insure that two cells within the minimum reuse distance do not share the same channel. The channel selection phase is concern for choosing a channel from the number of available free channels in order to get better channel utilization in terms of channel reuse. In general, the acquisition phase of the distributed dynamic channel algorithm consist of two approaches namely search and update. In search approach, when a cell requires a channel, it searches in its all interference neighbors to find the currently free available channel set and this set is used to select one channel-by-channel selection schemes. In the update approach, a cell maintains information about free available channels. When a cell requires a channel, the channel selection scheme is used to pick up one available channel and confirms with its all interference neighboring cells whether it can use the selected channel or not. After that, when a cell acquires or releases a channel at any time, inform its interference neighbors so that, every cell in the system model always knows the available channels of its interference neighboring cells.

A channel allocation algorithm includes a channel acquisition and a channel selection scheme. Most of the previous work concentrates on the channel selection algorithm since early channel acquisition algorithms are centralized and rely on a MSS to accomplish channel acquisition. The centralized schemes are neither scalable nor reliable. Recently, distributed dynamic channel
allocation algorithms have received considerable attention due to their high reliability and scalability. The most of the distributed algorithm is based on non-resource planning model in which a borrower needs to consult with every interference neighbors in order to borrow a channel. The proposed distributed dynamic channel allocation algorithm is based on resource-planning model, a borrower need not to receive replies from every interfering neighbors, it can borrow a channel from that neighbor whose all group members replies with common free channels within the predefined time period. The proposed algorithm makes efficient reuse of channels and evaluates the performance in terms of message complexity, blocking rate.

As we have seen Most of the previous work concentrates on the channel selection algorithm since early channel acquisition algorithm are centralized and rely on a MSS to accomplish channel acquisition. The centralized schemes are neither scalable nor reliable. Recently, distributed dynamic channel allocation algorithm has received considerable attention due to their high reliability and scalability. The most of the distributed algorithm is based on non-resource planning model in which a borrower needs to consult with every interference neighbors in order to borrow a channel. The proposed Hybrid channel allocation is based on resource planning model, It performs two types of allocation, In Fixed allocation (FCA) assignment policy is one in which each cell is allocated a fixed set of channels to performs a task and if no channel from fixed is free than channel is allocated from Distributed dynamic form where a borrower need not to receive replies from every interfering neighbors, it can borrow a channel from that neighbor whose all group members replies with common free channels within the predefined time period.

The channel assignment schemes in general can be classified into three categories: fixed channel assignment (FCA), dynamic channel assignment (DCA), and the hybrid channel assignment (HCA). In FCA, the set of channels are permanently allocated to each cell based on pre-estimated traffic intensity. In DCA, there is no permanent allocation of channels to cells. Rather, the entire set of available channels is accessible to all the cells, and the channels are assigned on a call-by-call basis. One of the objectives in DCA is to develop a channel assignment strategy, which minimizes the total number of blocked calls. FCA scheme is simple but does not adapt to changing traffic conditions and user distribution. These deficiencies are over-come by DCA but FCA out performs most known schemes in DCA under heavy load conditions. To overcome the
drawbacks of FCA and DCA, HCA was proposed by Kahwaetal. , which combines the features of both FCA and DCA techniques.

In hybrid channel allocation, few channels are permanently allocated to each cell and the remaining channels are allocated dynamically. The performance of the hybrid channel allocation schemes are intermediate between fixed and dynamic channel allocation schemes. In HCA one set of channels is allocated as per the FCA scheme, and the another set is allocated as per the DCA scheme. DCA schemes can be implemented as centralized or distributed. In the centralized approach all requests for channel allocation are forwarded to a central controller that has access to system wide channel usage information. The central controller then assigns the channel by maintaining the required signal quality. In distributed DCA, the decision regarding the channel acquisition and release is taken by the concerned base station based on the information from the surrounding cells. As the decision is not based on the global status of the network, it can achieve suboptimal allocation as compared to the centralized DCA and may cause forced termination of ongoing calls.
14. ANDROID

Digambar Dilip Dhole
Indira Institute of Management (MCA), Pune
digambardhole@ymail.com
Mo.9552691728

History:
Android was founded in Palo Alto, California, United States in October, 2003 by Andy Rubin, Rich Miner, Nick Sears, and Chris White.

Version History
Android has seen a number of updates since its original release, each fixing bugs and adding new features. Each version is named, in alphabetical order, after a dessert.

1.1 Gingerbread refined the user interface, improved the soft keyboard and copy/paste features, improved gaming performance, added SIP support (VoIP calls), and added support for Near Field Communication.

1.2 Honeycomb was a tablet-oriented release which supports larger screen devices and introduces many new user interface features, support for multi-core processors, hardware acceleration for graphics and full system encryption. The first device featuring this version, the Motorola Xoom tablet, went on sale in February 2011.

1.3 Honeycomb, released in May 2011, added support for extra input devices, USB host mode for transferring information directly from cameras and other devices, and the Google Movies and Books apps.
1.4 **Honeycomb**, released in July 2011, added optimization for a broader range of screen sizes, new "zoom-to-fill" screen compatibility mode, loading media files directly from SD card, and an extended screen support API. Huawei MediaPad is the first 7 inch tablet to use this version.

**Definition:**

Android is a **Linux-based operating system** for mobile devices such as **smart phones** and **tablet computers**. It is developed by the **Open Handset Alliance** led by **Google**.

Android phones typically come with several built-in applications and also support third-party programs. Android programs are written in Java and run through Google's "Davlik" virtual machine, which is optimized for mobile devices.

- **Applications**
  Applications are usually developed in the **Java** language using the Android Software Development Kit, but other development tools are available, including a Native Development Kit for applications or extensions in C or C++, **Google App Inventor**, a visual environment for novice programmers and various cross platform mobile web applications frameworks

- **Android Market**
  - Android Market is the online software store developed by Google for Android devices. An application program ("app") called "Market" is preinstalled on most Android devices and allows users to browse and download apps published by third-party developers, hosted on Android Market. As of October 2011 there were more than 300,000 apps available for Android, and the estimated number of applications downloaded from the
Android Market as of December 2011 exceeded 10 billion. The operating system itself is installed on 130 million total devices.

Only devices that comply with Google's compatibility requirements are allowed to preinstall Google's closed-source Android Market app and access the Market. The Market filters the list of applications presented by the Market app to those that are compatible with the user's device, and developers may restrict their applications to particular carriers or countries for business reasons.

- **Security**
  - An example of app permissions in Android Market.

Android applications run in a sandbox, an isolated area of the operating system that does not have access to the rest of the system's resources, unless access permissions are granted by the user when the application is installed. Before installing an application, Android Market displays all required permissions. A game may need to enable vibration, for example, but should not need to read messages or access the phonebook. After reviewing these permissions, the user can decide whether to install the application.
Some Android malware incidents have been reported involving rogue applications on Android Market. In August 2010, Kaspersky Lab reported detection of the first malicious program for Android, named Trojan-SMS.AndroidOS.FakePlayer.a, an SMS trojan which had already infected a number of devices. In some cases applications which contained Trojans were hidden in pirated versions of legitimate apps. Google has responded by removing malicious apps from the Android Market, remotely disabling them on infected devices, and scanning newly-uploaded apps for potentially malicious software. Several security firms have released antivirus software for Android devices, in particular, AVG Technologies, Avast!, F-Secure, Kaspersky, McAfee and Symantec.

Privacy

Android smartphones have the ability to report the location of Wi-Fi access points, encountered as phone users move around, to build vast databases containing the physical locations of hundreds of millions of such access points. These databases form electronic maps to locate smartphones, allowing them to run apps like Foursquare, Latitude, Places, and to deliver location-based ads.

Third party monitoring software such as TaintDroid, an academic research-funded project, can, in some cases, detect when personal information is being sent from applications to remote servers.

Marketing:

The Android logo was designed along with the Droid font family made by Ascender Corporation.
**Market share**

- Research company Canalys estimated in Q2 2009 that Android had a 2.8% share of worldwide smartphone shipments. By Q4 2010 this had grown to 33% of the market, becoming the top-selling smartphone platform. This estimate includes the Tapas and OMS variants of Android. By Q3 2011 Gartner estimates more than half (52.5%) of the smartphone market belongs to Android.

**Usage share**

- Usage share of the different versions, by February 1, 2012

  Usage share of the different versions, by February 1, 2012:

<table>
<thead>
<tr>
<th>Distribution</th>
<th>API level</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.x <em>Ice Cream Sandwich</em></td>
<td>14-15</td>
<td>1.0%</td>
</tr>
<tr>
<td>3.x.x <em>Honeycomb</em></td>
<td>11-13</td>
<td>3.4%</td>
</tr>
<tr>
<td>2.3.x <em>Gingerbread</em></td>
<td>9-10</td>
<td>58.6%</td>
</tr>
<tr>
<td>2.2 <em>Froyo</em></td>
<td>8</td>
<td>27.8%</td>
</tr>
<tr>
<td>2.0, 2.1 <em>Eclair</em></td>
<td>7</td>
<td>7.6%</td>
</tr>
</tbody>
</table>
### Distribution

<table>
<thead>
<tr>
<th>Distribution</th>
<th>API level</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6 Donut</td>
<td>4</td>
<td>1.0%</td>
</tr>
<tr>
<td>1.5 Cupcake</td>
<td>3</td>
<td>0.6%</td>
</tr>
</tbody>
</table>

### Retail stores

- The carrier Telstra opened the world's first Android store, Androidland, on Bourke Street, Melbourne in December 2011.

### Features:

- Handset layouts
- Storage
- Messaging
- Multiple language support
- Media support
- GSM Telephony (hardware dependent)
- Video calling
- Voice based features
- Additional hardware support
- Media support
Bluetooth
External storage
Screen capture
Integrated browser
Optimized graphics

Uses:

- Android is designed primarily for smartphones and tablets, the open and customizable nature of the operating system allows it to be used on other electronics, including laptops and netbooks, smart books, and eBook readers.
- Now android OS has seen niche applications on wristwatches, headphones, car CD and DVD players, digital cameras, portable media players and landlines.

Android version:

1) v1.0:
   The first commercial version of the software was released on 23 September 2008.

2) v2.0/2.1 Éclair:

3)
   The Android 2.0.1 SDK was released on 3 December 2009 and deployable to Android-powered handsets, including minor API changes, bug fixes and framework behavioral changes.

4) v3.x Honeycomb:
The first device featuring this version, the Motorola Zoom tablet, was released on 24 February 2011.

5) v4.x Ice Cream Sandwich:
Officially launched at the Galaxy Nexus and Ice Cream Sandwich release event on 19 October 2011.

Technical Information:

1) Debugging:
Android is a large and complex system. This section includes tips and tricks about debugging at the platform level.

2) Encryption
The Android Open-Source Project includes the ability to encrypt the user's data. This document is written for 3rd parties developing Android devices who want to include support for encryption on their device.

3) Security Technical Information
Android provides a robust multi-layered security architecture that provides the flexibility required for an open platform.

4) Input Technical Information
Android's input subsystem is responsible for supporting touch screens, keyboard, joysticks, mice and other devices.

Intellectual property:

- Trademarks
In order to use the Android trademark, device manufacturers must ensure that the device complies with the Compatibility Definition Document (CDD) and then get permission from Google. Devices must also meet this definition to be eligible to license Google's closed-source applications, including the Android Market.[139] Participation in the compatibility program is free of charge.[40]
Licensing

The source code for Android is available under free and open source software licenses. Google published their Linux kernel changes under the GNU General Public License version 2, and the rest of the code (including network and telephony stacks) under the Apache License version 2.0.

Patents

Both Android and Android phone manufacturers have been the target of numerous patent lawsuits. On 12 August 2010, Oracle sued Google over claimed infringement of copyrights and patents related to the Java programming language. Specifically, the patent infringement claim references seven United States patents including US 5966702 "Method and apparatus for pre-processing and packaging class files", and US 6910205 "Interpreting functions utilizing a hybrid of virtual and native machine instructions".
15. Cloud Computing Services, Techniques, Security Issues and Their Resolution

Mr. Mane Dnyaneshwar, JSPM’s Jayawant Institute of Computer Applications, Pune, E-mail:- dnyaneshit@gmail.com, Mob No.: 9730304422

The term “cloud” was probably inspired by IT depicted as remote environments (e.g., the Internet) as cloud images in order to conceal the complexity that lies behind them. However, by understanding the type of services offered by cloud computing, one begins to understand what this new approach is all about.

1. **On-demand self-service:** Customers can provision computing capabilities (e.g., storage, memory, network bandwidth, user accounts) on-demand basis. Capabilities can be provided independently and automatically without human interaction with services providers.

2. **Broad network access:** Capabilities are available over the network. They can be accessed through standard mechanisms with different client platforms such as personal computers and mobile phones.

3. **Resource pooling:** Services provider pools capabilities to serve multiple consumers using multi-tenant model. Different customers (tenants) share the same underlying resources.

4. **Rapid elasticity:** Capabilities can be rapidly scaled in and out (i.e., provisioned and released) at any given time. The supply of capabilities from customer perspective appears to be infinite.

5. **Measured service:** Appropriate metering system is employed and customer’s usage of capabilities can be transparently monitored, controlled, and reported.

1. User friendliness
2. Virtualization
3. Internet centric
4. Variety of resources
5. Automatic adaptation
6. Scalability
7. Resource optimization
8. Pay per use
9. Service SLAs
10. Infrastructure SLAs
1. **Infrastructure as a Service (IaaS):** Products offered via this mode include the remote delivery (through the Internet) of a full computer infrastructure (e.g., virtual computers, servers, storage devices, etc.).

2. **Platform as a Service (PaaS):** To understand this cloud computing layer one needs to remember the traditional computing model where each application managed locally required hardware, an operating system, a database, middleware, Web servers, and other software. One also needs to remember the team of network, database, and system management experts that are needed to keep everything up and running. With cloud computing, these services are now provided remotely by cloud providers under this layer.

3. **Software as a Service (Saas):** Under this layer, applications are delivered through the medium of the Internet as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management. This type of cloud service offers a complete application functionality that ranges from productivity (e.g. office-type) applications to programs such as those for Customer Relationship Management (CRM) or enterprise-resource.

There are numerous services that can be delivered through cloud computing, taking advantage of the distributed cloud model. Here are some brief descriptions of a few of the most popular cloud-based IT solutions:

Hosted desktops remove the need for traditional desktop PCs in the office environment, and reduce the cost of providing the services that you need. A hosted desktop looks and behaves like a regular desktop PC, but the software and data customers use are housed in remote, highly secure data centers, rather than on their own machines. Users can simply access their hosted desktops via an internet connection from anywhere in the world, using either an existing PC or laptop or, for maximum cost efficiency, a specialized device called a thin client.
As more organizations look for a secure, reliable email solution that will not cost the earth, they are increasingly turning to hosted Microsoft Exchange® email plans. Using the world’s premier email platform, this service lets organisations both large and small reap the benefits of using MS Exchange® accounts without having to invest in the costly infrastructure themselves. Email is stored centrally on managed servers, providing redundancy and fast connectivity from any location. This allows users to access their email, calendar, contacts and shared files by a variety of means, including Outlook®, Outlook Mobile Access (OMA) and Outlook Web Access (OWA).

VOIP (Voice Over IP) is a means of carrying phone calls and services across digital internet networks. In terms of basic usage and functionality, VOIP is no different to traditional telephony, and a VOIP-enabled telephone works exactly like a 'normal' one, but it has distinct cost advantages. A hosted VOIP system replaces expensive phone systems, installation, handsets, BT lines and numbers with a simple, cost-efficient alternative that is available to use on a monthly subscription basis. Typically, a pre-configured handset just needs to be plugged into your broadband or office network to allow you to access features such as voicemail, IVR and more.

Cloud storage is growing in popularity due to the benefits it provides, such as simple, Cap Ex-free costs, anywhere access and the removal of the burden of in-house maintenance and management. It is basically the delivery of data storage as a service, from a third party provider, with access via the internet and billing calculated on capacity used in a certain period (e.g. per month).

Dynamic servers are the next generation of server environment, replacing the conventional concept of the dedicated server. A provider like Think Grid gives its customer access to resources that look and feel exactly like a dedicated server, but that are fully scalable. You can directly control the amount of processing power and space you use, meaning you don't have to pay for hardware you don't need. Typically, you can make changes to your dynamic
server at any time, on the fly, without the costs associated with moving from one server to another.

Methodology is the ability of multiple independent resources to act like a single resource. Cloud computing itself is a federation of resources, so the many assets, identities, configurations and other details of a cloud computing solution must be federated to make cloud computing practical. The requirements from the previous section are implemented via the following federation patterns:

The ability to write policies that examine security tokens to manage access to cloud resources. Access to resources can be controlled by more than one factor. For example, access could be limited to users in a particular role, but only across certain protocols and only at certain times of the day.

The ability to federate logins based on credentials from a trusted authority. Given an authenticated user with a particular role, federated single sign-on allows a user to login to one application and access other applications that trust the same authority. Federated single sign-off is part of this pattern as well; in many situations it will be vital that a user logging out of one application is logged out of all the others. The Single Sign-On pattern is enabled by the Identity Management pattern.

The ability to collect audit and compliance data spread across multiple domains, including hybrid clouds. Federated audits are necessary to ensure and document compliance with SLAs and regulatory requirements.

The ability to federate configuration data for services, applications and virtual machines. This data can include access policies and licensing information across multiple domains. Because existing best practices for security apply to the cloud, providers should use existing standards to deliver these federation patterns.
Thus the cloud computing is preferred by many small scale organizations and large scale organizations for managing their client server architecture for easy management of data on network easily, efficiently, with best performance and response time of server. While management of data using Cloud Computing Services some security issues regarding data is the main problem, so by using security methods prevents it. Thus it is the magical approach for managing data on network.
16. Green Computing

By Anna Gahininath Pol

Indira Institute Of Management MCA, Pune

anna310011@gmail.com

91-9145498366

As 21st century belongs to computers, electronic items, energy issues will get a serious ring in the coming days, as the public debate on carbon emissions, global warming and climate change gets hotter. Taking into consideration the popular use of information technology industry, it has to lead a revolution of sorts by turning green in a manner no industry has ever done before.

We love our computers for all the ways they make our lives (and the world) better – the wealth of knowledge of the Internet, the instantaneous communication, the sophisticated tools that help us work and create and share. But this modern world's greatest tool is among our most disposable and resource-heavy items. Performance-wise, computer design has progressed staggeringly well and astonishingly fast but looking at it from a green perspective, the work has barely begun. It takes a lot of energy to create, package, store, and move every 10-20 megabytes of data. Even with energy prices as cheap as they are now, it will soon cost more to power a computer for four years than it does to buy a new one. When a computer dies it either rots in a landfill, or children in the developing world end up wrestling its components apart by hand, melting toxic bits to recover traces of heavy metals.

Manufacturing computers means the use of lead, cadmium, mercury, and other toxics in general and laptop in particular. Normally, computers can contain 4 to 8 pounds of lead alone, according to green experts. It's no wonder that computers and other electronics make up two-fifths of all lead in landfills. To counter this growing pollution threat all over the world due to the growing use of electronic device in general and computers in particular there a need to look for a green computer. If we think computers are nonpolluting and consume very little energy we need to think again. It is estimated that out of $250 billion per year spent on powering computers worldwide only about 15% of that power is spent computing- the rest is wasted idling. Thus, energy saved on computer hardware and computing will equate tonnes of carbon emissions saved per year. Taking into consideration the popular use of
information technology industry, it has to lead a revolution of sorts by turning green in a manner no industry has ever done before.

The plan towards green IT should include new electronic products and services with optimum efficiency and all possible options towards energy savings. Faster processors historically use more power. Inefficient CPU’s are a double hit because they both use too much power themselves and their waste heat increases air conditioning needs. Power management soft-wares also help the computers to sleep or hibernate when not in use. It is important to design computers which can be powered with low power obtained from non-conventional energy sources like solar energy, pedaling a bike, turning a hand-crank etc.

Electronics giants are about to roll out eco-friendly range of computers (like desktops and laptops) that aim at reducing the e-waste in the environment. Besides desktops and laptops, other electronic hardware products should also be strictly adhering to the restricted use of hazardous substances. In other words, they should be free of hazardous materials such as brominated flame retardants, PVCs and heavy metals such as lead, cadmium and mercury, which are commonly used in computer manufacturing. Reliability about the use of green materials in computer is perhaps the biggest single challenge facing the electronics industry. Lead-tin solder in use today is very malleable making it an ideal shock absorber. So far, more brittle replacement solders have yet to show the same reliability in arduous real-world applications. Replacements like the front runner, a tin/copper/silver alloy, also require higher melting temperatures, which can affect chip life.

Here's how designers plan to make future computer more eco-friendly across its entire life span, from manufacture to recycling:

1. energy-intensive manufacturing of computer parts can be minimized by making manufacturing process more energy efficient
2. by replacing petroleum-filled plastic with bioplastics—plant-based polymers—require less oil and energy to produce than traditional plastics with a challenge to keep these bioplastic computers cool so that electronics won't melt them
3. landfills can be controlled by making best use of the device by upgrading and repairing in time with a need to make such processes (i.e., upgradation and repairing) easier and cheaper
4. avoiding the discarding will not only control e-waste out of dumps but also save energy and materials needed for a whole new computer
5. power-sucking displays can be replaced with green light displays made of LEDs, or OLEDs.

6. use of toxic materials like lead can be replaced by silver and copper.

7. future computers could knock 10 percent off their energy use just by replacing hard drives with solid-state, or flash, memory, which has no watt-hungry moving parts.

So far, consumers haven't cared about ecological impact when buying computers, they've cared only about speed and price. Consumers will become pickier about being green. Devices use less and less power while renewable energy gets more and more portable and effective. New green materials are developed every year, and many toxic ones are already being replaced by them. It'll be the product of years of improvements. The features of a green computer of tomorrow would be like: efficiency, manufacturing & materials, recyclability, service model, self-powering, and other trends. Green computer will be one of the major contributions which will break down the 'digital divide', the electronic gulf that separates the information rich from the information poor.

Green computing is the study and practice of using computing resources efficiently.

A green computing initiative must be systemic in nature and address increasingly sophisticated problems.

2. Green Computing

2.1. Green computing architecture

2.2. Regulations and industry initiatives

2.3. Approaches to green computing
2.1. Green computing architecture

Overview of Green Computing Architecture

The statistic results of the power consumption of each components of a laptop computer is shown bellow. With the statistic results of power consumption, we can realized which component consumes more power and can try to reduce the power consumption of these components.

Power Consumption in An Average Laptop

![Power Consumption Pie Chart]

The powerful new laptop with the terrifically beautiful video display might require a more expensive battery technology if the laptop’s weight is to be maintained as well as its battery life.

The Goals of Green Computing

The goals of green computing are similar to greenchemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste.

Research continues into key areas such as making the use of computers as energy-efficient as possible, and designing algorithms and systems for efficiency-related computer technologies.
2.2. Regulations and Industry Initiatives - Government

- Many governmental agencies abroad have continued to implement standards and regulations that encourage green computing.

- The Energy Star program was revised in October 2006 to include stricter efficiency requirements for computer equipment, along with a tiered ranking system for approved products.

- In 2008, a report published in the UK by the Department for Communities and Local Government, quantified that the potential carbon savings from increasing the usage of online public service delivery were significantly in excess of the negative impact of extra IT server capacity.

**Energy Star**

Energy Star is an international standard for energy efficient consumer products originated in the United States of America.

It was first created as a United States government program during the early 1990s, but Australia, Canada, Japan, New Zealand, Taiwan and the European Union have also adopted the program.

Devices carrying the Energy Star logo, such as computer products and peripherals, kitchen appliances, buildings and other products, generally use 20%-30% less energy than required by federal standards.

**2.3. Approaches to green computing**

1. Operation System Support

The dominant desktop operating system, Microsoft Windows, has included limited PC power management features since Windows 95. These initially provided for stand-by (suspend-to-RAM) and a monitor low power state.
Windows 2000 was the first NT based operating system to include power management, his required
dependent on major changes to the underlying operating system architecture and a new hardware driver model; it
also introduced Group Policy, a technology which allowed administrators to centrally configure most
Windows features. The most recent release, Windows 7 retains these limitations but does include
refinements for more efficient user of operating system timers, processor power management, and
display panel brightness.

The most significant change in Windows 7 is in the user experience.

The prominence of the default High Performance power plan has been reduced with the aim of encouraging users to save power.

2. Power Supply

Desktop computer power supplies (PSUs) are generally 70–75% efficient, dissipation the remaining energy as heat.

An industry initiative called 80 PLUS certifies PSUs that are at least 80% efficient; typically these models are drop-in replacements for older, less efficient PSUs of the same form factor.

As of 20 July 2007, all new Energy Star 4.0-certified desktop PSUs must be at least 80% efficient.

3. Storage

Smaller form factor (e.g. 2.5 inch) hard disk drives often consume less power than physically larger drives.

With no moving parts, power consumption may be reduced somewhat for low capacity flash based devices.

As hard drive prices have fallen, storage farms have tended to increase in capacity to make more data
available online, this includes archival and backup data that would formerly have been saved on tape or other offline storage.

The increase in online storage has increased power consumption.
Reducing the power consumed by large storage arrays, while still providing the benefits of online storage, is a subject of ongoing research.

4. Display

CRT monitors typically use more power than LCD monitors, they also contain significant amounts of lead.

LCD monitors typically use a cold-cathode fluorescent bulb to provide light for the display.

Some newer displays use an array of light-emitting diodes (LEDs) in place of the fluorescent bulb, which reduces the amount of electricity used by the display.

What You Can Do:

Suggested settings:

• Turn off monitor: After 15 mins
• Turn off hard disks: After 15 mins
• System Standby: Never

Green Computing Tips

1. Turn off your computer when not in use.

2. Make sure to activate “sleep mode” as a default when setting up your computer.

3. Always look for the EnergyStar label when purchasing a new computer.

4. Unplug all periphery equipment (speakers, printers, etc.) when not in use.

5. Do not leave your computer plugged in unless it is actively charging.

6. Use recycled paper, print double-sided, and only print what you need.

7. Do not print multiple copies if you don’t see your document at the printer; check your settings, it may have printed on another machine.
17. Green Computing

MITESH AGRAWAL
MCA, Indira Institute of Management, Pune
mitsag89@yahoo.co.in,
miteshagrawal@indiraiimpmca.edu.in
9096691828

Green computing is the study and practice of using computing resources efficiently. The primary objective of such a program is to account for the triple bottom line, an expanded spectrum of values and criteria for measuring organizational (and societal) success. The goals are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote recyclability or biodegradability of defunct products and factory waste.

Modern IT systems rely upon a complicated mix of people, networks and hardware; as such, a green computing initiative must be systemic in nature, and address increasingly sophisticated problems. Elements of such as solution may comprise items such as end user satisfaction, management restructuring, regulatory compliance, disposal of electronic waste, telecommuting, virtualization of server resources, energy use, thin client solutions, and return on investment (ROI).

As 21st century belongs to computers, gizmos and electronic items, energy issues will get a serious ring in the coming days, as the public debate on carbon emissions, global warming and climate change gets hotter. Taking into consideration the popular use of information technology industry, it has to lead a revolution of sorts by turning green in a manner no industry has ever done before.

Future of Green Computing

As 21st century belongs to computers, gizmos and electronic items, energy issues will get a serious ring in the coming days, as the public debate on carbon emissions, global warming...
and climate change gets hotter. If we think computers are non-polluting and consume very little energy we need to think again. It is estimated that out of $250 billion per year spent on powering computers worldwide only about 15% of that power is spent computing- the rest is wasted idling. Thus, energy saved on computer hardware and computing will equate tonnes of carbon emissions saved per year. Taking into consideration the popular use of information technology industry, it has to lead a revolution of sorts by turning green in a manner no industry has ever done before. Opportunities lie in green technology like never before in history and organizations are seeing it as a way to create new profit centers while trying to help the environmental cause. The plan towards green IT should include new electronic products and services with optimum efficiency and all possible options towards energy savings. Faster processors historically use more power. Inefficient CPU's are double hit because they both use too much power themselves and their waste heat increases air conditioning needs, especially in server farms--between the computers and the HVAC. The waste heat also causes reliability problems, as CPU's crash much more often at higher temperatures. Many people have been working for years to slice this inefficiency out of computers. Similarly, power supplies are notoriously bad, generally as little as 47% efficient. And since everything in a computer runs off the power supply, nothing can be efficient without a good power supply. Recent inventions of power supply are helping fix this by running at 80% efficiency or better.

Ways of Implementation

Power management software’s help the computers to sleep or hibernate when noting use. Reversible computing (which also includes quantum computing) promises to reduce power consumption by a factor of several thousand, but such systems are still very much in the laboratories. Reversible computing includes any computational process that is (at least to some close approximation) reversible, i.e., time-invertible, meaning that a time-reversed version of the process could exist within the same general dynamical framework as the original process. Reversible computing's efficient use of heat could make it possible to come up with 3-D chip designs, Bennett said. This would push all of the circuitry closer together and ultimately increase performance.
The best way to recycle a computer, however, is to keep it and upgrade it. Further, it’s important to design computers which can be powered with low power obtained from non-conventional energy sources like solar energy, pedalling a bike, turning hand-crank etc.

The electric utility industry is in an unprecedented era of change to meet increasing customer demand for greater reliability and different services in the face of substantial regulation and volatile energy costs. This requires new approaches and business models to allow greater network reliability, efficiency, flexibility and transparency. At the same time, the utility industry is digitizing, transforming from an electromechanical environment to a digitized one.

New Internet Protocol-enabled networks now allow for network integration along the entire supply chain – from generation, transmission, to end-use and metering - and create the opportunity for Intelligent Utility Networks (IUN) which applies sensors and other technologies to sense and respond in real-time to changes throughout the supply chain. The IP-enabled network connects all parts of the utility grid equipment.

Control systems, applications, and employees. It also enables automatic data collection and storage from across the utility based on a common information model and service-oriented architecture (SOA), which enables a flexible use of information technology. This in turn allows utilities to continuously analyse data so that they can better manage assets and operations.

Electronics giants are about to roll out eco-friendly range of computers (like desktops and laptops) that aim at reducing the e-waste in the environment. Besides desktops and laptops, other electronic hardware products should also be strictly adhering to the restricted use of hazardous substances. In other words, they should be free of hazardous materials such as brominated flame retardants, PVCs and heavy metals such as lead, cadmium and mercury, which are commonly used in computer manufacturing. Reliability about the use of green materials in computer is perhaps the biggest single challenge facing the electronics industry. Lead-tin solder in use today is very malleable making it an ideal shock absorber.
GREEN IT: The next burning issue for business

It is becoming widely understood that the way in which we are behaving as a society is environmentally unsustainable, causing irreparable damage to our planet. Rising energy prices, together with government-imposed levies on carbon production, are increasingly impacting on the cost of doing business, making many current business practices economically unsustainable. It is becoming progressively more important for all businesses to act (and to be seen to act) in an environmentally responsible manner, both to fulfil their legal and moral obligations, but also to enhance the brand and to improve corporate image. Companies are competing in an increasingly ‘green’ market, and must avoid the real and growing financial penalties that are increasingly being levied against carbon production.

IT has a large part to play in all this. With the increasing drive towards centralized mega data centres alongside the huge growth in power hungry blade technologies in some companies, and with a shift to an equally power-hungry distributed architecture in others, the IT function of business is driving an exponential increase in demand for energy, and, along with it, is having to bear the associated cost increases.

The Problem

Rising energy costs will have an impact on all businesses, and all businesses will increasingly be judged according to their environmental credentials, by legislators, customers and shareholders. This won’t just affect the obvious, traditionally power-hungry ‘smoke-belching’ manufacturing and heavy engineering industries, and the power generators. The IT industry is more vulnerable than most –it has sometimes been a reckless and profligate consumer of energy. Development and Improvements in technology have largely been achieved without regard to energy consumption.

The Impact

Rising energy costs and increasing environmental damage can only become more important issues, politically and economically. They will continue to drive significant increases in the cost of living, and will continue to drive up the cost of doing business. This will make it
imperative for businesses to operate as green entities, risking massive and expensive change. Cost and environmental concern will continue to force us away from the ‘dirtiest’ forms of energy (coal/oil), though all of the alternatives are problematic. We may find ourselves facing a greater reliance on gas, which is economically unstable and whose supply is potentially insecure, or at least unreliable.

It may force greater investment in nuclear power, which is unpopular and expensive, and it may lead to a massive growth of intrusive alternative energy infrastructure –including huge wind farms, or the equipment needed to exploit tidal energy. Solving the related problems of rising energy costs and environmental damage will be extremely painful and costly, and those perceived as being responsible will be increasingly expected to shoulder the biggest burden of the cost and blame. It may even prove impossible to reduce the growth in carbon emissions sufficiently to avoid environmental catastrophe. Some believe that the spotlight may increasingly point towards IT as an area to make major energy savings, and some even predict that IT may even become tomorrow’s 4x4/SUV, or aviation – the next big target for the environmental lobby, and the next thing to lose public support/consent.

**The Solution**

A fresh approach to IT and power is now needed, putting power consumption at the fore in all aspects of IT from basic hardware design to architectural standards, from bolt-on point solutions to bottom-up infrastructure build. IBM has a real appreciation of the issues, thanks to its size, experience and expertise, and can help its customers to avoid the dozens of ‘wrong ways’ of doing things, by helping to identify the most appropriate solutions. There is a real, economic imperative to change arising now, and it is not just a matter of making gestures simply to improve a company’s environmental credentials.

**Benefits of Green Computing**

Green Computing solutions benefit the environment, as well as the bottom-line. By focusing on Green Computing, an IT organization can:
Lower overall energy expenses including general energy consumption, as well as power and cooling costs.

- Optimize server capacities and performance.
- Reduce data center footprint, reclaiming valuable floor space through consolidation and/or virtualization.
- Provide required, rapid and secure access to data.
- Increase ease of systems and solutions management.
- Recycle end-of-life equipment.

In short, Green Computing enables companies to meet business demands for cost-effective, energy-efficient, flexible, secure and stable solutions while being environmentally responsible.

**Recent implementations of Green Computing:**

**Blackle:**

Blackle is a search-engine site powered by Google Search. Blackle came into being based on the concept that when a computer screen is white, presenting an empty wordage or the Google home page, your computer consumes 74W. When the screen is black it consumes only 59W. Based on this theory if everyone switched from Google to Blackle, mother earth would save 750MW each year. This was a really good implementation of Green Computing. The principle behind Blackle is based on the fact that the display of different colours consumes different amounts of energy on computer monitors.

**Fit-PC: a tiny PC that draws only 5w:**

Fit-PC is the size of a paperback and absolutely silent, yet fit enough to run Windows or Linux. Fit-PC is designed to fit where a standard PC is too bulky, noisy and power hungry. If you ever wished for a PC to be compact, quiet and green – then fit-PC is the perfect fit for you. Fit-PC draws only 5 Watts, consuming in a day less power than a traditional PC consumes in 1 hour. You can leave fit-PC to work 24/7 without making a dent in your electric bill.
Zonbu Computer:  
The Zonbu is a new, very energy efficient PC. The Zonbu consumes just one third of the power of a typical light bulb. The device runs the Linux operating system using a 1.2 gigahertz processor and 512 MB of RAM. It also contains no moving parts, and does even contain a fan. You can get one for as little as US$99, but it does require you to sign up for a two-year subscription.

Sunray thin client:  
Sun Microsystems is reporting increased customer interest in its Sun Ray, thin desktop client, as electricity prices climb, according to Subodh Bapat, vice-president and chief engineer in the Eco Responsibility office at Sun. Thin clients like the Sun Ray consume far less electricity than conventional desktops, he said. A Sun Ray on a desktop consumes 4 to 8 watts of power, because most of the heavy computation is performed by a server. Sun says Sunrays are particularly well suited for cost-sensitive environments such as call centres, education, healthcare, service providers, and finance. PCs have more powerful processors as well as hard drives, something thin clients don’t have. Thus, traditional PCs invariably consume a substantially larger amount of power. In the United States, desktops need to consume 50 watts or less in idle mode to qualify for new stringent Energy Star certification.

The Asus Eee PC and other ultra-portables:  
The "ultra-portable" class of personal computers is characterized by a small size, fairly low power CPU, compact screen, low cost and innovations such as using flash memory for storage rather than hard drives with spinning platters. These factors combine to enable them to run more efficiently and use less power than a standard form factor laptop. The Asus Eee PC is one example of an ultraportable. It is the size of a paperback, weighs less than a kilogram, has built-in Wi-Fi and uses flash memory instead of a hard drive. It runs Linux too.
References

2. “Green Computing: Whitepaper”.
3. Green IT’-IBM technology services.
18. Green Computing - A Way to Sustainable Development

Author - Prof. Mrs. Pallavi Niranjan Shintre

Email ID - pallavimanohar@gmail.com

PES’s, Modern College of Engineering, Off J.M.Road, Shivaji Nagar, Pune-05
Mobile No – 9822196760

Introduction:

When we hear the term “green living” many of us imagine of the trees, plants, mountains and lawns, but green living can start indoors by recycling, reducing, reusing i.e. Finding new and creative use for old items and trying to save the energy. Today due to globalization world has come closer. Each and every country is linked. All this is possible because of computers. We all know that computer is one of the most brilliant gifts of science. But the other side of this is the computers are deemed as one of the fastest-growing electricity loads in the universe.

Computers are considered as the most prevalent electronic device on our planet and solar system. They will become a part of almost every facet of our lives. With the growing use of computers we must also have a growing understanding of how their use affects our environment. According to one of the surveys’ carbon emission through software industry is equal to the carbon emission created from airline industry. A report by ScienceDaily cited that e-waste generation is growing by about 40 million tons a year which causes landfills. These materials when placed in a landfill, even in small doses, these materials contaminate soil as well as drinking water. According to Allen Hershkowitz, a senior scientist and authority on waste management at the Natural Resources Defense Council, All of these materials are known to have toxicological effects that range from brain damage to kidney disease to mutations, cancers"
Computers help us to conserve resources but one of the serious concerns is that they are creating plenty of E-waste, consuming a great amount of energy; high amount of carbon dioxide emission etc. Green computing or green IT, refers to environmentally sustainable computing. Green computing pursues the practice of reducing the energy consumption, minimizing waste associated with computer. By following the green computing ideology we can conserve energy and avoid environmental and financial losses. Reducing energy usage, which also reduces carbon dioxide emissions and organizations energy bill, this is nothing but the most effective thing which needs to done hence forth.

General working habits of computer users can be modified to minimize adverse impact on the global environment. According to me there are some ways if practiced sincerely will definitely make the green computing program successful. These facts are as follows

- Power-on and power-down energy-consuming peripherals such as Computers, laptops, laser printers, scanners, and projectors according to need and switch off Cable Modems, Routers and Wi-Fi Access Points when not in use.
- Refill Ink-jet cartridges and laser toner are considered to be cheaper and they don’t add to landfill.
- Use notebook computers rather than desktop computers or else use liquid-crystal-display (LCD) monitors rather than cathode-ray-tube (CRT) monitors.
- Minimize the use of paper and plastic and try to recycle waste paper and plastic, similarly there should be some incentive schemes for garbage collectors and general public for collecting and handing over e-waste.
- Dues should be collected from manufacturers/consumers for the systematic disposal of toxic materials (e-waste).
- Try to purchase equipment that uses fewer poisonous materials and more recycled components.
- Virtualization is energy friendly approach which is one of the most effective tools.
- Plantation at work place makes atmosphere pleasant and generate fresh air to keep healthy and pollution free atmosphere.
- Lastly, Conduct awareness programs to make the subject clearer.
19. Green computing: A waste minimization procedure

Sumit O. Sharma
Asst. Professor Department of Management Studies, Sevagram
Mob +91 (9970064212)
Email: sumitbcs29@rediffmail.com

The increase in U-M consumption of electricity and paper causes an increase in air pollution, solid waste, and the burning of fossil fuels. Much of the paper used by PCs is wasted. National estimates indicate that most PCs are not being used most of the time they are on. In addition, 30 - 40 percent of all PCs are left on overnight and on weekends.

On the U-M Ann Arbor campus, PC operation alone may account for at least $1.8 million in energy costs each year. This represents approximately 11 percent of the total amount spent by the U-M on electricity. It is estimated that a PC system can easily consume 300 watts of electricity per hour, the same amount of energy needed to operate three 100 watt light bulbs.

The following "green computing" habits can significantly reduce the amount of electricity and environmental waste for which PCs are responsible.

Waste Minimization Procedure

Electrical Conservation Tips:

- Turn the computer off overnight and on weekends;
- Wait until ready to use the PC before turning it on;
- If the computer is going to be inactive for more than 16 minutes, consider turning it off. After this time, the energy needed to run the computer outweighs the start-up energy;
- Do not turn on the printer until ready to print, even an idle printer consumes energy;
Try to schedule computer-related activities to do them all at once, keeping the computer off at other times;

- If spending a large amount of time at the computer, consider reducing the light level in your office. This may improve cathode ray tube screen visibility as well as save energy.

**Paper Conservation Tips:**

- Use "paperless" methods of communication such as electronic mail (e-mail) and fax modems. Also, do not print out copies of e-mail messages unless necessary;
- Use smaller font sizes and decrease the spacing between lines, or reformat to keep the document to as few pages as possible;
- Review documents on the screen instead of printing a draft. If you must print a draft, use the blank back side of used sheets;
- Use a printer that can print double-sided documents. When making copies, use double-sided copying;
- The U-M buys and uses recycled-content paper when possible. Look for papers with 50 - 100 percent post-consumer waste and non-chlorine bleached. Also, recycle paper when done.
- Store information on diskettes rather than in "hard copy" format. A single high-density 3.5 inch floppy disk can hold the equivalent of 750 sheets of paper, about one and a half reams. Also, be sure to reuse disks that contain outdated information.

**Purchasing and Use of Equipment:**

- Printer toner cartridges can be refilled, rebuilt and reused. Many manufacturers will take a spent cartridge, refurbish it, refill it, and return it for about half the price of buying a new one;
- Determine whether you can upgrade your existing equipment rather than purchasing new equipment;
- Donate an old computer to a school or charity; if it is permanently out of order, give it to a computer recycling facility instead of discarding in a landfill;
Only buy a monitor as large as you really need; a 17 inch monitor uses 40 percent more energy than a 14-inch monitor. Also, the higher the resolution, the more energy it needs;

Consider purchasing an ink jet printer instead of a laser printer. Although they are a little slower, they use 80-90 percent less energy;

Request recycled or recyclable packaging from your vendor;

Buy soy or non-petroleum based inks. These printer inks are made from renewable resources, require fewer hazardous solvents, which translates to fewer air emissions, and in many cases produce brighter, cleaner colors;

Try to buy energy efficient products such as those bearing the Energy Star Logo. The Energy Star Program was started by the Environmental Protection Agency (EPA) to encourage the production and use of energy-efficient equipment. In accordance with the EPA's voluntary guidelines, leading computer manufacturers are now producing equipment that can automatically power down to a "sleep mode" to save energy when not in use. They also use up to 30 percent less energy when running than conventional equipment. These added capabilities do not increase price or decrease performance.

Benefits

The production of electricity is the largest single source of air pollution, due to the burning of fossil fuels. A power plant used to generate electricity, burns oil, coal, or natural gas that emits gases such as carbon dioxide, sulfur dioxide and nitrogen oxides. These gases, in turn, cause acid rain, smog and global warming. Conserving energy reduces the amount of fuel that has to be consumed, thereby reducing the amount of pollution generated. Obviously, energy-efficiency is a positive step toward reducing air pollution.

Some of the tips given above to reduce paper use and reuse of toner cartridge and diskettes will go a long way towards reducing the amount of solid waste that ultimately ends up in a landfill.
20. Modify Green IT

Mr Vijay a Tathe
College of Science & Information Technology(CSIT)
E-Mail tathevijay@gmail.com.

“NEXT IT REVOLUTION GREEN COMPUTING”……..

“Save the Planet, Save Your Equipment, Save Money”

Green computing is the practice of using computing resources efficiently. Modern IT Systems rely upon a complicated mix of people, networks, and hardware, as such, a reen computing initiative must be systemic in nature, and address increasingly sophisticated problems. Green computing is the utmost requirement to protect environment and save energy along with operational expenses in today's increasingly competitive world.

Currently we are working on implementation of the green computing practices. But before implementing, it's also important to study about what kind of energy gains and operational gains can be achieved. Hence, analysis of the gap between what we have today and what we'll have to do is essential in order to achieve the benefits of green computing. Currently we are in that stage.

Also, every big change begins from small initiatives. For instance, we started some of the simple but effective initiatives like setting the power options on your computer or in phones to switch to sleep mode when it's not active. When you're going to be away from your PC for more than a few minutes, setting it to stand-by mode and turning off the monitor will save a huge amount of energy.

“Green computing” is the name attached to this movement, which represents an environmentally responsible way to reduce power and environmental e- waste.
Green Computing Vision

As 21st century belongs to computers, and electronic items, energy issues will get a serious ring in the coming days, as the public debate on carbon emissions, global warming and climate change gets hotter. Faster processors historically use more power. Inefficient CPU's are a double hit because they both use too much power themselves and their waste heat increases air conditioning needs.

The goals are to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote recyclability or biodegradability of defunct products and factory waste. Such practices include the implementation of energy-efficient central processing units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (E-Waste).

Need for Green Computing

Green computing is a new approach which aims at designing computer systems that achieves better processing and performance with least amount of power consumption. Numerous studies and surveys have already shown that the power costs put together form the lion’s share of total costs of management of a data center.

The extensive use of computers and IT has made our life easier and as such the use of IT is ever on the increase resulting in greater power consumption. Greater power consumption means greater emission of greenhouse gases like carbon dioxide. It is
observed that most of the computer energy is often wasteful. This is because we leave the computer ON even when it is not in use. The CPU and fan consume power; Screen savers consume power even when the system is not in use. Insufficient power and cooling capacities can also result in loss of energy. It is observed that most of the datacenters do not have sufficient cooling capacities. This results in environment pollution. This could be because of defects in manufacturing techniques, packaging, disposal of computers and components. Another effect is because of toxicity. There are toxic chemicals used in the manufacturing of new computers as well as disposal of old computers and water.

**Facts about Business Computing**

• Simply leaving a computer running consumes electricity and adds to computing costs.
• The use of screen savers does not save energy.
• It is estimated that a typical desktop PC with a 17-inch flat panel LCD monitor requires about 100 watts—65 watts for the computer and 35 watts for the monitor.
• If left on 24x7 for one year, this same system will consume 874 kilowatt hours of electricity—enough to release 750 pounds of carbon dioxide into the atmosphere and the equivalent of driving 820 miles in an average car.

**Scenario of India:-**

Indian IT Industry has witnessed huge growth in the last decade making it a unique brand in the world. However this has lead to increased power consumption and escalation of realty costs in major cities. Due to the already vast population India already struggles to put an end to its power shortage. In order to remain competitive, Indian IT companies need to adopt green and sustainable computing measures on a large scale. Recent down turns in the world economy has also forced companies to lower their operational costs to ensure profitability. Power costs form a major part of the total operational cost for IT firms. Hence it has become almost essential for IT firms to adopt green computing measures.

**Approaches for Green IT:-**
The motivation to reduce waste through Green Computing is clear, although identifying appropriate Green techniques for a given situation from among the many available is challenging. One of the easiest ways to reduce consumption and pollution is to reduce. Reducing consumption by printing documents double-sided, viewing documents on-screen, powering off electrical devices that are not in use, placing a computer in sleep mode or powered off when not in use, and similar techniques are effectively free. and adopting new approach Such as

- Cloud Computing
- Grid Computing
- Green Data Center

Methods for Green Computing:-

There are a number of more fundamental steps that can be taken to significantly decrease the environmental impact of computing. These mainly involve measures for reducing energy consumption.

1.1 **Lower Power Hardware**: PCs can be made to use less electricity by using a lower power processor, opting for onboard graphics (rather than a separate graphics card), using passive cooling (rather than energy consuming fans), and either a solid-state disk (SSD) in place of a spinning hard drive as the system disk.

1.2 **Virtualization**: Virtualization is the use of computer software to simulate hardware. Within data centers, server consolidation applies virtualization in its replacement of many stand-alone physical servers with virtual servers that run as software on a small number of larger computers. via a virtualized server consolidation a company can obtain a far more optimal use of computing resources by removing the idle server capacity that is usually spread across of physical servers.

* e.g. IBM, for example, is currently engaged in its Project Big Green, and which involves replacing about 2,900 individual servers with about 30 mainframes to achieve an expected 80 per cent energy saving over five years.

1.3 **Cloud Computing**: Cloud computing is where software applications, processing power, data and potentially even artificial intelligence are accessed over the Internet. Cloud Computing has many benefits, one of which is enabling anybody to obtain the
environmental benefits of virtualization By choosing to cloud compute and in particular by adopting online computer processing power in the form of PaaS or IaaS companies may therefore potentially reduce their carbon footprint. As well as allowing server capacity to run at a more optimal energy efficiency, cloud computing can also remove the need for most users to run high-power PCs and laptops.

1.4 **Less Pollutant Manufacture:**- A great many hazardous chemicals - including lead, mercury, cadmium, beryllium, bromine flame retardants (BFRs) and polyvinyl chloride (PVC) are used to make computers. By reducing the use of such substances, hardware manufacturers could prevent people being exposed to them, as well as enabling more electronics waste to be safely recycled.

1.5 **Wireless Network and Sensors:**- Sensors can be employed in different parts areas in a data center to determine the temperature of each area. This way it will be easily known which area needs more cooling and where to reduce the cooling.

1.6 **Recycle:**- Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner. Computers have toxin metals and pollutants that can emit harmful emissions into the environment. Never discard computers in a landfill. Recycle them instead through manufacturer programs.

**GREEN COMPUTING TECHNIQUES:**-

Understanding the ways in which power consumption impacts the “greenness” of any technology, and specifically computing technology, is an essential step toward reducing this consumption. the various specific techniques that can be used to reduce power consumption.

- Turn Off Equipment When Not In Use.
- Computer Power Savings Modes.
- Use Screen Savers.
- Monitor Sleep Mode.
- Hard Disk Sleep Mode.
- System Standby Mode.
- Hibernate Mode.
- Upgrade to Extend Computer Lifecycle.
GREEN DATA CENTERS:-

One of the main objectives of “green technologies” is to reduce the “carbon footprint” required or generated by the computer technology. Power plants are highly responsible for the production of greenhouse gases. This is why it is necessary to reduce the demand of electricity required throughout the world, in particular, that required by computing data centers. According to EPA, U.S. data centers alone consume as much power in a year as is generated by five power plants (U.S. Environmental Protection Agency, 2007). Thus, for any data center to be energy efficiency is a must. A green data center (GDC) is similar to any other data center used as a repository for the storage, management and distribution of data. However, what makes a data center “green” is that the mechanical, electrical and computer systems are designed simultaneously to achieve maximum energy efficient and minimum environmental impact.
21. Understanding the Cloud

Aakash Sangamnerkar
(MCA 1st year)
email id: akash.getin@gmail.com
Pimpri Chichwad College Of Engineering

Cloud computing is the next big thing in IT. Cloud computing promises to speed application deployment, increase innovation, lower costs, and also making software’s more attractive all while increasing business lightness. Developers with innovative ideas for new Internet services no longer require the large capital spending in hardware to deploy their service or the human expense to operate it. Cloud computing brings a new level of efficiency and economy to delivering IT resources on demand and in the process it opens up new business models and market opportunities. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000. Cloud computing isn’t only about hardware, it’s also a programming revolution. Nimble, easy-to-access, and even lightweight Web protocols bring a new era of productivity in developers.

Now-a-days, the number and quality of public, commercially available cloud-based service offerings is growing fast. Using the cloud is often the best option for startups, research projects, Web 2.0 developers, or niche players who want a simple, low-cost way to “load and go.” If you’re an Internet startup today, you will be mandated by your investors to keep your IT spends to a minimum. This is certainly what the cloud is for. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS) also some vendors use terms such as IaaS (Infra-structure as a Service) and PaaS (Platform as a Service) to describe their products, but we avoid these because accepted definitions for them still vary widely. The line
between “low-level” infrastructure and a higher-level “platform” is not crisp. We believe the two are more alike than different, and we consider them together. Similarly, the related term “grid computing,” from the high-performance computing community, suggests protocols to offer shared computation and storage over long distances, but those protocols did not lead to a software environment that grew beyond its community.

At a basic level, cloud computing was simply meant for delivering IT resources as services. Almost all IT resources can be delivered as a cloud service, applications, compute power, storage capacity, networking, programming tools, even communications services and collaboration tools and gradually the ubiquitous availability of high capacity networks, low cost computers and storage devices as well as the widespread adoption of virtualization, service-oriented architecture, autonomic, and utility computing have led to a tremendous growth in cloud computing. Details are abstracted from end-users, who no longer have need for expertise in, or control over, the technology infrastructure "in the cloud" that supports them.

This architectural model was immortalized by George Gilder in his October 2006 Wired magazine article titled “The Information Factories.” The server farms Gilder wrote about were architecturally similar to grid computing, but where grids are used for loosely coupled, technical computing applications, this new cloud model was being applied to Internet services.

He quoted as “In this architecture, the data is mostly resident on servers ‘somewhere on the Internet’ and the application runs on both the ‘cloud servers’ and the user’s browser.” -Eric Schmidt in ‘Information Factories’ by G. Gilder. The underlying concept of cloud computing dates back to the 1960s, when John McCarthy opined that "computation may someday be organized as a public utility." Almost all the modern-day characteristics of cloud computing (elastic provision, provided as a utility, online, illusion of infinite supply), the comparison to the electricity industry and the use of public, private, government, and community forms, were thoroughly explored in Parkhill’s 1966 book, The Challenge of the Computer Utility. Other scholars have shown that cloud computing’s roots go all the way back
to the 1950s when scientist Herb Grosch (the author of Grosch’s law) postulated that the entire world would operate on dumb terminals powered by about 15 large data centers.\(^3\)

The actual term "cloud" borrows from telephony in that telecommunications companies, who until the 1990s offered primarily dedicated point-to-point data circuits, began offering Virtual Private Network (VPN) services with comparable quality of service but at a much lower cost. By switching traffic to balance utilization as they saw fit, they were able to utilize their overall network bandwidth more effectively. The cloud symbol was used to denote the demarcation point between that which was the responsibility of the provider and that which was the responsibility of the user. Cloud computing extends this boundary to cover servers as well as the network infrastructure.

Cloud computing providers offer their services according to three fundamental models. Infrastructure as a service (IaaS), platform as a service (paas), and software as a service (SaaS) where iaas is the most basic and each higher model abstracts from the details of the lower models. A model adopted by cloud computing is depicted bellow.

1] **Software as a Service (SaaS)** - SaaS is at the highest layer and features a complete application offered as a service, on demand, provider’s infrastructure and serves multiple client organizations. The most widely known example include Google Apps offering of basic business services such as e-mail.
2] **Platform as a Service (PaaS)**- The middle layer, or PaaS, is the encapsulation of a development environment abstraction and the packaging of a payload of services. The archetypal payload is a Xen image (part of Amazon Web Services) containing a basic Web stack PaaS offerings can provide for every phase of software development and testing, or they can be specialized around a particular area, such as content management. Commercial examples include Google App Engine, which serves applications on Google’s infrastructure. PaaS services such as these can provide a great deal of flexibility but may be constrained by the capabilities that are available through the provider.

3] **Infrastructure as a Service (IaaS)**- IaaS is at the lowest layer and is a means of delivering basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches routers, and other systems are pooled to handle specific types of workloads from batch processing to server/storage augmentation during peak loads.

Thus, we can see that how cloud computer may offer many long-term benefits. Depending on the use case, IT organization using cloud computing have the potential to capture some or all of the benefits of reduced cost, reduced capital risk, increased flexibility, and greater business agility. Increased flexibility due to the fact that temporary and transient needs can be satisfied without making new investments in hardware.
22. Business implementation and security concerns of “Cloud Computing”

GAIKWAD SWAPNIL GENDAJI
MCA-Ist year,
JSPM’s Jayawant Institute of Computer Application, Tathawade, Pune.

Email ID sgg.gaikwad@gmail.com Mobile No. 9850241739

Few years back when internet was just born, business activities moved at very slow pace. Now in twenty first century the pace of business is much quicker and it continues to increase as the constant stream of new technologies make their way to stimulate business processes.

Cloud as a metaphor for "internet" is a combination of various servers and networks which is under veil to provide services like computation, software, data access and storage to end user hiding its actual physical location and configuration of the system that delivers the service. Cloud computing can be understood as more of a service rather than a product.

Cloud computing is an emerging computing model by which users can gain access to their applications from anywhere, through any connected device. A user-centric interface makes the cloud infrastructure supporting the applications transparent to users. “Cloud” is the aggregation of Servers, Low end computers and storage hosting the program and data Accessed via Internet anywhere from world.

User Centric: Easier for group members to collaborate.

Task Centric: User’s need is more important than features of application. It is not Network Computing

Application and Data are not confined to any specific Company’s Server ,No VPN Access, Encompasses multiple companies, multiple servers and multiple Networks, It is not Traditional Outsourcing, Not a contract to host data by 3rd party Hosting Business
Cloud computing is both a business delivery model and an infrastructure management methodology. The business delivery model provides a user experience by which hardware, software and network resources are optimally leveraged to provide innovative services over the Web, and servers are provisioned in accordance with the logical needs of the service using advanced, automated tools. The cloud then enables the service creators, program administrators and others to use these services via a Web-based interface that abstracts away the complexity of the underlying dynamic infrastructure.

The infrastructure management methodology enables IT organizations to manage large numbers of highly virtualized resources as a single large resource. It also allows IT organizations to massively increase their data center resources without significantly increasing the number of people traditionally required to maintain that increase. For organizations currently using traditional infrastructures, a cloud will enable users to consume IT resources in the data center in ways that were never available before. Companies that employ traditional data center management practices know that making IT resources available to an end user can be time-intensive. Cloud computing is an important topic. However, it is not a revolutionary new development, but an evolution that has taken place over several decades. The trend toward cloud computing started in the late 1980s with the concept of grid computing when, for the first time, a large number of systems were applied to a single problem, usually scientific in nature and requiring exceptionally high levels of parallel computation. It’s important to distinguish between grid computing and cloud computing. In the 1990s, the concept of virtualization was expanded beyond virtual servers to higher levels of abstraction—first the virtual platform, including storage and network resources, and subsequently the virtual application, which has no specific underlying infrastructure. Utility computing offered clusters as virtual platforms for computing with a metered business model. More recently software as a service (SaaS) has raised the level of virtualization to the application, with a business model of charging not by the resources consumed but by the value of the application to subscribers. The concept of cloud computing has evolved from the concepts of grid, utility and SaaS. It is an emerging model through...
which users can gain access to their applications from anywhere, at any time, through their connected devices.

Cloud computing Models

Basically there are three types of cloud computing models which are:

1. Public.
2. Private.
3. Hybrid.

Each type of cloud computing model—public, private or hybrid—faces different levels of IT risk.

In the private cloud delivery model, the cloud owner does not share resources with any other company. Private clouds are owned and operated by a single organization, delivering IT services within the constraints of their own network perimeter. In the public cloud computing model, IT activities and functions are provided as a service that can be billed on a pay-per-use or subscription basis via the Internet from external suppliers, using resources not owned by the consumer. The sharing of IT resources in a public, multitenant environment can help improve utilization rates and can reduce costs significantly while maintaining access to high quality technology. In a public cloud, an organization rents IT resources instead of having to invest in their own physical IT infrastructure or maintain under-utilized equipment to service peak loads. Instead, they can scale usage up or down, according to need, with costs directly proportional to need.

Many organizations embrace both public and private cloud computing by integrating the two models into hybrid clouds. These hybrids are designed to meet specific business and technology requirements, so that activities and tasks are allocated to traditional IT, external or internal clouds, as appropriate, helping to optimize security and privacy with a minimum investment in fixed IT costs.
Cloud Service models

In addition to the different cloud computing models, there are distinctions among the most common cloud service models as shown in Figure 3. Available to anyone with Internet access, cloud service models include:

- Software as a Service (SaaS) cloud model—Enables software to be delivered from a host source over a network as opposed to installations or implementations
- Platform as a Service (PaaS) cloud model—Enables operating systems and middleware services to be delivered from a managed source over a network
- Infrastructure as a Service (IaaS) cloud model—Enables the entire infrastructure to be delivered as a service over a network, including storage, routers, virtual systems, hardware and servers.

Cloud computing and security: the grand challenge

While cloud computing models are attractive because of their flexibility and cost effectiveness, certain challenges must be addressed in order to provide a viable option to traditional data services. First and foremost is the issue of security. The externalized aspect of outsourcing can make it harder to maintain data integrity and privacy, support data and service availability, demonstrate compliance, and secure highly available access to applications and information. In short, cloud computing can present an added level of risk.

Why cloud

1. Scalability.
2. Cost.
3. Instant.
23. Context-Aware Application

Sanket Kene
MCA, Indira Institute of Management (MCA) Pune
sanketkene1@gmail.com sanketkene1@yahoo.com

The last few years there has been major development in technologies with introduction of wireless communication medium, smaller and cheaper devices which has enabled people to get access to services anywhere, anytime. Context awareness is a capability whereby mobile computing devices can sense their physical environment and adapt their behavior accordingly. The term context-awareness, in ubiquitous computing, was introduced by Schilit in 1994 and has become one of the most exciting concepts in early 21st-century computing. These include computing devices worn by users, embedded devices, smart appliances, sensors surrounding users and a variety of wireless networking technologies.

Context-aware programming should enable an application design, which can change its behavior depending on the context in which it is running. By context, we mean information about an individual and his surrounding environment that may be used to deduce the ways in which the computing system can best serve the individual.

Examples of context-aware applications include advising a driver to take a particular route based on his location, his destination, and current traffic conditions; advising a nurse to attend to a particular patient based on the medical telemetry being received from all patients on a ward; and delivering a message either by cell phone or by e-mail depending on the recipient’s current context. The individuals who benefit from context-aware applications may not be sitting with a keyboard, mouse, and display, and may in fact be engrossed in other activities. They may remain unaware of the computer systems working on their behalf except when those systems interrupt them for some urgent purpose.
Objective

The main objective is to facilitate the development of context-aware applications, focusing on two aspects: on offering context modeling abstractions and on providing infrastructural support by means of a context handling platform.

1. The context modeling abstractions provide application developers with proper conceptual foundations that can be extended and specialized with specific application requirements.
2. The context handling platform allows application functionality to be delegated to the platform, which reduces application development effort, time and, therefore, costs.

The challenges of writing context-aware applications

Context-aware applications are difficult to write, for several reasons. First, sources of context information vary widely. Second, some sources of context information are unreliable, and may have to be replaced dynamically with other sources. Third, the task of composing low-level context information to deduce high-level context information can be complex.

Sources of context information include, among others, sensors, web services, publish-subscribe systems, instant-messaging systems, and relatively static repositories such as databases and calendars. Different sources of context information provide data in different formats, using different units of measurement, according to different protocols. Some sources actively push data to subscribers while others passively provide data when it is pulled.

The composition of context information is complex in part because some of the information comes from active (“push”) data sources and some from passive (“pull”) data sources. Polling passive data sources at regular intervals can result in excessive processor and network load if the polling interval is too short or in stale data if the polling interval is too long. Some active data sources may generate data at inopportune times, when the data is not really needed. The data must then be cached for later use or discarded.
Context-Aware Applications

Figure depicts an intuitive view of a user in his/her context, and a context-aware application (focusing on a single user only). We define a context-aware application as follows.

In Figure, the arrow “a” shows that the user and the context-aware application interact. Similarly, the arrow “b” shows that the user’s context and the context-aware application interact. The interactions represented by arrow “a” enable, for example, user’s input to be provided to the application, such as user commands and preferences, and the use of the service delivered by the context-aware application. The interactions represented by arrow “b” enable the context aware application to capture particular context conditions from the user’s context.

The intersection between a user’s context and a context-aware application includes sensors that detect the context conditions used by applications to respond accordingly. An example of a sensor which is useful for context-aware applications is a Global Positioning System (GPS) device, which can be used to continuously track a user’s location. Context information exchanged in interactions with the user’s context consists of geographical coordinates for the user’s current location. Another example of a sensor is a body thermometer, which can be used to monitor a patient’s body temperature.
information exchanged in interactions with the user’s context in this case consists of the
temperature measurements in degrees Celsius.

It is actually the responsibility of the application designer to decide whether context
information is relevant to the application, since this decision depends on the application’s
universe of discourse and the application’s state-of-affairs of interest. In addition, the
computational capabilities (sensor technology) available for building the context-aware
application typically determine the constraints for acquiring context automatically or
manually.

**Simplifying application development with Context Weaver**

Context Weaver simplifies the writing of context-aware applications by addressing
each of the difficulties. All sources of context information registered with a Context Weaver
installation provide data to applications through a simple, uniform interface. Applications
access data sources not by naming particular providers of the data, but by describing the kind
of data they need, and Context Weaver searches for an available source of such data. If the
source fails, Context Weaver automatically rebinds the application to another provider of the
same kind of data, if there is one.

A Context Weaver application includes client code, typically written in the Java
language, that issues a query for data providers, obtains data providers in response to the
query, and processes the data they provide. The Java code may be invoked from a standalone
application, an applet, a servlet, an Enterprise Java Bean, or Java Server Pages. The success
of Context Weaver will depend in large measure on the availability of many context-
information sources. Context Weaver must protect against unauthorized access to the
information.

As more sources of context information become widely deployed, it will be
increasingly important to be able to develop context-aware applications quickly, cheaply, and
reliably. By accepting a descriptive provider query that might be satisfied in one environment
by a sensor, in another environment by a web service, and in yet another environment by a programmed computation, Context Weaver makes it easier to write an application that will port to a wide variety of environments.

Context Weaver also simplifies the writing of context-aware applications by taking care of administrative details. These details include finding appropriate data providers, rebinding to new data providers when previously bound data providers fail or otherwise become inappropriate, and orchestrating asynchronous events in compliance with a nonprocedural specification.
24. Virtual Reality Technology

Partha Sardar

MCA, Indira Institute of Management, Pune

Mo: (+91) 8983275255

partha_746@yahoo.co.in

Virtual reality (VR), also known as virtuality, is a term that applies to computer-simulated environments that can simulate physical presence in places in the real world, as well as in imaginary worlds. Most current virtual reality environments are primarily visual experiences, displayed either on a computer screen or through special stereoscopic displays, but some simulations include additional sensory information, such as sound through speakers or headphones. Some advanced, haptic systems now include tactile information, generally known as force feedback, in medical and gaming applications. Furthermore, virtual reality covers remote communication environments which provide virtual presence of users with the concepts of telepresence and telexistence or a virtual artifact (VA) either through the use of standard input devices such as a keyboard and mouse, or through multimodal devices such as a wired glove, the Polhemus, and omnidirectional treadmills. The simulated environment can be similar to the real world in order to create a lifelike experience—for example, in simulations for pilot or combat training—or it can differ significantly from reality, such as in VR games. In practice, it is currently very difficult to create a high-fidelity virtual reality experience, due largely to technical limitations on processing power, image resolution, and communication bandwidth; however, the technology's proponents hope that such limitations will be overcome as processor, imaging, and data communication technologies become more powerful and cost-effective over time.

Virtual reality is often used to describe a wide variety of applications commonly associated with immersive, highly visual, 3D environments. The development of CAD software,
graphics hardware acceleration, head mounted displays, database gloves, and miniaturization have helped popularize the notion. In the book *The Metaphysics of Virtual Reality* by Michael R. Heim, seven different concepts of virtual reality are identified: simulation, interaction, artificiality, immersion, telepresence, full-body immersion, and network communication. People often identify VR with head mounted displays and data suits.

**Timeline**

Virtual reality can trace its roots to the 1860s, when 360-degree art through panoramic murals began to appear. An example of this would be Baldassare Peruzzi's piece titled, *Sala delle Prospettive*. In the 1920s, vehicle simulators were introduced. Morton Heilig wrote in the 1950s of an "Experience Theatre" that could encompass all the senses in an effective manner, thus drawing the viewer into the onscreen activity. He built a prototype of his vision dubbed the Sensorama in 1962, along with five short films to be displayed in it while engaging multiple senses (sight, sound, smell, and touch). Predating digital computing, the Sensorama was a mechanical device, which reportedly still functions today. Around this time, Douglas Englebart uses computer screens as both input and output devices. In 1966, Thomas A. Furness III introduces a visual flight stimulator for the Air Force. In 1968, Ivan Sutherland, with the help of his student Bob Sproull, created what is widely considered to be the first virtual reality and augmented reality (AR) head mounted display (HMD) system. It was primitive both in terms of user interface and realism, and the HMD to be worn by the user was so heavy it had to be suspended from the ceiling. The graphics comprising the virtual environment were simple wireframe model rooms. The formidable appearance of the device inspired its name, The Sword of Damocles. Also notable among the earlier hypermedia and virtual reality systems was the Aspen Movie Map, which was created at MIT in 1977. The program was a crude virtual simulation of Aspen, Colorado in which users could wander the streets in one of three modes: summer, winter, and polygons. The first two were based on photographs—the researchers actually photographed every possible movement through the city's street grid in both seasons—and the third was a basic 3-D model of the city. In the late 1980s, the term "virtual reality" was popularized by Jaron Lanier, one of the modern pioneers of the field. Lanier had founded the company VPL Research in 1985, which developed and built some of the seminal "goggles and gloves" systems of that decade. In 1991, Antonio
Medina, a MIT graduate and NASA scientist, designed a virtual reality system to "drive" Mars rovers from Earth in apparent real time despite the substantial delay of Mars-Earth-Mars signals. The system, termed "Computer-Simulated Teleoperation" as published by Rand, is an extension of virtual reality.

Virtual Reality Interactivity

Immersion within a virtual environment is one thing, but for a user to feel truly involved there must also be an element of interaction. Early applications using the technology common in VE systems today allowed the user to have a relatively passive experience. Users could watch a pre-recorded film while wearing a head-mounted display (HMD). They would sit in a motion chair and watch the film as the system subjected them to various stimuli, such as blowing air on them to simulate wind. While users felt a sense of immersion, interactivity was limited to shifting their point of view by looking around. Their path was pre-determined and unalterable.

Today, we can find virtual roller coasters that use the same sort of technology. DisneyQuest in Orlando, Florida features CyberSpace Mountain, where patrons can design their own roller coaster, then enter a simulator to ride their virtual creation. The system is very immersive, but apart from the initial design phase there isn't any interaction, so it's not an example of a true virtual environment.

Interactivity depends on many factors. Steuer suggests that three of these factors are speed, range and mapping. Steuer defines speed as the rate that a user's actions are incorporated into the computer model and reflected in a way the user can perceive. Range refers to how many possible outcomes could result from any particular user action. Mapping is the system's ability to produce natural results in response to a user's actions.

Navigation within a virtual environment is one kind of interactivity. If a user can direct his own movement within the environment, it can be called an interactive experience. Most virtual environments include other forms of interaction, since users can easily become bored after just a few minutes of exploration. Computer Scientist Mary Whitton points out that
3rd National Conference ETIT 2012 Proceeding

poorly designed interaction can drastically reduce the sense of immersion, while finding ways to engage users can increase it. When a virtual environment is interesting and engaging, users are more willing to suspend disbelief and become immersed.

True interactivity also includes being able to modify the environment. A good virtual environment will respond to the user's actions in a way that makes sense, even if it only makes sense within the realm of the virtual environment. If a virtual environment changes in outlandish and unpredictable ways, it risks disrupting the user's sense of telepresence.

U.S. Navy personnel using a VR parachute trainer

Virtual Reality Games

Scientists are also exploring the possibility of developing biosensors for VR use. A biosensor can detect and interpret nerve and muscle activity. With a properly calibrated biosensor, a computer can interpret how a user is moving in physical space and translate that into the corresponding motions in virtual space. Biosensors may be attached directly to the skin of a user, or may be incorporated into gloves or bodysuits. One limitation to biosensor suits is that they must be custom made for each user or the sensors will not line up properly on the user’s body.
Mary Whitton, of UNC-Chapel Hill, believes that the entertainment industry will drive the development of most VR technology going forward. The video game industry in particular has contributed advancements in graphics and sound capabilities that engineers can incorporate into virtual reality systems’ designs. One advance that Whitton finds particularly interesting is the Nintendo Wii’s wand controller. The controller is not only a commercially available device with some tracking capabilities; it’s also affordable and appeals to people who don’t normally play video games. Since tracking and input devices are two areas that traditionally have fallen behind other VR technologies, this controller could be the first of a new wave of technological advances useful to VR systems.

Some programmers envision the Internet developing into a three-dimensional virtual space, where you navigate through virtual landscapes to access information and entertainment. Web sites could take form as a three-dimensional location, allowing users to explore in a much more literal way than before. Programmers have developed several different computer languages and Web browsers to achieve this vision. Some of these include:

**Virtual Reality Modeling Language (VRML)** - the earliest three-dimensional modeling language for the Web.

**3DML** - a three-dimensional modeling language where a user can visit a **spot** (or Web site) through most Internet browsers after installing a plug-in.

**X3D** - the language that replaced VRML as the standard for creating virtual environments in the Internet.

**Collaborative Design Activity (COLLADA)** - a format used to allow file interchanges within three-dimensional programs.

Of course, many VE experts would argue that without an HMD, Internet-based systems are not true virtual environments. They lack critical elements of immersion, particularly tracking and displaying images as life-sized.
Therapeutic Uses

The primary use of VR in a therapeutic role is its application to various forms of exposure therapy, ranging from phobia treatments to newer approaches to treating PTSD. A very basic VR simulation with simple sight and sound models has been shown to be invaluable in phobia treatment, like zoophobia, and acrophobia, as a step between basic exposure therapy such as the use of simulacra and true exposure. A much more recent application is being piloted by the U.S. Navy to use a much more complex simulation to immerse veterans suffering from PTSD in simulations of urban combat settings. Much as in phobia treatment, exposure to the subject of the trauma or fear leads to desensitization, and a significant reduction in symptoms.

Other research fields in which the use of virtual reality is being explored are physical medicine, rehabilitation, physical therapy, and occupational therapy. In adult rehabilitation, a variety of virtual reality applications are currently being evaluated within upper and lower limb motor rehabilitation for individuals recovering from stroke or spinal cord injury. In pediatrics, the use of virtual reality is being evaluated to promote movement abilities, navigational abilities, or social skills in children with cerebral palsy, acquired brain injury, or other disabilities. Research evidence is emerging rapidly in the field of virtual reality for therapeutic uses. A number of recent reviews published in peer-reviewed journals have summarized the current evidence for the use of Virtual Reality within pediatric and adult rehabilitation. One such review concluded that the field is potentially promising.

Implementation

To develop a real time virtual environment, a computer graphics library can be used as embedded resource coupled with a common programming language, such as C++, Perl, Java, or Python. Some of the most popular computer graphic libraries are OpenGL, Direct3D, Java3D, and VRML, and their use are directly influenced by the system demands in terms of performance, program purpose, and hardware platform. The use of multithreading can also accelerate 3D performance and enable cluster computing with multi-user interactivity.
Virtual Reality Development

NASA, the Department of Defense and the National Science Foundation funded much of the research and development for virtual reality projects. The CIA contributed $80,000 in research money to Sutherland. Early applications mainly fell into the vehicle simulator category and were used in training exercises. Because the flight experiences in simulators were similar but not identical to real flights, the military, NASA, and airlines instituted policies that required pilots to have a significant lag time (at least one day) between a simulated flight and a real flight in case their real performance suffered.

For years, VR technology remained out of the public eye. Almost all development focused on vehicle simulations until the 1980s. Then, in 1984, a computer scientist named Michael McGreevy began to experiment with VR technology as a way to advance human-computer interface (HCI) designs. HCI still plays a big role in VR research, and moreover it lead to the media picking up on the idea of VR a few years later.

Jaron Lanier coined the term Virtual Reality in 1987. In the 1990s, the media latched on to the concept of virtual reality and ran with it. The resulting hype gave many people an unrealistic expectation of what virtual reality technologies could do. As the public realized that virtual reality was not yet as sophisticated as they had been lead to believe, interest waned. The term virtual reality began to fade away with the public’s expectations. Today, VE developers try not to exaggerate the capabilities or applications of VE systems, and they also tend to avoid the term virtual reality.

Ms. Akanksha M. Bavare, Email bavareakanksha1@gmail.com

&

Ms. Hemangi S. Prabhu hemangi.prabhu28@gmail.com

(MCA II)

JSPM’s Rajarshi Shahu College of Engineering, Pune-33.

Does your organization use wireless technologies? If yes, do you have a strategy for managing these technologies? How is wireless technology being used in your organization and how does it operate? Who has access to it? Do you know how your wireless capabilities, including 3G mobile phones and other IP based products interact with other IT systems? Are wireless applications becoming critical to the operation of your business? How would any degradation of your wireless services impact on the bottom line? These are just some of the questions that you need to have answered in an environment where these new technologies are being more widely deployed.

Organizations and users are increasingly looking for systems that provide higher productivity and cost savings. In light of this many organizations have embraced wireless technologies that not only provide convenience and flexibility of use, but also deliver cost savings. As a result in recent years the application of wireless technologies in home and business networking solutions has seen significant growth.

Due to the benefits offered by wireless technologies they are now being used to control critical infrastructures such as railway networks, energy transmission and other utilities.

Whilst there are several advantages of wireless technologies there are also risks associated with them. Wireless networks are exposed to many of the same risks as wired
networks, but they are also vulnerable to additional risks. Wireless networks transmit data through radio frequencies, and are open to intruders unless protected. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users.¹

This paper should not be taken as an exhaustive list of vulnerabilities or risks associated with these technologies. It mainly deals with the IEEE 802.11 group of standards for Wireless Local Area Networks (WLANs), since these are the most widely used in the critical infrastructure sectors.

Overview of Wireless Technologies

As mentioned above wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and mobile phones including the new generation of 3G mobile phones², to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include Infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into five groups based on their coverage range: Wireless Wide Area Networks (WWAN); Wireless Metropolitan Area Network (WMAN); Wireless Local Area Network (WLANs), Mobile Broadband Wireless

¹ Page 1 Security for Wireless Networks and Devices, Shirley Raddock, National Institute of Standards and Technology http://www.itl.nist.gov/lab/bullets/bltnmar03.htm.
² Next generation (3G) wireless networks are not IEEE 802.11 networks. Rather, they are networks dedicated to personal devices, including PDAs and cellular telephones.
Access (MBWA), and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS) and Mobitex. WMAN and MBWA represents wireless internet connection at broadband speeds within city or suburbs, it includes 802.16 and emerging standards such as 802.20. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR.

Wireless Technologies and Standards

There are a number of standards used in wireless technologies. Some of the key ones include:

- The IEEE 802.11 standards provide specifications for high-speed networks that support most of today’s applications. The IEEE 802.11 specifications are wireless standards that specify an "over-the-air" interface between a wireless client and a base station or access point, as well as among wireless clients. These 802.11 standards can be compared to the IEEE 802.3 standard for Ethernet for wired LANs. The IEEE 802.11 specifications address both the Physical (PHY) and Media Access Control (MAC) layers and are tailored to resolve compatibility issues between manufacturers of Wireless LAN equipment.

- IEEE802.15 provides standards for low complexity and low-power consumption connectivity.

- IEEE 802.16 standard, the “Air Interface for Fixed Broadband Wireless Access Systems” is also known as the IEEE WirelessMAN air interface. This technology is designed to provide wireless last-mile broadband access in the Metropolitan Area Network (MAN), delivering performance comparable to traditional cable, DSL, or T1 offerings.

- Bluetooth (Wireless Personal Area Network) is an alternative wireless network technology that has followed a different development path than the 802.11 family. Bluetooth supports a very short range (approximately 10 meters) and relatively low bandwidth (1 Mbps). In practice, Bluetooth networks PDAs or cell phones with PCs
but does not offer much value for general-purpose WLAN networking. The Bluetooth standard was developed by a computer and communications industry consortium, specifying how mobile phones, computers, and PDAs interconnect with each other, with home and business phones, and with computers using short-range wireless connections.

- IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

This list of standards is in no way comprehensive. This paper does not go into the detail of each of the standards within the IEEE 802.11 family but in general terms stipulates the concerns/risks/vulnerabilities within this group of standards and some ways to manage them. There are several standards within IEEE 802.11 ranging from IEEE 802.11a to IEEE 802.11R. There are also emerging standards including IEEE 802.11j, 802.11k, 802.11m and 802.20.

It is also important to note that this paper does not focus on other WLAN standards besides IEEE 802.11 such as the European Telecommunications Standards Institute’s (ETSI) HiperLan and the HomeRF standard for the home user and small businesses.

**Security Features of IEEE 802.11**

The IEEE 802.11 WLAN – or WiFi specification has identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection\(^3\). However, there are a number of problems with the WEP protocol and its vulnerabilities significantly limit its ability to safeguard data. Commonly available tools such as AirSnort, WEPCrack and dweputils have the ability to

---

\(^3\) Page3-13 NIST, Special Publication 800-48, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, Tom Karygiannis and Les Owens
crack WEP keys by analysing traffic from totally passive data captures\(^4\). An improvement on WEP is the Wi-Fi Protected Access (WPA) which was introduced in 2003. WPA avoids most of WEP’s vulnerabilities and WPA-PSK\(^5\) is the current minimum standard and WPA2 (Advanced Encryption Standard (AES) with RADIUS\(^6\) authentication), is industry best practice.

The three basic security services defined by IEEE for the WLAN environment are:

- **Authentication**—provides access control to the network by denying access to client stations that cannot authenticate properly. This service addresses the question, “Are only authorized persons allowed to gain access to my network?”
- **Confidentiality**—“Are only authorized persons allowed to view my data?”
- **Integrity**—Ensure that messages have not been modified in transit between the wireless clients and the access point in an active attack. This service addresses the question, “Is the data coming into or exiting the network trustworthy—has it been tampered with?”

### Threats

There have been many reports describing attacks on 802.11 wireless networks that expose organizations to security risks\(^7\). These attacks, either active or passive, are essentially on confidentiality, integrity and network availability.

According to the US National Institute of Standards and Technology (NIST) there are six different types of attacks under passive and active categories against IEEE 802.11\(^8\) networks:

---


\(^5\) PSK is Pre-shared key mode (also known as personal mode) is designed for home and small office networks that cannot afford the cost of more complex systems such as an 802.1X authentication server.

\(^6\) RADIUS (Remote Authentication Dial In User Service) is an AAA (authentication, authorisation and accounting) protocol for applications such as network access or IP mobility.

\(^7\) http://csrc.nist.gov/
Passive Attack—An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e. eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis) and are described below:

- **Eavesdropping**—The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.
- **Traffic analysis**—The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

Active Attack—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible for these attacks to be detected but they may not always be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below:

- **Masquerading**—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
- **Replay**—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
- **Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service**—The attacker prevents or prohibits the normal use or management of communications facilities.

---

8 Page 3-20 NIST, Special Publication 800-48, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, Tom Karygiannis and Les Owens
Security Countermeasures for Wireless Networks

The National Institute of Standards and Technology (NIST) have suggested countermeasures at the management, technical and operational level for securing wireless networks. These include:

- **Management Countermeasures**

  Management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy and compliance therewith, is the foundation on which other countermeasures—operational and technical—are rationalized and implemented. A WLAN security policy should be able to do the following:

  - Centralize the management of Access Points so that each Access Point must authenticate to the controller before it is allowed onto the network
  - Identify who may use WLAN technology in an agency
  - Identify whether Internet access is required
  - Describe who can install access points and other wireless equipment
  - Provide limitations on the location of and physical security for access points
  - Describe the type of information that may be sent over wireless links
  - Describe conditions under which wireless devices are allowed
  - Define standard security settings for access points
  - Describe limitations on how the wireless device may be used, such as location
  - Describe the hardware and software configuration of all wireless devices
  - Provide guidelines on reporting losses of wireless devices and security incidents
  - Provide guidelines for the protection of wireless clients to minimize/reduce theft
  - Provide guidelines on the use of encryption and key management
  - Define the frequency and scope of security assessments to include access point discovery, and
  - Use channel hopping Access Points to detect and triangulate rogue Access Points.

---

Organizations should institute and regularly update security manuals which include established procedures for preventing and handling cyber attacks as well as physical security issues. It may contain security policies, incident response team, etc. Organizations should also ensure that all critical personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the Security risks that WLANs and devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack. Finally, the most important countermeasure is trained and aware users.

**Operational Countermeasures**

Physical security is a fundamental step for ensuring that only authorized users have access to wireless computer equipment. Physical security combines measures such as access controls, personnel identification, and external boundary protection. As with facilities housing wired networks, facilities supporting wireless networks need physical access controls. For example, photo identification, card badge readers, or biometric devices can be used to minimize the risk of improper penetration of facilities. External boundary protection can include locking doors and installing video cameras for surveillance around the perimeter of a site to discourage unauthorized access to wireless networking components such as wireless access points (APs). While such steps are important, an attacker or intruder can be located outside your physical perimeter and be on your network and therefore organizations should also use wireless security assessment tools (e.g. vulnerability assessment) and regularly conduct scheduled security audits.

**Technical Countermeasures**

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment. Software countermeasures include proper Access Point (AP) configurations (i.e. the operational and security settings on an AP), software patches and upgrades, authentication, intrusion detection systems (IDS), personal firewalls for wireless devices and encryption. Hardware solutions include smart cards, virtual private networks (VPNs), public key infrastructure (PKI), a separate switching infrastructure for the wireless...
network (separating it from a wired network) and biometrics. It should be noted that hardware solutions, which generally have software components, are listed simply as hardware solutions. Additionally, due to the mobile nature of wireless networks, hard disk encryption is also highly recommended or mandatory.

New, Integrated Technologies such as Blackberry Devices and 3G Mobile Phones

While 3G mobile phones have introduced efficiencies, they have also resulted in a convergence of the inherent security risks associated with each integrated technology. Integrated technologies that may be contained include:

- planning tools, such as Calendar, Schedule, Calculator, To-Do list;
- wireless communications - WiFi, WAP, Bluetooth, Infra Red, and/or SMS;
- web applications such as Web browsing, e-mailing, faxing and chat facilities; and
- Multimedia applications including audio visual recording.

CIOs must consider the security liabilities inherent in allowing these devices into their IT environment and must amend their organization’s IT security policy to take these risks into account. The risks can be categorized into:

- Loss of information: wireless communications produce signals that can be intercepted; and
- Loss of control: Bluetooth enabled mobile phones are susceptible to covert remote control. This gives the 'controller' access to the features and information contained on the phone.

Other 3G technologies, such as Blackberry devices have similar, but more complex, security liabilities. Blackberry devices are a derivative of 3G mobile phones.
Conclusion

It is essential that organizations have suitable protective measures for their IT systems particularly where wireless technologies are used. Management policies and procedures should ensure that new technologies such as 3G telephones cannot be introduced without the knowledge of IT management. The wireless group of standards IEEE 802.11, although not foolproof, do provide basic security as do the security countermeasures promoted by NIST. Implementing these will mitigate the risks associated with the use of wireless technologies and save your organization from potentially costly attacks.

References:

Further information on wireless technologies and their security can be found at:


This is the website for the IEEE standards. It provides information on the wireless IEEE standards and helps to answer questions on the IEEE wireless standards initiative. It also provides links to the various working groups on the IEEE standards.

http://csrc.nist.gov/

This is the website for NIST’s Computer Security Research Centre. It provides a link to the NIST document (referenced in this paper) “Wireless Network Security 802.11, Bluetooth and Handheld Devices” by Tom Karygiannis and Les Owens. This paper will help you to understand the security issues pertaining to wireless technologies such as IEEE 802.1 and Bluetooth and provides some strategies that you can put in place to protect your wireless applications.


This provides a link to the article “802.1X provides user authentication” by Paul Goransson, Network World Fusion, 24 March 2002. This article will help you to understand the capabilities of the 802.1X standard

http://insight.zdnet.co.uk/communications/wireless/0,39020430,2132483,00.htm
This provides a link to the article “A to Z of Wireless Standards” by Rupert Goodwins, ZDNet UK, 26 March 2003. It provides a guide to the IEEE 802.11 family of standards.

http://www.firstmonday.dk/issues/issue8_8/critical/#c2

This provides a link to the paper “A Social Ecology of Wireless Technology” by Critical Friends of Technology. This paper looks at both costs and risks of wireless technologies, employing a holistic framework for evaluating technological impacts.

http://nc3ta.nc3a.nato.int/vol2-sup2/ch02s02.html

This provides a link to the paper “2.2. Wireless Networking - 802.11 Standards” by The NATO C3 Technical Architecture. This paper provides a guide to the IEEE 802.11 family of standards.

http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm

This provides a link to the NIST Paper “Security for Wireless Networks And Devices” by Shirley Radack. The paper provides a snapshot of security issues associated with wireless technologies.
26. Network Security

Mr. Abhijit B. Kulkarni & Ms. Kranti B. Yadav

JSPM’s Rajarshi Shahu College of Engineering, Pune

abhi_kulkarni44@rediffmail.com

kranti.b.y@gmail.com

This is not world shattering problem, some times outlined of the pages of press, nor does other suggest it the nonexistent ‘urban myth’. But, the threat is real: the problem is “network security”. Like other problems facing IT professionals, this threat should also be assessed realistically.

It is important to identify those areas, which are causing insecurity to the computer, and which are the likely sources of the threat. The appropriate security tools should be selected, designed to provide a layered defense of the system. It is important that to look at the way data is handled within the organization; and to take the routine precaution to minimize the risk.

Any computer that is connected to the network can never be completely secured. The threat from viruses is always ready to attack.

These days everybody is more security conscious as they browse and conduct business on the Internet. As with any type of security, be it personnel or domestic, the likelihood of an internet security breach depends on one’s degree of preparedness and use of proper prevention tools. This report mainly focuses on creating an effective “internet security policy”.

The report provides certain practices that can be implemented by any organization, if it wants to protect the confidentiality, availability and integrity of its system data when it contracts with outside parties to install, configure, manage or update any of its Information technology.

Finally the report highlights some current issues as such as Network security.

What is a Network?
A “network” has been defined as “any set of interlinking lines resembling a net, a network of roads or interconnected system, a network of alliances.” A computer network is simply a system of interconnected computers. They may be connected in a number of ways.

Figure 3: A Simple Local Area Network

Network security

Providing network security means controlling system to prevent any accidental or intentional data loss. There are two types of the security

1. Physical security
2. Logical security

Where physical security includes all the hardware units of a network against unauthorized access. The logical security deals with protecting your data from unauthorized access.

Problems:

- Data destruction or modification
- Interface and interruption of network traffic.
- Theft of viewing and private information
- Execution of authorized transaction
- Installation or transfer of malicious application or virus

These threats in a network fall into general categories as follow:

Destruction:
Data and hardware can be destroyed accidentally or intentionally.

**Corruption:**

Data that has been corrupted is often wormless.

**Interruption:**

If the network goes down, you cannot use resource’s you need and this is downloading. Thus, downtime means unavailability of data, which indirectly results in loss of money.

**Disclosure:**

Any confidential data can be encrypted.

This whole task of network security is divided into two basic types:

1. Internal network security
2. External network security

1. **Internal Network Security:**

It is nothing but preventing users on the same LAN from accessing files and other resources. They are not authorized for that data. General consideration and methods of managing internal security:

- Create acceptable use policies for all users of the network
- Required complex passwords for their respective account.
- Design a hierarchy of group permission
- Carefully implement your files and folder share.
- Understand the security methods of your network operating system.

Some topics related to internal security:

- Account security
- Files and directory permission

**Account Security:**
A network operating system uses ‘logon’ process so that no access to information is given without accountability. Window NT use concept of user account to security and accountability for information contain on the server. In this step it requires the authenticable user and password. Authenticable user can access network recourses.

Basic security model used by windows are:

- User level security
- Share level security

User level security model is based on individual account create for each user, where administrator will be set different permission to access recourses by this account. In share level each user can set his password and can protect his data on his computer only.

To manage account security following point should be followed:

- Remove the guest account or carefully limit it
- Remove default name.
- Remove access to important resources
- To maintain password security
- Restrict login time
- Limit access to network resources
- Use software that employee encryption
- Set account lock out policies

Let’s see how to maintain password security and set account lock out policies.

1. Maintain Password Security:

In fact user account property specify users password, password change and specify the whether the user has permission to change his/her password. Following are the group policies that maintain password security.

- Get user to change their network password regularly.
- Set reused policies or enforce password history.
- Enforce password complexity
- Control password encryption
Minimum password length

The password must meet complexity requirement. The password that supply for their account must meet following criteria:

- Password must contain at least size character account
- Password cannot contain any part of user name
- Password must contain three of following four characteristics: Uppercase, Lowercase letters, numeric & symbols.

2. To set account lock out policies:

One can make sufficient numbers of guesses and find out a password for any specific account. This is known as “Burst Force” method. Most of the operating system user an account lockout policies feature that prevents anyone from repeatedly trying to guesses a password to a given account. There are three policies:

- Account lock out duration
- Account lock out threshold
- Reset account lock out counter.

Files and directory permission

When working on a network, user can decide which files and directories should be shared. If files and directories contain important data then it should not be shared, if shared then users should not be given permission to change the content of files.

External Security:

There are potential hazards outside private network, these hazards come in network through Internet connection. The other users outside private network may attack systems and access private data illegally.
3rd National Conference ETIT 2012 Proceeding

To avoid this unauthorized access to private data of network by external user Network Security System is provided which is nothing but 'External security'. In short external security is a process of securing the private network from external threats.

Different threats are given as below

- Front door threats
- Back door threats

**Front door threats:**

These threats arise, when user from outside your network finds users password and log on to your network. It prints to issue of "password cracking". Here external attacker try to gain system access through another user's account i.e. it is possible because selecting of weak password. Different solutions for the front door threat are as follows

- Separate network recourses access from outside the wan
- Control users accessing LAN from outside the LAN
- Setup the separate remote account for remote user
- Maintain password security
- Change password regularity

**Back door threat:**

Any software or hardware bugs in network security. The common method for gaining access to a system by external users includes:

- Password weakness
- Social engineering

**VANISH : Enhancing the privacy**

Vanish is new emerging Technology, developed in a way to make electronic messages "self destruct" after a certain period of time. The new software called 'vanish' which requires encrypting messages will be needed more and more as personal and business information is stored not on PCs but on centralized machines or servers.
Architecture

The approach utilized here in this software relies on "shattering" an encryption key that is held by neither party in an email exchange but is widely scattered across a peer to peer file sharing system. Vanish uses a key based encryption system in a different way making it possible for a decrypted message to be automatically re-encrypted at a specified point in the future without fear that a third party will be able to gain access to the key needed to read the message.

The Pisces of the key, small numbers tend to 'erode' over time as they gradually fall out of use. To make keys erode, or timeout 'Vanish' takes advantage of the structure of peer to peer file system. Such networks are based on millions of personal computers whose internet addresses change as they come and go from the network. This would make it exceedingly difficult for an eavesdropper or spy to reassemble the pieces of the key is never held in single location.

CONCLUSION

Everyone has a different idea of what "security" is, and what levels of risk are acceptable in networking. The key for building a secure network is to define what security means to any organization. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system.

Today cryptography can be used easily & efficiently to provide secure authentication which has been widely adopted by many organization
We also saw how these concepts are used in the real world applications. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

Traditional encryption like PGP can protect the privacy of messages now against attackers who do not know the decryption key. Vanish can protect the privacy of messages into the future, even if an attacker can learn all of the user's private cryptographic keys and passphrases

**REFERENCES**

1. COMPUTER NETWORKS -TANNENBAUM

2. NETWORKING: A BEGINNER GUIDE -BRUCE A. HALLBURGE.
27. Network Security

Nikhil Sonkamble

Indira Institute Of Management (MCA) Pune

Before going to actual topic, here are some funny & interesting but facts about network and security.

**Some interesting facts about network security:**

- Nobody believes anything bad can happen to them, until it does
- Security only works if the secure way also happens to be the easy way
- If you don't keep up with security fixes, your network won't be yours for long
- It doesn't do much good to install security fixes on a computer that was never secured to begin with
- Eternal vigilance is the price of security
- There really is someone out there trying to guess your passwords
- The most secure network is a well-administered one
- The difficulty of defending a network is directly proportional to its complexity
- Security isn't about risk avoidance; it's about risk management
- Technology is not a panacea

**Computer Network:**

A *computer network*, also referred to as just a *network*, consists of two or more *computers*, and typically other devices as well (such as printers, external *hard drives*, modems and *routers*), that are linked together so that they can communicate with each other and thereby exchange *commands* and share *data*, hardware and other resources.
While communicating the participated devices may transfer very important information across network. Such information play very crucial role in the organization and loss of such information may be hazardous. There are following types of attacks.

**Types of Attacks**

Networks are subject to attacks from malicious sources. Attacks can be from two categories "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

Types of attacks include:

- **Passive**
  - Network
    - **Wiretapping**: Using an electronic device to listen in on telephone lines, which is illegal unless allowed by court order based upon a showing by law enforcement of "probable cause" to believe the communications are part of criminal activities.
    - **Port scanner**: A port scan or port scanner attempts to connect to all 65536 ports on a server to see whether there are services listening (that is, waiting for connections) on those ports. The purpose of a port scan is to audit network computers for likely vulnerabilities or exploits. Typically, scanners have built-in databases of known port vulnerabilities.

- **Active**
  - **Denial-of-service attack**: Denial of Service can result when a system, such as a Web server, has been flooded with illegitimate requests, thus making it impossible to respond to real request or tasks.
  - **Spoofing**: If the attacker obtains control over the software running on a network device, they can then easily modify the device's protocols to place an arbitrary IP address into the data packet's source address field. This is known as IP spoofing, which makes any payload appear to come from any source.
  - **Man in the middle**: Hijacking occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently.
Network security concepts:

Following are some of the concepts by using which we can secure our network as well as communication being carried out between them.

- **Authentication**: The user of the system or network is provided with the username and password to use resources of the network.

- **Firewall**: A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.

- **Antivirus software**: A protective software designed to defend your computer against malicious software. Malicious software, or "malware" includes: viruses, Trojans, keyloggers, hijackers, dialers, and other code that vandalizes or steals your computer contents.

- **Network analyzer**: A specialized hardware device or software in a desktop or laptop computer that captures packets transmitted in a network for routine inspection and problem detection.

- **Physical security**: Measures necessary to protect a facility against the effects of unauthorized access, theft, fire, malicious destructions, loss, or other intentional crime or damage.

The above mentioned are general techniques and used almost everywhere. Following are some advanced techniques related to how your system should be configured to be safe in the network communication.

**Security by design**

The technologies of computer security are based on logic. As security is not necessarily the primary goal of most computer applications, designing a program with security in mind often imposes restrictions on that program’s behavior.
There are 4 approaches to security in computing, sometimes a combination of approaches is valid:

1. Trust all the software to abide by a security policy but the software is not trustworthy (this is computer insecurity).
2. Trust all the software to abide by a security policy and the software is validated as trustworthy (by tedious branch and path analysis for example).
3. Trust no software but enforce a security policy with mechanisms that are not trustworthy (again this is computer insecurity).
4. Trust no software but enforce a security policy with trustworthy hardware mechanisms.

**Security architecture**

Security Architecture can be defined as the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes, among them confidentiality, integrity, availability, accountability and assurance.

**Hardware mechanisms that protect computers and data**

Hardware based or assisted computer security offers an alternative to software-only computer security. Devices such as dongles may be considered more secure due to the physical access required in order to be compromised.

**Secure operating systems**

One use of the term computer security refers to technology to implement a secure operating system. Much of this technology is based on science developed in the 1980s and used to produce what may be some of the most impenetrable operating systems ever. Though still valid, the technology is in limited use today, primarily because it imposes some changes to system management and also because it is not widely understood. Such ultra-strong secure operating systems are based on operating system kernel technology that can guarantee that certain security policies are absolutely enforced in an operating environment.

**Secure coding**
In commercial environments, the majority of software subversion vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. It is to be immediately noted that all of the foregoing are specific instances of a general class of attacks, where situations in which putative "data" actually contains implicit or explicit, executable instructions are cleverly exploited.

Unfortunately, there is no theoretical model of "secure coding" practices, nor is one practically achievable, insofar as the code (ideally, read-only) and data (generally read/write) generally tends to have some form of defect.

**Laws for Network security**

- CFAA - Computer Fraud and Abuse Act
- DMCA - The Digital Millennium Copyright Act
- State Laws - Filling the Gaps Left by CFAA and DMCA
28. Using Wireless Technology Securely

Sharad S. Salve Email: sharad.gcontact@gmail.com

Indira Institute of Management (MCA) Pune

Introduction

In recent years, wireless networking has become more available, affordable, and easy to use. Home users are adopting wireless technology in great numbers. On-the-go laptop users often find free wireless connections in places like coffee shops and airports.

If you’re using wireless technology, or considering making the move to wireless, you should know about the security threats you may encounter.

Home Wireless Threats

By now, you should be aware of the need to secure traditional, wired internet connections. If you’re planning to move to a wireless connection in your home, take a moment to consider what you’re doing: You’re connecting a device to your DSL or cable modem that broadcasts your internet connection through the air over a radio signal to your computers. If traditional wired connections are prey to security problems, think of the security problems that arise when you open your internet connection to the airwaves. The following sections describe some of the threats to home wireless networks.

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer within range of your wireless access point can hop a free ride on the internet over your wireless connection. The typical indoor broadcast range of an access point is 150 – 300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could potentially open your internet connection to a surprising number of users. Doing so invites a number of problems:

Service violations: You may exceed the number of connections permitted by your internet service provider.
Bandwidth shortages: Users piggybacking on your internet connection might use up your bandwidth and slow your connection.

Abuse by malicious users: Users piggybacking on your internet connection might engage in illegal activity that will be traced to you.

Monitoring of your activity: Malicious users may be able to monitor your internet activity and steal passwords and other sensitive information.

Direct attack on your computer: Malicious users may be able to access files on your computer, install

Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections possible outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is nicknamed “wardriving.” Wardrivers often note the location of unsecured wireless networks and publish this information on web sites. Malicious individuals wardrive to find a connection they can use to perpetrate illegal online activity using your connection to mask their identities. They may also directly attack your computer, as noted in the “Piggybacking” section above.

Unauthorized Computer Access

An unsecured wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Protecting Home Wireless

While the security problems associated with wireless networking are serious, there are steps you can take to protect yourself. The following sections describe these steps.
Make Your Wireless Network Invisible

Wireless access points can announce their presence to wireless-enabled computers. This is referred to as “identifier broadcasting.” In certain situations, identifier broadcasting is desirable. For instance, an internet cafe would want its customers to easily find its access point, so it would leave identifier broadcasting enabled.

However, you’re the only one who needs to know you have a wireless network in your home. To make your network invisible to others, see your access point’s user manual for instructions on disabling identifier broadcasting.

While this kind of “security through obscurity” is never foolproof, it’s a starting point for securing your wireless network.

Rename Your Wireless Network

Many wireless access point devices come with a default name. This name is referred to as the “service set identifier” (SSIS) or “extended service set identifier” (ESSID). The default names used by various manufacturers are widely known and can be used to gain unauthorized access to your network. When you rename your network, you should choose a name that won’t be easily guessed by others.

Encrypt Your Network Traffic

Your wireless access point device should allow you to encrypt traffic passing between the device and your computers. By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code.

Change Your Administrator Password

Your wireless access point device likely shipped with a default password. Default passwords for various manufacturers are widely known and can be used to gain unauthorized access to your network. Be sure to change your administrator password to one that is long, contains non-alphanumeric characters (such as #, $, and &), and does not contain personal information (such as your birth date). If your wireless access point does not have a default password, be sure to create one and use it to protect your device.

Use File Sharing with Caution
If you don’t need to share directories and files over your network, you should disable file sharing on your computers. You may want to consider creating a dedicated directory for file sharing, and move or copy files to that directory for sharing. In addition, you should password protect anything you share, and use a password that is long, contains non-alphanumeric characters (such as #, $, and &), and does not contain personal information (such as your birth date). Never open an entire hard drive for file sharing.

Keep Your Access Point Software Patched and Up to Date

From time to time, the manufacturer of your wireless access point will release updates to the device software or patches to repair bugs. Be sure to check the manufacturer’s web site regularly for any updates or patches for your device’s software.

Check Your Internet Provider’s Wireless Security Options

Your internet service provider may provide information about securing your home wireless network. Check the customer support area of your provider’s web site or contact your provider’s customer support group.

Public Wireless Threats

A wireless-enabled laptop can make you more productive outside your office or home, but it can also expose you to a number of security threats. The following sections describe some of the security threats you face when using a public access point.

Evil Twin Attacks

In an evil twin attack, the attacker gathers information about a public access point, then sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the stronger, bogus signal. Because the victim is connecting to the internet through the attacker’s system, it’s easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, addresses, and other personal information.

Wireless Sniffing
Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted “in the clear,” malicious users can use “sniffing” tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.

Peer-to-Peer Connections

Many laptop computers, particularly those equipped with 802.11-type WiFi wireless networking cards, can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections, a situation that creates security concerns you should be aware of. An attacker with a network card configured for ad hoc mode and using the same settings as your computer may gain unauthorized access to your sensitive files. You should note that many PCs ship from the manufacturer with wireless cards set to ad hoc mode by default.

Unauthorized Computer Access

As is the case with unsecured home wireless networks, an unsecured public wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Shoulder Surfing

In public wireless areas, the bad guys don’t even need a computer to steal your sensitive information. The fact that you may be conducting personal business in a public space is opportunity enough for them. If close enough, they can simply glance over your shoulder as you type. Or, they could be peering through binoculars from an apartment window across the street. By simply watching you, they can steal all kinds of sensitive, personal information.

Safe Wireless Networking in Public Spaces

Accessing the internet via a public wireless access point involves serious security threats you should guard against. These threats are compounded by your inability to control the security setup of the wireless network. What’s more, you’re often in range of numerous
wireless-enabled computers operated by people you don’t know. The following sections describe steps you can take to protect yourself.

**Watch What You Do Online**

Because you’re likely to have an unsecured, unencrypted network connection when you use a public wireless access point, be careful about what you do online—there’s always the chance that another user on the network could be monitoring your activity. If you can’t connect securely using a VPN then consider avoiding

- online banking
- online shopping
- sending email
- typing passwords or credit card numbers

**Connect Using a VPN**

Many companies and organizations have a virtual private network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

**Disable File Sharing**

File sharing in public wireless spaces is even more dangerous than it is on your home wireless network. This is because you and your wireless-enabled laptop are likely to be even closer to other wireless computers operated by people you don’t know. Also, many public wireless networks feature peer-to-peer networking in which other computers will attempt to connect directly to yours. To leave file shares open in this kind of environment is to invite risk. To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point. Consult the help file for your operating system to learn how to disable file sharing.

**Summary**

The following sections provide a quick summary of the steps you should take to secure your home wireless network and to use wireless technology safely in public spaces.
Home Wireless Security

When you use a wireless router or access point to create a home network, you trade wired connectivity for connectivity delivered via a radio signal. Unless you secure this signal, strangers can piggyback on your internet connection or, worse, monitor your online activity or access files on your hard drive. By taking the following actions, you can help secure your wireless home network against these threats.

- Change the default system ID of your wireless access point or router.
- Change the default password for your system.
- Turn off identifier broadcasting.
- Encrypt wireless communications.
- Use your router’s built-in firewall to restrict access to your network.
- Keep your wireless system patched and up to date.

Public Wireless Security

Accessing a wireless connection from a coffee shop or airport terminal may be convenient and even fun, but you should note that public access points (frequently called hot spots) are often insecure. The following are some steps you should consider taking before connecting to a public access point:

- Use a virtual private network (VPN) if possible.
- Avoid using passwords and providing personal information to web sites.
- Encrypt your files.
- Be aware of your surroundings.
29. Ecommerce as a Recent Trend in IT

Author: Mr. Sagar Rajendra Kulkarni
M.E (Computer Engineering) students from Pillai Institute of Technology,
Media studies & Research, New Panvel

Introduction to e-commerce

Every day is a new day in the commerce and the term marketplace is evolved from commerce. The last generation of commerce over the internet has given the birth to the concept of e-commerce. Electronic commerce or e-commerce is nothing but selling and buying of products, services and information using Internet or through any other computer network.

Dimension of e-commerce

In the past people were exchanging the goods and services directly for other goods and services without the use of money. This type of trade is known as the Barter Process. After that people use to go to market and purchasing selling by using money then instead going to market people use to take the advantage of teleshopping where the products are delivered at home by using the virtual mall with payment using credit card and the last generation of commerce is known as e-commerce.
E-commerce business Models

There are main four models of e-commerce as:

- Business-to-Business (B2B) model
- Business-to-Consumer (B2C) model
- Consumer-to-Consumer (C2C) model
- Consumer-to-Business (C2B) model

1. Business-to-Business (B2B) model:

In business-to-business model one Business organization performs commercial transaction with other. It involves electronic transaction for ordering, purchasing, as well as other administrative tasks between two businesses. It also includes trading goods, such as business subscriptions, professional services, manufacturing, and wholesale dealings. The diagram of B to B model is as follows:

Consider an example of B 2 B model as:

ABC company sells automobile parts and XYZ company assembles these parts and then sells automobile to the customer. XYZ Company comes across the web site of the ABC company and finds it’s suitable. XYZ therefore, request for more information about ABC
3rd National Conference ETIT 2012 Proceeding
Company and finally decides to purchase automobile part from ABC. To do this XYZ places an order on the website of ABC. After receiving the order details, it validates the information and the same. After order confirmation the payment procedure are settled. ABC sends an acknowledgement of payment to XYZ & delivers goods as per the shipment details decides between them.

2. Business-to-Consumer (B2C) model:

The B2C model involves transaction between business organization and consumers. It applies to any business organization that sells its products or services to consumer over the Internet. These sites display the product information in an online catalog and store it in the database. It also includes services such as online banking, travel services, and health information. This model makes more emphasize on advertising product and security threats because individual consumers provide their credit card and personal information onsite of a business organization. With the help of this model business’s can understands today's trends and make the changes into the product. Because of this model cost maintaining is done very easily.

![B2C Model Diagram]

Consider an example of B-to-C model as:
LMN department store, displays and sales a range of product on their web site, www.lmn.com. The detailed information of their entire product is contained by in the huge catalogs. Now a customer wants to buy a gift; therefore he logs on to the site of LMN store.
and select gift from catalog. He also gets the detailed information about gift from catalog. Finally, he decides to buy a gift, for that, he places an order on their web site (www.lmn.com). He needs to specify his personal and credit card details on database. The information is then validated by the LMN department stores and stored in their database. On verification of the information the order is processed.

3. Consumer-to-Consumer (C2C) model: -

The C2C model involves transaction between consumers; here a consumer auction sells directly to another consumer. (e.g.www.eBay.com)

Auction web sites that provide a consumer to advertise and sell their products online to another consumer. However, it is essential that both the seller and the buyer must register with the auction site. While the seller needs to pay a fixed fee to the online auction house to sell their products, the buyer can bid without paying any fee. The site brings the buyer and seller together to conduct deals. The diagram of this model is as shown below:

![C2C Model Diagram](image)

4. Consumer-to-Business (C2B) model:-

The C2B model involves a transaction that is conducted between a consumer and a business organization. The consumer decides the price of a particular product rather than the supplier. This category includes individuals who sell products and services to organizations.
Consider an example of this model:

www.monster.com is a web site on which a consumer can post his Bio-data for the services he can offer. Any business that is interested in deploying the services of the consumer can conduct him and then employ him, if suitable. Mr. A needs to buy an airline ticket for his journey; he needs travel immediately. Therefore he searches web site for ticket. The web sites offer bidding facility to people who want to buy tickets immediately. On the web site, Mr. A quotes the highest price and gets ticket.

**Scope of e-commerce**

Scope of e-commerce is as wide as an ocean. As information sharing is the major part of the commerce industries, networking has given boost to e-commerce. This change in view-point has opened door for new opportunities.

The adoption and usage of E-Commerce in the country is a function of the overall environment for Internet usage in a country. Some of the key variables that need to be
understood are the proportion of computer literates, internet penetration, frequency of access to the internet, purpose of internet access etc. A correct mapping of these would help in understanding the overall framework of E-Commerce in the country.

**E-commerce transactions in India**

In India the e-commerce industry was worth of s.7080 crores at end of 2006-07.According to the total B2B transactions in India in the year 2008 are likely to be US$100 billion. India’s largest B2B portal Tradeindia, maintained by Infocom Network Ltd, also stated that e-commerce transactions in India show a growth rate of 30 percent to 40 percent and will soon reach the $100 billion mark. In near future, e-commerce is going to play a major role in multimedia, entertainment and fashion industry. The foreign branded companies are eager to take full advantage of the growing Indian market and are trying to create market for their products over the net. Gucci Co. an Italian iconic fashion and leather goods label is eager to make its hold in India with Business to business transactions.Some of the key B2B exchanges in India are tradeindia.com, matexnet.com, Alibaba.com, AuctionIndia.com, Indiamart.com, TeaAuction.com, MetalJunction.com, etc

Railway and Airlines have played a vital role in e-commerce transactions in India. Travel portals are exploding in India. Recently MakeMyTrip.com has shown Rs 1000 crores of turnover. Travel alone constituted 50% of Rs 4800 crore online market in 2007-08.

The following table gives the market size idea in various segments like Online travels (like tours, railways, hotel etc), e-tailing (like online retailer, online auction), Classifieds (like online jobs, online matrimony, etc) Paid content subscription (like research, articles, exclusive videos etc) and Digital Downloads (download from Internet)

<table>
<thead>
<tr>
<th>MARKET SIZE FOR THE YEAR</th>
<th>2006-07 (Figures in Rs. Crores)</th>
<th>2007-08 (Figures in Rs Crores.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online travel industry</td>
<td>5,500</td>
<td>7,000</td>
</tr>
<tr>
<td>Online non-travel industry</td>
<td>1,580</td>
<td>2,210</td>
</tr>
<tr>
<td>- eTailing</td>
<td>850</td>
<td>1,105</td>
</tr>
<tr>
<td>- Online classifieds</td>
<td>540</td>
<td>820</td>
</tr>
</tbody>
</table>
Cheaper e-commerce

Cheap e-commerce is the e-commerce done on budget. It is basically gives the idea about how to design the e-commerce sites without using the lot of budget. This idea is very useful for the start up of business. It makes getting into the global marketplace very easily and is affordable. It starts with the website development and it is the storefront of your business while designing of website the look and user friendliness should be there and it should allow the user to shop fast and easily, get the detail information of all, the site should be clean and simple. This is the beauty of e-commerce it allows to start up a business very easily and without spending a lot of money and you can grow up your business with little startup capital.

Future e-commerce

The Internet is changing the way we do business — the way we market, sell, service, distribute, communicate, and work. Businesses are already beginning to communicate with customers, distributors, suppliers, shareholders, and employees in a way that is truly one-to-one and real-time. “Personalized” web sites are delivering tailored messages to an infinite number of target markets. These sites can change based on the user’s buying and surfing habits, past usage of the site, demographics, relationship to the company, and a multitude of other attributes which could be collected from the users online or culled from corporate legacy databases. The Internet has also become the most economical distribution system of information available. Companies can ship “bits” - weightless electrons - around the world at the speed of light, for a fraction of what it costs to ship heavy “atoms” at the speed of freight. Online sales have proved over the years the substantial growth that their area of the market has occupied, yet marketers find it almost impossible to track consumer trends. People are
buying online Consumers buy certain items online because they have a large variety of items to choose from at a reasonable price, they don’t have the hassle of driving and waiting in line, and the convenience of time is probably the most important of all. Although the high likeliness of potential growth consumers still buy things at grocery stores, hair salons, and places where you basically have to be there for this type of purchase to take place. Making consumers not exactly reliant one hundred percent on e-commerce but still convenient and inexpensive enough to grow and survive.

For the future of e-commerce to grow computer literacy must also continuously grow. Only 52% of people deny pop-up ads which can be a problem when consumers’ computers are jammed and have less and less time to order online. Especially if consumers need to go in and have their computers looked at the total time that these potential customers are available to purchase products online shrinks. Consumer polls have shown that people really don’t like web-pages that have too much junk and clutter on them that 35% of the time frustrates these customers and leads to business elsewhere.

As the Internet becomes a safer place to transact, the amount spent by the Internet Users online is bound to increase. Those apprehensive of divulging their credit card and bank details would be active online shoppers. The Internet users are expected to buy high-end products like automobile, property, home durables online. Also the internet users mature, the demand for customization will increase. The content would adopt the regional flavors. More niches will be formed, seeking for offerings made for them and content that meets their requirements.
30. Ethical Hacking

Mr. Deepak B. Kadve & Ms. Reshma P. Mavkar
Email: deepkadve55@gmail.com & rnavkar@gmail.com
JSPM’s Rajarshi Shahu College of Engineering, Pune

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization’s secrets to the open Internet. With these concerns and others, the ethical hacker can help. This paper describes ethical hackers: their skills, their attitudes, and how they go about helping their customers find and plug up security holes.

Introduction:

HACKER:

1. A person who enjoys learning the details of computer systems and how to stretch their capabilities—as opposed to most users of computers, who prefer to learn only the minimum amount necessary.

2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.
Ethical hacking --- also known as penetration testing or white-hat hacking — involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target’s permission. The intent of ethical hacking is to discover vulnerabilities from a hacker’s viewpoint so systems can be better secured. Ethical hacking is the use of hacking knowledge to forcefully attempt to enter a network to find its loopholes and back doors.

To catch a thief, think like a thief. That’s the basis for ethical hacking. Protecting your systems from the bad guys — and not just the generic vulnerabilities that everyone knows about is absolutely critical. When you know hacker tricks, you can see how vulnerable your systems are.

Firewalls and encryption can create a false feeling of safety. These security systems often focus on high-level vulnerabilities, such as viruses and traffic through a firewall, without affecting how hackers work. Identifying and dealing with vulnerabilities of your own systems is a step to making them more secure. This is the only proven method of greatly hardening your systems from attack. You must think like them to protect your systems from them.

Who are ethical hackers?

Ethical hackers typically have very strong programming and computer networking skills and have been in the computer and networking business for several years. They are also adept at installing and maintaining systems that use the more popular operating systems (e.g., UNIX** or Windows NT**) used on target systems.

When they encounter a system with which they are unfamiliar, ethical hackers will spend the time to learn about the system and try to find its weaknesses. Finally, keeping up with the ever-changing world of computer and network security requires continuous education and review.

Preparing the attack:
Proxy servers:

Proxy server is a server (a computer system or an application program) which services the requests of its clients by forwarding requests to other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server provides the resource by connecting to the specified server and requesting the service on behalf of the client. In this case, it would ‘cache’ the first request to the remote server, so it could save the information for later, and make everything as fast as possible. A proxy server can be placed in the user's local computer or at specific key points between the user and the destination servers or the Internet. Therefore the attacker’s identity is thereby protected from the target system because the attacker’s system has not established a direct connection with the victim’s machine. This means that attacker's identity is hidden from the victim but preserved as a log file in the proxy server. So to trace an attacker, one should go looking at the log files present in the proxy database.

Tracing the IP Address:

As a first step in preparing for an attack, the attacker first tries to trace you on the globe. The uses the proxy servers to monitor your IP Address. Once he gains your IP Address, it is quite easy for him to trace it to the exact location on the world map. The structure of an IP address is designed in such a manner that it is impossible to simply look at an IP address and deduce its geographic location. This means that there is no mechanism whereby a particular field of an IP address represents the country in which the system having the IP address resides. But with a bit of luck an attacker can get a lot of information on the target system using only its IP address. This includes

- continent country and city
- ISP’s name
- Phone number and home address (requires a bit of luck)
- Office phone number and address (requires a bit of luck)
- Full name of the target individual (requires a bit of luck)

Some of the common techniques used here are
WHOIS:

An important method to trace an IP address is to use the WHOIS database a world wide database maintained by various domain registration companies across the globe containing the listings of the domains registered for the company or country. We can easily perform WHOIS queries using readymade tools available on the web like www.allwhois.com, www.internic.com, www.samspade.org and tools like super scan etc. Here, I have traced the WHOIS information for the website www.yukti.in whose results are shown above. As seen
above the result contained sensitive information like Registrant name, ID, Address, E-Mail and also most importantly the name of the service provider.

Traceroute:

The traceroute tool is available on all windows and most UNIX based systems. It can be used to trace the path between the source and destination computer, listing all routers on the route as well. Traceroute is commonly used by attackers for network reconnaissance purposes. It can be effectively used to determine network topology information and to identify potential entry points to the network.

One of the most important tools for this purpose is the neotrace tool. The neotrace tool is a fantastic tool that allows you to geographically trace an IP address or host name graphically on the world map. It is very accurate, quick and has a number of extremely useful functionalities. This tool has also links to online tools with advanced features.

The diagram shows you the trace route path of a yukti server.

Gathering information for the attack:

Pingsweeping:

![Diagram showing the trace route path of a yukti server]
There may be times when you are not sure whether or not a particular host is connected to the internet in such cases you can use the ping utility, which relies on the echo request and echo reply of ICMP messages to determine whether or not a remote host is alive. The ping tool is also commonly used to determine the amount of time taken by a packet to travel from source to the destination. It allows attackers to automatically map out the entire target network and pinpoint all target systems within a particular range of IPAddress. This process of ping to map out the entire packet network is called ping sweeping.

Traceroute:

When data packets travel in the internet from the source system to destination host they do not necessarily take the shortest possible, indeed more often than not several packets pass through several routers spanning vast geographical location their way from one system to another. It is possible to trace the path from source to destination system with the help of traceroute tool. Traceroute is used by hackers to trace the path taken by a packet from the source system to the destination system over the internet displaying all routers through which the packet travels. It is one of the most common network reconnaissance tools commonly used to determine the topology of the target network and to identify the possible entry points. The trace tool is able to display the network topology, the path between the source and destination system and possible entry points by making use of ICMP packets and error messages displayed by the ICMP protocol.
**Port scanning:**

Port scanning is the art of scanning the target system to obtain a list of open ports that are listening for connections. In other words, port scanning is carried out to determine a list of open ports on the remote host that have certain services or daemons running. It helps in determining the list of open ports on the target system, the services running on them, and any vulnerability that might exist. In certain cases port scanning can also be used to determine the operating system running on the target system. The traditional example of a port scan technique is the manual port scan. Manual port scans require a full three-way hand shake to take place in between the attacker and the target system. A typical TCP/IP three-way hand shake is described in these three steps.

1. The client sends a SYN (synchronize) packet to the server.
2. The server replies with a SYN packet and acknowledges the client’s SYN packet by sending an ACK (acknowledge) packet.
3. The client acknowledges the SYN sent by the server.

![Port Scanner](image)

**Executing the attack:**
Dos attacks:

A denial of service (DOS) attack is an attack that clogs up so much memory on the target system that it cannot serve its users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users. A DOS attack can be perpetrated in a number of ways. There are basic kinds of attacks:

1. Ping of Death
2. Teardrop attacks
3. Land attacks
4. Smurf attacks
5. Distributed DOS attacks

Ping of death:

A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer

Teardrop attacks:

Teardrop is a program that sends IP fragments to a machine connected to the Internet or a network. Teardrop exploits an overlapping IP fragment bug present in Windows 95, Windows NT and Windows 3.1 machines. It should be noted, though, that while this attack is considered to be non-destructive, it could cause problems if there is unsaved data in open applications at the time that the machine is attacked. The primary problem with this is a loss of data Attempts to re-assemble the packets with overlapping data can cause the computer to crash if the software is not prepared to handle erroneous packet header information.

Land attacks:

A LAND attack is a DOS (Denial of Service) attack that consists of sending a special poison spoofed packet to a computer, causing it to lock up. The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address and an open
port as both source and destination. The reason a LAND attack works is because it causes the machine to reply to itself continuously.

**Smurf attacks:**

The smurf attack is a way of generating a lot of computer network traffic to a victim site. That is, it is a type of denial-of-service attack. Specifically, it floods a target system via spoofed broadcast ping messages. In such an attack, a perpetrator sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses, all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

**Distributed dos attacks:**

A distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. These attacker advantages cause challenges for defense mechanisms.

**Preventive measures from being hacked!**

1. **Disable file and print sharing on your computer:** Use of the file sharing feature increases the risk that other Internet users could gain access to any of the files on your computer's hard drive.

2. **Install antivirus software:** Install at least one type of antivirus and keep it up to date with the latest virus definitions. Even with updated antivirus software, running online virus scans as a supplement the current program is a good idea.
3. **Install a firewall:** A firewall is designed to monitor data coming in and going out of your computer, blocking unwanted traffic based on the rules that have been configured. Be sure to take the time to configure it properly using the documentation provided.

4. **Install a router:** A router is a good extra line of defense and can be purchased for relatively cheap. In addition to helping protect your computer against portscans, it can allow multiple computers to share the same internet connection.

5. **Browser Security:** Frequently new exploits are discovered in web browsers that can lead to the compromising of your system. Usually patches are available for download from the vendors website.

6. **Turn off your computer or put your modem on standby if you’re going to be away for an extended period of time:** With Road Runner, your computer is always connected to the Internet, which can increase your computer's vulnerability from security related problems. If you turn your computer off or put your modem on standby mode when you aren't using it, the time the computer may be vulnerable is decreased.

7. **Windows Updates** Keep up to date with Microsoft's critical system updates. Keeping these up to date can help secure your system. These updates are free and can be downloaded from [http://windowsupdate.microsoft.com](http://windowsupdate.microsoft.com).

8. **Turn off unused services** After a normal installation, most services in Windows are turned on by default regardless if you use them or not. We recommend turning off as many unused services as possible. The service for Windows NT, 2000, and XP are located in Start->Settings->Control Panel-> Administrative Tools-> Services.

9. **Research your downloads** If at all possible, research your intended downloads before you download and install them. Especially if using file and music sharing programs such as Kazaa,Gnutella or BitTorrent. These files can come from unknown sources and could contain viruses or trojans.

10. **Email attachments** Be wary of email attachments, even from people you know. Viruses will often forge email address to try to spread itself. For an extra security measure disable the preview pane in your email program. This will require you to
**Conclusion:**

Identification of vulnerabilities is useless without regular auditing, persistent intrusion detection, high-quality system administration practice, and computer security knowledge. A simple breakdown can expose an organization to cyber attacks, loss of income or mind share, or even something worse. So it is the necessity of every computer user to practice ethical hacking. It is moreover, a Risk management technique and it is the need of the hour to counter the attacks of the Hackers. A simple breakdown can expose an organization to cyber attacks, loss of income or mind share, or even something worse. Adverse effects like Mass destruction and threat to your personal data is inevitable. Therefore, Knowledge about hacking tricks is needed and need of the hour to implement the security measures.

**References:**


31. Growth of Blu-Ray Disc

(Mr. Birajdar Bhaurao, Dr. D.Y.Patil ACS College, Pimpori
E-Mail: bhauraobirajdar_it@rediffmail.com, Mob: 9665200322)

Blu-ray disc is a next-generation optical disc format jointly developed by a group of leading consumer electronics and PC companies called the Blu-ray Disc Association (BDA), which succeeds the Blu-ray Disc Founders (BDF). Because it uses blue lasers, which have shorter wavelengths than traditional red lasers, it can store substantially more data in the same amount of physical space than previous technologies such as DVD and CD. A current, single-sided, standard DVD can hold 4.7 GB (gigabytes) of information. That’s about the size of an average two-hour, standard-definition movie with a few extra features. The Blu-ray disc’s higher storage capacity is enabled by a blue laser that has a shorter wavelength than the standard red laser used in CD (780nm) and DVD (650nm) technology. Blu-ray disc utilizes a blue laser with a wavelength of only 405nm combined with a strong lens system with a numerical aperture of 0.85. This results in a ultra-small laser spot which allows writing smaller data pits which increases the amount of data on the disc. Due to the small data entry spot on the disc surface hard coating is needed on Blu-ray discs.

When the CD was introduced in the early '80s, it meant an enormous leap from traditional media. Not only did it offer a significant improvement in audio quality, its primary application, but its 650 MB storage capacity also meant a giant leap in data storage and retrieval. For the first time, there was a universal standard for pre-recorded, recordable and rewritable media, offering the best quality and features consumers could wish for themselves, at very low costs.

After CD DVD come in 1990, it store the 4.7 gb data. This enabled high quality, standard definition video distribution and recording. Furthermore, the increased capacity accommodated more demanding data applications. At the same time, the DVD spec used the
same form factor as the CD, allowing for seamless migration to the next generation format and offering full backwards compatibility.

Now, in the next millennium, high definition video demands a new solution. History proved that a significant 5-10 x increase in storage capacity and the ability to play previous generation formats are key elements for a new format to succeed. This new format has arrived with the advent of Blu-ray Disc, the only format that offers a considerable increase in storage capacity with its 25 to 50 GB data capacity. This allows for the next big application of optical media: the distribution and recording of high definition video in the highest possible quality. In fact, no other format can offer the data capacity of Blu-ray Disc, and no other format will allow for the same high video quality and interactive features to create the ultimate user experience. As with DVD, the Blu-ray Disc format is based on the same, bare disc physical form factor, allowing for compatibility with CD and DVD.

Cd store the 700 mb and dvd store the 4.7gb data on single layer. But blu ray store the 25gb data on single layer and 50gb on dual layer. It’s copy speed is 36 mbps. It store the high definition (HD) of audio and video. Because of its storing capacity it is so popular. It also gives security of data. It uses hard coating that avoid the damage of data.

Features:-

Capacity
The Blu-ray Disc format offers the highest capacity of any consumer media format to date, also greatly surpassing the capacity of other format proposals. Blu-ray Disc's huge capacity allows not only for the highest quality High Definition video to be recorded at large bitrates (thereby eliminating the need for tight compression that could affect picture quality), it also opens the doors to new and existing applications. In 2005 Pioneer company develop blu ray disc which capacity is 500 gb that uses 20 layers.

Lifespan
The Blu-ray Disc format is designed to stay relevant for at least 10 to 15 years. Its high storage capacity of 25 to 50 GB allows for the best-possible High Definition video quality
and satisfies even the most demanding data storage needs. As we have seen with DVD in the past, most premium titles require two discs. This is why Blu-ray Disc incorporates the additional storage space that is required for a High Definition feature film including bonus bonus material in the new standard from the beginning.

**Broasted Industry Support**

History has shown that unified industry support for a particular format is most likely to lead to success. Therefore, the participation of the world’s most renowned consumer electronics manufacturers and IT companies are leading in the success of the best standard for next-generation storage: Blu-ray Disc. Blu-ray Disc is supported by leading hardware manufacturers across the CE and IT fields from the U.S., Europe, Japan and Korea, including Dell, HP, Hitachi, LG Electronics, Matsushita (Panasonic), Mitsubishi, Pioneer, Philips, Samsung, Sharp, Sony and Thomson/RCA.

**Content Protection**

Blu-ray Disc provides some of the strongest copy protection methods ever developed for any consumer format. It makes Blu-ray Disc the best choice for any content publisher wanting assurance that their valuable assets are protected from piracy. Based on feedback from the content industry and taking a cue from the lessons learned by other formats, the Blu-ray Disc format incorporates a robust copy protection mechanism. The copy protection mechanism for Blu-ray Disc is mandatory and will be governed by strict licensing procedures.

**Format Of Blu Ray Disc:**

- **BD-ROM (read-only)** - for pre-recorded content
- **BD-R (recordable)** - for PC data storage
- **BD-RW (rewritable)** - for PC data storage
- **BD-RE (rewritable)** - for HDTV recording.
By using new Blu-Ray disc we can store large amount of data. Generally it stores 25 Gb data on single layer and 50 Gb data on double layer. It stores High definition (HD) video and audio. So much of the people uses blu ray disc. Very soon BD’s will replace CDs and DVDs.
32. World of Inventory

MANISH MANOJ UPADHYAY

Asst. Professor (HRM) & Training In charge-MBA

Department of Management Studies, Sevagram

Mob +91 (9763735511)

Email: mmupadhyay@rediffmail.com

Materials are equivalent to cash and they make up an important part of the total cost. It is essential that materials should be properly safeguarded and correctly accounted. Proper control of material can make a substantial contribution to the efficiency of a business. The success of a business concern largely depends upon efficient purchasing, storage, consumption and accounting.

Concept of Inventory:

Inventory refers to the stock of resources that possess economic value, held by an organization at any point of time. These resource stocks can be manpower, machines, capital goods or materials at various stages.

Inventory is a quantity or store of goods that is held for some purpose or use (the term may also be used as a verb, meaning to take inventory or to count all goods held in inventory). Inventory may be kept "in-house," meaning on the premises or nearby for immediate use; or it may be held in a distant warehouse or distribution center for future use. With the exception of firms utilizing just-in-time methods, more often than not, the term "inventory" implies a stored quantity of goods that exceeds what is needed for the firm to function at the current time (e.g., within the next few hours).

In single line we can say Inventory is a detailed list of all the items in stock.
Why Inventory:

Why would a firm hold more inventory than is currently necessary to ensure the firm's operation? The following is a list of reasons for maintaining what would appear to be "excess" inventory.

A. Meet Demand
B. Keep Operations Running
C. Lead Time
D. Hedge
E. Quality Discount
F. Smoothing Requirements

Inventory Management:

Management is nothing but the act of managing something. Inventory Management is maintaining adequate stocks to ensure uninterrupted service.

Inventory Management:

Inventory Management isn't easy. If it were, more companies would be good at it. But being competent at managing your inventory isn't all that difficult either. It just requires that you invest the time to develop an understanding of the factors that should be affecting your inventory management decisions. Now a days, companies should ask following questions to themselves for Managing Inventory:

✓ What and how much stock you have?
✓ When to order fresh supplies?
✓ What and how much has been ordered?
✓ When it was ordered?
✓ Where all supplies are stored?
✓ When and how much fresh stock was received and by whom?
Typically, Inventory Management techniques include Pareto Curve, ABC Classification and Economic Order Quantity Management. A more sophisticated method takes these two techniques further, combining certain aspects of each to create the K Curve Methodology.

In short we can say, Inventory management, or inventory control, is an attempt to balance inventory needs and requirements with the need to minimize costs resulting from obtaining and holding inventory. There are several schools of thought that view inventory and its function differently.

Inventory Management and Inventory Control must be designed to meet the dictates of the marketplace and support the company's strategic plan.

**BIBLIOGRAPHY:**

**WEBSITES:**

2. http://www.inventorymatters.co.uk.noisegate2.webhoster.co.u"
33. The Impact of Social Media on Online Marketing of Financial Services

Mr. Gajanan Panditrao Mudholkar, Research Scholar, SRTM University, Nanded.

The phenomenon called “social media” that has finally begun to enter into the financial services industry brings with it promise and hope. However, there is much debate on the subject of whether or not this new phenomenon will have an impact on the bottom line. Financial advisors are asking “will social media bring us new clients”?

The answer is not a simple one. It depends on how you approach and integrate the new social tools, technologies, and networks into your practice. There will be many financial advisors who evolve their practices and commit to learning the tools and techniques, and there will be others who won’t dedicate the time required to make new media a part of their practice. There will also be those advisors who will not use the tools, technologies, and networks in a way that will build trust with potential clients.

The truth is, nothing has changed other than the fact that we now have social tools, technologies, and venues that allow us to publicly teach, share, connect, access, and engage with people in real time.

Social networks are just like real life networks. If you use the tools to constantly promote yourself, or you stalk potential prospects and go for the jugular prior to building trust, you will have zero success.

Just as you develop relationships with prospects offline, that same process needs to apply online. If you adhere to the principles in this post as you develop prospects online, you can accelerate your ability to fill your pipeline and potentially close new business.
What I’ve found in my experience as an online marketer is that those who are successful have developed a comprehensive online marketing system that allows them to provide ongoing value to their target markets. They are personable and accessible, and they give, share, teach, coach, and nurture their following. In a sense, they are building their own “tribes”, and the members of those tribes are extremely loyal. In fact, many of them become paying customers and clients.

How can you do the same to build and grow your financial services practice in the age of social media?

Not only will need to develop a comprehensive online marketing system, you will also need to implement the fundamental client acquisition process within your strategy, which is exactly what the successful online marketers do. They have a relationship mindset, and they focus on building relationships first, business second.

What is the fundamental client acquisition process?

1. Identify new potential prospects
2. Remain consistently “top of mind”, visible, and valuable with those prospects
3. Find creative ways to help, engage, and have meaningful conversations with those prospects
4. Create opportunities to get in front of prospects (i.e. phone consultations, online or face to face meetings)
5. Ask for the appointment/order.

If you are tempted to abandon the fundamental client acquisition process with a “sell first” mentality, you will not get the business no matter how savvy you are with social media tools.

Build Trust with Clients and Prospects
Unless you share your thought leadership (as I am with you through this blog which then goes out to email and social media channels) as a means for teaching and helping the people in your target markets, you’re not really creating any value or building any loyalty. Sure I could plug in some stock articles here on my blog and choose not to share my own thoughts, insights, passions, lessons learned, and experiences, but how effective would that be for building trust? My goal is to have you know, like, and trust me over time. Therefore, I’m going to give you my best stuff. I’m going to teach you as much as I can, over time!

This should also be your goal for building your online presence. Don’t be afraid to give away your best insights, lessons, ideas, and information. Knowledge is power and people want to learn. They want you to teach them how to be better stewards of their wealth.

To build trust online, you’ve got to show your personality, passions, insights and experiences while also connecting and engaging with your clients and prospects through multiple channels. You’ve got to be visible, valuable, and seemingly accessible 24/7 (even though none of us really are).

What are the essential components of a modern online marketing system?

- **HUB:** A professional blog is my number one choice here. Traditional websites are dead. They are not designed to build relationships. All of the successful online marketers are using professional looking blogs to build trust and authority online.

- **SPOKES:** Social Media Profiles (personal and business) for LinkedIn, Facebook, Twitter, YouTube, Google+, Slide share etc.

- **CONTENT:** Preferably content that YOU create: articles, videos, images, ebooks, presentations, podcasts

- **SPECIAL OFFER:** What can you give to prospects for free in exchange for permission into their email inboxes? (For example, I give away a free email coaching course that works really well for lead capture)
Implementing a comprehensive online marketing system combined with the fundamental client acquisition process will give you a better chance for success in growing your business in the age of social.

Also, you need to sprinkle in a lot of patience. It takes time to build trust. People need to see that you are here for the long haul. That’s why if you set up a blog or social media profiles but rarely post to your blog or participate in social networks, you won’t have success. You’ve got to make the commitment to this in addition to having your online marketing system and client acquisition process. If you do, the leads will come. **Having a modern online marketing system is critical to helping you manage your time and focus on high impact activities.**

In fact, I’ve had financial advisors who subscribed to this blog over a year ago eventually join the platform. They need to see value and they need to see it consistently. If they do, eventually many of them will sign-up for our programs and I can estimate based on my subscribers what that number might look like over time.

Online marketing works and I’m excited about the opportunities for forward thinking financial advisors who get this right!

References:-

1) Financial Services in India – V.A. Avadhani, Himalaya Publication House.
2) Financial Services- M.Y. Khan
4) The Future of Global Financial Services- Global Dimensions in Business- blackwell publishing
5) Social media sites like facebook, twitter, linked in