UNIT-II

Introduction to Cyber Offence

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.
The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following −

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows −

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences Under The It Act 2000

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer,

computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation − For the purpose of this section "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Object − The object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law
Essential ingredients of the section
knowingly or intentionally concealing
knowingly or intentionally destroying
knowingly or intentionally altering
knowingly or intentionally causing others to conceal
knowingly or intentionally causing another to destroy
knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programs.
Penalties − Section 65 is tried by any magistrate.
This is cognizable and non-bailable offence.
Penalties − Imprisonment up to 3 years and / or

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation	Imprisonment of either	Offence is Bailable,

	by using computer resource	description up to 3 years and /or fine up to Rs. 1 lakh	Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.

	resource		
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic	Imprisonment up to 2 years	Offence is Bailable, Non-

	Signature Certificate false in certain particulars	and/or fine up to Rs. 1 lakh	Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

Fine − Two lakh rupees.

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act –

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if −

- The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR
- Offence affects the socio economic conditions of the country; OR
- Offence has been committed against a child below the age of 18 years; OR
- Offence has been committed against a woman.

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

Cyber Laws are the sole savior to combat cyber-crime. It is only through stringent laws that unbreakable security could be provided to the nation's information. The I.T. Act of India came up as a special act to tackle the problem of Cyber Crime. The Act was sharpened by the Amendment Act of 2008.

Cyber Crime is committed every now and then, but is still hardly reported. The cases of cyber-crime that reaches to the Court of Law are therefore very few. There are practical difficulties in collecting, storing and appreciating Digital Evidence. Thus the Act has miles to go before it can be truly effective.

How criminals plan the attacks

Cybercriminals commit cybercrimes using different tools and techniques. But, the basic process of performing the attacks is same in general. The process or steps involved in committing the cybercrime can be specified in 5 steps namely:

1) Reconnaissance
2) Scanning and Scrutinizing
3) Gaining Access
4) Maintaining Access and
5) Covering the tracks

The simplified or condensed process consists of 3 steps namely:

1) Reconnaissance
2) Scanning and Scrutinizing and
3) Launching an Attack

The 3 step process of how cybercriminals plan attacks is illustrated in the below image.

Reconnaissance
Reconnaissance is an act of exploring to find someone or something. Reconnaissance phase begins with **Footprinting**. Footprinting involves gathering information about the target's environment to penetrate it. It provides an overview of system vulnerabilities. The objective of this phase (reconnaissance) is to understand the system, its networking ports and services, and any other related data. An attacker attempts to gather information in two phases: a) passive and b) active attacks.

Passive Attacks
This attack is used to gather information about a target without their knowledge. These attacks include:

- Google or Yahoo search
- Facebook, LinkedIn, other social sites
- Organization's website (target)
- Blogs, newsgroups, press releases, etc
- Job postings on Naukri, Monster, Craiglist, etc
- Network sniffing

Active Attacks

This attack involves exploring the network to discover individual hosts to confirm the data gathered using passive attacks. This attack involves the risk of being detected and so it is called "Active Reconnaissance". This attack allows the attacker to know the security measures in place.

Scanning and Scrutinizing
Scanning involves intelligent examination of gathered information about target. The objectives of scanning are:

- Port scanning
- Network scanning
- Vulnerability scanning

Scrutinizing is also called enumeration. 90% of the time in hacking is spent in reconnaissance, scanning and scrutinizing information. The objectives are:

- Find valid user accounts or groups
- Find network resources or shared resources

- OS and different applications running on the target

Launch an Attack

An attack follows the below steps:

- Crack the password
- Exploit the privileges
- Execute malicious software (backdoor)
- Hide or destroy files (if required)
- Cover the tracks

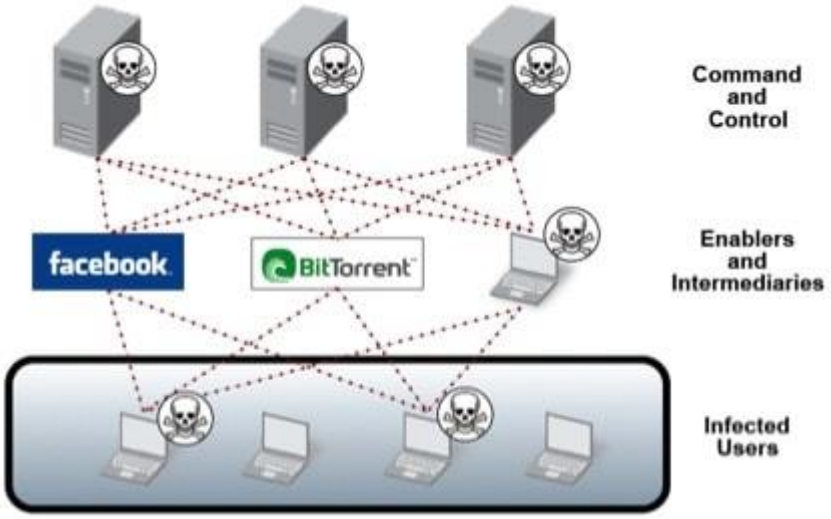
Botnets: A bot is a piece of malware that infects a computer to carry out commands under the remote control of the attacker.

A botnet (short for "robot network") is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder." Each individual machine under the control of the bot-herder is known as a bot. From one central point, the attacking party can command every computer on its botnet to simultaneously carry out a coordinated criminal action. The scale of a botnet (many comprised of millions of bots) enables the attacker to perform large-scale actions that were previously impossible with malware. Since botnets remain under control of a remote attacker, infected machines can receive updates and change their behaviour on the fly. As a result, bot-herders are often able to rent access to segments of their botnet on the black market for significant financial gain.

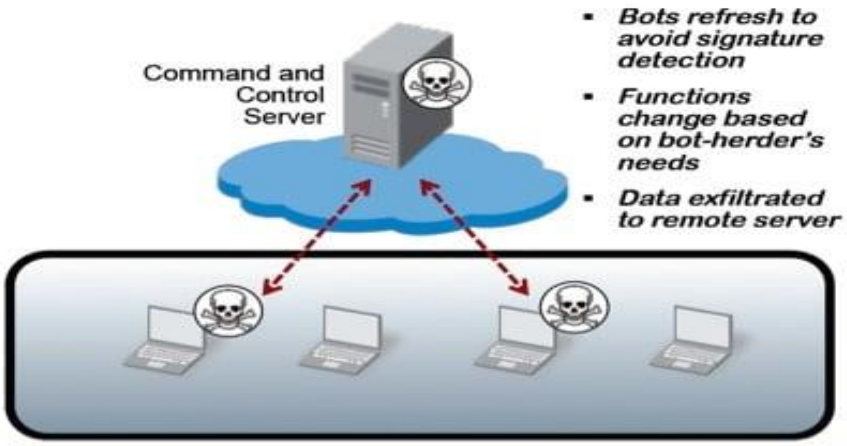
Common botnet actions include:

- **Email spam**– though email is seen today as an older vector for attack, spam botnets are some of the largest in size. They are primarily used for sending out spam messages, often including malware, in towering numbers from each bot. The Cut wail botnet for example, can send up to 74 billion messages per day. They are also used to spread bots to recruit more computers to the botnet.
- **DDoS attacks**– leverage the massive scale of the botnet to overload a target network or server with requests, rendering it inaccessible to its intended users. DDoS attacks target organizations for personal or political motives or to extort payment in exchange for ceasing the attack.
- **Financial breach**– includes botnets specifically designed for the direct theft of funds from enterprises and credit card information. Financial botnets, like the ZeuS botnet, have been responsible for attacks involving millions of dollars stolen directly from multiple enterprises over very short periods of time.
- **Targeted intrusions**– smaller botnets designed to compromise specific high-value systems of organizations from which attackers can penetrate and intrude further into the network. These intrusions are extremely dangerous to organizations as attackers specifically target their most valuable assets, including financial data, research and development, intellectual property, and customer information.

Botnets are created when the bot-herder sends the bot from his command and control servers to an unknowing recipient using file sharing, email, or social media application protocols or other bots as an intermediary. Once the recipient opens the malicious file on his computer, the bot reports back to command and control where the bot-herder can dictate commands to infected computers. Below is a diagram illustrating these relationships:



A number of unique functional traits of bots and botnets make them well suited for long-term intrusions. Bots can be updated by the bot-herder to change their entire functionality based on what he/she would like for them to do and to adapt to changes and countermeasures by the target system. Bots can also utilize other infected computers on the botnet as communication channels, providing the bot-herder a near infinite number of communication paths to adapt to changing options and deliver updates. This highlights that infection is the most important step, because functionality and communication methods can always be changed later on as needed.



As one of the most sophisticated types of modern malware, botnets are an immense cyber security concern to governments, enterprises, and individuals. Whereas earlier malware were a swarm of independent agents that simply infected and replicated themselves, botnets are centrally coordinated, networked applications that leverage networks to gain power and resilience. Since infected computers are under the control of the remote bot-herder, a botnet is like having a malicious hacker inside your network as opposed to just a malicious executable

program.

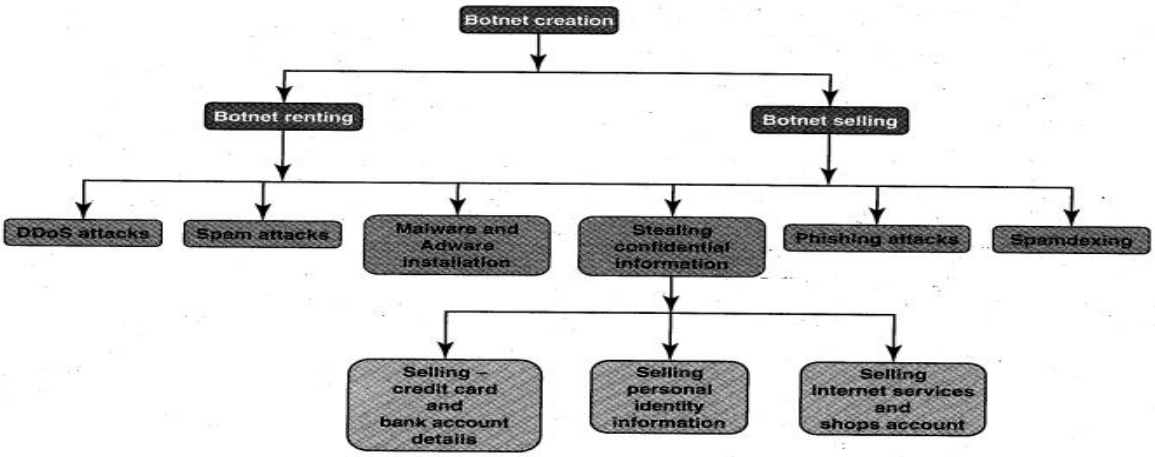


Figure 1: Botnets are used for gainful purposes

Attack Vector: In cyber security, an attack vector is a method or pathway used by a hacker to access or penetrates the target system. Hackers steal information, data and money from people and organizations by investigating known attack vectors and attempting to exploit vulnerabilities to gain access to the desired system. Once a hacker gains access to an organization's IT infrastructure, they can install a malicious code that allows them to remotely control IT infrastructure, spy on the organization or steal data or other resources.

Attack vectors may be exploited by a variety of groups, from a disgruntled former employee of your organization that wants to disrupt your business to the intelligence service of a foreign government that wants to steal your technology. There are also many different known attack vectors that these groups can effectively exploit to gain unauthorized access to your IT infrastructure. IT organizations can militate against cyber-attacks through a number of different methods, including real-time event detection and response capabilities that neutralize cyber-attacks before they can lead to data loss.

Difference between Attack Vector and Attack Surfaces

An attack vector is the path that a hacker takes to exploit cyber security vulnerabilities. Whereas an attack surface is all of the public and privately exposed nexus points of your company's data and human or software interaction.

Why are Attack Vectors Exploited in Cyber Security Attacks?

Hackers make money by performing malicious cyber-attacks on software systems, but they aren't always looking to steal credit card data or banking information. Some hackers have developed more sophisticated ways of monetizing their actions that are less obvious than a compromised credit card number.

- Infecting your systems with bots that the hacker can remotely access from an off-site command and control server. Some hackers infect hundreds or thousands of computers with bots to establish a network known as a botnet. What's a botnet? Botnets can be used to send spam, perform cyber-attacks, steal data or mine crypto currency.
- Customer data theft is a common motivation for hackers who target organizations that collect and store large amounts of personal data from their customers. Hackers love to

steal personalized healthcare information as it can be used to commit insurance or credit card fraud or to illegally obtain prescription drugs.
- A denial of service (DoS) attack can overload your systems and lead to unplanned service outages. Businesses may initiate DoS attacks against their competitors to damage their IT infrastructure and harm their sales.

There are hackers with motivations other than money, such as those that want to leak secret information to the public, embarrass someone they disagree with, or make a political statement. For most IT organizations, however, the majority of cyber-attacks will come from hackers that are trying to steal personal and financial data.

How to Exploit Attack Vectors?

There are many different types of hackers who commit cyber-attacks.

Types of Hackers Who Exploit Attack Vectors

- A disgruntled former employee may be aware of vulnerable attack vectors due to their role in the company.
- An individual hacker may be trying to steal personalized information.
- A hacktivist might initiate a cyber-attack against your organization to make a political statement.
- Business competitors may try to attack your IT infrastructure to gain a competitive edge.
- Cyber-criminal groups combine their expertise and resources to penetrate complex security systems and steal large volumes of data from big companies.

Attack Vector Methodology

In all of these cases, the general methodology of exploiting attack vectors is the same:

1. Hackers identify a target system that they wish to penetrate or exploit
2. Hackers use data collection and observation tools such as sniffing, emails, malware or social engineering to obtain more information about the target
3. Hackers use this information to identify the best attack vector, then create tools to exploit it
4. Hackers break the security system using the tools they created, then install malicious software applications
5. Hackers begin to monitor the network, stealing your personal and financial data or infecting your computers and other endpoint devices with malware bots

Securing potential attack vectors against exploitation by hackers requires IT organizations to implement policies and procedures that prevent hackers from obtaining useful information about IT security vulnerabilities.

What Are Common Attack Vectors in the IT Infrastructure?

IT organizations need to be aware of the most common attack vectors for malicious cyber-attacks to effectively safeguard their networks against unauthorized access.

Most Common Attack Vectors

These are most common attack vectors used by hackers and how to militate against them.

Phishing Emails - Phishing emails are one of the most common types of cyber-attacks. They can be especially hard to mitigate because while IT personnel may be savvy about verifying the contents of an email, members of the business may not be. Phishing emails try to trick the recipient into giving up restricted information, often by presenting them with a link to a malicious website.

Mitigation strategy: The IT organization should encourage reporting of phishing emails and block known senders of malicious mail through a centralized email filter to prevent users from being bombarded with phishing emails. Simple heuristics like "Always make sure you are at the company login page before you enter your credentials" can help less sophisticated users avoid being tricked by phishing emails.

Malware - Malware is a catch-all term that describes any program that introduces malicious code into your IT infrastructure. Viruses, worms and trojans are all examples of Malware. Malware infections can spread throughout the IT infrastructure, creating a lot of overtime for IT SecOps teams and potentially compromising valuable data while impacting service availability.

Mitigation strategy: Zero-day attacks are difficult to avoid, but maintaining an up-to-date antivirus and firewall can significantly reduce the probability of a successful virus attack against your organization.

Unpatched Vulnerabilities - When a software developer identifies major security vulnerability in its application, it writes a patch for it and releases the patch so users can install it. If your IT organization neglects to install patches on a regular basis, hackers can use the known vulnerability as an attack vector to defeat your security.

Mitigation Strategy: Regularly monitor all of your applications and servers for available patches and perform updates as soon as possible to reduce your vulnerability.

Cloud Computing:

Cloud computing is a model to give ubiquitous, on-demand access to a shared pool of resources and these resources can be provisioned and released with minimal management effort.

Cloud Computing has following Models

- Infrastructure as a Service (IaaS): This is the lowest of all layers and in this model customer owns the software and purchases the virtual power to execute it.
- Platform as a Service (PaaS): This is the middle layer and in this layer platform is provided which include API's, portal etc. on which the customer can develop their applications.
- Software as a Service (SaaS): This is the topmost layer. It provides everything and simply rent out the software to user.

Cloud Computing: Attacks

When it comes to Cloud Security, unfortunately vulnerabilities have been found in the Cloud environment which leads to attacks. Following are some of the well-known attack in the cloud environment.

- **Denial of Service Attacks (DoS Attacks):** DoS attack definition remains same in the Cloud i.e. it prevents users from accessing a service. However, in a Cloud environment, DoS attacks get nasty. Cloud by its design will keep on adding more computational power thus making the attack even stronger. The Cloud model gives the DoS attack even more computational

power. This problem is further aggravated when DDoS comes into picture as more machines will be compromised to attack large number of systems.

- **Malware Injection Attack**: This attack focuses on adding/injecting a service implementation or evil virtual machine to cloud environment. The main goal of this type of attack is to take control of victim's data in cloud, so the attacker uploads a crafted image and tricks the image to be part of the victim's cloud environment. After the adverse system/service is added to the cloud environment, user requests will start forwarding to it causing the vulnerable code to execute.
- **Side Channel Attack**: This attack is directed to compromise IaaS by placing a virtual machine co-resident to the victim VM and then it targets cryptographic implementation in system. By co-resident means that the VM has to be in the same host. As you might have guessed this attack is done is 2 phases. First placement of malicious VM as co-resident to target VM. Second phase is to extract useful information from the target VM. Attacker has to be sure that he has placed hos VM as a co-resident to the target VM. How can he be sure? Is there a way to check it? Answer to this is **Yes**. There are ways in which in which co-residency can be checked. Some of the ways are described below:
  - **Network based co-residence check:** This can be done in following ways. However, this is specific to EC2:
    - **Dom0 IP address:** This is specific to Xen hypervisor and is referred to as the initial domain started. For an instance the Dom0 IP can be checked for the first hop on any route form the host. So this Dom0 IP can be determined from another instance if the target is uncontrolled by performing a TCP SYN probe and tracing the last hop.
    - **Packet Round trip times:** According to research, round trip times for VM's in a same host show a pattern.
    - **Closeness of Internal IP address:** Co-Residency can be checked in how internal ip address is allotted to a set of VM's from a single box.
  - **Brute forcing:** In this, the attacker brings up VM and then checks for target in a Zone repeatedly. For VM's spawned up in wrong Zone, attacker shut down that VM and repeat the process.
- **Authentication and MiTM Attack**: As most of the upfront services being offered relies on username/password combination, authentication is considered to be the weak point in Cloud Security Model. Also if attacker can place themselves between the user and the service provider then the MiTM attacks are also possible.

Cloud Computing: Attack's Countermeasures

- As customers lose control over their data as soon as they move that to cloud, Customers must make sure that the data stored in cloud is encrypted and if possible should retain the keys with them only.
- Detect the side-channel attack during the placement phase only. This can be done by collecting logs for new machines starting and stopping and feed them to a SIEM solution. High number of new machines being spawned and shut down within a defined time interval could be an indicator of an attacker perform the co-residency check.
- Instead of simple username and password authentication check, multifactor authentication must be implemented.
- Hiring a CCSP (Certified Cloud Security Professional) to manage the cloud.
- Check for the integrity of data by implement encryption /decryption for the data over wire.

- Implement Firewalls, IPS and other ACL filters at perimeter. Apply black holing and sink holing.
- Implement a combination of Virtual Firewall and Randomized Encryption/Decryption: Placement can be protected by enabling virtual firewalls at VM level which restricts traffic between VM'a and to protect against 2nd step in side-channel attack, implement randomized encryption and decryption thus making the process more complex to break.

Cybercrime: Mobile and Wireless devices

Below are some of the most common types of Wireless and Mobile Device Attacks:

- **SMiShing:** Smishing become common now as smartphones are widely used. SMiShing uses Short Message Service (SMS) to send fraud text messages or links. The criminals cheat the user by calling. Victims may provide sensitive information such as credit card information, account information, etc. Accessing a website might result in the user unknowingly downloading malware that infects the device.
- **War driving:** War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.
- **WEP attack: Wired** Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption.
  WEP uses a key for encryption. There is no provision for key management with Wired Equivalent Privacy, so the number of people sharing the key will continually grow. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.
- **WPA attack:** Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic. WPA2 is susceptible to attack because cyber criminals can analyse the packets going between the access point and an authorized user.
- **Bluejacking:** Blue jacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.
- **Replay attacks:** In Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.
- **Bluesnarfing:** It occurs when the attacker copies the victim's information from his device. An attacker can access information such as the user's calendar, contact list, e-mail and text messages without leaving any evidence of the attack.
- **RF Jamming:** Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station.

Proliferation of mobile and wireless devices:

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device

provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure below helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.

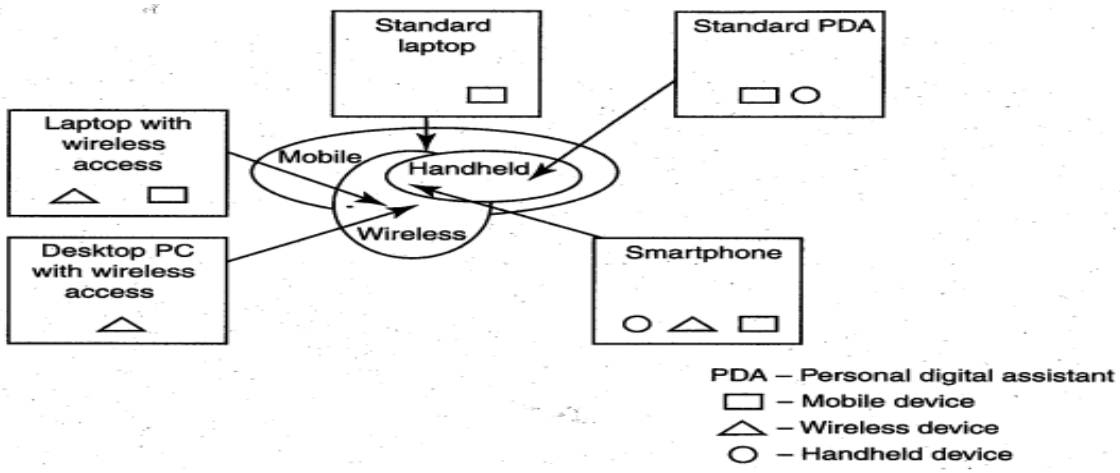


Figure : Mobile, Wireless and hand-held Devices

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s. They are as follows:

1. **Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.
2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touchscreen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
3. **Internet tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
4. **Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. **Ultramobile (PC):** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
6. **Smartphone:** It is a PDA with integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
7. **Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound system, and global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
8. **Fly Fusion Pentop computer:** It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Trends in Mobility:

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to readers to realize the seriousness of cyber security issues in the mobile computing domain. Figure below shows the different types of mobility and their implications.

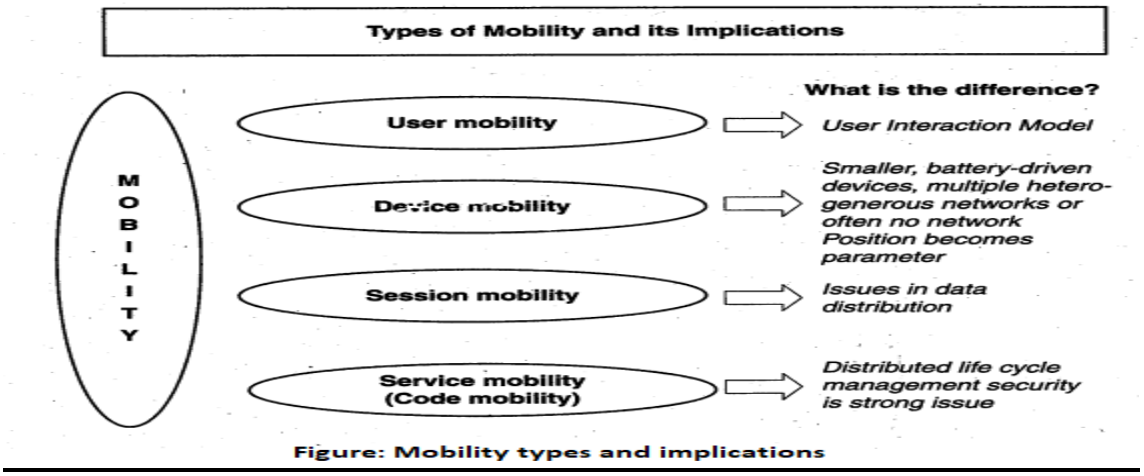


Figure: Mobility types and implications

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and the other is within the mobile networks-that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Popular types of attacks against 3G mobile networks are as follows:

1. Malwares, viruses and worms: Although many users are still in the transient process of switching from 2G, 2.5G to 3G, 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

- ***Skull Trojan:*** It targets Series 60 phones equipped with the Symbian mobile OS.
- ***Cabir Worm***: It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
- ***Mosquito Trojan:*** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
- ***Brador Trojan:*** It affects the Windows CE OS by creating a svchost. exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.
- ***Lasco Worm:*** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. Denial-of-service (DoS): The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Presently, one of the most common cyber security threats to wired

Internet service providers (iSPs) is a distributed denial-of-service (DDos) attack .DDoS CYBER SECURITY attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

3. Overbilling attack: Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.

4. Spoofed policy development process (PDP): These of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunnelling Protocol].

5. Signalling-level attacks: The Session Initiation Protocol (SIP) is a signalling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VolP systems.

Credit Card Frauds in Mobile and Wireless Computing Era:

These are new trends in cybercrime that are coming up with mobile computing - mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Today belongs to "mobile computing," that is, anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment.

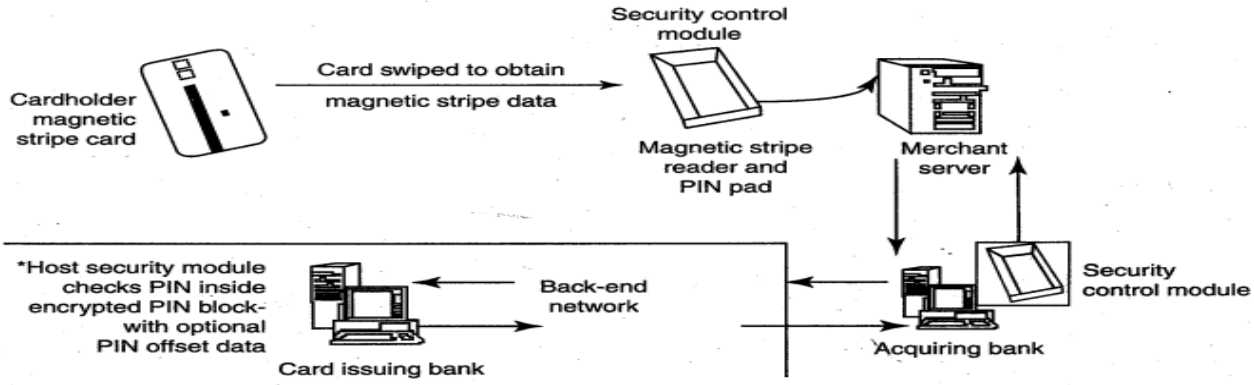


Figure : Online environment for credit card transactions

There is a system available from an Australian company "Alacrity" called closed-loop environment for for wireless (CLEW). Figure above shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.

As shown in Figure, the basic flow is as follows:

1. Merchant sends a transaction to bank
2. The bank transmits the request to the authorized cardholder
3. The cardholder approves or rejects (password protected)
4. The bank/merchant is notified
5. The credit card transaction is completed.

Security Challenges Posed by Mobile Devices:

Mobility brings two main challenges to cyber security: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cyber security challenges are important in devising appropriate security operating procedure. When people are asked about important in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in below figure.

As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro-challenges."

Some well-known technical challenges in mobile security are: managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API), security etc.

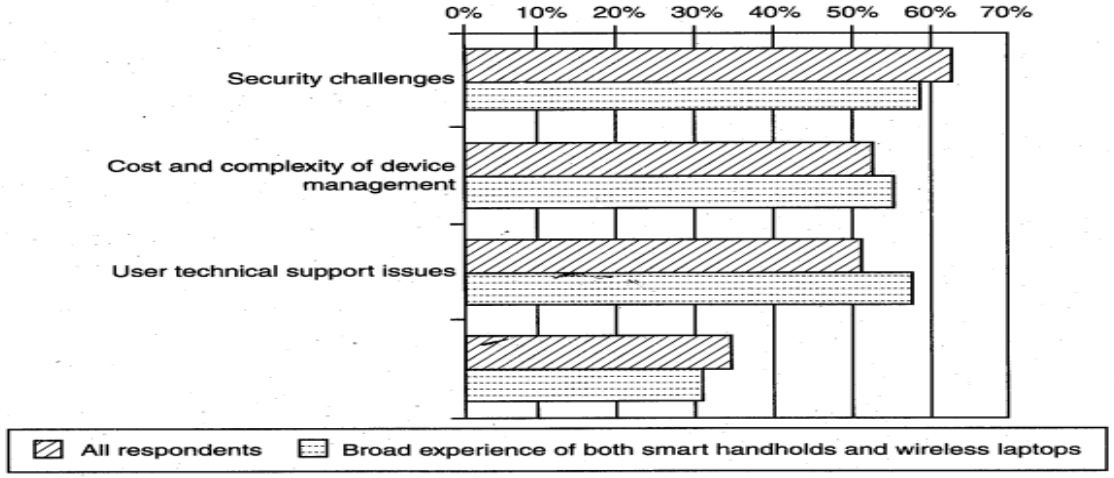


Figure: Important issues for managing mobile devices

Registry Settings for Mobile Devices:

Let us understand the issue of registry settings on mobile devices through an example: Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the "gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device.

In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Authentication Service Security:

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices.

Some eminent kinds of attacks to which mobile devices are subjected to be: push attacks, pull attacks and crash attacks.

Authentication services security is important given the typical attacks on mobile devices through wireless networks: Dos attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless

Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

Attacks on Mobile-Cell Phones:

 Mobile Phone Theft:

Mobile phones have become an integral part of everybody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.

The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.

2. Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.

3. Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

- **Mobile - Viruses**
- **Concept of Mishing**
- **Concept of Vishing**
- Concept of Smishing
- **Hacking - Bluetooth**

Organizational security Policies and Measures in Mobile Computing Era:

Proliferation of hand-held devices used makes the cyber security issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their-hand-held devices.One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.

2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and

physical locks. Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
4. Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.,
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized
7. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

Organizational Policies for the Use of Mobile Hand-Held Devices

There are many ways to handle the matter of creating policy for mobile devices. One way is creating distinct mobile computing policy. Another way is including such devices existing policy. There are also approaches in between where mobile devices fall under both existing policies and a new one.In the hybrid approach, a new policy is created to address the specific needs of the mobile devices but more general usage issues fall under general IT policies. As a part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices.

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time the the they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices. For example, wireless devices pose different challenges than non-wireless Also, employees who use mobile devices more than 20%% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs.

Concept of Laptops:

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect.

The thefts of laptops have always been a major issue, according to the cyber security industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptops, Thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive..

Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops.

1. Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of

aircraft-grade steel and Kevlar brand fiber, thus making these cables 40%% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

2. Laptop safes: Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.

3. Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to their loud nature, they help in deterring thieves. Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.

4. Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or key employees of the organizations.

5. Other measures for protecting laptops are as follows:

 Engraving the laptop with personal details

 Keeping the laptop close to oneself wherever possible

Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves

 Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop

 Making a copy of the purchase receipt, laptop serial number and the description of the laptop

 Installing encryption software to protect information stored on the laptop

 Using personal firewall software to block unwanted access and intrusion

 Updating the antivirus software regularly

 Tight office security using security guards and securing the laptop by locking it down in lockers when not in use

 Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti-theft device;

 Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

Information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical or access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/ access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handling of removable drives/storage mediums /unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls / intrusion detection system (IDSs).
10. Encrypting critical file systems.