JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY ANANTAPUR

B. Tech IV-II Sem. (CSE)

L	T	P	C
3	1	0	3

15A05806 CYBER SECURITY (MOOCS-III)

Course Objectives:

- Appraise the current structure of cyber security roles across the DoD enterprise, including the roles and responsibilities of the relevant organizations.
- Evaluate the trends and patterns that will determine the future state of cyber security

Course Outcomes:

- Analyze threats and risks within context of the cyber security architecture
- Appraise cyber security incidents to apply appropriate response
- Evaluate decision making outcomes of cyber security scenarios

Unit-I

Cyber crime: Mobile and Wireless devices-Trend mobility-authentication service security-Attacks on mobile phones-mobile phone security Implications for organizations-Organizational measurement for Handling mobile-Security policies and measures in mobile computing era. Cases.

Unit-II

Tools and methods used in cyber crime-Proxy servers and Anonymizers- Phishing Password cracking-Key loggers and Spy wares-Virus and worms-Trojan Horse and Backdoors-Steganography-SQL Injection-Buffer overflow-Attacks on wireless network. Cases.

Unit-III

Understanding computer forensic-Historical background of cyber forensic Forensic analysis of e-mail-Digital forensic life cycle-Network forensic-Setting up a computer forensic Laboratory-Relevance of the OSI 7 Layer model to computer Forensic-Computer forensic from compliance perspectives. Cases.

Unit-IV

Forensic of Hand –Held Devices-Understanding cell phone working characteristics-Hand-Held devices and digital forensic- Toolkits for Hand-Held device-Forensic of i-pod and digital music devices-Techno legal Challenges with evidence from hand-held Devices. Cases.

Unit-V

Cyber Security –Organizational implications-cost of cybercrimes and IPR issues Web threats for organizations: the evils and Perils-Social media marketing Security and privacy Implications-Protecting people privacy in the organizations Forensic best practices for organizations. Cases.

Text book:

1. Nina Godbole & Sunit Belapure “Cyber Security”, Wiley India, 2012.

Unit – 1

➔ Cyber Crime

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime may also be referred to as computer crime.

➔ Mobile, Wireless Devices and hand-held devices

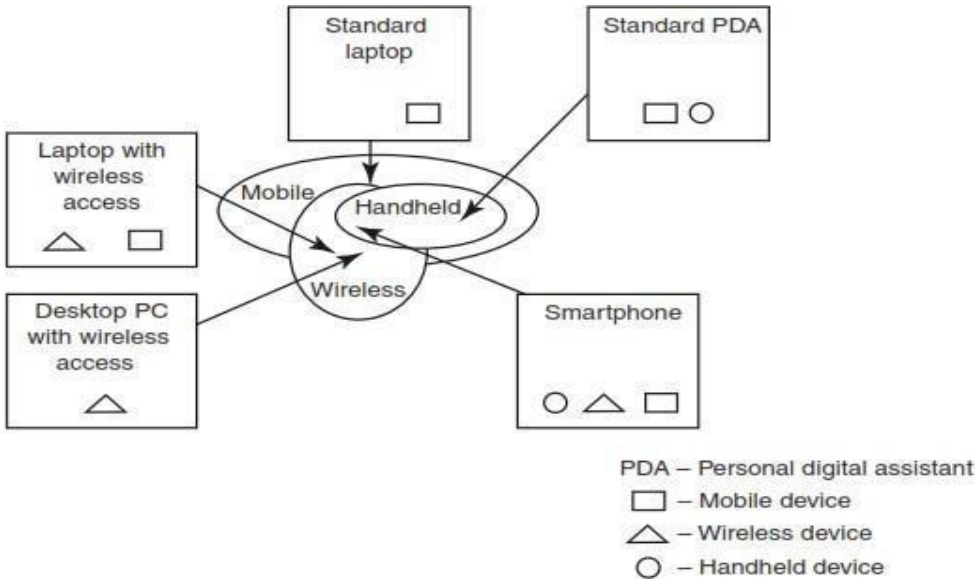


Fig: Mobile, wireless and hand-held devices.

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 touch- screen 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. **Ultra Mobile PC**

It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).

6. **Smartphone**

It is a PDA with an 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.

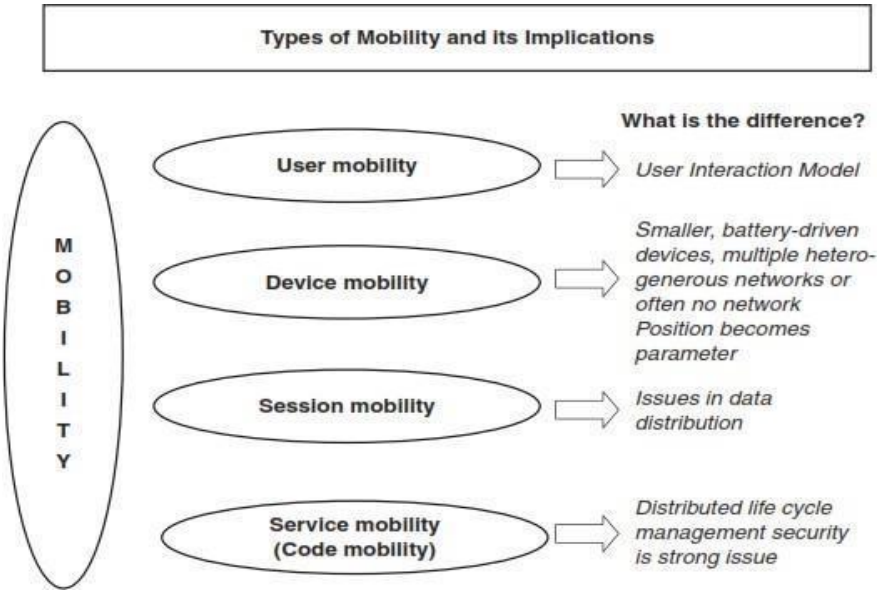


Fig: Mobility types and implications.

1. **Key Findings for Mobile Computing Security Scenario**
    1. With usage experience, awareness of mobile users gets enhanced
    2. People continue to remain the weakest link for laptop security
    3. Wireless connectivity does little to increase burden of managing laptops
    4. Laptop experience changes the view of starting a smart hand-held pilot
    5. There is naivety and/or neglect in smart hand-held security
    6. Rules rather than technology keep smart hand-helds' usage in check
2. **Popular types of attacks against 3G mobile networks**
    1. Malwares, viruses and worms
    2. Denial-of-service (DoS)
    3. Overbilling attack
    4. Spoofedpolicydevelopmentprocess (PDP)
    5. Signaling-levelattacks

➔ **Authentication Service Security**

1. There are two components of security in mobile computing: security of devices and security in networks.
2. A secure network access involves mutual authentication between the device and the base stations or Web servers.
3. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services.
4. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to.
5. 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 are: push attacks, pull attacks and crash attacks.
6. Authentication services security is important given the typical attacks on mobile devices through wireless networks: DoS attacks, traffi c analysis, eavesdropping, man-in-the-middle attacks andsessionhijacking.

1. **Cryptographic Security for Mobile Devices**

We will discuss a technique known as cryptographically generated addresses (CGA). CGA is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address. The address the owner uses is the corresponding private keyto assert address ownership.

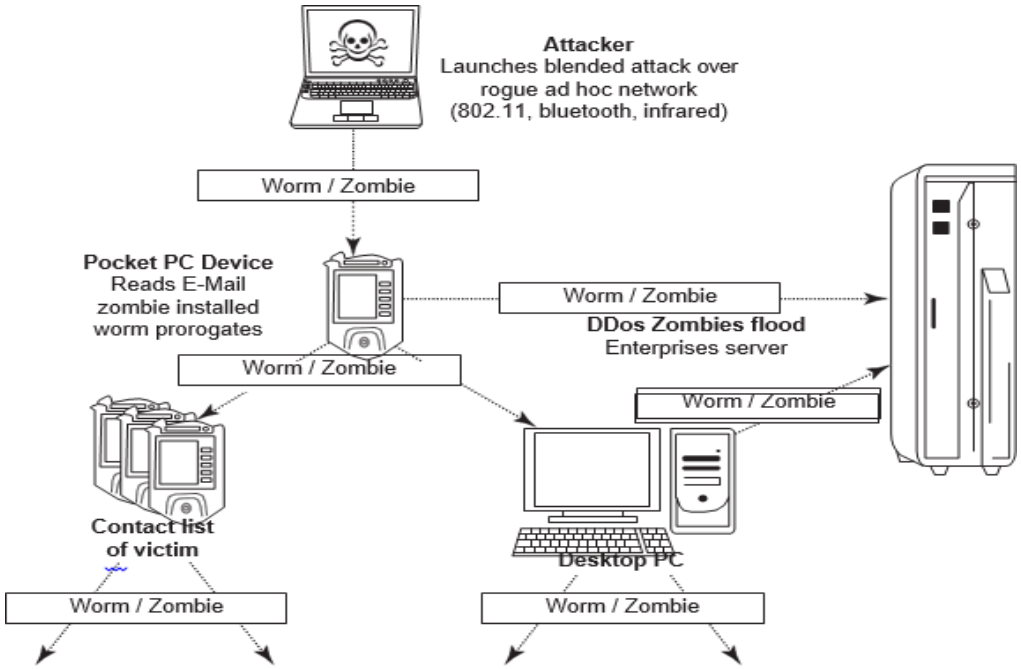


Fig: Push attack on mobile devices. DDos implies distributed denial-of-service attack.

2. LDAP Security for Hand-Held Mobile Computing Devices

LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network (i.e., on the public Internet or on the organization's Intranet). In a network, a directory tells you where an entity is located in the network.

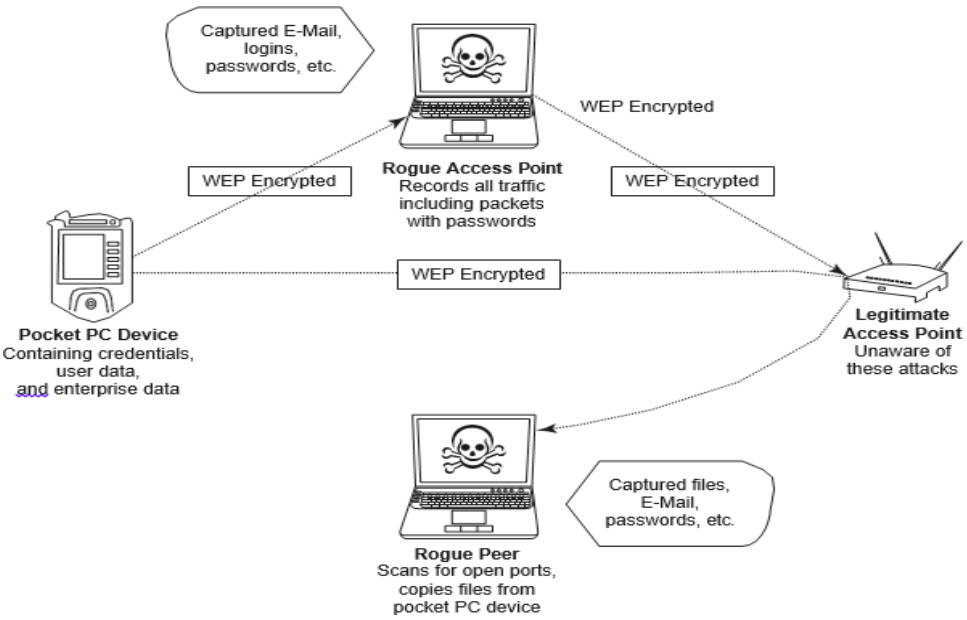


Fig: Pull attack on mobile devices.

3. RAS Security for Mobile Devices

RAS is an important consideration for protecting the business-sensitive data that may reside on the employees' mobile devices. In terms of cyber security, mobile devices are sensitive.

4. Media Player Control Security

1. Given the lifestyle of today's young generation, it is quite common to expect them embracing the mobile hand-held devices as a means for information access, remote working and entertainment.
2. Music and video are the two important aspects in day-to-day aspects for the young generation.
3. Given this, it is easy to appreciate how this can be a source for cyber security breaches. Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the "music gateways."
4. There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices.
5. For example, in the year 2002, Microsoft Corporation warned about this.
6. According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack people's computer systems and perform a variety of actions.
7. According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.

5. Networking API Security for Mobile Computing Applications

1. With the advent of electronic commerce (E-Commerce) and its further off-shoot into M-Commerce, online payments are becoming a common phenomenon with the payment gateways accessed remotely and possibly wirelessly.
2. With the advent of Web services and their use in mobile computing applications consideration.
3. Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple securityplatforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.
4. Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices).
5. Technological developments such as these provide the ability to significantly improve cyber security of a wide range of consumer as well as mobile devices.
6. Providing a common software framework, APIs will become an important enabler of new and higher value services.

➔ Attacks on Mobile/Cell Phones

1. Mobile Phone Theft

1. Mobile phones have become an integral part of ever body's life and the mobile phone has transformed from being a luxury to a bare necessity.
2. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users.
3. Theft of mobile phones has risen dramatically over the past few years.
4. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims.

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.

2. Mobile Viruses

1. A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it.
2. Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays. In total, 40 mobile virus families and more than 300 mobile viruses have been identified.
3. First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.
4. Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS.
5. Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones (i.e., if Bluetooth is always ENABLED into a mobile phone) whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

Following are some tips to protect mobile from mobile malware attacks.

1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

3. Mishing

1. Mishing is a combination of mobile phone and Phishing Mishing attacks are attempted using mobile phone technology.
2. M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.
3. A typical Mishing attacker uses call termed as Vishing or message (SMS) known as Smishing.
4. Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
5. Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

4. Vishing

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V – voice and Phishing.

Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.

The most profitable uses of the information gained through a Vishing attack include

1. ID theft;
2. Purchasing luxury goods and services;
3. Transferring money/funds;
4. Monitoring the victims' bank accounts;
5. Making applications for loans and credit cards.

How Vishing Works

The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

1. Internet E-Mail: It is also called Phishing mail.
2. Mobile text messaging.
3. Voicemail: Here, victim is forced to call on the provided phone number, once he/she listens to voicemail.
4. Direct phone call: Following are the steps detailing on how direct phone call works:
   - The criminal gathers cell/mobile phone numbers located in a particular region and/or steals cell/ mobile phone numbers after accessing legitimate voice messaging company.
   - The criminal often uses a war dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.
   - When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity.
   - When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
   - Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
   - Such calls are often used to harvest additional details such as date of birth, credit card expiration date, etc.

Some of the examples of vished calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:

1. **Automated message:** Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options.
   - Press 1 if you need to check you're banking details and live balance.
   - Press 2 if you wish to transfer funds.
   - Press 3 to unlock your online profile.
   - Press 0 for any other query.
2. Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself: "The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key."
3. The victim enters his/her bank account number and hears the next prompt: **"**Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950."

4. The caller enters his/her date of birth and again receives a prompt from the automated system:
   "Thank you. Now please type your PIN, followed by the pound key."
5. The caller enters his PIN and hears one last prompt from the system: "Thank you. We will now transfer you to the appropriate representative."

How to Protect from Vishing Attacks

Following are some tips to protect oneself from Vishing attacks.

1. Be suspicious about all unknown callers.
2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company – caller ID Spoofing is easy.
3. Be aware and ask questions, in case someone is asking for your personal or financial information.
4. Call them back.
5. Report incidents:

5. Smishing

Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "**SMS** Ph**ISHING**." SMS – Short Message Service– is the text messages communication component dominantly used into mobile phones. To know how SMS can be abused by using different methods and techniques other than information gathering under cybercrime.

How to Protect from Smishing Attacks

Following are some tips to protect oneself from Smishing attacks:

1. Do not answer a text message that you have received asking for your PI.
2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message.
3. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.
3. Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites.

6. Hacking Bluetooth

1. Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances between fixed and/or mobile devices.
2. Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication.

S. No.	Name of the Tool	Description
1	BlueScanner	This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2	BlueSniff	This isa GUI-based utilityforfindingdiscoverableandhiddenBluetoothenabled devices.
3	BlueBugger	The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4	Bluesnarfer	If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5	BlueDiving	Bluediving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.

1. **Bluejacking:** It means Bluetooth Jacking where Jacking is short name for hijack – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers.
2. **Bluesnarfing:** It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.
3. **Bluebugging:** It allows attackers to remotely access a user's phone and use its features without user's attention.
4. **Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo.

→ Mobile Devices: Security Implications for Organizations

1. **Managing diversity and proliferation of hand-held devices**

We have talked about the micro issues of purelytechnical nature in mobile device security. Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their security objectives, subject to legaland otherexternalconstraints.

2. Unconventional/stealth storage devices

We would like to emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees.

As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes – unconventional/stealth storage devices available nowadays are difficult to detect and have become a prime challenge for organizational security.

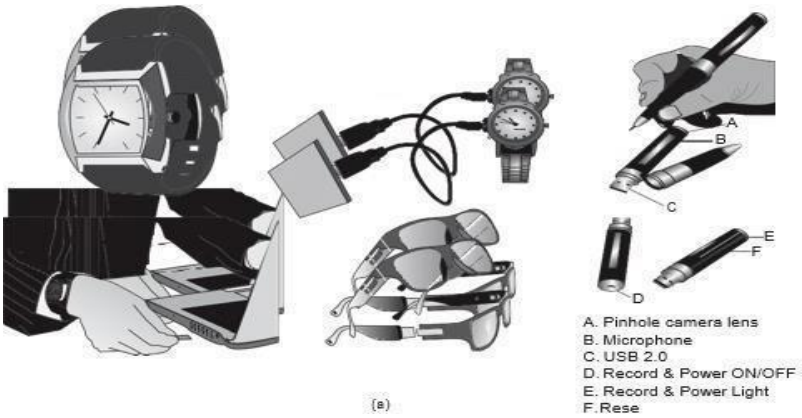


Fig: Unconventional/stealth storage devices.

The features of the software allows system administrator to:

1. Monitor which users or groups can access USB Ports,
2. Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.
3. Control the access to devices depending on the time of the day and day of the week.
4. Create the white list of USB devices which allows you to authorize only specific devices that will not be locked regardless of any other settings.
5. Set devices in read-only mode.
6. Protect disks from accidental or intentional formatting.

3. Threats through lost and stolen devices

This is a new emerging issue for cyber security. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations.

A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period.

4. Protecting data on lost devices

Readers can appreciate the importance of data protection especially when it resides on a mobile hand-held device. At an individual level, employees need to worry about this.

5. Educating the laptop users

Often it so happens that corporate laptop users could be putting their company's networks at risk by down- loading non-work-related software capable of spreading viruses and Spyware.

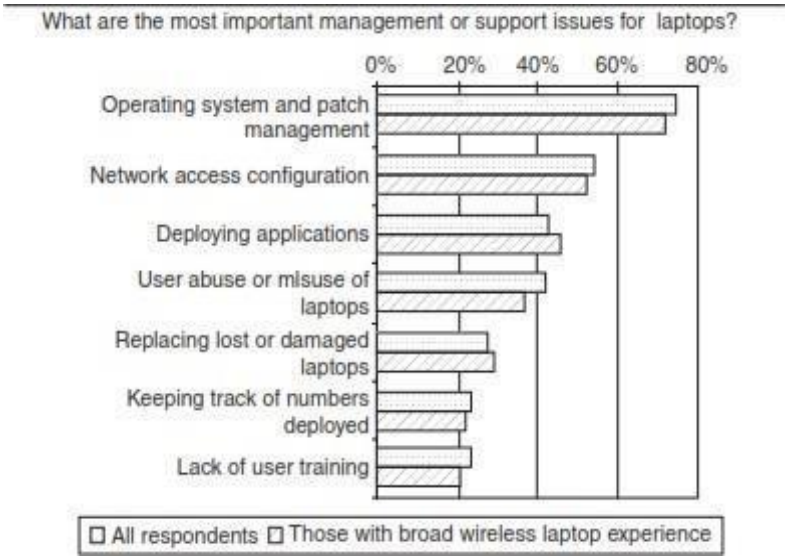


Fig: Most important management or support issues for laptops.

➔ Organizational Measures for Handling Mobile Devices-Related Security Issues

We have discussed micro- and macro level security issues with mobile devices used for mobile computing purposes and what individuals can do to protect their personal data on mobile devices. We discuss what organizations can do toward safeguarding their information systems in the mobile computing paradigm.

1. Encrypting Organizational Databases

Critical and sensitive data reside on databases [say, applications such as customer relationship management (CRM) that utilize patterns discovered through data warehousing and data mining (DM) techniques] and with the advances in technology, access to these data is not impossible through hand-held devices. It is clear that to protect the organizations' data loss, such databases need encryption.

2. Including Mobile Devices in Security Strategy

These discussion so far makes a strong business case – in recognition of the fact that our mobile workforce is on the rise, organizational IT departments will have to take the accountability for cyber security threats that come through inappropriate access to organizational data from mobile-device–user employees. Encryption of corporate databases is not the end of everything.

A few things that enterprises can use are:

1. Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.
2. Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.
3. Develop a system of more frequent and thorough security audits for mobile devices.
4. Incorporate security awareness into your mobile training and support programs so that everyone understands just how important an issue security is within a company's overall IT strategy.
5. Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

→ Organizational Security Policies and Measures in Mobile Computing Era

1. Importance of Security Policies relating to Mobile Computing Devices

Proliferation of hand-held devices used makes the cyber security issue graver than what we would tend to think. People (especially, the youth) have grown so used to their handhelds that they are treating them like wallets! The survey asked the participants about the likelihood of six separate scenarios involving the use of cell phones to communicate sensitive and confidential information occurring in their organizations.

The scenarios described the following:

1. A CEO's administrative assistant uses a cell phone to arrange ground transportation that reveals the CEO's identity and location.
2. The finance and accounting staff discusses earnings of press release and one participant on the call is using a cell phone.
3. A conference call among senior leaders in the organization in which cell phones are sometimes used.
4. A sales manager conducting business in Asia uses, his/her cell phone to communicate with the home office.
5. An external lawyer asks for proprietary and confidential information while using his cell phone.
6. A call center employee assists a customer using a cell phone to establish an account and collects personal information (including SSN).

2. 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.
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 inventory database.
7. Label the devices and register them with a suitable service that helps return recovered devices to the owners.
8. Establish procedures to disable remote access for any mobile devices reported as lost or stolen. Many devices allow the users to store usernames and passwords for website portals, which could allow a thief to access even more information than on the device itself.
9. Remove data from computing devices that are not in use or before re-assigning those devices to new owners (in case of company-provided mobile devices to employees). This is to preclude incidents through which people obtain "old" computing devices that still had confidential company data.
10. 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.

3. Organizational Policies for the Use of Mobile Hand-Held Devices

Securing mobile devices is creating company policies that address the unique issues these devices raise. Such questions include what an employee should do if a device is lost or stolen.

There are many ways to handle the matter of creating policy for mobile devices. One way is creating a distinct mobile computing policy. Another way is including such devices under existing policy.

Unit-2

➔ Tools and methods used in Cyber Crime

Network attack incidents reveal that attackers are often very systematic in launching their attacks. The basic stages of an attack are described here to understand how an attacker can compromise a network here

1. Initial Uncovering
2. Network probe
3. Crossing the line toward electronic crime (E-crime)
4. Capturing the network
5. Grab the data
6. Covering tracks

1. Initial Uncovering

Two steps are involved here. In the first step called as reconnaissance, the attacker gathers information, as much as possible, about the target by legitimate means – searching the information about the target on the Internet by Googling social networking websites and people finder websites.

2. Network probe

At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool.

3. Crossing the line toward electronic crime (E-crime)

Now the attacker is toward committing what is technically a "computer crime." He/she does this by exploiting possible holes on the target system.

4. Capturing the network

At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack.

5. Grab the data: Now that the attacker has "captured the network" he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.

6. Covering tracks

This is the last step in any cyber-attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.

➔ Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connections with other computers on that network. The attacker first connects to a proxy server and establishes a

connection with the target system through existing connection with proxy.

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for securityreasons).
2. Speed up access to a resource (through "caching"). It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxyserver can be used as IP address multiplexer to enable to connect number ofcomputers onthe Internet, whenever one has only one IP address

One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by diff erent users, it is likely to be in the proxy's cache memory, whichwillimproveuserresponsetime. Infacttherearespecialserversavailableknownascache servers? A proxy can also do logging.

Listed are few websites where free proxy servers can be found:

1. http://www.proxy4free.com
2. http://www.publicproxyservers.com
3. http://www.proxz.com
4. http://www.anonymitychecker.com
5. http://www.surf24h.com
6. http://www.hidemyass.com

An Anonymizers or an anonymous proxy is a tool that attempts to make activityon the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.

Listed are few websites where more information about Anonymizers can be found:

1. http://www.anonymizer.com
2. http://www.browzar.com
3. http://www.anonymize.net
4. http://www.anonymouse.ws
5. http://www.anonymousindex.com

➔ **Phishing Password Cracking**

While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening him/her to closethebankaccount ifhe/shedoesnotreplyimmediately. Althoughthemessage seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail.

It is believed that Phishing is an alternative spelling of "fishing," as in "to fish for information." The first documented use of the word "Phishing" was in 1996.

1. How Phishing Works?

Phishers work in the following ways

1. **Planning:** Criminals, usually called as phishers, decide the target and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques as spammers.
2. **Setup:** Once phishers know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves E-Mail addresses and a webpage.
3. **Attack:** This is the step people are most familiar with the phisher sends a phony message that appears to be from a reputable source.
4. **Collection:** Phishers record the information of victims entering into webpages or pop-up windows.
5. **Identity theft and fraud:** Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Phishing started off as being part of popular hacking culture. Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level. We have explained Phishing and Identity theft.

2. Password Cracking

Password is like a key to get an entry into computerized systems like a lock. Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps

1. Find a valid user account such as an administrator or guest;
2. Create a list of possible passwords;
3. Rank the passwords from high to low probability;
4. Key-in each password;
5. Try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information:

1. Blank (none);
2. The words like "password," "passcode" and "admin";
3. Series of letters from the "qwerty" keyboard, for example, qwerty, asdf or qwertyuiop.

4. User's name or login name;
5. Name of user's friend/relative/pet;
6. User's birthplace or date of birth, or a relative's or afriend's;
7. User's vehicle number, office number, residence number or mobile number;
8. Name of a celebrity who is considered to be an idol bythe user;
9. Simple modification of one ofthe preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

Online Attacks

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack."

Offline Attacks

Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.

Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found byexecuting a brute force attack and byusing a subset ofall possible passwords.

Here are some of the examples of "weak passwords":

1. **Susan:** Common personal name;
2. **aaaa:** repeated letters, can be guessed;
3. **rover:** common name for a pet, also a dictionary word;
4. **abc123:** can be easily guessed;
5. **admin:** can be easily guessed;
6. **1234:** can be easily guessed;
7. **QWERTY:** a sequence of adjacent letters on many keyboards;
8. **12/3/75:** date, possibly of personal importance;
9. **nbusr123:** probably a username, and if so, can be very easily guessed;
10. **p@$$\/\/0rd:** simple letter substitutions are preprogrammed into password cracking tools;
11. **password:** used very often – trivially guessed;
12. **December12:** using the date of a forced password change is very common.

Here are some examples of strong passwords:

1. **Convert_£100 to Euros!:** Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.

2. **382465304H:** It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly.
3. **4pRte!ai@3:** It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.
4. **MoOoOfIn245679:** It is long with both alphabets and numerals.
5. **t3wahSetyeT4:** It is not a dictionary word; however, it has both alphabets and numerals.

Random Passwords

We have explained in the previous section how most secure passwords are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters.
3. There should be computer-controlled lists of prescribed password rules and periodic testing to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues.
5. Passwords shall be changed every 30/45 days or less.
6. User accounts should be frozen after five failed logon attempts.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.
8. Successful logons should display the date and time of the last logon and logoff.
9. Logon IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user.

➔ **Keyloggers and Spywares**

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

1. Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usually arelocatedbetweenthe OSandthekeyboardhardware, andeverykeystrokeisrecorded.

SC-KeyLog PRO

It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected log file.

Spytech SpyAgent Stealth

It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.

All in one Keylogger

It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs.

Stealth Keylogger

Perfect Keylogger

KGB Spy

Spy Buddy

Elite Keylogger

CyberSpy

Powered Keylogger

2. Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices.

Listed are few websites where more information about hardware keyloggers can be found:

1. http://www.keyghost.com
2. http://www.keelog.com
3. http://www.keydevil.com
4. http://www.keykatcher.com

3. Antikeylogger

Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool. Visit http://www.anti-keyloggers.com for more information.

Advantages of using Antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, Antikeylogger can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs..
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

➔Spywares

Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.

The features and functions of such Spywares are beyond simple monitoring.

1. **007 Spy:** It has following key features:
   - Capability of overriding "antispy" programs like "ad-aware";
   - Record all websites url visited in internet;
   - Powerful keylogger engine to capture all passwords;
   - View logs remotely from anywhere at any time;
   - Export log report in html format to view it in the browser;
   - Automatically clean-up on outdated logs;
   - Password protection.
2. **Spector Pro:** It has following key features:
   - Captures and reviews all chats and instant messages;
   - captures E-Mails (read, sent and received);
   - captures websites visited;
   - captures activities performed on social networking sites such as MySpace and Facebook;
   - enables to block any particular website and/or chatting with anyone;
   - acts as a keylogger to capture every single keystroke (including usernames and passwords).
3. **eBlaster:** Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording Myspace and Facebook activities and anyother program activity.
4. **Remotespy:** Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, it records keystrokes(keylogger), screenshots, E-Mail, passwords, chats, instantmessengerconversations and websites visited.
5. **Stealth Recorder Pro:** It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features:
   - Real-time mp3 recording via microphone, cd, line-in and stereo mixer as mp3, wma or wav formatted files;
   - Transferring via e-mail or ftp, the recorded files to a user-defined e-mail address or ftp automatically;
   - Controlling from a remote location;
   - Voice mail, records and sends the voice messages.
6. **Stealth Website Logger:** It records all accessed websites and a detailed report can be available on a specified E-Mail address.

It has following key features:

- Monitor visited websites;
- Reports sent to an E-Mail address;
- Daily log;
- Global log for a specified period;
- Log deletion after a specified period;
- Hotkey and password protection;
- Not visible in add/remove programs or task manager.

7. **Flexispy:** It is a tool that can be installed on a cell/mobile phone.
   After installation, Flexispy secretly records coversation that happens on the phone and sends this information to a specified E-Mail address.
8. **Wiretap Professional:** It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. ftis spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.
9. **PC Phone Home:** It is a software that tracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC Phone Home has been installed, connected to the Internet, a stealth E-Mail is sent to a specified E-Mail address of the user's choice.
10. **SpyArsenal Print Monitor Pro:** It has following features:
    - Keep track on a printer/plotter usage;
    - record every document printed;
    - find out who and when certain paper printed with your hardware.

➔ **Virus and Worms**

Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.

Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;
2. Delete files inside the system into which viruses enter;
3. Scramble data on a hard disk;
4. Cause erratic screen behavior;
5. Halt the system (PC);
6. Just replicate themselves to propagate further harm. E

Explain how viruses spread

(a) Through the internet,

(b) Through a stand-alonecomputer system and

(c) Through local networks.

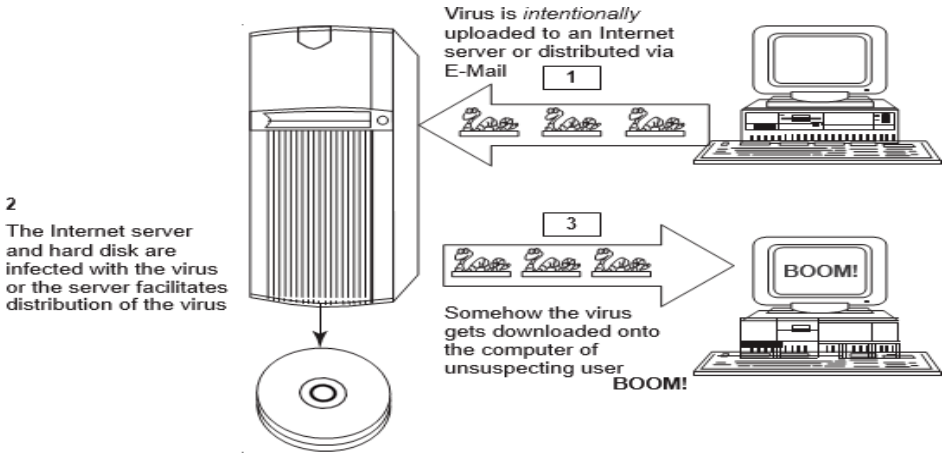


Fig: Virus spreads through the Internet.

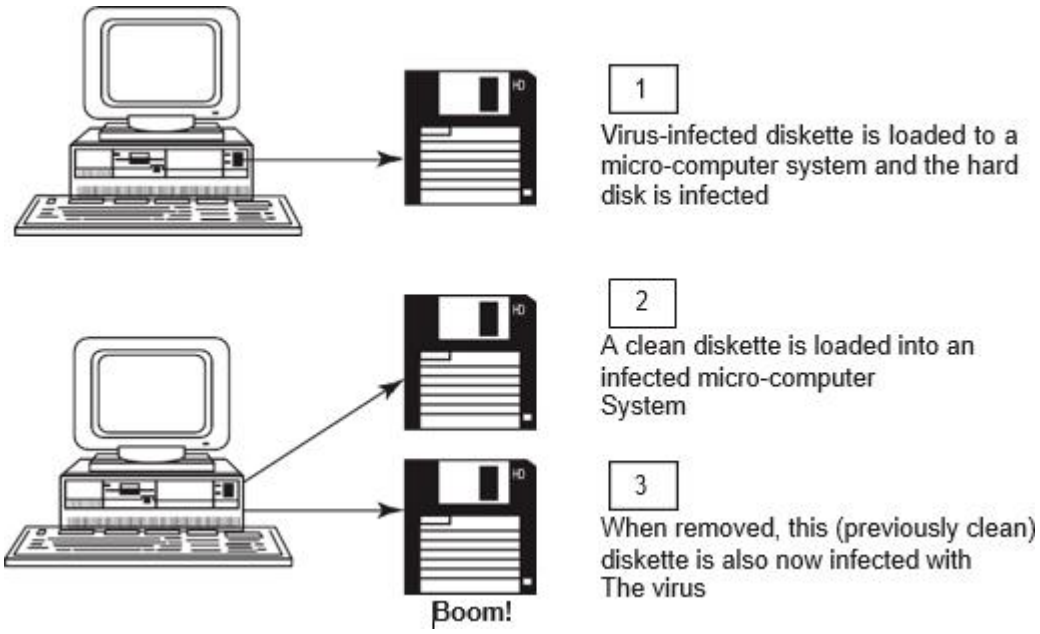


Fig: Virus spreads through stand-alone system.

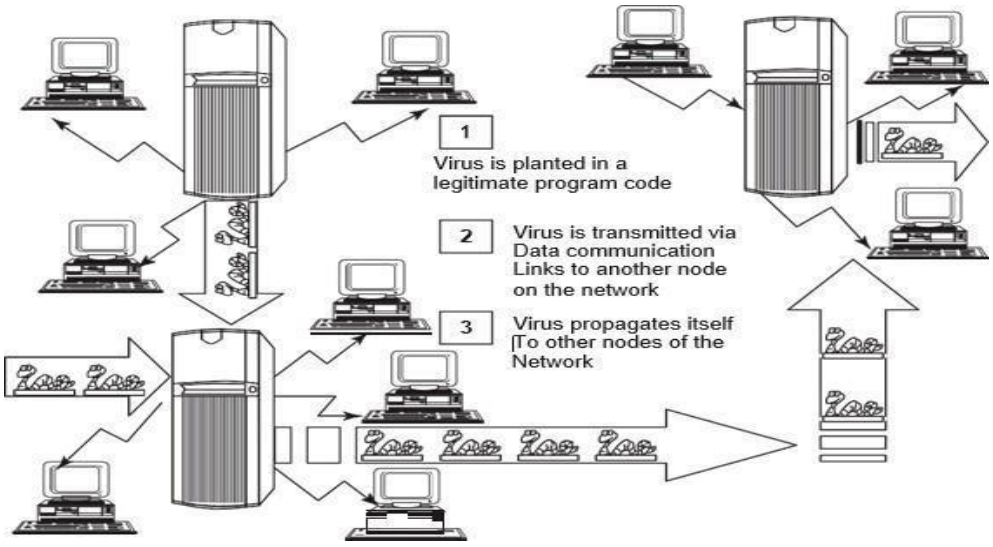


Fig: Virus spreads through local networks.

Difference between computer virus and worm

Sr. No.	*Facet*	*Virus*	*Worm*
1	Different types	Stealth virus, self-modified virus, Encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software pro-Gram that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as The first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses Have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

➢ Types of Viruses

Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., floppy diskettes and hard drives) and which is used to start the computer system. The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors..
2. **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com, .exe, .ovl, .drv) is executed (i.e., opened – program is started). Once these program files get infected, the virus makes copies of itself and infects the other programs on the computer system.
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.

4. **Stealth viruses:** It camouflages and/or masks itself and so detecting this type of virus is very difficult. It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system.
5. **Polymorphicviruses:** It acts likea "chameleon" that changesitsvirus signature (i.e., binarypattern) every time it spreads through the system (i.e., multiplies and infects a new file).
6. **Macro viruses:** Manyapplications, such as Microsoft Wordand Microsoft Excel, support MACROs (i.e., macro languages). These macros are programmed as a macro embedded in adocument.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls. Little awareness is needed about managing and controlling these settings of a web browser.

A typical definition of computer virus/worms might have various aspects such as:

1. A virus attacks specific file types (or files).
2. A virus manipulates a program to execute tasks unintentionally.
3. An infected program produces more viruses.
4. An infected program may run without error for a long time.
5. Viruses can modify themselves and may possibly escape detection this way.

➔ **Trojan Horses and Backdoors**

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk. ATrojan Horse mayget widelyredistributed as part of a computer virus. The term Trojan Horse comes from Greek mythology about the Trojan War.

Some typical examples of threats by Trojans are as follows

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.
6. They gather E-Mail addresses and use them for Spam.
7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. Theydisablethecontrol panel.

➔ **Backdoor**

A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.

Following are a few examples of backdoor Trojans:

1. **Back Orifice:** It is a well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS froma remote location. The name is a word play on Microsoft BackOffice Server software. Readers may visit http://www.cultdeadcow.com/tools/bo.html to know more about backdoor.
2. **Bifrost:** It is another backdoor Trojan that can infect Windows 95 through Vista. It uses the typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.
3. **SAP backdoors:** SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning.
4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests. Readers may visit http://www.onapsis.com/research.html to know more about this tool.

How to Protect from Trojan Horses and Backdoors

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. Stay away from suspect websites/weblinks: Avoid downloading free/pirated software's that often get infected by Trojans, worms, viruses and other things.
2. Surf on the Web cautiously: Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats.
3. It may be experienced that, after downloading the file, it never works and here is a threat that although the file has not worked, something must have happened to the system the malicious software deploys its gizmos and the system is at serious health risk.
4. Install antivirus/Trojan remover software: Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses.

Peer-to-Peer (P2P) Networks

Peer-to-peer, commonly abbreviated as P2P, is any distributed network architecture composed of participants that make a portion of their resources.

1. **Hybrid P2P:** There is a central server that keeps information about the network. The peers are responsible for storing the information.
2. **Pure P2P:** There is absolutely no central server or router. Each peer acts as both client and server at the same time. This is also sometimes referred to as "serverless" P2P.

2. **Mixed P2P:** It is between "hybrid" and "pure" P2P networks. An example of such a network is Gnutella that has no central server but clusters its nodes around so-called "supernodes."

➔ **Steganography**

Steganography is a Greek word that means "sheltered writing." It is a method that attempts to hide the existence of a message or communication. The word "steganography" comes from the two Greek words: steganos meaning "covered" and graphein meaning "to write" that means "concealed writing."

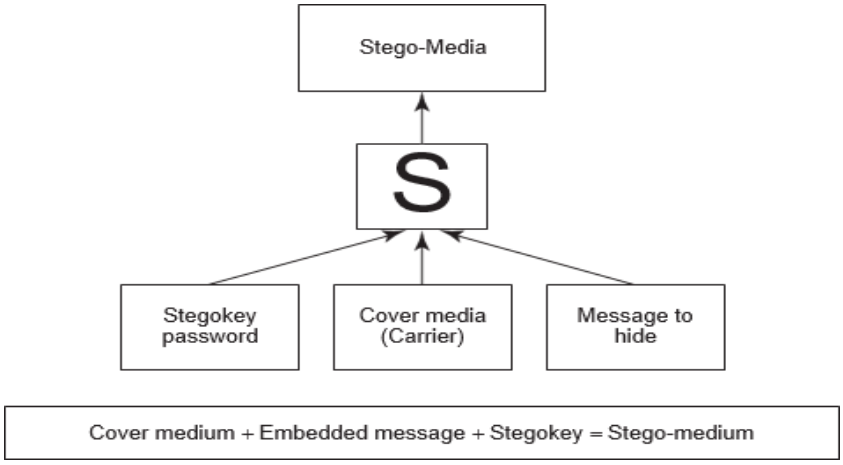


Fig: How steganography works.

1. **Steganography tools**

DiSi-Steganograph

It is a very small, DOS-based steganographic program that embeds data in PCX images.

Invisible Folders

It has the ability to make any file or folder invisible to anyone using your PC even on a network.

Invisible Secrets

It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places such as picture or sound files or webpages. These types of files are a perfect disguise for sensitive information.

Stealth Files

It hides any type of file in almost any other type of file. Using steganography technique, Stealth Files compresses, encrypts and then hides any type of file inside various types of files (including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, and BMP) and other types of video, image and executable files.

2. Steganalysis

Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography. The goal of steganalysis is to identify suspected packages and to determine whether or not theyhave a payload encoded into them, and if possible recover it. Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

➔ SQL Injection

Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS). SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks

1. Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc.
2. To check the source code of any website, right click on the webpage and click on “view source” (if you are using IE – Internet Explorer) – source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for “FORM” tag in theHTML code. Everything between the

   <FORM< and </FORM> have potential parameters that might be useful to find the vulnerabilities.

   <FORM action=Search/search.asp method=post>

<input type=hidden name=A value=C></FORM>

3. The attacker inputs a single quote under the text box provided on the webpage to accept the user- name and password. This checks whether the user-input variable is sanitized or interpreted literally by the server.
4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

2. Blind SQL Injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be the one that displays data.

Using SQL injections, attackers can:

1. Obtain some basic information if the purpose of the attack is reconnaissance.
2. May gain access to the database by obtaining username and their password.
3. Add new data to the database.
4. Modify data currently in the database.

3. Tools used for SQL Server penetration

1. AppDetectivePro
2. DbProtect
3. Database Scanner
4. SQLPoke
5. NGSSQLCrack
6. Microsoft SQL Server Fingerprint (MSSQLFP) Tool

4. How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. fte following steps can be taken to prevent SQL injection.

1. Input validation
2. Modify error reports
3. Other preventions

➔ Buffer Overflow

Buff er overflow, or buff er overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data. This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash) or a breach of system security.

In C and C++, there are no automatic bounds checking on the buffer – which means a user can write past a buffer. For example,

```
int main ()
{
 int buffer[10]; buffer[20] = 10;
}
```

Types of Buffer Overflow

1. **Stack-Based Buffer Overflow**
   1. Stack buffer overflow occurs when a program writes to a memory address on the program's call stack out- side the intended data structure usually a fixed length buffer.
   2. "Stack" is a memory space in which automatic variables are allocated.
   3. Function parameters are allocated on the stack and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.
   4. Once a function has completed its cycle, the reference to the variable in the stack is removed.

The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting:

1. A local variable that is near the buffer in memory on the stack to change the behavior of the program that may benefit the attacker.
2. The return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input-filled buffer.
3. A function pointer, or exception handler, which is subsequently executed. The factors that contribute to overcome the exploits are

1. Null bytes in addresses.
2. Variability in the location of shell code.
3. Differences between environments.

2. **NOPs**

NOP or NOOP (short form of no peration or no operation performed) is an assembly language instruction/ command that effectively does nothing at all.

3. **Heap Buffer Overflow**

Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. In either case, the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain. The characteristics of stack-based and heap-based programming are as follows:

1. "Heap" is a "free store" that is a memory space, where dynamic objects are allocated.
2. The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions.
3. Dynamically created variables are created on the heap before the execution program is initialized to zeros and are stored in the memory until the life cycle of the object has completed.

How to Minimize Buffer Overflow

Although it is difficult to prevent all possible attacks, the following methods will definitely help to minimize such attacks:

1. Assessment of secure code manually
2. Disable stack execution
3. Compilertools

➔ **Attacks on Wireless Networks**

Even when people travel, they still need to work. Thus, work seems to be moving out of the traditional offices into homes, hotels, airport lounges and taxis.

The following are diff erent types of "mobile workers":

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. **Road warrior:** This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels.

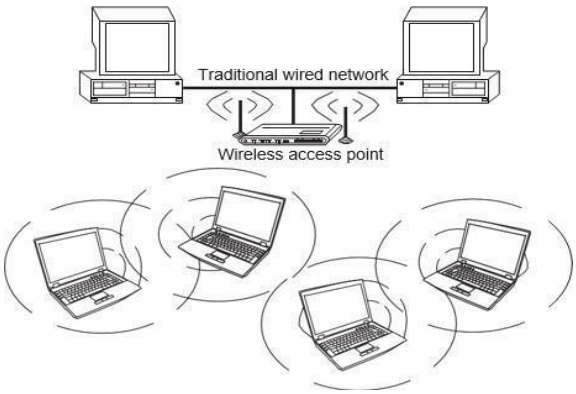


Fig: Wireless Networks

Wireless technology is no more buzzword in today's world. Let us understand important components of wireless network, apart from components such as modems, routers, hubs and firewall, which are integral part of any wired network as well as wireless network.

1. **802.11 networking standards:**

   Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6 and 5 GHz frequency bands.

2. **Access points:** It is also termed as AP. It is a hardware device and/or a software that acts as a central transmitter and receiver of WLAN radio signals.
3. **Access points:** It is also termed as AP. It is a hardware device and/or a software that acts as a central transmitter and receiver of WLAN radio signals.
   1. Free Wi-Fihotspots.
   2. Commercial hotspots.
4. **Service Set Identifier (SSID)**
5. **Wired Equivalence Privacy (WEP):**
6. **Wi-Fi Protected Access (WPA AND WPA2)**
7. **Media Access Control (MAC)**

Traditional Techniques of Attacks on Wireless Networks

1. **Sniffing:** It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network.
2. **Spoofing:** The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage.
   1. MAC address Spoofing
   2. IP Spoofing
3. FrameSpoofing
3. **Denial of service (DoS)**
4. **Man-In-The-Middle Attack (MITM)**
5. **Encryption Cracking**

Unit-3

→ Understanding Computer Forensics

Use of forensic techniques in the investigation of cybercrimes. "Cyber forensics" is a very large domain and addressing it in a single chapter is indeed a challenge. Complex technical aspects involved in digital forensics/computer forensics are not possible to cover in a single chapter. Therefore, this chapter is aimed at only providing a broad understanding about cyber forensics.

Cyber forensics plays a key role in investigation of cybercrime. "Evidence" in the case of "cyber offenses" is extremely important from legal perspective. There are legal aspects involved in the investigation as well as handling of the digital forensics evidence. Only the technically trained and experienced experts should be involved in the forensics activities.

→ Historical Background of Cyber forensics

The Florida Computer Crimes Act was the first computer crime law to address computer fraud and intrusion. It was enacted in Florida in 1978.

"Forensics evidence" is important in the investigation of cybercrimes.

Computer forensics is primarily concerned with the systematic "identification," "acquisition," "preservation" and "analysis" of digital evidence, typically after an unauthorized access to computer or unauthorized use of computer has taken place; while the main focus of "computer security" is the prevention of unauthorized access to computer systems as well as maintaining "confidentiality," "integrity" and "availability" of computer systems.

There are two categories of computer crime: one is the criminal activity that involves using a computer to commit a crime, and the other is a criminal activity that has a computer as a target.

Forensics means a "characteristic of evidence" that satisfies its suitability for admission as fact and its ability to persuade based upon proof.

The goal of digital forensics is to determine the "evidential value" of crime scene and related evidence.

- **Digital Forensics Science**

Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence.

1. **Computer forensics**

It is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations. In other words, it is the collection of techniques and tools used to find evidence in a computer.

2. **Digital forensics**

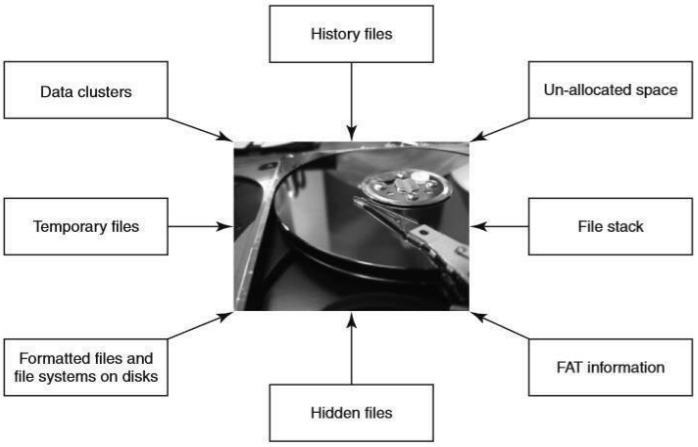
It is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

It is difficult to provide a precise definition of "digital evidence" because the evidence is recovered from devices that are not traditionally considered to be computers. Some researchers prefer to expand the definition by including the "collection" and "examination" of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices.

1. Uncover and document evidence and leads.
2. Corroborate evidence discovered in other ways.
3. Assist in showing a pattern of events (data mining has an application here).
4. Connect attack and victim computers.
5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.
   Extract data that may be hidden, deleted or otherwise not directly available.

The typical scenarios involved are:

1. Employee Internet abuse.
2. Data leak/data breach.
3. Industrial espionage.
4. Damage assessment.
5. Criminal fraud and deception cases;
6. Criminal cases.
7. Copyright violation – more about this is mentioned.



Data seen using forensics tools. FAT means file allocation table.

Using digital forensics techniques, one can:

1. Corroborate and clarify evidence otherwise discovered.
2. Generate investigative leads for follow-up and verification in other ways.
3. Provide help to verify an intrusion hypothesis.
4. Eliminate incorrect assumptions.

- **The Need for Computer Forensics**

The convergence of Information and Communications Technology (ICT) advances and the pervasive use of computers worldwide together have brought about many advantages to mankind. At the same time, this tremendously high technical capacity of modern computers/computing devices provides avenues for misuse as well as opportunities for committing crime.

Chain of custody means the chronological documentation trail, etc. that indicates the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic.

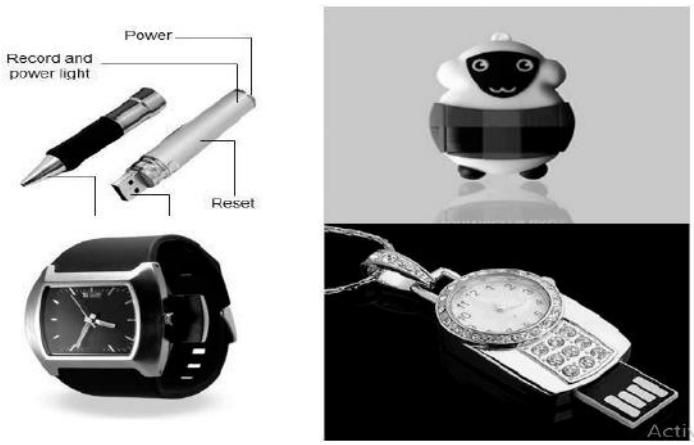


Fig: Hidden and miniaturized storage media.

"Fungibility" means the extent to which the components of an operation or product can be inter- changed with similar components without decreasing the value of the operation or product.

Chain of custody is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.

- **Cyber forensics and Digital Evidence**

Cyber forensics can be divided into two domains:

1. Computer forensics.
2. Network forensics.

Network forensics is the study of network traffic to search for truth in civil, criminal and administrative matters to protect users and resources from exploitation, invasion of privacy and any other crime fostered by the continual expansion of network connectivity.

As compared to the "physical" evidence, "digital evidence" is different in nature because it has some unique characteristics. First of all, digital evidence is much easier to change/manipulate! Second, "perfect" digital copies can be made without harming original.

- **The Rules of Evidence**

This is a very important discussion, especially, for those who are students of legal courses. It was mentioned in that the Indian IT Act amended the Indian Evidence Act. According to the "Indian Evidence Act 1872," "Evidence" means and includes:

1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.
2. All documents that are produced for the inspection of the court are called documentary evidence.

Paper evidence, the process is clear and intuitively obvious. Digital evidence by its very nature is invisible to the eye. Therefore, the evidence must be developed using tools other than the human eye.

There are number of contexts involved in actually identifying a piece of digital evidence:

1. **Physical context:** It must be definable in its physical form, that is, it should reside on a specific piece of media.
2. **Logical context:** It must be identifiable as to its logical position, that is, where does it reside relative to the file system.
3. **Legal context:** We must place the evidence in the correct context to read its meaning. This may require looking at the evidence as machine language, for example, American Standard

Code for Information Interchange (ASCII).

Following are some guidelines for the (digital) evidence collection phase:

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel.
2. Capture a picture of the system as accurately as possible.

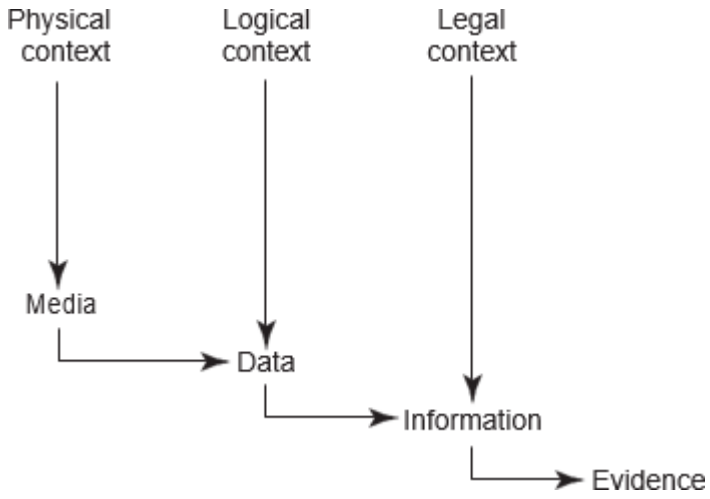


Fig: Path of the digital evidence.

- **Forensics Analysis of E-Mail**

It was mentioned how criminals can use fake mails for various cybercrime offenses. There are tools available that help create fake mails. Forensics analysis of E-Mails is an important aspect of cyber forensics analysis it helps establish the authenticity of an E-Mail when suspected.

Mail server software is a network server software that controls the flow of E-Mail and the mail client software helps each user read, compose, send and delete messages.

E-Mail tracing is done by examining the header information contained in E-Mail messages to determine their source.

- **Digital Forensics Life Cycle**

As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene. That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination.

1. Is admissible.
2. Is authentic.
3. Is complete.
4. Is reliable.
5. Is understandable and believable.

Let us now understand what is involved in the digital forensics process.

- **The Digital Forensics Process**

The digital forensics process needs to be understood in the legal context starting from preparation of the evidence to testifying. Digital forensics evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter to help jurors establish the facts of the case and support or refute legal theories of the case.

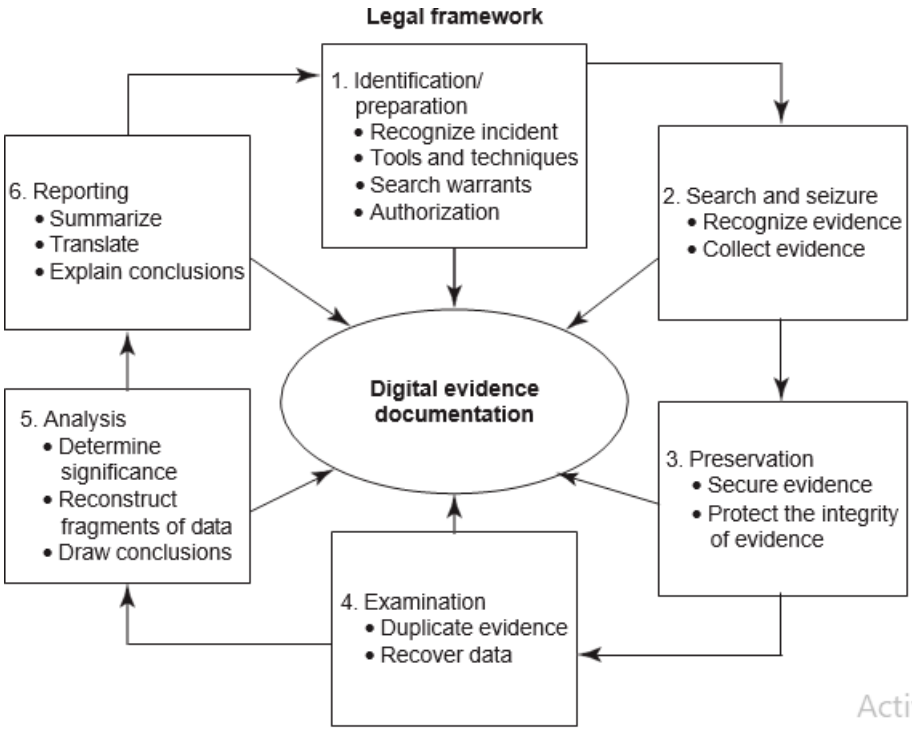


Fig: Process model for understanding a seizure and handling of forensics evidence legal framework.

- **The Phases in Computer Forensics/Digital Forensics**

The investigator must be properly trained to perform the specific kind of investigation that is at hand. Tools that are used to generate reports for court should be validated. There are many tools to be used in the process.

One should determine the proper tool to be used based on the case. Broadly speaking, the forensics life cycle involves the following phases:

1. Preparation and identification
2. Collection and recording
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation and attribution
6. Reporting and
7. Testifying.

To mention very briefly, the process involves the following activities:

1. **Prepare:** Case briefings engagement terms, interrogatories, spoliation prevention, disclosure and discovery planning, discovery requests.
2. **Record:** Drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.
3. **Investigate:** Triage images, data recovery, keyword searches, hidden data review, communicate, iterate.
4. **Report:** Oral vs. written, relevant document production, search statistic reports, chain of custody reporting, case log reporting.
5. **Testify:** Testimony preparation, presentation preparation, testimony.

- **Preparing for the Evidence and Identifying the Evidence**

In order to be processed and applied, evidence must first be identified asevidence. It can happen that there is an enormous amount of potential evidence available for a legal matter, and it is also possible that the vast majority of the potential evidence may never get identified.

- **Collecting and Recording Digital Evidence**

Digital evidence can be collected from many sources. Obvious sources include computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices and so on. Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change).

Fig: Media that can hold digital evidences.

Fig: Some more media that can hold digital evidences.

- **Storing and Transporting Digital Evidence**

  The following are specific practices that have been adopted in the handling of digital evidence:

  1. Image computer media using a write-blocking tool to ensure that no data is added to the suspect device;
  2. establish and maintain the chain of custody.

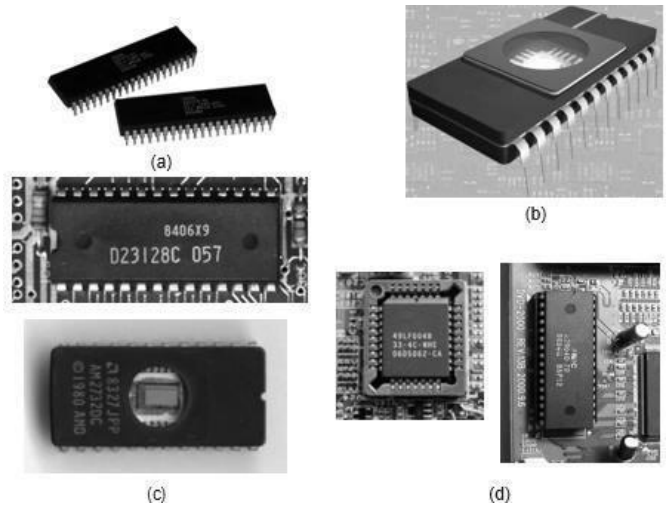


Fig: Embedded memories inside computer. (a) Read-only memory (ROM) chips; (b) erasable programmable read-only memory (EPROM) chip; (c) programmable read-only memory (PROM) chips; (d) electrify erasable programmable read-only memory (EEPROM) chips.

Some of the most valuable information obtained in the course of a forensics examination will come from the computer user. An interview with the user can yield valuable information about the system configuration, applications, encryption keys and methodology. Forensics analysis is much easier when analysts have the user's passphrases to access encrypted files, containers and network servers.

As a general rule, one should not examine digital information unless one has the legal authority to do so. Amateur forensics examiners should keep this in mind before starting any unauthorized investigation.

For the purpose of digital evidence examination, "imaging of electronic media" (on which the evidence is believed to be residing) becomes necessary.

- **Analysis, Interpretation and Attribution**

Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics analysts. In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence.

Examples of common digital analysis types include:

1. Media Analysis
2. Media Management Analysis
3. File System Analysis
4. Application Analysis
5. Network Analysis
6. OS Analysis
7. Executable Analysis
8. Image Analysis
9. Video Analysis

- **Reporting**

The following are the broad-level elements of the report

1. Identity of the reporting agency
2. Case identifier or submission number
3. Case investigator
4. Identity of the submitter
5. Date of receipt
6. Date of report
7. Descriptive list of items submitted for examination, including serial number, make and model
8. Identity and signature of the examiner
9. Brief description of steps taken during examination, such as string searches, graphics image searches and recovering erased files
10. Results/conclusions.

- **Testifying**

This phase involves presentation and cross-examination of expert witnesses. Depending on the country and legal frameworks in which a cybercrime case is registered, certain standards may apply with regard to the issues of expert witnesses.

- **Chain of Custody Concept**
  1. Chain of custody is the central concept in cyber forensics/digital forensics investigation.
  2. The purpose of the chain of custody is that the proponent of a piece of evidence must demonstrate that it is what it purports to be.
  3. The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition until its final disposition.

- **Network Forensics**

Recall the mention of network forensics. We have already discussed that open networks can be the source of many network-based cyberattacks. A situation like this leads to the point that network forensics professionals need to understand how wireless networks work and the fundamentals of related technology.

Wireless forensics is a discipline included within the computer forensics science, and specifically, within the network forensics field. The goal of wireless forensics is to provide the methodology and tools required to collect and analyze (wireless) network traffic that can be presented as valid digital evidence in a court of law.

- **Approaching a Computer Forensics Investigation**

From the discussion so far, we can appreciate that computer forensics investigation is a detailed science. Now, let us understand how a forensics investigation is typically approached and the broad phases involved in the investigation. The phases involved are as follows:

1. Secure the subject system (from tampering or unauthorized changes during the investigation);
2. take a copy of hard drive/disk (if applicable and appropriate);
3. identify and recover all files (including deleted files);
4. access/view/copy hidden, protected and temp files;
5. study "special" areas on the drive (e.g., the residue from previously deleted files);
6. investigate the settings and any data from applications and programs used on the system;
7. consider the system as a whole from various perspectives, including its structure and overall contents;
8. consider general factors relating to the user's computer and other activity and habits in the context of the investigation;

9. create detailed and considered report, containing an assessment of the data and information collected.

- **Typical Elements Addressed in a Forensics Investigation Engagement Contract**

Typically, the following important elements are addressed before while drawing up a forensics investigation engagement contract

1. Authorization
2. Confidentiality
3. Payment
4. Consent and acknowledgment
5. Limitation of liability

Laboratory responsible for any accidental damages to the data or equipment in its possession including but not limited to surface scratches, deformations and cracks.

1. **Customer's representation:** Customer needs to warrant the forensics laboratory that he/she is the owner of, and/or has the right to be in possession of, all equipment/data/media furnished to the laboratory and that collection, possession, processing and transfer of such equipment/data/media are in compliance with data protection laws to which customer is subject to.

2. **Legal aspects/the law side:** Both the parties need to agree that the agreement shall be governed by prevailing law in every particular way including formation and interpretation and shall be deemed to have been made in the country where the contract is signed.

3. **Data protection:** The computer forensics laboratory (engaged in the investigation) will hold the information that the customer has given verbally, electronically or in any submitted form for the purpose of the forensics investigation to be carried out as per contracted services from the forensics laboratory.

4. **Waiver/breach of contract:** The waiver by either party of a breach or default of any of the provisions on this agreement by either party shall not be construed as a waiver of any succeeding breach of the same or other provisions, nor shall any delay or omission on the part of either party to exercise or avail itself of any right, power or privilege that it has, or may have hereunder operates as a waiver of any breach or default by either party.

→ **Solving a Computer Forensics Case**

These are just some broad illustrative steps and they may vary depending on the specific case in hand.

1. Prepare for the forensics examination.
2. Talk to key people to find out what you are looking for and what the circumstances surrounding the case are.
3. If you are convinced that the case has a sound foundation, start assembling your tools to collect the data in question. Identify the target media.
4. Collect the data from the target media. You will be creating an exact duplicate image ofthe device in question. To do this, you will need to use an imaging software application like the commercial in Case or the open-source Sleuth Kit/Autopsy.
5. To extract the contents of the computer in question, connect the computer you are investigating to a portable hard drive or other storage media and then boot the computer under investigation according to the directions for the software you are using.
6. When collecting evidence, be sure to check E-Mail records as well. Quite often, these messages yield a great deal of information.
7. Examine the collected evidence on the image you have created. Document anything that you find and where you found it.
8. Analyze the evidence you have collected by manually looking into the storage media and, if the target system has a Windows OS, check the registry.
9. Report your findings back to your client. Be sure to provide a clear, concise report; this report may end up as evidence in a court case.

- **Setting up a Computer Forensics Laboratory Understanding the Requirements**

There are four broad types of requirements, namely, the physical space, the hardware equipment, the software tools and the forensics procedures to be followed to aid those involved in the cybercrime investigation.

Fig: Cyber forensics laboratory– 1

Fig: Cyber forensics laboratory – 2

Apart from the physical space requirement, another key requirement for a computer forensics laboratory is the hardware items. The laboratory requires a number of computers,

including a network server with a large storage capacity (preferably configured for the standard removable hard drives).

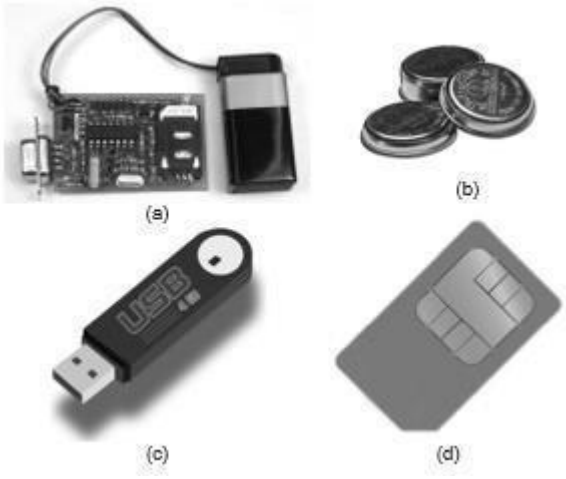


Fig: (a) SIM card reader, (b) iButtons, (c) flash memory, (d) SIM card.

On the software side, there are several requirements for setting up a forensics laboratory. The standard forensics software package, such as EnCase, Web Case, Forensics Tool Kit, Password Recovery Tool Kit, etc. are expensive products.

The main issues that are attacked when evidence is presented in a court of law are credentials and methodology. In some countries, the court may prefer the forensics evidence from government appointed and/or neutral party laboratories rather than the evidence from private agencies where opportunities for manipulation/exploitation are perceived.

- **Computer Forensics and Steganography**

Steganography is the art of information hiding. The threat raised by steganography is very real. Its use is not easy to detect or intercept, as the information does not need to be broadcast across the Internet. the hidden message can reside unsuspectingly on a website, for example, and can be viewed from around the world.

Steganography is the art of information hiding. The threat raised by steganography is very real. Its use is not easy to detect or intercept, as the information does not need to be broadcast across the Internet. The hidden message can reside unsuspectingly on a website, for example, and can be viewed from around the world.

Rootkits

The term rootkit is used to describe the mechanisms and techniques whereby malware including viruses, Spyware and Trojans attempt to hide their presence from Spyware blockers, antivirus and system management utilities.

Information Hiding

Let us now have an overview of some characteristics of information hiding and then we discuss about analysis methods for determining the existence of and potential locations of hidden information.

➔ Relevance of the OSI 7 Layer Model to Computer Forensics

The OSI 7 Layer Model is useful from computer forensics perspective because it addresses the network protocols and network communication processes. The basic familiarity with the OSI 7 Layer Model is assumed for the discussion in this section.

Step 1: Foot Printing

Foot printing includes a combination of tools and techniques used to create a full profile of the organization's security posture. These include its domain names, IP addresses and network blocks.

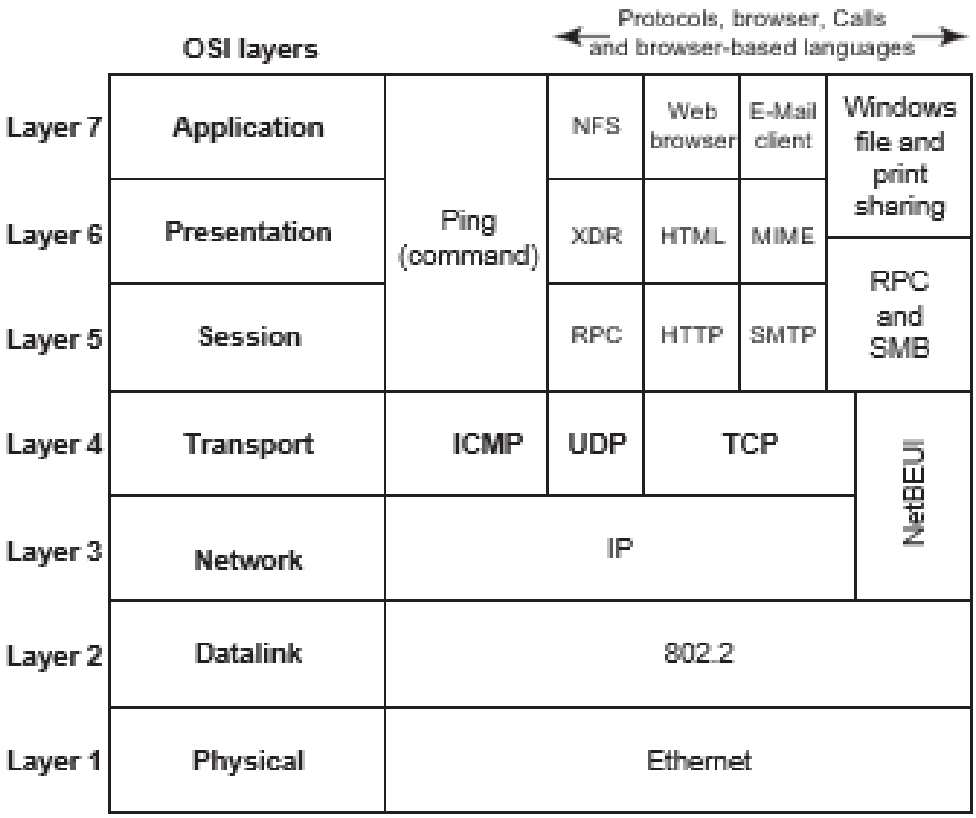


Fig: The OSI 7 Layer Model with Internet Protocols.

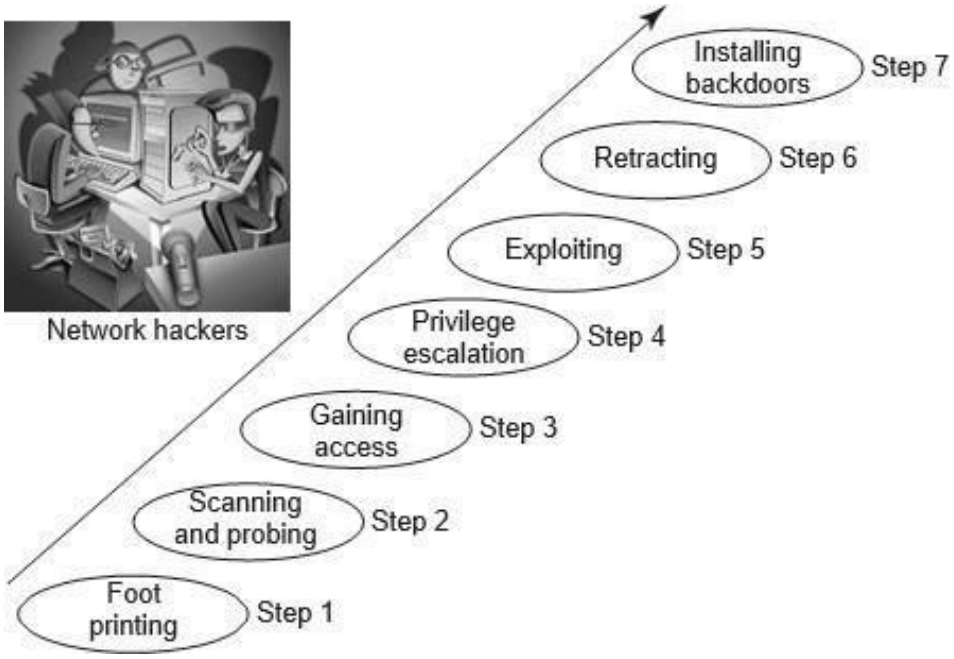


Fig: Network hacking steps

Step 2: Scanning and Probing

The hacker will typically send a ping echo request packet to a series of target IP addresses. As a result of this exploratory move by the hacker, the machines assigned to one of these IP address will send out echo response thereby confirming that there is a live machine associated with that address. Similarly, a TCP scan sends a TCP synchronization request to a series of ports and to the machines that provide the associated service to respond.

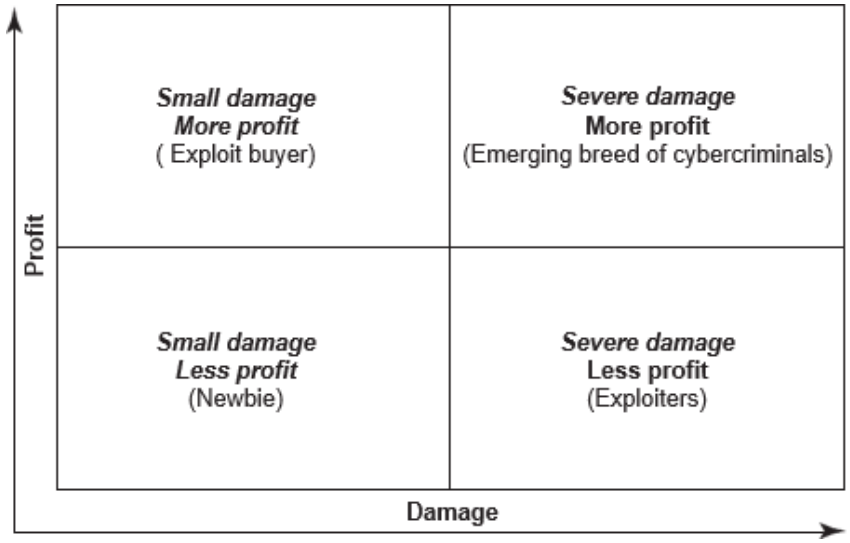


Fig. Hacker categories (profit and damage).

Step 3: Gaining Access

The hacker's ultimate goal is to gain access to your system so that he/she can perform some malicious action, such as stealing credit card information, downloading confidential files or manipulating critical data.

Step 4: Privilege

When a hacker gains access to the system, he will only have the privileges granted to the user or account that is running the process that has been exploited.

Step 5: Exploit

Gaining root access gives the hacker full control on the network. Every hacker seems to have his/her own reasons for hacking. Some hackers do it for fun or a challenge, some do it for financial gain and others do it to "get even".

Step 6: Retracting

There are many reasons that drive cybercriminals to hacking.

Step 7: Installing Backdoors

Finally, most hackers will try creating provisions for entry into the network/hacked system for later use. this, they will do by installing a backdoor to allow them access in the future.

➔ Computer Forensics from Compliance Perspective

With the rampant use of the Internet, there is so much at stake; corporate data is not safe anymore given that almost all information assets lie on the corporate networks. We are in the era of Net-centric digital economy.

Criminals can gather small pieces about you, about your confidential data to generate what is known as "digital persona," that is, they keep track about your Internet activities, what resides on your corporate networks, etc.

- **The Regulatory Perspective for Forensics at the International Level**

These laws/regulations specify investigation and response to security breaches or policy violations. Computer forensics makes it easier to meet these requirements.

These laws/legislations become relevant in the context of forensics with cybercrimes.

1. **The Sarbanes Oxley Act (SOX):** The Act was enacted to fight corporate fraud.

2. **California SB 1386**

3. **Gramm-Leach Bliley Act (GLBA)**

   The Safeguards Rule of GLB calls for financial institutions to:

   a) Ensure the security and confidentiality of customer information;
   b) Protect against any anticipated threats or hazards to the security or integrity of such information;

   c) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

4. **HIPAA (Health Insurance Portability and Accountability Act of 1996)**

HIPAA has the primary goal for healthcare providers to improve the privacy and security of their clients' medical information.

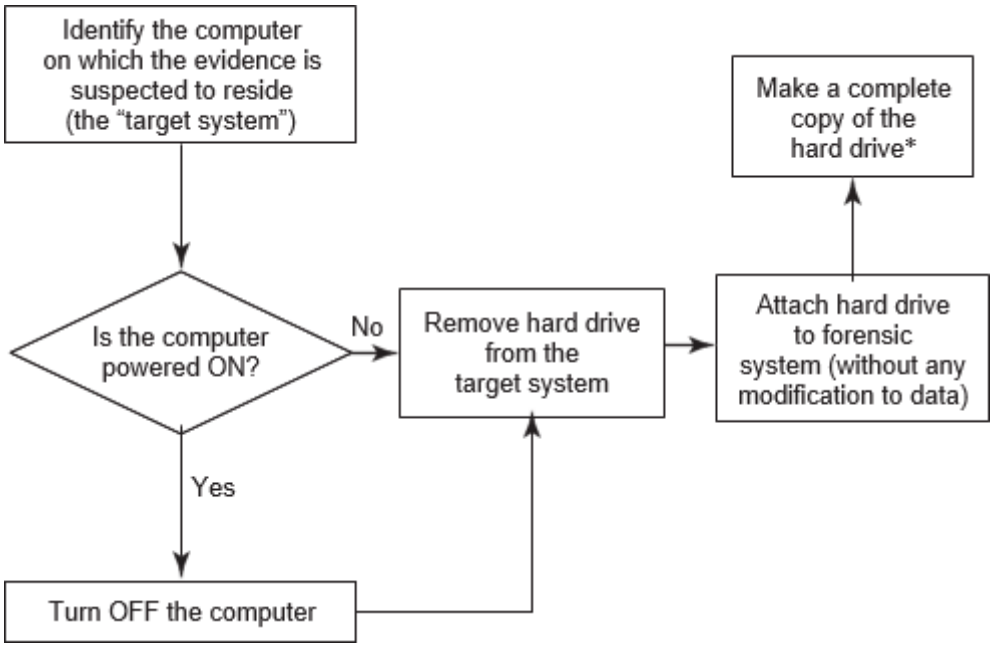


Fig: Traditional approach to forensics analysis. *denotes tools/devices mentioned

Unit-4

→ Forensics of Hand-Held Devices

"Computer forensics" is the application of forensic science techniques to the systematic discovery, collection and analysis of digital evidence. It is the preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis using well-defined methodologies and procedures.

Fig: Hand-held devices. (a) iPhone; (b) iPod; (c) palm pilot; (d) digital diary; (e) Smartphones; 2 GB MP2 player; (g) portable printer; (h) handycam and (i) PDA.

The methodology used is acquiring the evidence without altering or damaging (safe custody of the evidence) the original digital evidence, authenticating that the recovered evidence is the same as the original seized and analyzing the data without modifying it (chain of custody concept). They are relevant here too because we will be introducing some more legal aspects of forensics

The terms "device forensics" and "hand-held forensics" are used interchangeably.

According to the Internet and Mobile Association of India, Internet usage in the country has risen by 20% in the last year alone with people progressively spending more time online. Indians are increasingly accessing and transmitting sensitive information from their workstations/PCs, from home and while in transit through their laptops, netbooks or Smartphones.

➔ Understanding Cell Phone Working Characteristics

In modern times, cellular mobile phones have become an integral part of communication around the world. Forensics and digital analysis of mobile phones, therefore, is an area of interest, as crimes involving mobile devices are becoming increasingly common in the community.

While mobile phones outsell personal computers (PCs) three to one, mobile phone forensics still lags behind computer forensics.

- **Understanding the Types of Cellular Networks**

There are different types of digital cellular networks. these networks exist due to the distinct and incompatible sets of network protocol standards. the two most dominant types of digital cellular networks are:

1. Code Division Multiple Access (CDMA).
2. Global System for Mobile Communications (GSM) network.

There are other common cellular networks; they include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN). iDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols.

- **NTT DoCoMo**

Digital Advanced Mobile Phone Service (D-AMPS) is the digital version of the original analog standard for cellular telephone phone service. Now "Do Communication over the Mobile Network" (DoCoMo) is also available. NTT DoCoMo is Japan's largest wireless network carrier.

- **Cell Phones: Hardware and Software Features**

Different devices have different technical and physical features/characteristics (e.g., size, weight, processor speed and memory capacity). Devices may also use different types of expansion capabilities to provide additional functionality. Cell phone capabilities sometimes include those of other devices such as personal digital assistants (PDAs), global positioning systems (GPS) and cameras.

Irrespective of a cell phone type, all devices support voice and text messaging, a set of basic personal information management (PIM) applications including phonebook and date book facilities, and a means to synchronize PIM data with a desktop computer. More advanced devices also provide the ability to perform multimedia messaging, connect to the Internet and surf the Web, exchange E-Mail or chat using instant messaging.

➔ Hand-Held Devices and Digital Forensics

There is no dearth of hand-held devices in the modern world of today. The use of these devices is rampant given the modern lifestyles in our digital economy.

"Device forensics" has many aspects such as mobile phone forensics, PDA forensics, digital music forensics, iPod forensics and printer and scanner forensics.

o Mobile Phone Forensics

Mobile phone or cell phone is the most familiar hand-held device because it is the most ubiquitous one. Nathan B. Stubble field invented and patented the first mobile telephone 100 years ago.

As mentioned before, modern cell phones are highly mobile communications devices designed to perform a range of functions from that of a simple digital organizer to that of a low-end PC. Designed for mobility, they are compact in size, battery powered and lightweight, often use proprietary interfaces or OS and may have unique hardware characteristics for product diff erentiation.

"Mobile phone forensics" is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

The "IMEI number" (International Mobile Equipment Identity) of a cell phone is a very important starting point for the First Information Report (FIR) procedure as the FIR would most probably require the IMEI number as the basis when a compliant about a lost/stolen mobile phone is to be registered with the police. This is because a cell phone can be traced with its IMEI number.

Mobile device representation comes in various forms:

1. Cellular phones
   - CDMA: typically, handset only;
   - GSM: handset and SIM;
   - iDEN: handset and SIM.
2. PDAs
   - Palm Pilots (Palm OS);
   - Pocket PC's (Windows CE, Windows Mobile);
   - BlackBerry's (RIM OS) that contain no radio (cellular) capability;
   - others (Linux, Newton).
   - Smartphones: They are the hybrid between 1 and 2 have radio capability

- **PDA Forensics**

Personal digital assistant (PDA) is also referred to as "palm device" or "hand-held." The most common operating system (OS) used are the Palm OS (Palm, Sony, Handspring), Windows for Palm (HP), MS Pocket PC (Compaq), Embedix (Sharp).

PDAs differ in several important ways compared with PCs. PDAs vary in areas of OS, interface style and hardware components, and they work with different OS such as Linux, Palm OS and Microsoft Pocket PC.

Investigating crimes involving PDAs are more challenging than those involving normal computers. This is mainly because these devices are more compact, battery operated and store data in volatile memory.

Relevant software in this segment is listed below:

1. **PDD:** It is based on the Unix dd. This is the most popular Palm forensics software.
2. **CodeWarrior for Palm OS:** It is used to put palm devices into "Debug Mode." This allows communication via serial port, imaging and can be used to overcome lockout protection.
3. **PDA defense:** It is a third-party lockout software. It is difficult to bypass.

Forensics tools acquire data from a device in one of the following two ways: "physical acquisition" and "logical acquisition."

- **Printer Forensics**

One may wonder how printers can pose security risks. Printers are not generally considered to be "hand- held" devices although "portable printers" are now available in the market.

Modern day printers have computer-like characteristics with internal storage, FTP uploading, Simple Network Management Protocol (SNMP), etc. Some printers are loaded with vulnerable applications.

No two printers of the same model will behave in the exact same pattern. This is because the mechanical parts that make the printer will not be 100% equivalent.

- **Scanner Forensics**

Today, a large portion of digital image data is available. Acquisition devices such as digital cameras and scanners are used to create that data. With cameras, it is possible to digitally reproduce scenes that may look almost as real as natural scenes

- **Smartphone Forensics**

Workforce mobility is on the rise and Smartphones are gaining momentum as a device option for people working at the field (field workers include, e.g., sales personnel, technicians, insurance agents, medical officers, pathological laboratory technicians who offer door-to-door medical service, etc.). The main reason for rising popularity of Smartphones is their high functionality that comes in a relatively low-cost device.

Smartphones are mobile phones based on high-level OS that are open to third-party application development.

- **Printer Forensics**

One may wonder how printers can pose security risks. Printers are not generally considered to be "hand- held" devices although "portable printers" are now available in the market.

Modern day printers have computer-like characteristics with internal storage, FTP uploading, Simple Network Management Protocol (SNMP), etc. Some printers are loaded with vulnerable applications.

Possible attacks through printer exploits are as follows

1. Modifying IP address of the printer to an unused address on the same subnet.
2. Changing IP address of the target machine to the previous IP address of the printer.
3. Capturing all traffic sent over Port 9100 to the IP address to which end-users are configured to print. The attacker can keep collecting print jobs until it is found out.
4. Forwarding all print jobs onto the "new" IP address of the printer; when the end-user who submit- ted the jobgoes to the printer in question to collect the print job, he/she finds that it has been processed as normal.

- **Scanner Forensics**

Today, a large portion of digital image data is available. Acquisition devices such as digital cameras and scanners are used to create that data. With cameras, it is possible to digitally reproduce scenes that may look almost as real as natural scenes.

- **Smartphone Forensics**

  Workforce mobility is on the rise and Smartphones are gaining momentum as a device option for people working at the field (field workers include, e.g., sales personnel, technicians, insurance agents, medical officers, pathological laboratory technicians who offer door-to-door medical service, etc.).

  Smartphones are mobile phones based on high-level OS that are open to third-party application development.

- **iPhone Forensics**

  The iPhone was introduced by Apple Inc. in January 2007. Since then, Apple has sold more than 33 million iPhones and has now surpassed RIM (BlackBerry) as the third largest provider of Smartphones.

➔ **Toolkits for Hand-Held Device Forensics**

So far, we have been through the forensics aspects of PDAs, Smartphones, cell phones, printers, scanners, iPhones BlackBerrys and digital images/digital cameras.

Acquisition of data from a hand-held device is carried out in the following two ways:

1. Physical acquisition: In this particular type of acquisition, an exact copy bit-by-bit iscollected of the entire physical storage which can be either a RAM chip or a disk drive.

2. Logical acquisition: This is an exact copy bit-by-bit of the logical storage such as file and directories, involved residing on a logical store which could be several disk drives.

- **EnCase**

EnCase is a popular software toolkit for hand-held device forensics. Its features support many features: analytical tools, suspect media acquisition, data capture, documentation and search features.

- **Device Seizure and PDA Seizure**

These are two famous tools from Paraben. Paraben's device seizure is one of the many products used for viewing cell phone data.

- **Palm DD (PDD)**

There was a mention of this tool (PDA Forensics). The PDD tool runs only on Windows based systems and is mainly used by forensics examiners for physical acquisition.

- **Forensics Card Reader**

The Forensics Card Reader (FCR) consists of FCR software. It allows forensics examiners to acquire data from SIM cards without modification and a smart card reader with USB connection.

- **Cell Seizure**

Cell Seizure is a forensics software toolkit. It is used for acquiring, searching, examining and reporting data associated with cell phones operating over CDMA, TDMA and GSM networks.

Large type of data that can be obtained on most cell phones, using Cell Seizure includes:

1. **SMS history:** Inbox/outbox.
2. **Phonebook:** SIM card, own numbers, speed dialling, fixed dialling.
3. **Call logs:** Dialled numbers, received calls, missed calls.
4. **Calendar:** Reminder, meeting, memo.
5. **Graphics:** Wallpaper, picture camera images, EMS template images.
6. **Wireless Application Protocol (WAP):** WAP settings, WAP bookmarks.
7. **SIM:** GSM-specific data.

- **MOBILedit!**

This is a forensics application that allows examiners to acquire logically, search, examine and report data fromCDMA, Personal Communications Services (PCS) and GSM cell phones.

- **Forensic SIM**

This toolkit comes from Radio Tactic. Its components include: acquisition terminal, analysis application, control card, data storage cards and the card reader.

➔ **Forensics of iPods and Digital Music Devices**

In this section we focus on discussion about iPods and other hand-held devices available for music in digital form. Apple is the leading brand in the market today and there are three separate digital media players available from Apple Inc. All the players from Apple have the iPod brand – they are either the original iPod, the iPod Nano or an iPod shuffle.

- **The New Avatar of Digital Music Hand-Held Devices**

Storage capacities of hand-held devices as well as the functionalities of PDAs are continuously improving. Many digital music devices have emerged with additional functionality than just playing music.

Criminals can use the iPod with all its features in a variety of ways. Calendar entries may contain dates of crimes or other events that could be related to a crime. The contact information of conspirators or victims, along with photos or other documentation, could all be transferred and stored on the iPod.

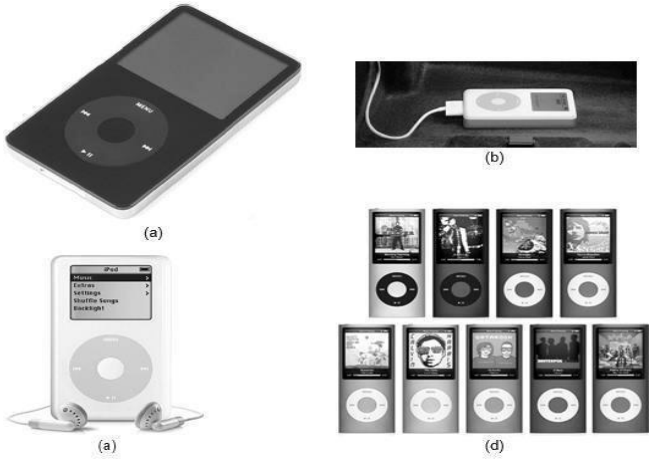


Fig: Apple iPods. (a) Apple iPOD (regular), (b) Apple iPOD (mini), (c) Apple iPOD (fourth generation) and (d) Apple iPOD

- **iPod Forensics: Evidence Handling and Crime Scene Considerations**

As mentioned before, the iPod is one of the most popular digital music devices in today's marketplace. The newest versions of the iPod have become similar to PDA/storage like never before.

The market for digital music device is continuously growing - with that comes higher use of iPods in criminal activity.

Here are some important considerations when an iPod is found at a crime scene:

1. Before collecting any evidence, the first responder should wait for the advice of a forensics specialist.
2. Documentation of device location on the crime scene should be notedtaking a photograph of its location along with the photograph of anything around the device.
3. The device should be left in its current state, as it is possible that the device could be booby trapped with a delete command set to execute if the device is disconnected from a charger or computer.

➔ **Techno-Legal Challenges with Evidence from Hand-Held Devices**

Hackers are getting sophisticated. This is true for mobile phone-based crimes as well as crimes performed with other small hand-held devices.

"Forensically sound" evidence is required for presentation in the court.

- **Role of Computer Forensics in Litigations**

Computers have appeared in the course of litigation for several years.

The arrival of computers in commercial disputes and in criminal cases did not create immediate difficulties as judges sought to allow computer-based evidence on the basis that it was not any different from traditional forms of evidence.

The ultimate aim of a forensics investigation is that the evidence can be used in legal proceedings. As we have learned by now, forensic computer examinations are unlike ordinary data recovery eff orts.

Computer evidence in the court is used by the following entities

1. **Criminal Prosecutors:** They use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record keeping and child pornography.
2. **Civil litigations:** They can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination and harassment cases.
3. **Insurance Companies** may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson and workman's compensation cases.
4. **Corporations** often hire computer forensics specialists to ascertain evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.
5. **Law Enforcement Officials** frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
6. **Individuals** sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment or age discrimination.

- **Challenges Due to Forensics Validity Issues about Evidences**

There are many issues and challenges. Such issues can pose a threat to the validity of mobile phone forensics. For example, there are difficulties in acquiring certain types of data that stem from the proprietary nature of mobile phones.

Proprietary OS makes retrieving information from phone memory difficult.

Some of the current mobile forensics tools claim that they acquire evidence from mobile phones in a forensically sound manner, and maintain their integrity upon further examination.

- **Challenges to Law Enforcement Authorities**

There are additional challenges apart from the "evidence integrity" issues mentioned in the previous section. When it comes to dealing with digital evidence obtained from mobile devices, law enforcement and digital forensics still lag behind. ftis could be partly due to some of the following reasons

1. Specialized interfaces, storage media and hardware are required to support evidence extraction given the mobility aspects of modern hand-held devices.
2. the diff erence between file system residing in volatile memory vs. stand-alone hard disk drives.
3. hibernation behavior in which processes are suspended when the device is powered OFF or is idle but at the same time, remaining active.
4. the diverse variety of embedded OS in use today.
5. the short product cycles for new devices and their respective OS.

A key difference between computers and mobile phones is the data storage medium. While volatile memory is used to store user data in mobile phones, computers use non-volatile hard disk drives instead as a storage medium.

Mobile phone hardware architecture is designed keeping in mind features such as mobility, extended battery life, simple functionality and light weight. Owing to this architecture, the general characteristics of a mobile phone are very different from those of a computer in the way it uses the OS, how its processor behaves and how it handles its internal and external memory.

- **Toolkit Constraints**

There are constraints for forensics tools and toolkits too and that is for historical reasons. When initially mobile phones came into market, they did not have the capacity for large amount of information storage.

There are third-party companies that develop mobile forensics toolkits. However, the toolkits are not independently verified or tested for forensics soundness.

- **Generally Accepted Evidence Principles and the Difference with Hand-Held Devices**

Principles that are generally accepted in the forensics community about computer based electronic evidence are as follows:

1. Actions taken by law enforcement agencies or by their agents should NOT modify data held on a computer or storage media because this is the data on which in the court relies upon.

Exceptional circumstances are to be considered

Typically, potential evidences considered from small hand-held devices are appointment calendars/ information, password, caller identification information, phone book, electronic serial number, text messages, E-Mail, voice mail, memos and web browsers. However, it should not be forgotten that mobile devices could have external storage attached to them.

When it comes to handling instructions for mobile phones, the following key principles should be remembered:

Evidence may get lost during any interaction with the handset on a mobile phone; therefore, it is important not to interrogate the handset or SIM.

Before handling the evidence, consider if any other evidence is required from the phone. In case additional evidence, apart from electronic data, is required, adhere to the general evidence handling procedures for that particular type of evidence laid out in the scenes of crime handbook.

- **Battery and Memory Storage Considerations from Forensics Perspective**

Typically, three types of batteries are used in mobile phones: Liion (lithiumion), NiMH (nickel metal hydride) and Lipolymer.

Unit-5

Cybersecurity: Organizational Implications

In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices or intense scans from criminal groups.

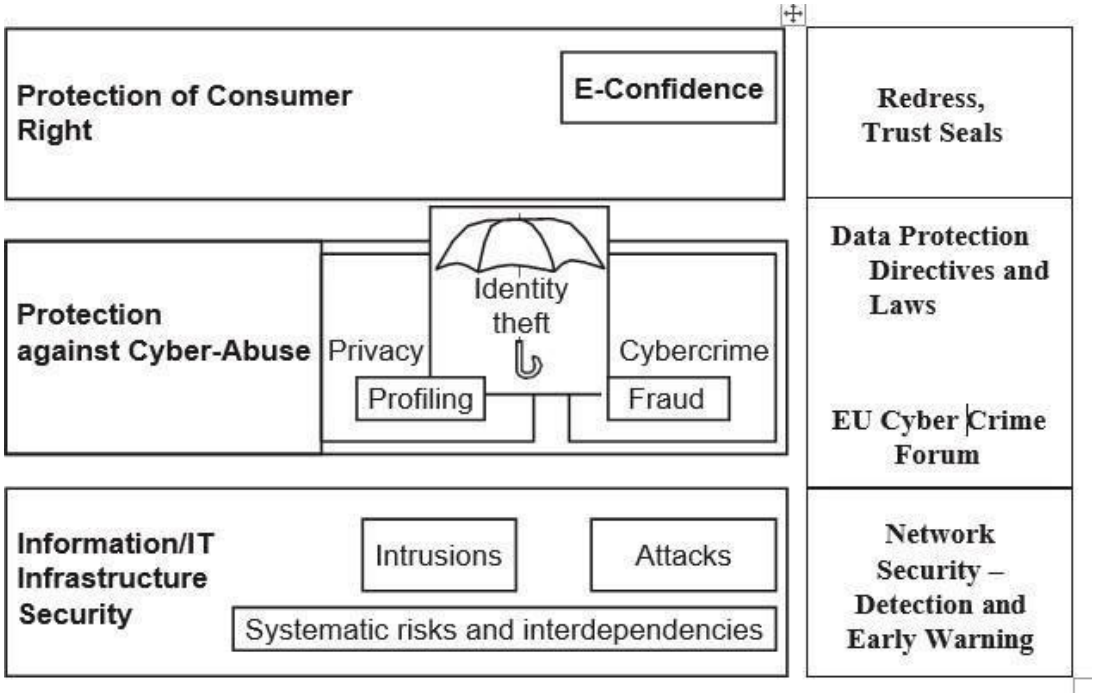


Fig: A cybersecurity perspective. EU is the European Union.

PI is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Most information the organization collects about an individual is likely to come under "PI" category if it can be attributed to an individual. For an example, PI is an individual's first name or first initial and last name in combination with any of the following data:

1. Social security number (SSN)/social insurance number.
2. Driver's license number or identification card number.
3. Bank account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account.
4. Home address or E-Mail address.
5. Medical or health information.

An insider threat is defined as "the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other 'trusted' individuals."

Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of "insiders" such as:

1. A malicious insider is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrity and/or availability.
2. A careless insider can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.
3. A tricked insider is a person who is "tricked" into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via "pretexting" (known as social engineering).

- **Insider Attack Example 1: Heartland Payment System Fraud**

A case in point is the infamous "Heartland Payment System Fraud" that was uncovered in January 2010. This incident brings out the glaring point about seriousness of "insider attacks. In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is trans- mitted through a payment network.

- **Insider Attack Example 2: Blue Shield Blue Cross (BCBS)**

Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private information of approximately 500,000 customers at risk in at least 32 states. The two lessons to be learnt from this are:

1. Physical security is very important.
2. Insider threats cannot be ignored.

What makes matters worse is that the groups/agencies/entities connected with cybercrimes are all linked. There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc. to name a few.

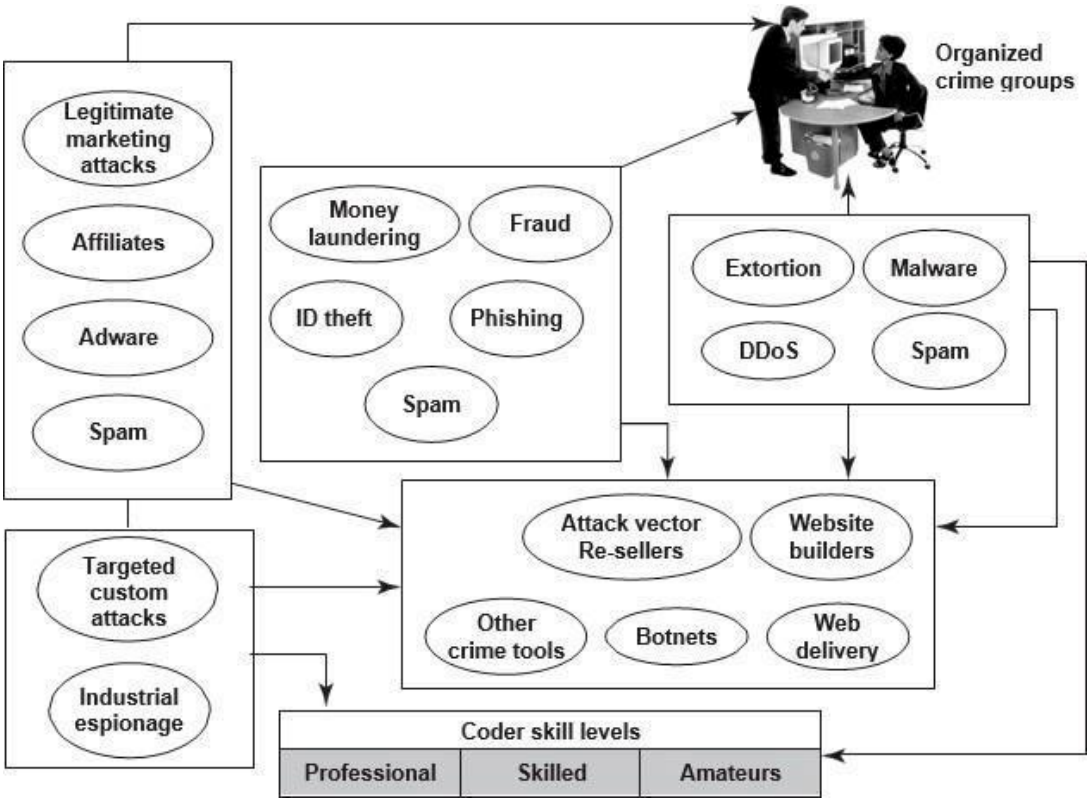


Fig: Cybercrimes – the flow and connections.

A key message from this discussion is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cybersecurity practices and "privacy" which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

1. **Informational/data privacy:** It is about data protection, and the users' rights to determine how, when and to what extent information about them is communicated to other parties.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.
3. **Communication privacy:** This is as in networks, where encryption of data being transmitted is important.
4. **Territorial privacy:** It is about protecting users' property for example, the user devices from being invaded by undesired content such as SMS or E-Mail/Spam messages. The paradigm shift in computing brings many challenges for organizations; some such key challenges are described here.

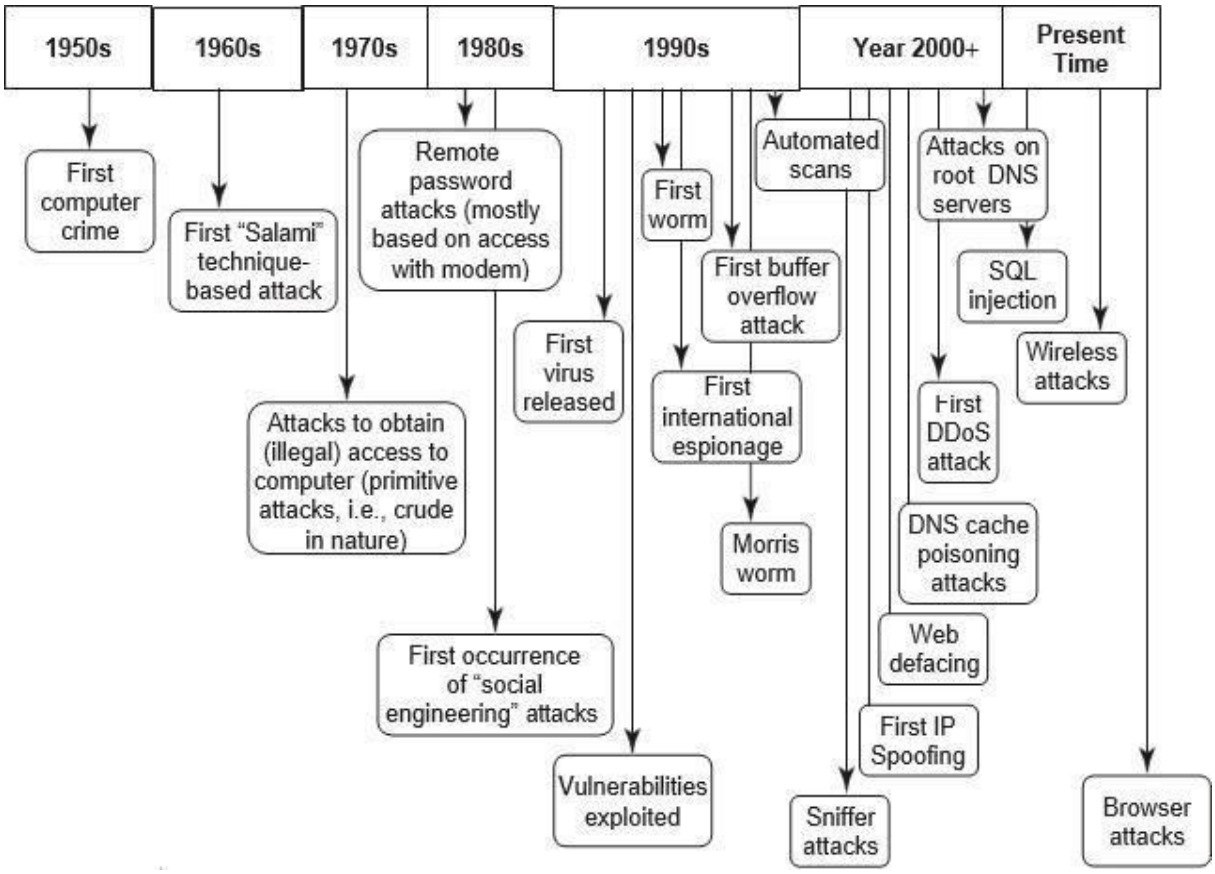


Fig: Security threats – paradigm shift.

The key challenges from emerging new information threats to organizations are as follows:

1. **Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names.
3. **IP-based "cloaking":** Businesses are global in nature and economies are interconnected.
4. **Cyberterrorism:** "Cyberterrorism" refers to the direct intervention of a threat source toward your organization's website.
5. **Confidential information leakage:** "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solutions.

➔ **Cost of Cybercrimes and IPR Issues: Lessons for Organizations**

Reflecting on the discussion in the previous sections brings us to the point that cybercrimes cost a lot to organizations.

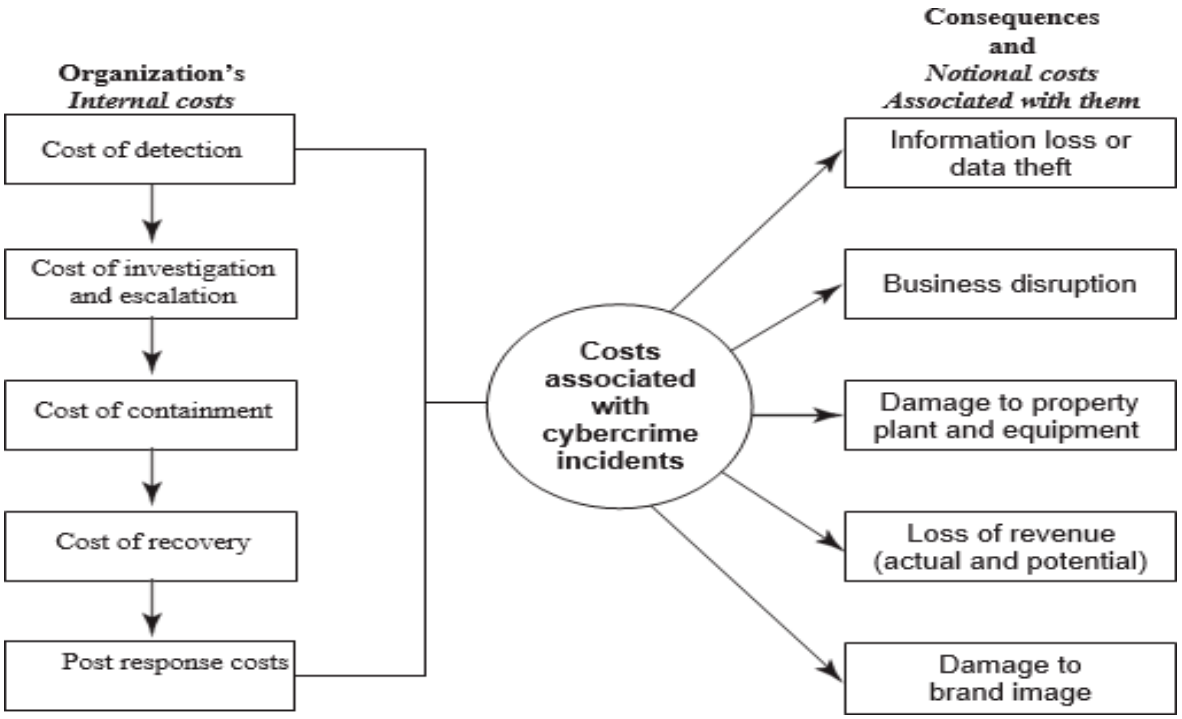


Fig: Cost of cybercrimes.

When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

Detection and recovery constitute a very large percentage of internal costs. This is supported by a benchmark study conducted by Ponemon Institute USA carried out with the sample of 45 organizations representing more than 10 sectors and each with a head count of at least 500 employees.

- **Organizations have Internal Costs Associated with Cybersecurity Incidents**

The internal costs typically involve people costs, overhead costs and productivity losses. The internal costs, in order from largest to the lowest and that has been supported by the benchmark study mentioned:

1. Detection costs.
2. Recovery costs.
3. Post response costs.
4. Investigation costs.
5. Costs of escalation and incident management.
6. Cost of containment.

- **The consequences of cybercrimes and their associated costs, mentioned**
  1. Information loss/data theft.
  2. Business disruption.

3. Damages to equipment, plant and property.
4. Loss of revenue and brand tarnishing.
5. Other costs.

- **There are many new endpoints in today's complex networks; they include hand-held devices.**

Again, there are lessons to learn:

1. **Endpoint protection:** It is an often-ignored area but it is IP-based printers, although they are passive devices, are also one of the endpoints.
2. **Secure coding:** These practices are important because they are a good mitigation control to protect organizations from "Malicious Code" inside business applications.
3. **HR checks:** These are important prior to employment as well as after employment.
4. **Access controls:** These are always important, for example, shared IDs and shared laptops are dangerous.
5. **Importance of security governance:** It cannot be ignored policies, procedures and their effective implementation cannot be over-emphasized.

- **Organizational Implications of Software Piracy**

Use of pirated software is a major risk area for organizations.

From a legal standpoint, software piracy is an IPR violation crime. Use of pirated software increases serious threats and risks of cybercrime and computer security when it comes to legal liability.

The most often quoted reasons by employees, for use of pirated software, are as follows:

1. Pirated software is cheaper and more readily available.
2. Many others use pirated software anyways.
3. Latest versions are available faster when pirated software is used.

➔ **Web Threats for Organizations: The Evils and Perils**

Internet and the Web is the way of working today in the interconnected digital economy. More and more business applications are web based, especially with the growing adoption of cloud computing.

- **Overview of Web Threats to Organizations**

The Internet has engulfed us! Large number of companies as well as individuals have a connection to the Internet. Employees expect to have Internet access at work just like they do at home.

IT managers must also find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

- **Employee Time Wasted on Internet Surfing**

This is a very sensitive topic indeed, especially in organizations that claim to have a "liberal culture." Some managers believe that it is crucial in today's business world to have the finger on the pulse of your employees.

People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.

- **Enforcing Policy Usage in the Organization**

An organization has various types of policies. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization.

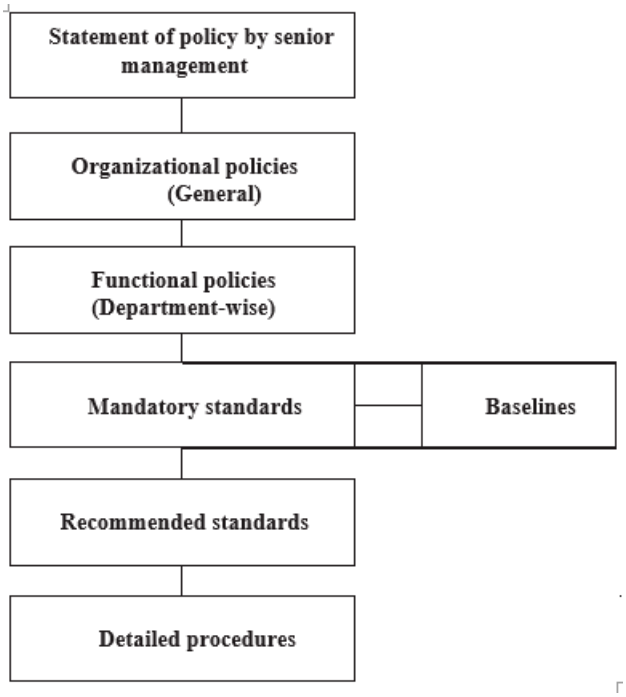


Fig: Policy hierarchy chart.

- **Monitoring and Controlling Employees' Internet Surfing**

A powerful deterrent can be created through effective monitoring and reporting of employees' Internet surfing.

Even organizations with restrictive policies can justify a degree of relaxation; for example, allowing employees to access personal sites only during the lunch hour or during specified hours.

- **Keeping Security Patches and Virus Signatures Up to Date**

Updating security patches and virus signatures have now become a reality of life, a necessary activity for safety in the cyberworld! Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management.

- **Surviving in the Era of Legal Risks**

As website galore, most organizations get worried about employees visiting inappropriate or offensive websites. We mentioned about Children's Online Privacy Protection.

Serious legal liabilities arise for businesses from employee's misuse/inappropriate use of the Internet.

- **Bandwidth Wastage Issues**

Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images.

There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

- **Mobile Workers Pose Security Challenges**

Use of mobile handset devices in cybercrimes. Most mobile communication devices for example, the personal digital assistant

- **Challenges in Controlling Access to Web Applications**

Today, a large number of organizations' applications are web based. There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications.

- **The Bane of Malware**

Many websites contain malware. Such websites are a growing security threat. Although most organizations are doing a good job of blocking sites declared dangerous, cyber attackers, too, are learning. Criminals change their techniques rapidly to avoid detection.

- **The Need for Protecting Multiple Offices and Locations**

Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today. Most large organizations have several offices at multiple locations.

➔ **Social Media Marketing: Security Risks and Perils for Organizations**

Social media marketing has become dominant in the industry.

According to fall 2009 survey by marketing professionals, usage of social media sites by large business-to-business (B2B) organizations shows the following:

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. My Space is used by 6% of the organizations.

Although the use of social media marketing site is rampant, there is a problem related to "social computing" or "social media marketing" – the problem of privacy threats.

Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of "social media marketing."

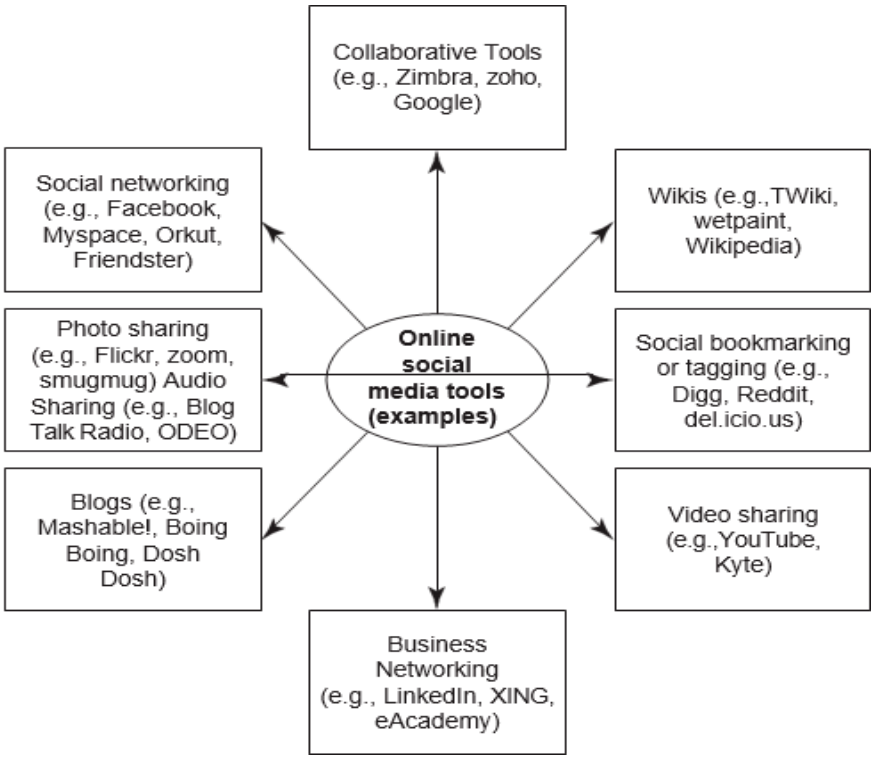


Fig: Social media - online tools.

- **Understanding Social Media Marketing**

Most professionals today use social technologies for business purposes. Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development.

Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
2. To increase traffic to their website coming from other social media websites by using Blogs and social and business-networking. Companies believe that this, in turn, may increase their "page rank" resulting in increased traffic from leading search engines.
3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
4. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.

5. To collect potential customer profiles. Social media sites have information such as user profile data, which can be used to target a specific set of users for advertising

There are other tools too that organizations use; industry practices indicate the following:

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
2. Professional networking tool LinkedIn is used to connect with and create a community of top executives from the Fortune 500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
4. YouTube (the video capability tool to run demonstrations of products/services, etc.) is used to increase the brand awareness and create a presence for corporate videos.
5. Wikipedia is also used for brand building and driving traffic.

Security and Privacy Implications from Cloud Computing

There are data privacy risks associated with cloud computing. Basically, putting data in the cloud may impact privacy rights, obligations and status. There is much legal uncertainty about privacy rights in the cloud. Organizations should think about the privacy scenarios in terms of "user spheres."

There are three kinds of spheres and their characteristics are as follows:

1. **User sphere:** Here data is stored on users' desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to users and monitor that access to ensure misuse does not happen.
2. **Recipient sphere:** Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data.
3. **Joint sphere:** Here data lies with web service provider's servers and databases. This is the in between sphere where it is not clear to whom does the data belong.

➔ Protecting People's Privacy in the Organization

The costs associated with cybercrimes. A key point in that discussion is that people perceive their PI/SPI to be very sensitive. From privacy perspective, people would hate to be monitored in terms of what they are doing, where they are moving.

In the US, Social Security Number is a well-established system/mechanism for uniquely identifying all American citizens; however, similar thoughts are now emerging in India. The UID Project was started by Government of India and is running through an agency called Unique Identification Authority of India (UIDAI) based on the similar concept.

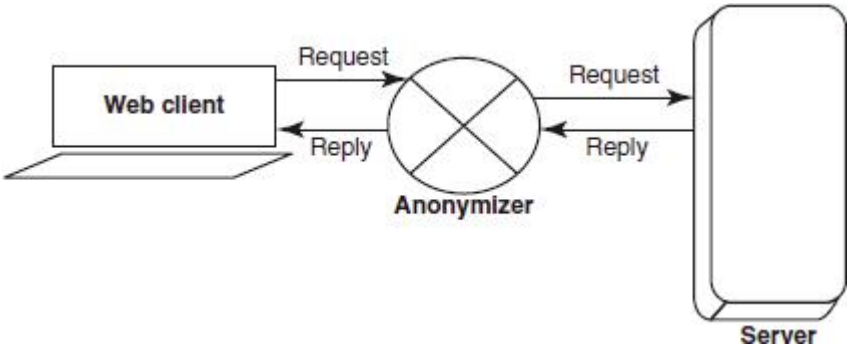


Fig: Anonymity by web proxy.

➔ **Forensics Best Practices for Organizations**

This section focuses on forensics readiness of organizations. Organization's forensics readiness is important forensics readiness is defined as the ability of an organization to maximize its potential to use digital evidence while minimizing the costs of an investigation.

Preparation to use digital evidence is not easy – it involves system and staff monitoring, technical, physical and procedural means to secure data to evidential standards of admissibility, processes and procedures. All this becomes essential for ensuring that staff recognizes the importance and legal sensitivities of evidence, and appropriate legal advice and interfacing with law enforcement.

The prime factor in understanding the need for forensics readiness is a risk assessment.

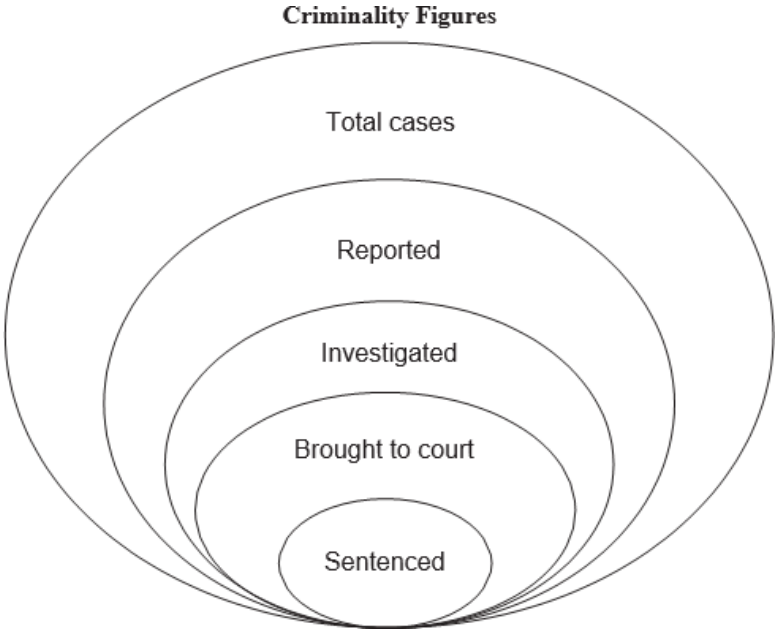


Fig: Cyber forensics and case investigation: Where it ends.

- **Organizations must Understand Digital Forensics Investigation and Digital Evidences**

Organizations must appreciate that the quality and availability of evidence is a passive aspect of the DFI.

Cybercriminals are known to exploit the fact that investigation is costly and takes time.

The categories of guiding procedures and activities that facilitate DFI are as follows:

1. Retaining information;
2. Planning the response;
3. Training;
4. Accelerating the investigation;
5. Preventing anonymous activities;
6. Protecting the evidence.

- **Concerns with Being a Forensically Ready Organization**

An eff ective incident response system is pertinent to an organization's forensics readiness this is because digital evidence is required whenever it can be used to support a legal process.

- **Key Activities for Organizations Getting Forensically Ready**

In the context of forensic readiness discussion, the key activities are presented. These are the activities that an organization should consider if they wish to be forensically ready.

- **Benefits of Being a Forensically Ready Organization**

To conclude the discussion on forensics readiness, we present the benefits that an organization can derive from its forensics readiness:

1. The ability to gather evidence that can serve in the company's defense if subjected to a lawsuit.
2. Comprehensive evidence gathering can be developed as a deterrent to the insider threat
3. In case of a major incident, a rapid and efficient investigation can be conducted and actions can be taken with a view to minimal disruption to the business.
4. Reduction in cost and time of an internal investigation through a systematic approach to evidence storage.
5. A structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data.
6. Forensics readiness can widen the scope of information security to the wider threat from cybercrime, such as IP protection, fraud or extortion.
7. It demonstrates due diligence and good corporate governance of the company's information assets.
8. It can improve and facilitate the interface to law enforcement, if involved.
9. It can improve the prospects for a successful legal action.
10. It can provide evidence to resolve a commercial dispute.

It can support employee sanctions based on digital evidence.