UNIT-1 (Syllabus)

Text Book-1(TB1): Sunit Belapure Nina Godbole “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, WILEY, 2011.

TB1: Chapter 1.1 to 1.5

Introduction to Cybercrime**:** Introduction, Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Cyber criminals, Classifications of Cybercrime,

TB1: Chapter 2.4 to 2.7

Cyberstalking, Cybercafe and Cybercrimes, Botnets. Attack Vector,

TB1: Chapter 3.1, 3.2, 3.3, 3.5 to 3.8

Proliferation of Mobile and Wireless Devices, Security Challenges Posed by Mobile Devices, Attacks on Mobile/Cell Phones.

INTRODUCTION TO CYBERCRIME:

- INTRODUCTION
- CYBERCRIME: DEFINITION AND ORIGIN
- CYBERCRIME AND INFORMATION SECURITY
- WHO ARE CYBERCRIMINALS?
- CLASSIFICATIONS OF CYBERCRIMES



UNIT-1 (PART-A)

INTRODUCTION



- The phenomenal growth of Internet
- Unrestricted access to information on internet has lead to Cybercrime.
- These activities include the use of Computers, Internet, Cyberspace and the WWW.
- The Frist Recorded Cyber Crime : 1820
- Around 2328 cyber crimes are thought to occur each day. Over the last 21 years from 2001 to 2021, cyber crime has claimed at least 6.5 million victims with an estimated loss of nearly $26 billion over the same period.
- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.

INTRODUCTION (CONT..)

CYBER SECURITY

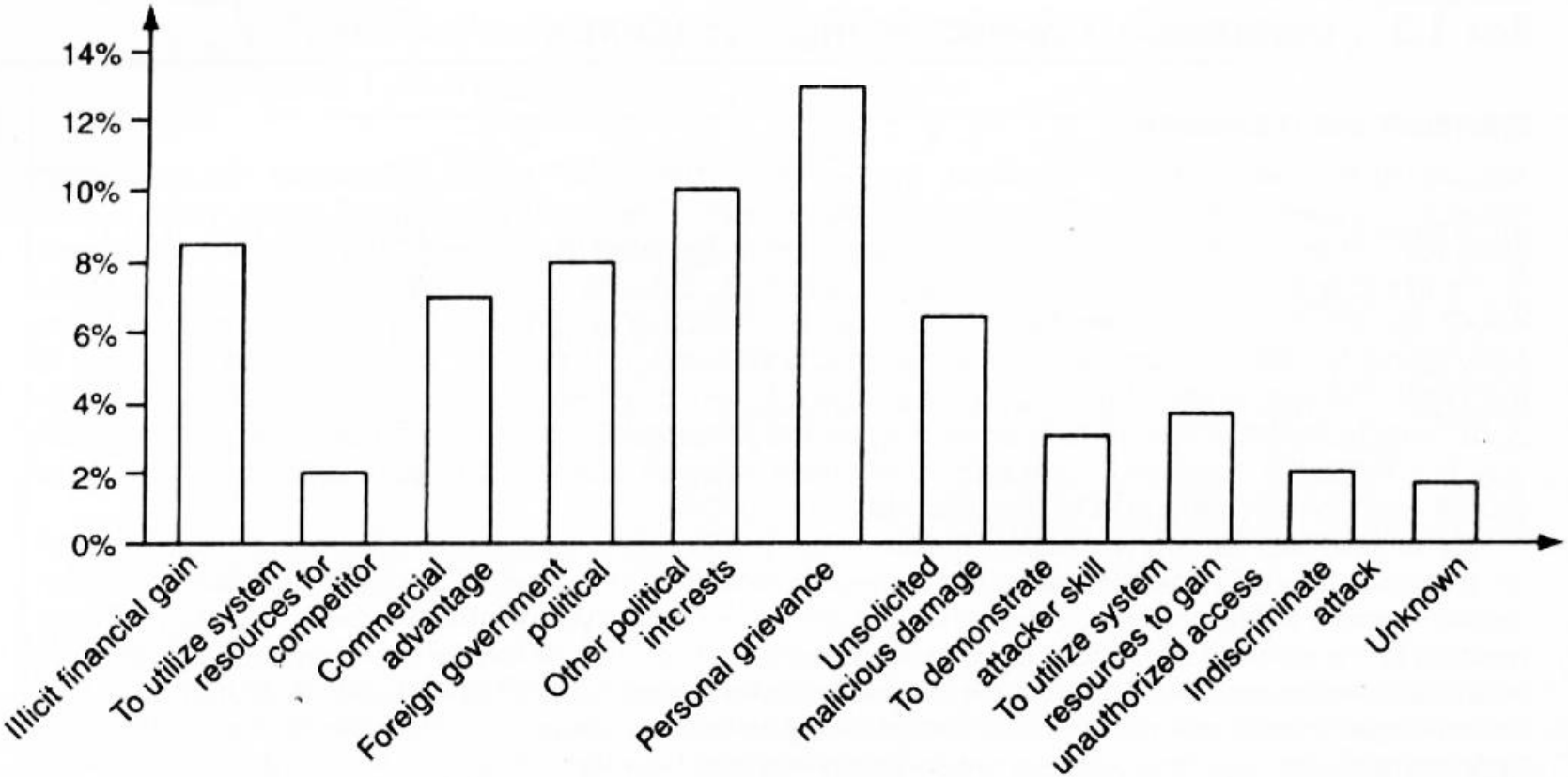


Fig: Cyber Crime Trend (2008 statistics)

CYBER CRIME: DEFINITION & ORIGINS



- "A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime."

- Alternative definitions of Cybercrime are as follows:
  1. Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.
  2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
  3. Any financial dishonesty that takes place in a computer environment.
  4. Any threats to the computer itself, such as theft of hardware or software, damage and demands for money.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)



- "Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them."

- Synonyms:
  - Computer-related crime, Computer crime, Internet crime, E-crime, High-tech crime, etc.

- Cybercrime specifically can be defined in a number of ways; a few definitions are:
  1. A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
  2. Crimes completed either on or with a computer.
  3. Any illegal activity done through the Internet or on the computer.
  4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW

CYBER CRIME: DEFINITION & ORIGINS (CONT..)



- Cybercrime is any criminal activity which uses network access to commit a criminal act.
- Cybercrime refers to the act of performing a criminal act using cyberspace as the communications vehicle.
- Cybercrime may be internal or external.
- Some people argue that a cybercrime is not a crime as it is a crime against software and not against a person or property.
- The legal systems around the world scramble to introduce laws to combat cyber criminals, 2 types of attacks are prevalent:
  1. **Techno-crime:** A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system.
  2. **Techno-vandalism:** These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)



- There is a very thin line between the two terms “computer crime” and “computer fraud”; both are punishable.
- Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways:
  a. how to commit them is easier to learn,
  b. they require few resources relative to the potential damage caused,
  c. they can be committed in a jurisdiction without being physically present in it &
  d. they are often not clearly illegal.
- The term ***cyber*** has some interesting synonyms: fake, replicated, pretend, imitation, virtual, computer generated. Cyber means combining forms relating to Information Technology, the Internet and Virtual Reality
- Important Definitions related to Cyber Security:

Cyber Space, Cybersquatting , Cyberpunk & Cyberwarfare, Cyberterrorism

CYBER CRIME: DEFINITION & ORIGINS (CONT..)



Cyberspace:

- This is a term coined by William Gibson, a science fiction writer in 1984.
- Cyberspace is where users mentally travel through matrices of data. Conceptually, cyberspace is the nebulous place where humans interact over computer networks.
- The term “cyberspace” is now used to describe the Internet and other computer networks.
- In terms of computer science, “cyberspace” is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data.
- Cyberspace is most definitely a place where you chat, explore, research and play.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)



Cybersquatting :

- The term is derived from “squatting” which is the act of occupying an abandoned/unoccupied space/ building that the user does not own, rent or otherwise have permission to use.
- Cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else’s trademark. In this nature, it can be considered to be a type of cybercrime. Cybersquatting is the practice of buying “domain names” that have existing businesses names.
- The World Intellectual Property Organization (WIPO) has also outlined anti-cybersquatting tactics. which hove been endorsed by Internet Corporation for Assigned Names and Numbers (ICANN).
- In India, Cybersquatting is considered to be an Intellectual Property Right (IPR). In India, Cybersquatting is seen to interfere with “Uniform Dispute Resolution Policy” (a contractual obligation to which all domain name registrants are presently subjected to).

CYBER CRIME: DEFINITION & ORIGINS (CONT..)



Cyberpunk :

- According to science fiction literature, the words “cyber” and “punk” emphasize the two basic aspects of cyberpunk: “technology” and “individualism.”
- The term “cyberpunk” could mean something like “anarchy via machines” or “machine/computer rebel movement.”

Cyberwarfare:

- Cyberwarfare means information attacks against an unsuspecting opponent’s computer networks, destroying and paralyzing nations.
- This perception seems to be correct as the terms cyberwarfare and Cyberterrorism have got historical connection in the context of attacks against infrastructure.
- The term “information infrastructure” refers to information resources, including communication systems that support an industry, institution or population.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)



Cyberterrorism :

- The use of information technology and means by terrorist groups & agents is called as Cyberterrorism.
- **"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives."**

(or)

- **Cyberterrorism is defined as "any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism."**

CYBERCRIME AND INFORMATION SECURITY



- Lack of information security gives rise to cybercrimes.
- The amended Indian Information Technology Act (ITA) 2000 in the context of cybercrime. From an Indian perspective, the new version of the Act (referred to as ITA 2008) provides a new focus on “Information Security in India".
- "Cybersecurity” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- The term incorporates both the physical security of devices as well as the information stored therein. It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction.

CYBERCRIME AND INFORMATION SECURITY (CONT..)



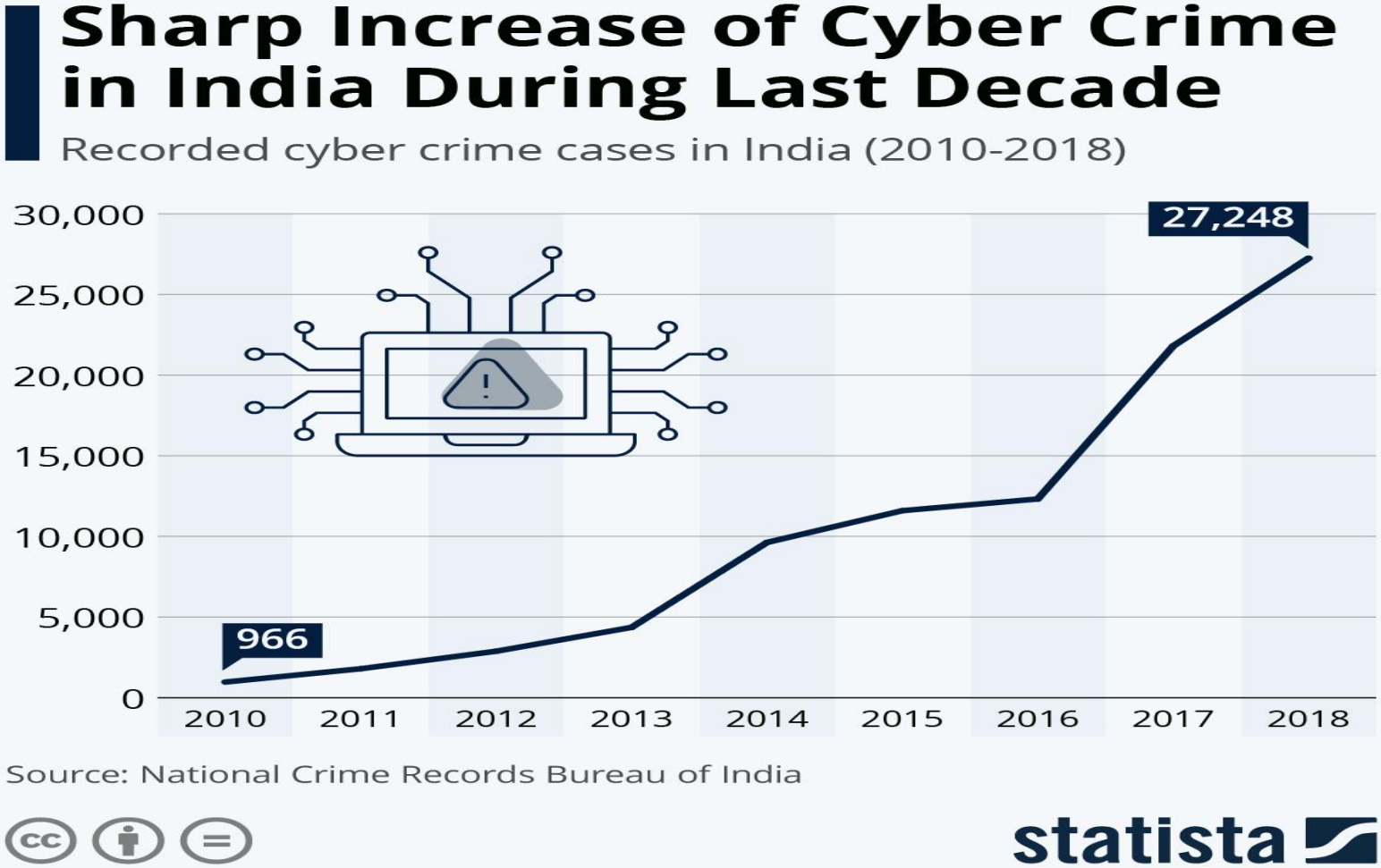
- Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft.
- The 2008 CSI Survey on computer crime and security supports this. Cybercrimes occupy an important space in information security domain because of their impact.
- The other challenge comes from the difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost (through loss/theft of laptops).
- Because of these reasons, reporting of financial losses often remains approximate.

CYBERCRIME AND INFORMATION SECURITY (CONT..)

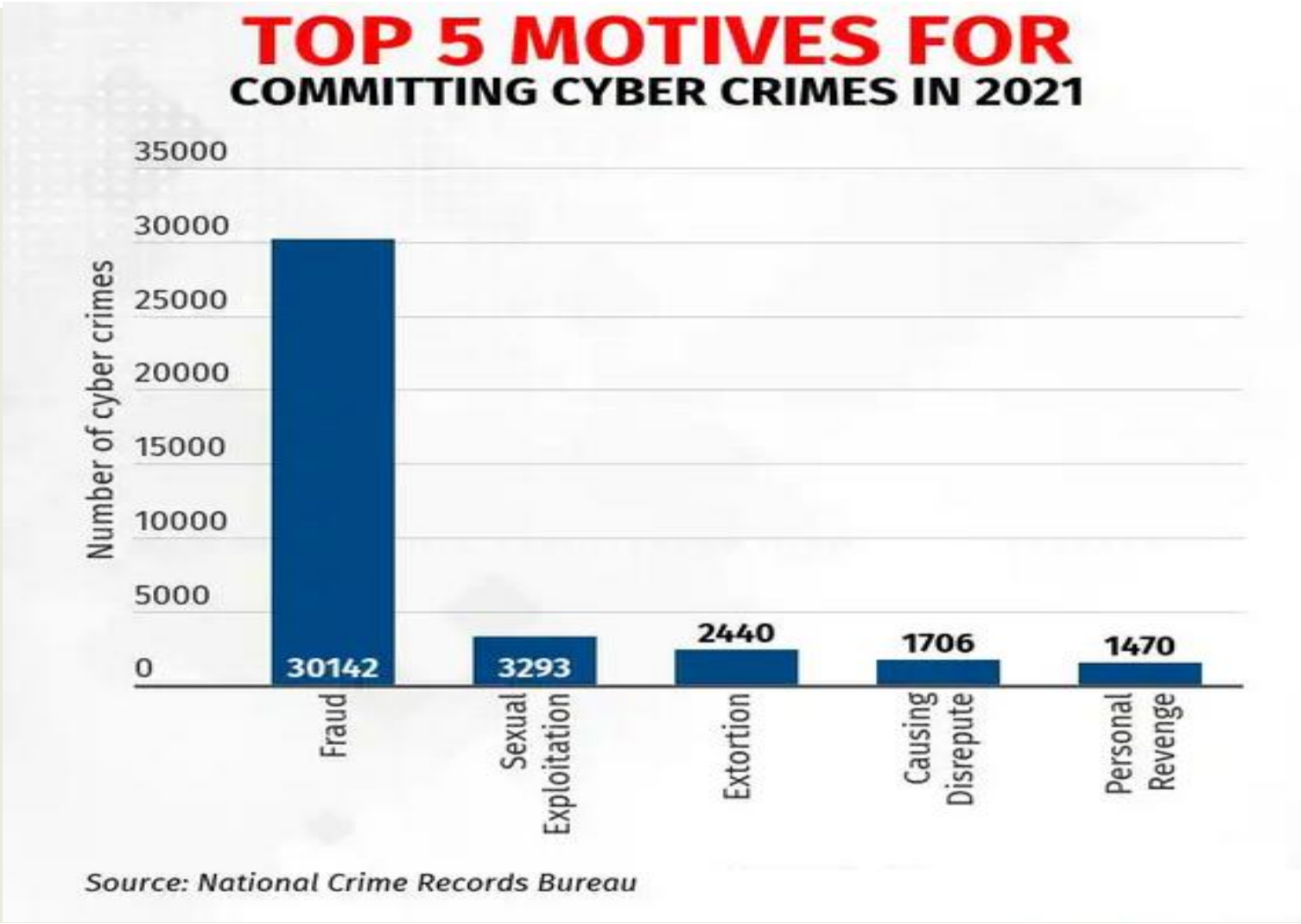


- In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about "security incidents" including cybercrime.
- In general, organizations perception about "insider attacks" seems to be different than that made out by security solution vendor.
- Awareness about "data privacy" too tends to be low in most organizations.
- When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such "crimes" may not be detected by the victimized organization and no direct costs may be associated with the theft.
- Several categories of incidences include - *viruses, insider abuse, laptop theft* and *unauthorized access* to systems, implications in mobile computing paradigm, Typical network misuses are for Internet radio/screaming audio, screaming video, file sharing, instant messaging and online gaming

CYBERCRIME STATISTICS



CYBERCRIME STATISTICS



CYBERCRIME STATISTICS



State/UT	IT Act		IPC	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
Maharashtra	1458	976	403	345
Andhra Pradesh (Including Telangana)	1413	708	64	111
Karnataka	1076	194	54	29
Kerala	845	437	95	47
Uttar Pradesh	678	518	367	428
Madhya Pradesh	514	414	128	63
Rajasthan	508	335	89	42
West Bengal	449	142	259	206
Punjab	277	247	36	33
Delhi	257	76	76	44

CYBERCRIME STATISTICS



ANNEXURE-I
RS USQ. NO. 226 FOR 27.11.2024

STATE/UT-WISE CASES REGISTERED UNDER CYBER CRIMES DURING 2018-2022

SL	State/UT	2018	2019	2020	2021	2022
1	Andhra Pradesh	1207	1886	1899	1875	2341
2	Arunachal Pradesh	7	8	30	47	14
3	Assam	2022	2231	3530	4846	1733
4	Bihar	374	1050	1512	1413	1621
5	Chhattisgarh	139	175	297	352	439
6	Goa	29	15	40	36	90
7	Gujarat	702	784	1283	1536	1417
8	Haryana	418	564	656	622	681
9	Himachal Pradesh	69	76	98	70	77
10	Jharkhand	930	1095	1204	953	967
11	Karnataka	5839	12020	10741	8136	12556
12	Kerala	340	307	426	626	773
13	Madhya Pradesh	740	602	699	589	826
14	Maharashtra	3511	4967	5496	5562	8249
15	Manipur	29	4	79	67	18
16	Meghalaya	74	89	142	107	75
17	Mizoram	6	8	13	30	1
18	Nagaland	2	2	8	8	4
19	Odisha	843	1485	1931	2037	1983
20	Punjab	239	243	378	551	697

CYBERCRIME STATISTICS

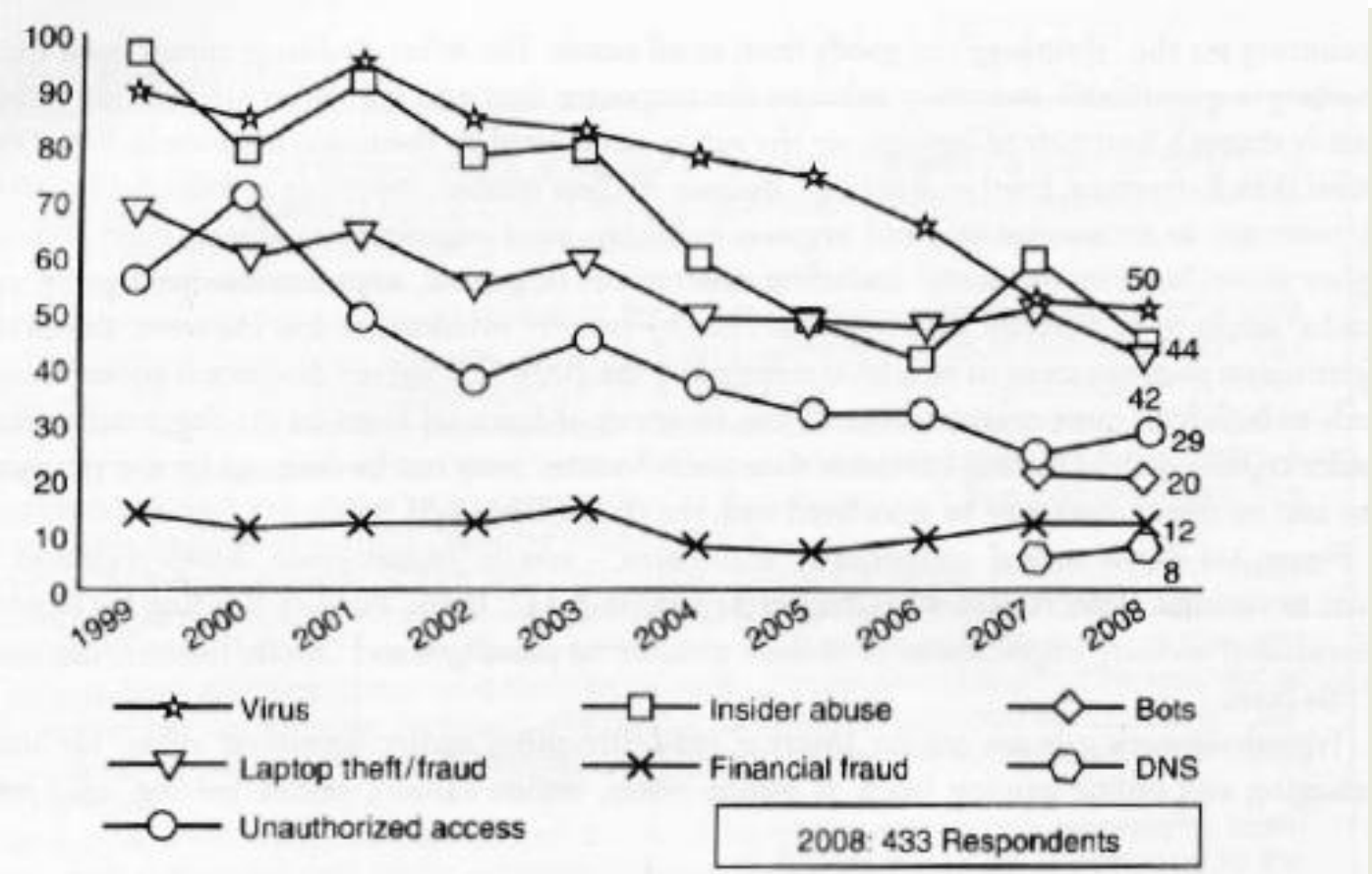


Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11
Bots (see Box 1.2; more in Chapter 2)				21	20
DoS attacks				6	8
Instant messaging abuse				25	21
Password sniffing (explained in Chapter 2)				10	9
Theft/loss of customer data				17	17
• from mobile devices					8
• from all other sources					8

Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

CYBERCRIME STATISTICS

CYBER SECURITY



Major types of incidents by percentage.
Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

WHO ARE CYBER CRIMINALS?



- Cybercrime involves such activities as child pornography; credit card fraud; cyberstalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark protection; overriding encryption to make illegal copies; software piracy and stealing another's identity (known as identity theft) co perform criminal acts.
- Cybercriminals are those who conduce such acts.
- They can be categorized into three groups that reflect their motivation:
  - **Type I: Cybercriminals- hungry for recognition**
  - **Type II: Cybercriminals - not interested in recognition**
  - **Type III: Cybercriminals - the insiders**

WHO ARE CYBER CRIMINALS? (CONT..)



Type I: Cybercriminals- hungry for recognition

- Hobby hackers;
- IT professionals (social engineering is one of the biggest threat);
- politically motivated hackers;
- terrorist organizations.

Type II: Cybercriminals - not interested in recognition

- Psychological perverts;
- financially motivated hackers (corporate espionage);
- state-sponsored hacking (national espionage, sabotage);
- organized criminals.

Type III: Cybercriminals - the insiders

- Disgruntled or former employees seeking revenge;
- competing companies using employees to gain economic advantage through damage and/or theft.

WHO ARE CYBER CRIMINALS? (CONT..)



- Thus, the typical "motives" behind cybercrime seem to be greed, desire to gain power and/or publicity, desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mindset and *desire* to sell network security services.

- Cybercafes are known to play role in committing cybercrimes.

CLASSIFICATIONS OF CYBERCRIMES



- "Crime is defined as an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the off ender liable to punishment by that law".
- Cyber crimes are classified as follows:
  - Cybercrime against individual
  - Cybercrime against property
  - Cybercrime against organization
  - Cybercrime against society
  - Crimes emanating from Usenet newsgroup

CLASSIFICATIONS OF CYBERCRIMES

CYBER SECURITY

	Cybercrime in Narrow Sense	*Cybercrime in Broad Sense*	
Role of computer	*Computer as an object* The computer/information stored on the computer is the subject/target of the crime	*Computer as a tool* The computer/or information stored on the computer constitutes an important tool for committing the crime	*Computer as the environment or context* The computer/information stored on the computer plays a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, computer sabotage, DDoS-attacks (distributed denial-of-service attacks), virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

Fig: Classifying cybercrimes - broad and narrow

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cybercrime against individual :

- Electronic mail (E-Mail) Spoofing and other online frauds
- Phishing, Spear Phishing and various forms
- Spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses
- Password sniffing

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cybercrime against individual :

Electronic mail (E-Mail) Spoofing:

- A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source.

Phishing, Spear Phishing and various forms:

- **Phishing** is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate.
- **Spear Phishing** is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering.
- **Vishing** (voice phishing) is a type of phishing attack that is conducted by phone and often targets users of Voice over IP (VoIP) services like Skype.
- **Smishing** (SMS phishing) is a type of phishing attack conducted using SMS (Short Message Services) on cell phones.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Spamming:

- Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately.
- Examples: email spam, instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions, social networking Spam, file sharing network Spam, video sharing sites, etc
- Spamming is difficult to control because it has economic viability. Spammers are numerous; the volume of unrequested mail has become very high because the barrier to entry is low.
- Search Engine Spamming: Use of Subversive techniques to ensure that their site is more frequent – penalties are imposed on such activities

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cyber defamation :

- It is a cognizable (Software) offense. “Whoever, by words either spoken(libel) or intended to be read(slander), or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.”
- Cyber defamation happens when the above takes place in an electronic form. In other words, cyber defamation occurs when defamation takes place with the help of computers and/or the Internet.
- Punishable under IPC Section 499.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cyber stalking and harassment :

- Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.
- Cyberstalking may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Computer sabotage:

- The use of the Internet to stop the normal functioning of a computer system through the introduction of worms, viruses or logic bombs, is referred to as computer sabotage.
- It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes.
- Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Pornographic offenses:

- Child pornography means any visual depiction, including but not limited to the following:
  1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
  2. film, video, picture;
  3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.
- Child Pornography is considered an offense. The internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet has become a household commodity in the urban areas of the nation. Its explosion has made the children a viable victim to the cybercrime.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Password sniffing:

- It is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic.
- And yet, password sniffers aren't always used for malicious intent. They are often used by IT professionals as a tool to identify weak applications that may be passing critical information unencrypted over the Local Area Network (LAN). IT practitioners know that users download and install risky software at times in their environment, running a passive password sniffer on the network of a business to identify leaky applications is one legitimate use of a password sniffer.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cybercrime against Property:

- Credit Card Frauds
- Intellectual Property (IP) Crimes
- Internet time theft

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Credit Card Frauds:

- Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help businesses process card payments securely and reduce card fraud. Credit card fraud can be authorized, where the genuine customer themselves processes a payment to another account which is controlled by a criminal, or unauthorized, where the account holder does not provide authorization for the payment to proceed and the transaction is carried out by a third party.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Intellectual Property (IP) Crimes:

- With the growth in the use of internet these days the cyber crimes are also growing. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers.
- Copyrights and trade secrets are the two forms of IP that is frequently stolen. For example, stealing of software, business strategies etc. Generally, the stolen material is sold to the rivals or others for further sale of the product. This may result in the huge loss to the company who originally created it.
- Another major cyber theft of IP faced by India is piracy. These days one can get pirated version of movies, software etc. The piracy results in a huge loss of revenue to the copyright holder. It is difficult to find the cyber thieves and punish them because everything they do is over internet, so they erase the data immediately and disappear within fraction of a second.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Internet time theft:

- Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person. Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent. The issue of Internet time theft is related to the crimes conducted through identity theft.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cybercrime against Organization:

- Unauthorized accessing of Computer
- Password Sniffing
- Denial-of-service Attacks (DoS Attacks)
- Virus attacks/dissemination of Viruses
- E-Mail bombing/Mail bombs
- Salami Attack/Salami technique
- Logic Bomb
- Trojan Horse
- Data Diddling
- Newsgroup Spam/Crimes emanating from Usenet newsgroup
- Industrial spying/Industrial espionage
- Computer network intrusions
- Software piracy

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Unauthorized accessing of Computer

- Hacking is one method of doing this and hacking is punishable offense. Unauthorized computer access, popularly referred to as hacking, describes a criminal action whereby someone uses a computer to knowingly gain access to data in a system without permission to access that data.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Denial-of-service Attacks (DoS Attacks)

- It is an attempt to make a computer resource (i.e.., information systems) unavailable to its intended users. In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with spam mail depriving him of the services he is entitled to access or provide. The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following:
  - Flood a network with traffic, thereby preventing legitimate network traffic.
  - Disrupt connections between two systems, thereby preventing access to a service.
  - Prevent a particular individual from accessing a service.
  - Disrupt service to a specific system or person.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Virus attacks/dissemination of Viruses:

- Computer virus is a program that can "infect" legitimate (valid) 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. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. Viruses can take some typical actions:
  - Display a message to prompt an action which may set of the virus
  - Delete files inside the system into which viruses enter
  - Scramble data on a hard disk
  - Cause erratic screen behavior
  - Halt the system (PC)
  - Just replicate themselves to propagate further harm

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



E-Mail bombing/Mail bombs

- E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account (in the case of an individual) or to make victim's mail servers crash (in the case of a company or an E-Mail service provider). Computer program can be written to instruct a computer to do such tasks on a repeated basis. In recent times, terrorism has hit the Internet in the form of mail bombings. By instructing a computer to repeatedly send E-Mail to a specified person's E-Mail address, the cybercriminal can overwhelm the recipient's personal account and potentially shut down entire systems. This may or may not be illegal, but it is certainly disruptive.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Salami Attack/Salami technique

- These attacks are used for committing financial crimes. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed; For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Logic Bomb

- A Logic Bomb is a piece of often-malicious code that is intentionally inserted into software. It is activated upon the host network only when certain conditions are met. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Trojan Horse

- A Trojan Horse, Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Data Diddling

- A data diddling (data cheating) attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties computerize their systems.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Newsgroup Spam/Crimes emanating from Usenet newsgroup

- This is one form of spamming. The word “Spam” was usually taken to mean Excessive Multiple Posting (EMP). The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever. Spamming of Usenet newsgroups actually predates E-Mail Spam.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Industrial spying/Industrial espionage

- Industrial spying is not new; in fact it is as old as industries themselves. The use of the Internet to achieve this is probably as old as the Internet itself.
- Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of registered organizations (it is said that they get several hundreds of thousands of dollars, depending on the "assignment"). With the growing public availability of Trojans and Spyware material, even low-skilled individuals are now inclined to generate high volume profit out of industrial spying. This is referred to as "Targeted Attacks" (which includes "Spear Phishing").

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Software piracy

- This is a big challenge area indeed. Cybercrime investigation cell of India defines “software piracy” as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. There are many examples of software piracy:
  - end-user copying: friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
  - hard disk loading with illicit means: hard disk vendors load pirated software;
  - counterfeiting: large-scale duplication and distribution of illegally copied software;
  - Illegal downloads from the Internet: by intrusion, by cracking serial numbers, etc.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Computer network intrusions

- "Crackers" who are often misnamed "Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords. Network intrusions are illegal, but detection and enforcement are difficult. Current laws are limited and many intrusions go undetected. The cracker can bypass existing password protection by creating a program to capture logon IDs and passwords. The practice of "strong password" is therefore important.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cybercrime against Society:

- Forgery
- Cyberterrorism
- Web Jacking

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Forgery

- Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake mark-sheets or even degree certificates. These are made using computers and high quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Cyberterrorism

- Cyberterrorism is a controversial term. Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Web Jacking

- Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves “password sniffing”. The actual owner of the website does not have any more control over what appears on that website.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)



Crimes emanating from Usenet newsgroup:

- By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.
- Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects. Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.

CYBER OFFENSES: HOW CRIMINALS PLAN THEM:

INTRODUCTION
HOW CRIMINALS PLAN THE ATTACKS
CYBER STALKING
CYBER CAFE AND CYBERCRIMES
BOTNETS: THE FUEL FOR CYBERCRIME
ATTACK VECTOR



UNIT-1 (Part-B)

INTRODUCTION



- Technology is a "double-edged sword" as it can be used for both good and bad purposes.
- Computers and tools available in IT are also no exceptions; like other cool, they are used as either target of offense or means for committing an offense.
- In today's world of Internet and computer networks, a criminal activity can be carried out across national borders with "false sense of anonymity"; without realizing, we seem to pass on tremendous amount of information about ourselves.
- The criminals take advantage of the widespread lack of awareness about cybercrimes and cyberlaws among the people who are constantly using the IT infrastructure for official and personal purposes.

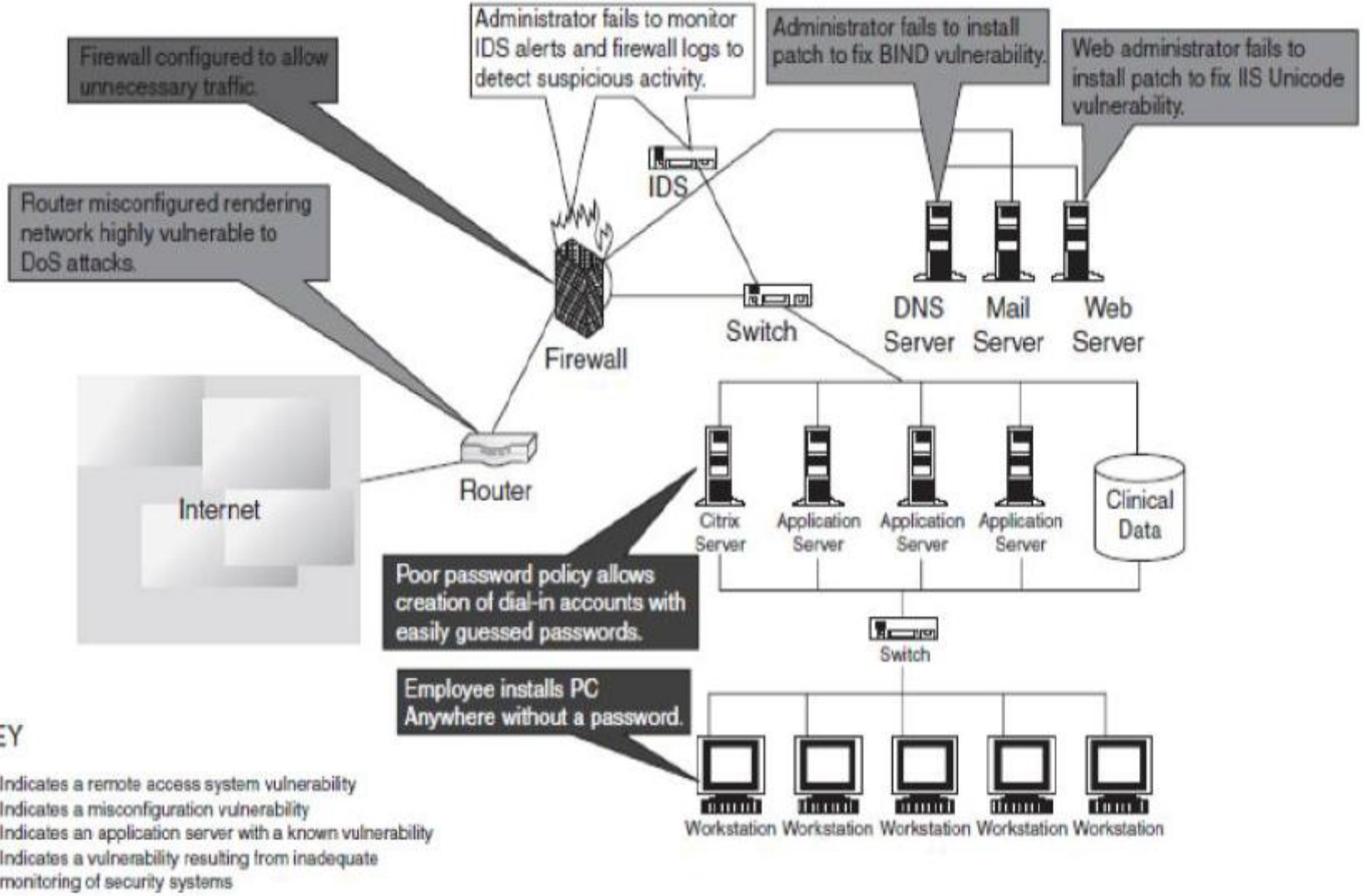
INTRODUCTION (CONT...)



- The categories of vulnerabilities that hackers typically search for are the following:
  - Inadequate border protection (border as in the sense of network periphery);
  - remote access servers (RASs) with weak access controls;
  - application servers with well-known exploits;
  - misconfigured systems and systems with default configurations.

INTRODUCTION (CONT...)





INTRODUCTION (CONT...)



- A **black hat hacker** is also called a “cracker” or “dark side hacker.” Such a person is a malicious or **criminal hacker**. Typically, the term “cracker” is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of “hacker” can be much broader. The name comes from the opposite of “white hat hackers.”

- A **white hat hacker** is considered an ethical hacker. In the realm of IT, a “white hat hacker” is a person who is ethically opposed to the abuse of computer systems. As a simplified explanation, a “white hat” generally focuses on securing IT systems, whereas a “black hat” (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

INTRODUCTION (CONT...)



- A **brown hat hacker** is one who thinks before acting or committing a malice or non-malice deed. A grey hat commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

HOW CRIMINALS PLAN THE ATTACKS



- Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization.
- Criminals plan passive and active attacks
- **Active attacks** are usually used to alter the system (i.e., computer network) whereas **passive attacks** attempt to gain information about the target. Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to violation of confidentiality.
- Attacks can be categorized as either inside or outside.
- An attack originating and/or attempted within the security perimeter of an organization is an **inside attack**; it is usually attempted by an "insider" who gains access to more resources than expected. An **outside attack** is attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

HOW CRIMINALS PLAN THE ATTACKS



- The following phases are involved in planning cybercrime:
  1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
  2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
  3. Launching an attack (gaining and maintaining the system access).

HOW CRIMINALS PLAN THE ATTACKS



Phase-1: Reconnaissance (information gathering) is the first phase and is treated as passive attacks.

- The literal meaning of "Reconnaissance" is an **act of finding something or somebody (especially to gain information about an enemy or potential enemy**).
- In the world of "hacking," reconnaissance phase begins with "Footprinting" – this is the preparation toward pre-attack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.
- Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities. The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack. Thus, an attacker attempts to gather information in two phases: passive and active attacks.

HOW CRIMINALS PLAN THE ATTACKS



Passive Attacks:

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises.
- However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information
  - Google or Yahoo search: People search to locate information about employees.
  - Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
  - Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target
  - Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
  - Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

HOW CRIMINALS PLAN THE ATTACKS



- Network sniffing is another means of passive attack to yield useful information such as Internet Protocol (IP) address ranges, hidden servers or networks, and other available services on the system or network.
- Along with Google search, various other tools are also used for gathering information about the target/victim.

HOW CRIMINALS PLAN THE ATTACKS



Active Attacks:

- An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase. It involves the risk of detection and is also called “Rattling the doorknobs” or “Active reconnaissance.” Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

HOW CRIMINALS PLAN THE ATTACKS



Phase-2: Scanning and Scrutinizing Gathered Information

- Scanning is a key step to examine intelligently while gathering information about the target.
- The objectives of scanning are as follows:
  1. Port scanning: Identify open/close ports and services.
  2. Network scanning: Understand IP Addresses and related information about the computer network systems.
  3. Vulnerability scanning: Understand the existing weaknesses in the system.

HOW CRIMINALS PLAN THE ATTACKS



- **Ports and Ports Scanning**
- A port is an interface on a computer to which one can connect to device. TCP/IP Protocol suite made out of the two protocols, TCP and UDP, is used universally to communicate on the Internet. The port numbers ore divided into three ranges:
  - Well-known ports (from 0 to 1023)
  - Registered ports (from 1024 to 49151)
  - Dynamic and/or private ports (from 49152 to 65535)

HOW CRIMINALS PLAN THE ATTACKS



Port Number	*Port Description*	*Port Number*	*Port Description*
1	TCP port service multiplexer (TCPMUX)	118	Structured query language (SQL) services
5	Remote job entry (RJE)	119	NNTP (Newsgroup)
7	ECHO	137	NetBIOS name service
18	Message Send Protocol (MSP)	139	NetBIOS datagram service
20	FTP – Data	143	Internet Message Access Protocol (IMAP)
21	FTP – Control	150	NetBIOS session service
22	Secure shell (SSH) remote log-in protocol	156	SQL server
23	Telnet	161	Simple Network Management Protocol (SNMP)
25	Simple Mail Transfer Protocol (SMTP)	179	Border Gateway Protocol (BGP)
29	MSG ICP	190	Gateway Access Control Protocol (GACP)

HOW CRIMINALS PLAN THE ATTACKS



37	Time	194	Internet relay chat (IRC)
42	Nameserv (host name server)	197	Directory location service (DLS)
43	WHOIS	389	Lightweight Directory Access Protocol (LDAP)
49	Log-in (log-in host protocol)	396	Novell netware over IP
53	Domain name system (DNS)	443	Secure Hypertext Transfer Protocol (S-HTTP)
69	Trivial File Transfer Protocol (TFTP)	444	Simple Network Paging Protocol (SNPP)
70	Gopher services	445	Microsoft-DS
79	Finger	458	Apple quick time
80	HTTP	546	DHCP client
103	X.400 Standard	547	DHCP server
108	SNA gateway access server	563	SNEWS
109	POP2	569	MSN
110	POP3	1080	Socks
115	Simple File Transfer Protocol (SFTP)		

HOW CRIMINALS PLAN THE ATTACKS



- **Port Scanning**
- A "port" is a place where information goes into and out of a computer and so, with port scanning, one can identify open doors to a computer. Ports are basically entry/exit points that any computer has, to be able to communicate with external machines.
- Each computer is enabled with three or more external ports. These are the ports used by the computer to communicate with the other computers, printer, modem, mouse, video game, scanner, and other peripherals.
- Port scanning is often one of the first things an attacker will do when attempting to penetrate a particular computer. Tools such as Nmap offer an automated mechanism for an attacker to not only scan the system to find out what ports are "open" (meaning being used), but also help to identify what operating system (OS) is being used by the system.

HOW CRIMINALS PLAN THE ATTACKS



- The result of a scan on a port is usually generalized into one of the following three categories:

  1. **Open or accepted:** The host sent a reply Indicating that a service is listening on the port.

  2. **Closed or not listening:** The host sent a reply indicating that connections will be denied to the port.

  3. **Filtered or blocked:** There was no reply from the host.

- Security administrators as well as attackers have a special eye on few well-known ports and protocols associated with it.
- Open ports present two vulnerabilities of which administrators must be wary:
  - Vulnerabilities associated with the program that is delivering the service.
  - Vulnerabilities associated with the OS that is running on the host.
- Closed ports present only the latter of the two vulnerabilities that open ports do.
- Blocked ports do not present any reasonable vulnerabilities.

HOW CRIMINALS PLAN THE ATTACKS



- **The scrutinizing phase** is always called "enumeration" in the hacking world. The objective behind this is to identify:

  1. The valid user accounts or groups;
  2. network resources and/or shared resources;
  3. OS and different applications that are running on the OS.

HOW CRIMINALS PLAN THE ATTACKS



Phase-3: Attack (Gaining and Maintaining the System Access)

- After the scanning and enumeration, the attack is launched using the following steps:
  1. Crack the password.
  2. exploit the privileges.
  3. execute the malicious commands/applications.
  4. hide the files (if required).
  5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

CYBER STALKING



- The dictionary meaning of “stalking” is an “act or process of following prey stealthily – trying to approach somebody or something.”
- Cyber stalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.
- Cyber stalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person’s home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person’s property.

CYBER STALKING



Types of Stalkers

1. Online stalkers:

- They aim to start the interaction with the victim directly with the help of the Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.

2. Offline stalkers:

- The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet. The victim is not aware that the Internet has been used to perpetuate an attack against them.

CYBER STALKING



How Stalking Works?

It is seen that stalking works in the following ways:

- 1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
- 2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
- 3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
- 4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

CYBER STALKING



- 5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
- 6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone no's), asking for sexual services or relationships.
- 7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

CYBER STALKING



Cyber Bullying

- The National Crime Prevention Council defines *Cyber bullying* as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."
- www.StopCyberbullying.org. on expert organization dedicated to Internet safety, security, and privacy defines cyber bullying as "a situation when a child, tween or teen is repeatedly 'tormented, threatened. harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween or teen using text messaging, E-Mail, instant messaging or any other type of digital technology."
- The practice of cyber bullying is not limited to children and while the behavior is identified by the some definition in adults. the distinction In age groups is referred to as cyber stalking or cyber harassment when perpetrated by adults toward adults.

CYBER CAFE AND CYBERCRIMES



- In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students. Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes. Cybercafes have also been used regularly for sending obscene mails to harass people.
- Public computers, usually referred to the systems, available in cybercafes, hold two types of risks.
  - First, we do not know what programs are installed on the computer – that is, risk of malicious programs such as keyloggers or Spyware, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior.
  - Second, over-the-shoulder surfing can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.

CYBER CAFE AND CYBERCRIMES



- Indian Information Technology Act (ITA) 2000, does not define cybercafes and interprets cybercafes as “network service providers” referred to under the Section 79, which imposed on them a responsibility for “due diligence” failing which they would be liable for the offenses committed in their network.
- Cybercriminals prefer cybercafes to carry out their activities.
- A recent survey conducted in one of the metropolitan cities in India reveals the following facts:
- 1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
- 2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
- 3. Several cybercafes had installed the software called “Deep Freeze” for protecting the computers from prospective malware attacks. **Deep Freeze** can wipe out the details of all activities carried out on the computer when one clicks on the “restart” button. Such practices present challenges to the police or crime investigators when they visit the cybercafes.

CYBER CAFE AND CYBERCRIMES



- 4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down.
- 5. Pornographic websites and other similar websites with indecent contents are not blocked.
- 6. Cyber cafe owners have very less awareness about IT Security and IT Governance.
- 7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cyber cafe owners.
- 8. Cyber cafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cyber cafes – one of the cyber cafe owners whom we interviewed expressed a view that the police will not visit a cyber cafe unless criminal activity is registered by filing an First Information Report (FIR). Cyber cafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security. There are thousands of cyber cafes across India.



- Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout**
2. **Stay with the computer**
3. **Clear history and temporary files**
4. **Be alert**
5. **Avoid online financial transactions**
6. **Change passwords**
7. **Use Virtual keyboard**
8. **Security warnings**

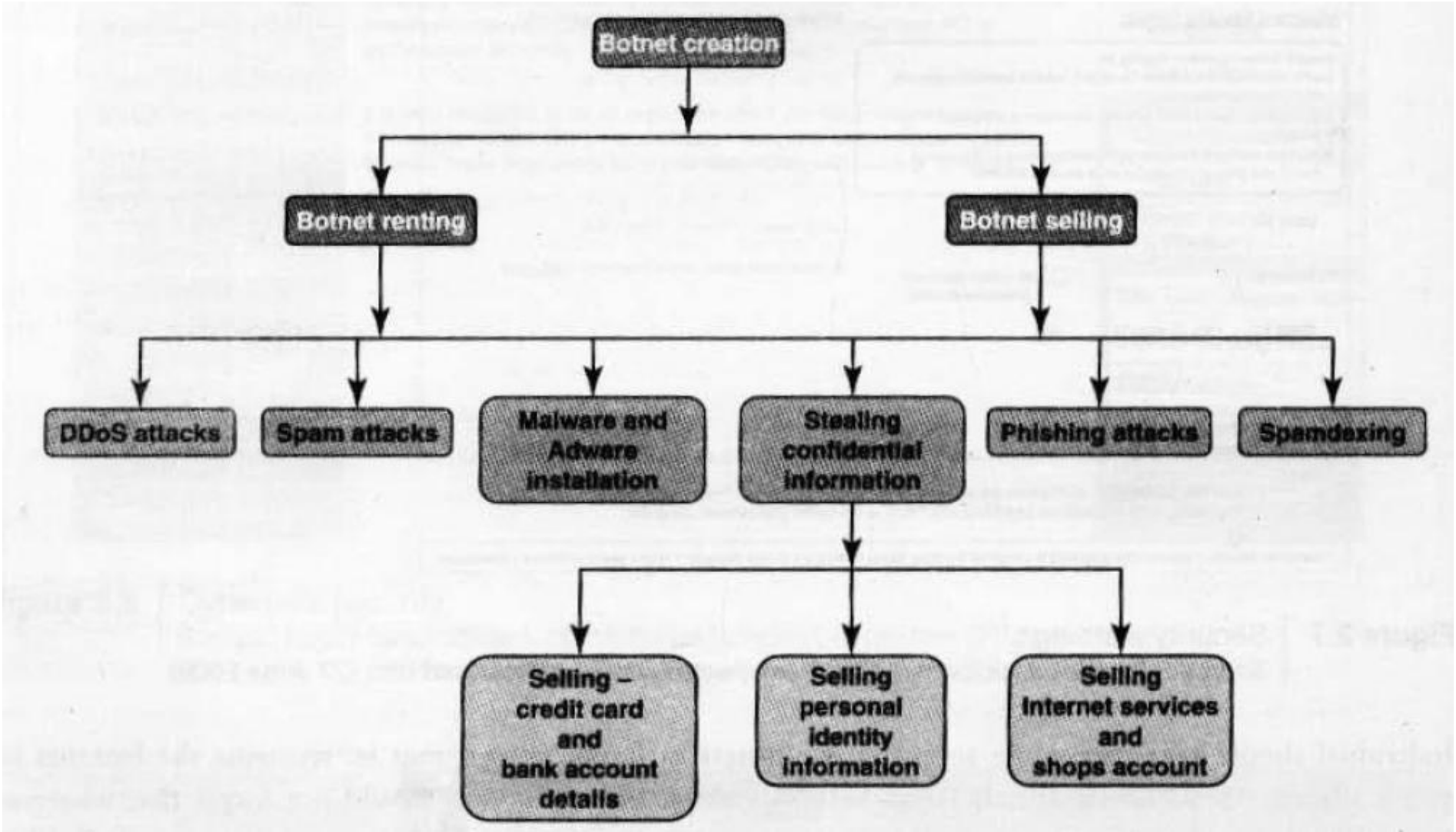
BOTNETS: THE FUEL FOR CYBERCRIME



- The dictionary meaning of Bot is “(computing) an automated program for doing some particular task, often over a network.”
- Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically. The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer program One can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access.
- Computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users’ knowledge.
- “Zombie networks” have become a source of income for entire groups of cybercriminals. If someone wants to start a “business” and has no programming skills, there are plenty of “Bot for sale” offers on forums. ‘encryption of these programs’ code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet.

BOTNETS: THE FUEL FOR CYBERCRIME





BOTNETS: THE FUEL FOR CYBERCRIME



- One can reduce the chances of becoming part of a Bot by limiting access into the system.
- One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer:
5. Downloading the freeware only from websites that are known and trustworthy.
6. Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send.
7. Take an immediate action if your system is infected.

ATTACK VECTOR



- An “attack vector” is a path, which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors enable attackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.
- To some extent, firewalls and antivirus software can block attack vectors. However, no protection method is totally attack-proof.
- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

ATTACK VECTOR



- In the technical terms, payload is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs.
- From the technical perspective, payload does not include the "overhead" data required to get the packet to its destination. Payload may depend on the following point of view: "What constitutes it?" To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles.
- The attack vectors described here are how most of them are launched.
- **1. Attack by E-Mail:** The content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something "free" or tempting is a suspect.

ATTACK VECTOR



- **2. Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
- **3. Attack by deception**: Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer's operator to succeed. Social engineering are other forms of deception that are often an attack vector too.
- **4. Hackers**: Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use variety of hacking tools, heuristics, They often install a Trojan Horse to commandeer the computer for their own use.

ATTACK VECTOR



- **5. Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.
- **6. Attack of the worms**: Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses.
- **7. Malicious macros**: Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart(IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.

ATTACK VECTOR



- **8. Foistware (sneakware)**: Foistware is the software that adds hidden components to the system with cunning nature. Spyware is the most common form of foistware. Foistware is partial- legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some “revenue opportunity” that the foistware has set up.
- **9. Viruses**: These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

CYBERCRIME: MOBILE AND WIRELESS DEVICES

- INTRODUCTION
- PROLIFERATION OF MOBILE AND WIRELESS DEVICES
- SECURITY CHALLENGES POSED BY MOBILE DEVICES
- ATTACKS ON MOBILE/CELL PHONES



UNIT-1 (Part-C)

INTRODUCTION

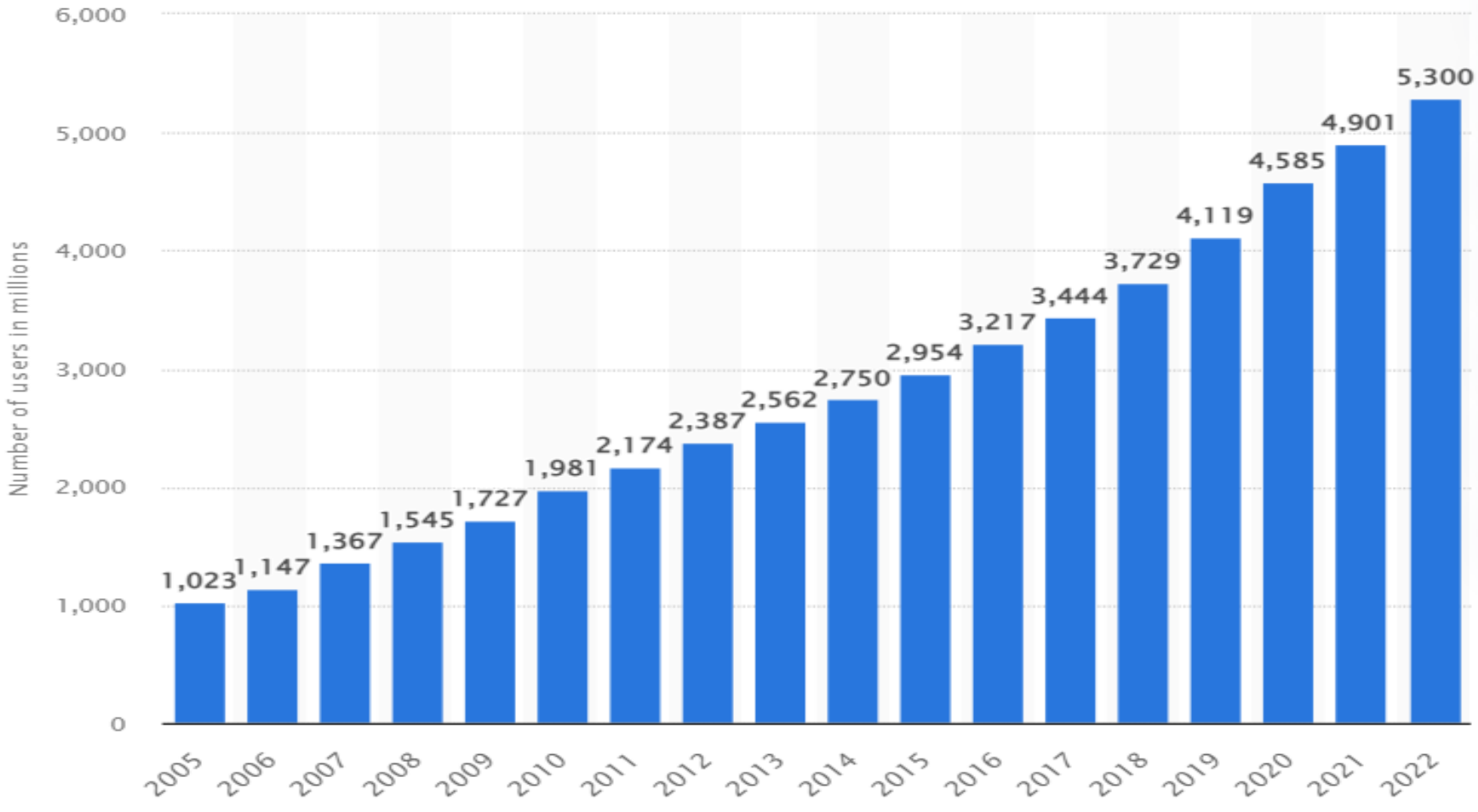


- In this modern era, electronic gadgets (i.e., mobile hand-held devices) have become an integral part of business, providing connectivity with the Internet outside the office.
- This challenges to secure these devices from being a victim of cybercrime.
- In the recent years, the use of laptops, PDAs and mobile phones has lead to widespread desktop replacement.
- The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address.
- Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart hand-held devices such as PDAs have become networked, converging with mobile phones.

INTRODUCTION



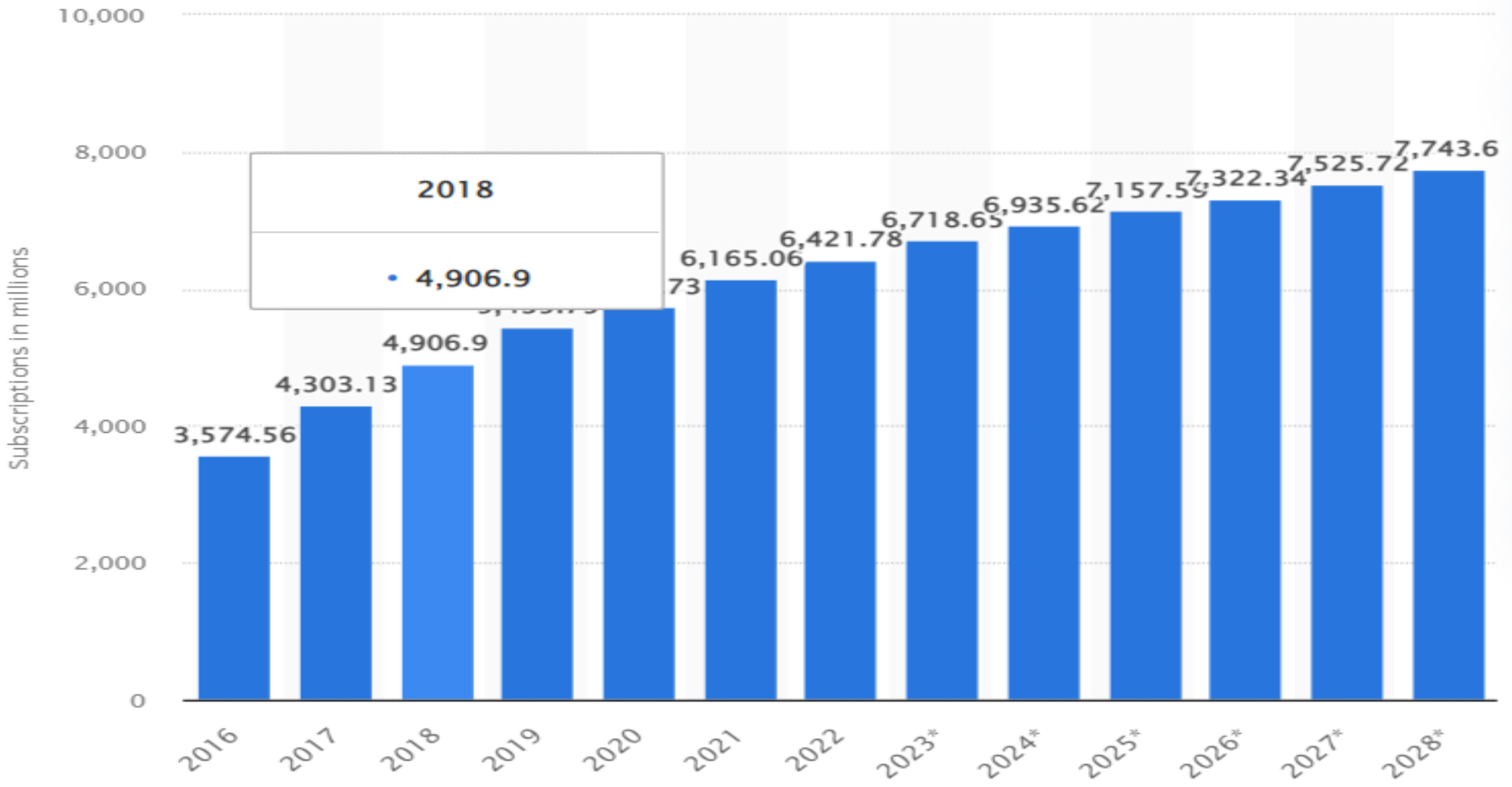
- Number of internet users



INTRODUCTION



- Number of Mobile Phone users



INTRODUCTION



- The maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: *the Smartphone*.
- Smartphones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool.
- Although IT departments of organizations as yet are not swapping employees' company-provided PDAs for the Smartphones, many users may bring these devices from home and use them in the office.
- Thus, the larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity.
- Clearly, these technological developments present a new set of security challenges to the global organizations.

PROLIFERATION OF MOBILE AND WIRELESS DEVICES



- Today, incredible advances are being made for mobile devices.
- The trend is for smaller devices and more processing power and with wireless Web-browsing capabilities.
- A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls.
- As the term “mobile device” includes many products since 1990s like:

  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.

PROLIFERATION OF MOBILE AND WIRELESS DEVICES



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 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, 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.

PROLIFERATION OF MOBILE AND WIRELESS DEVICES

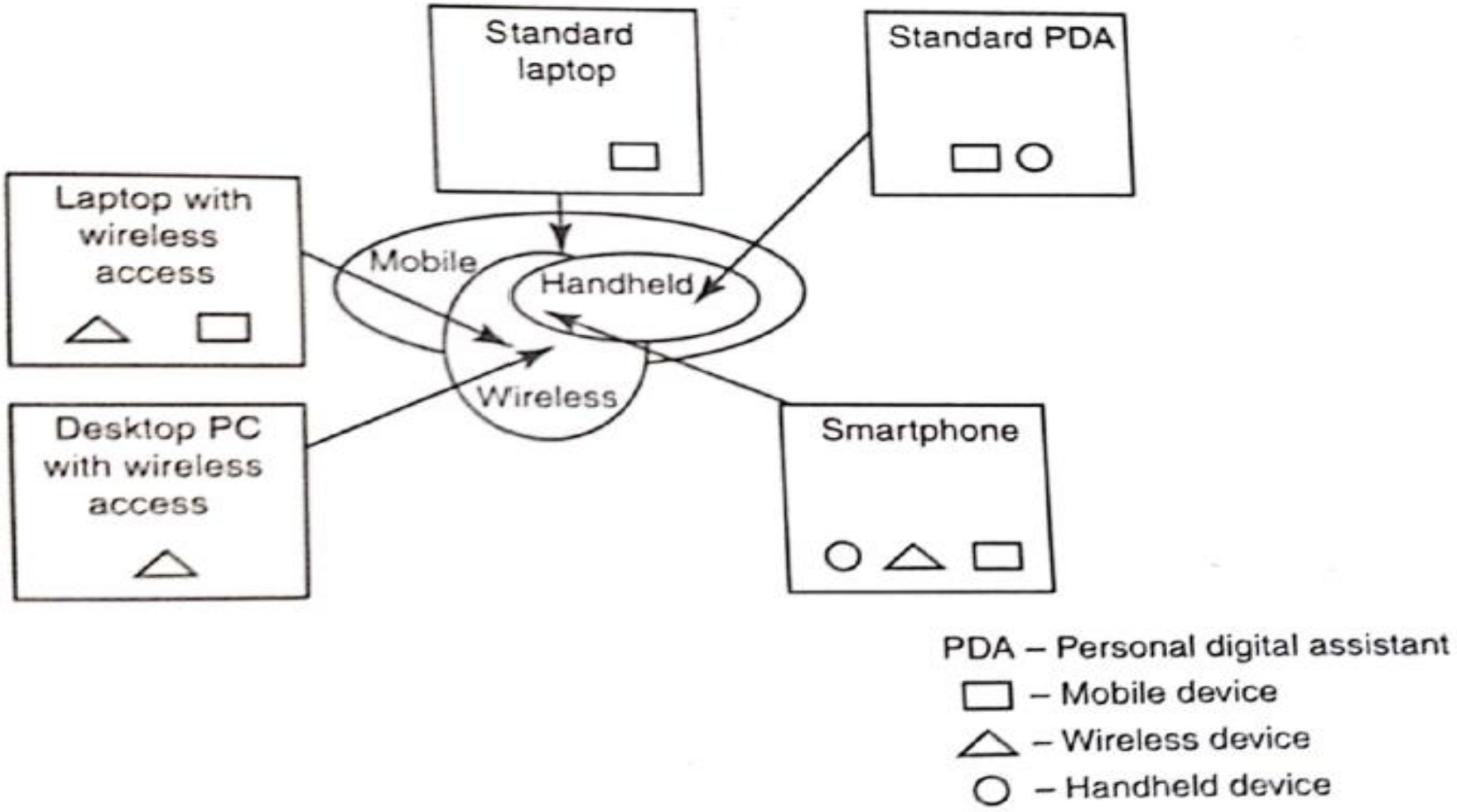


Figure: Mobile, Wireless & Hand-held devices

PROLIFERATION OF MOBILE AND WIRELESS DEVICES



- Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection.
- Not all wireless communication technologies are mobile.
- For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted to a desktop that is not tethered.
- As more personal devices find their way into the enterprise, corporations are realizing cyber security threats that come along with the benefits achieved with mobile solutions.

TRENDS IN MOBILITY



- Mobile computing is moving into a new era, New generations (3G, 4G, 5G, etc.), which promises greater variety in applications and have highly improved usability as well as speedier networking.
- “iPhone” from Apple and Google-led “Android” phones are the best examples of this trend and there are plenty of other developments that point in this direction.
- This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.
- It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain.

TRENDS IN MOBILITY



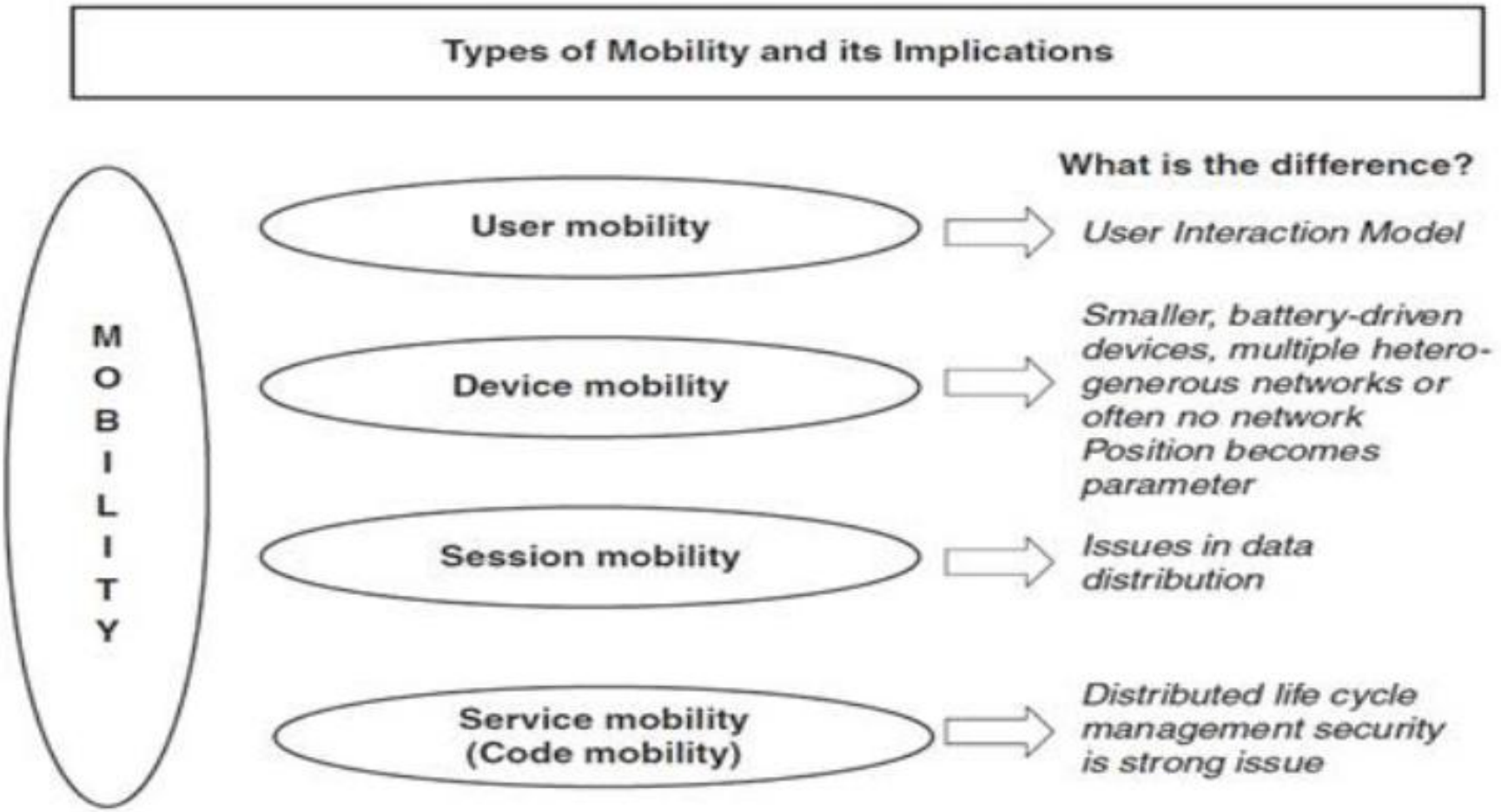


Figure: Mobility types & implications

TRENDS IN MOBILITY



- 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

TRENDS IN MOBILITY



- Popular types of attacks against mobile networks are as follows:

  1. Malwares, Viruses and Worms: Although many users are still in the transient process of switching from 3G,4G, 5G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices.

  2. Denial-of-Service (DoS): The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable.

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

  4. Spoofed Policy Development Process (PDP): These types of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

  5. Signaling-level Attacks: The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

SECURITY CHALLENGES POSED BY MOBILE DEVICES



- Mobility brings two main challenges to cybersecurity:
  1. on the hand-held devices, information is being taken outside the physically controlled environment and
  2. remote access back to the protected environment is being granted

- Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. As the number of mobile device users increases, two challenges are presented:
  1. at the device level called “microchallenges” and
  2. at the organizational level called “macrochallenges”

SECURITY CHALLENGES POSED BY MOBILE DEVICES

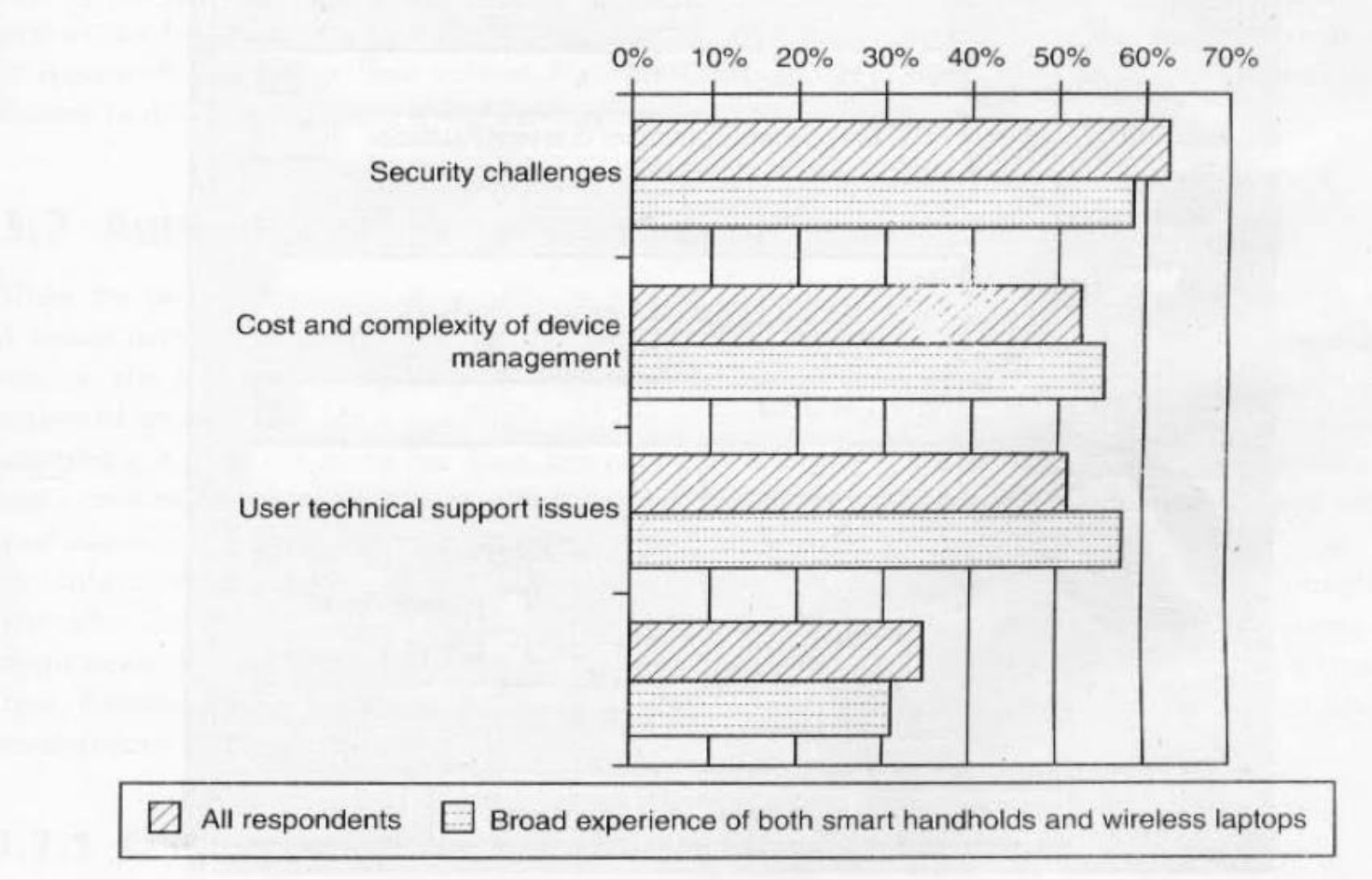


Fig: Important issues for managing mobile devices.

SECURITY CHALLENGES POSED BY MOBILE DEVICES



- Some well-known technical challenges in mobile security are:
  - Managing the registry settings and configurations, authentication service security
  - Cryptography security
  - Lightweight Directory Access Protocol (LDAP) security
  - Remote Access Server (RAS) security
  - Media player control security
  - Networking application program interface (API) security, etc.

REGISTRY SETTINGS FOR MOBILE DEVICES



- Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook.
- ActiveSync acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device.
- In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs.
- In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

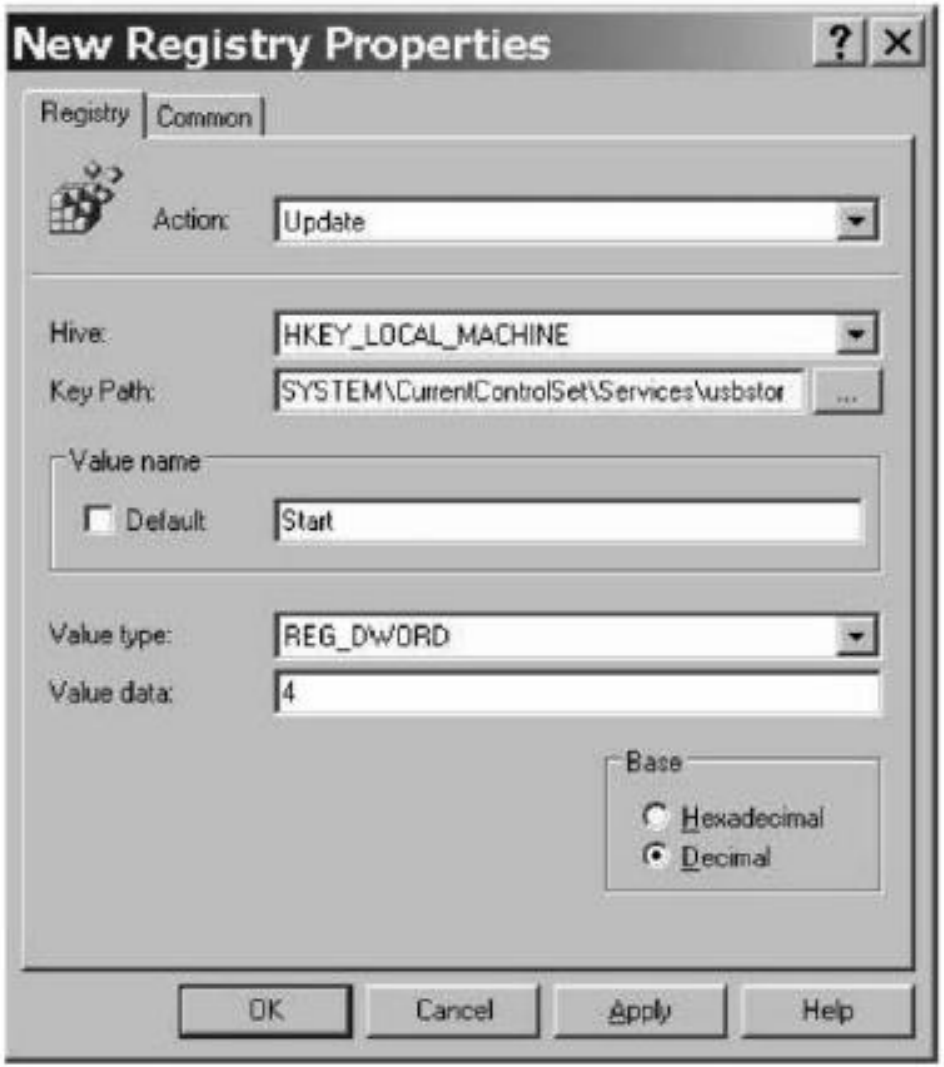
REGISTRY SETTINGS FOR MOBILE DEVICES



- One of the most prevalent areas where this attention to security is applicable is within “group policy.” Group policy is one of the core operations that are performed by Windows Active Directory.
- There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against Spyware, viruses, worms, malware and other Malicious Codes that run through the networks and the Internet. The mobile security issues on a Windows platform is that the baseline security is not configured properly.
- Even if users go through every Control Panel setting and group policy option, they may not get the computer to the desired baseline security.
- The only way to get a Windows computer to a security level is to make additional registry changes that are not exposed through any interface. There are many ways to complete these registry changes on every computer, but some are certainly more efficient than others.
- Naïve (Innocent) users may think that for solving the problem of mobile device security there are not many registry settings to tackle. However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of “registry hacks”

REGISTRY SETTINGS FOR MOBILE DEVICES





AUTHENTICATION SERVICE SECURITY



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

AUTHENTICATION SERVICE SECURITY



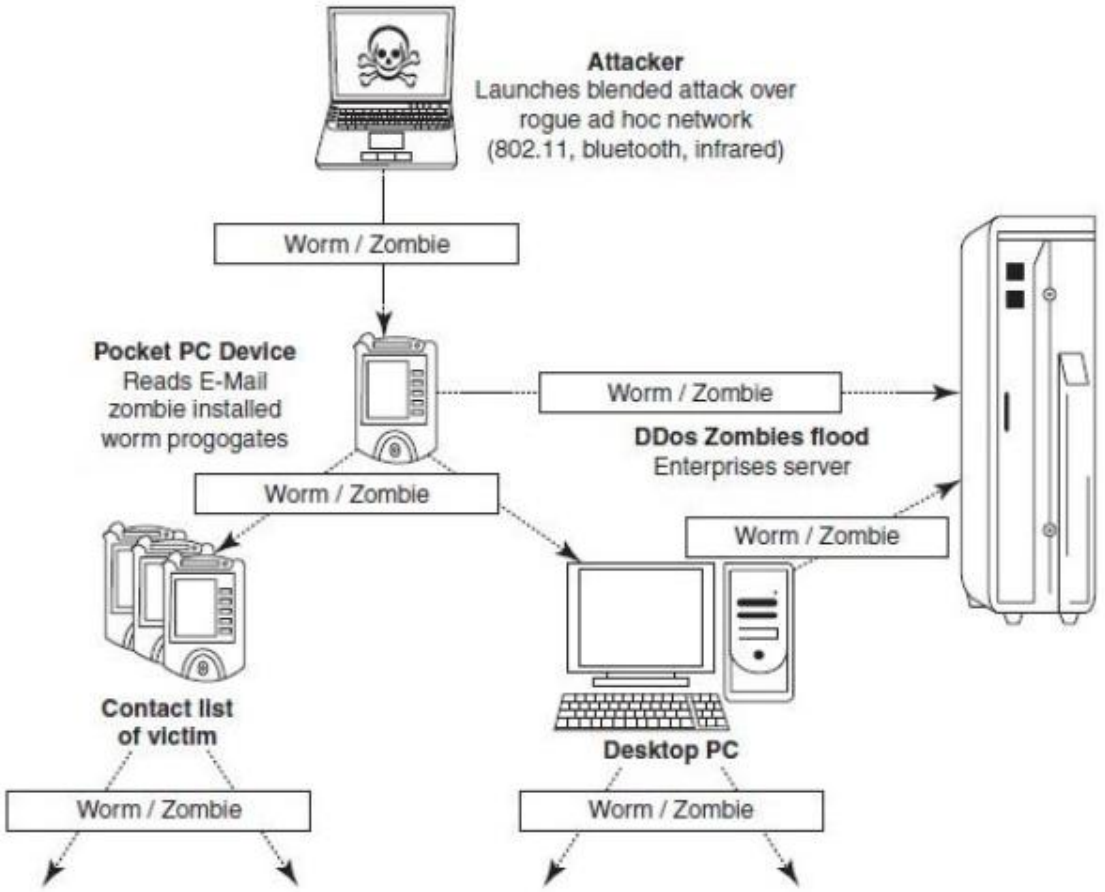


Figure: Push attack on mobile devices. DDoS implies distributed denial-of-service attack

AUTHENTICATION SERVICE SECURITY



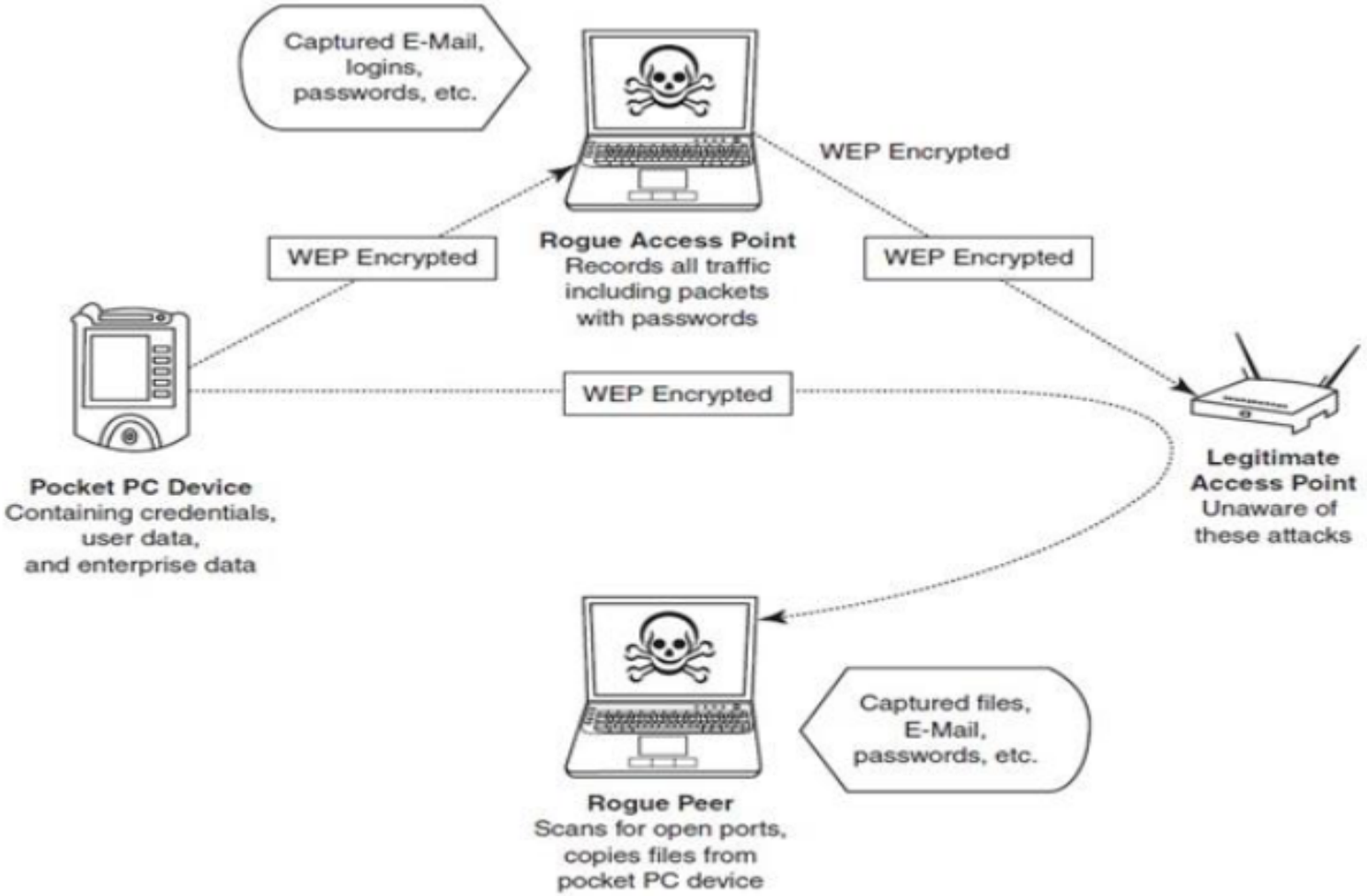


Figure: Pull attack on mobile devices

AUTHENTICATION SERVICE SECURITY



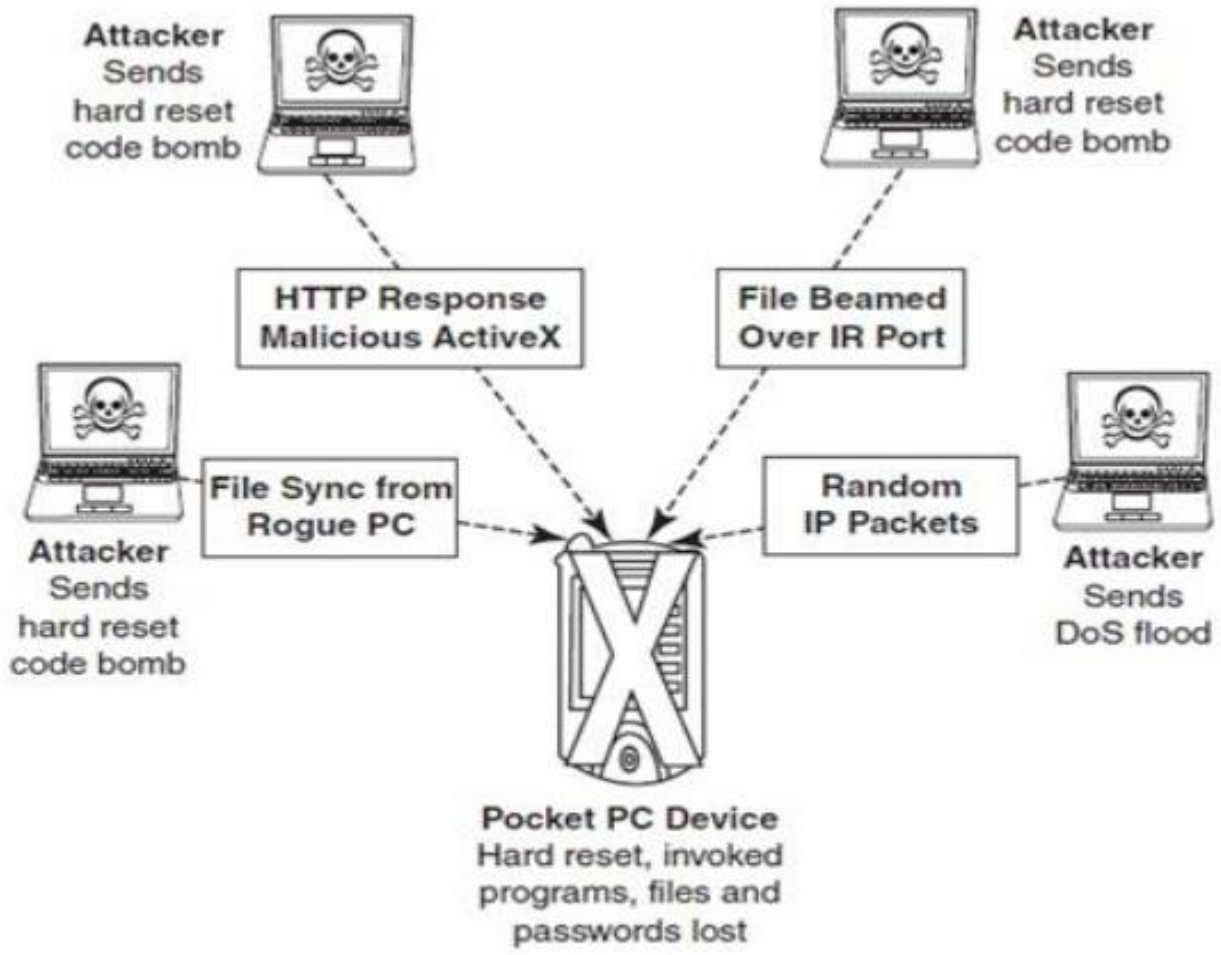


Figure: Crash attack on mobile devices. DoS- Denial-of-service attack

AUTHENTICATION SERVICE SECURITY



- Authentication services security is important given the typical attacks on mobile devices through wireless networks: DoS attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking.
- Security measures in this scenario come from *Wireless Application Protocols* (WAPs), use of *VPNs, media access control (MAC) address filtering* and development in 802.xx standards.

CRYPTOGRAPHIC SECURITY FOR MOBILE DEVICES



- Cryptographically Generated Addresses (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 key to assert address ownership and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure. Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices.
- CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in context-aware mobile computing applications) and mobility protocols.
- It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms (devices that can be held in one's palm) are one of the most common hand-held devices used in mobile computing. Cryptographic security controls are deployed on these devices.
- For example, the Cryptographic Provider Manager (CPM) in Palm OS5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

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 organizations's Intranet).
- In a network, a directory tells you where an entity is located in the network.
- LDAP is a light weight (smaller Attacker Launches blended attack over rogue ad hoc network (802.11, bluetooth, infrared) amount of code) version of Directory Access Protocol (DAP) because it does not include security features in its initial version.

RAS SECURITY FOR MOBILE DEVICES



- RAS (Remote Access Server) is an important consideration for protecting the business-sensitive data that may reside on the employees' mobile devices.
- In terms of cybersecurity, mobile devices are sensitive. Below Figure: organization's sensitive data can happen through mobile hand-held devices carried by employees.
- In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user (impersonating or masquerading) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.

RAS SECURITY FOR MOBILE DEVICES



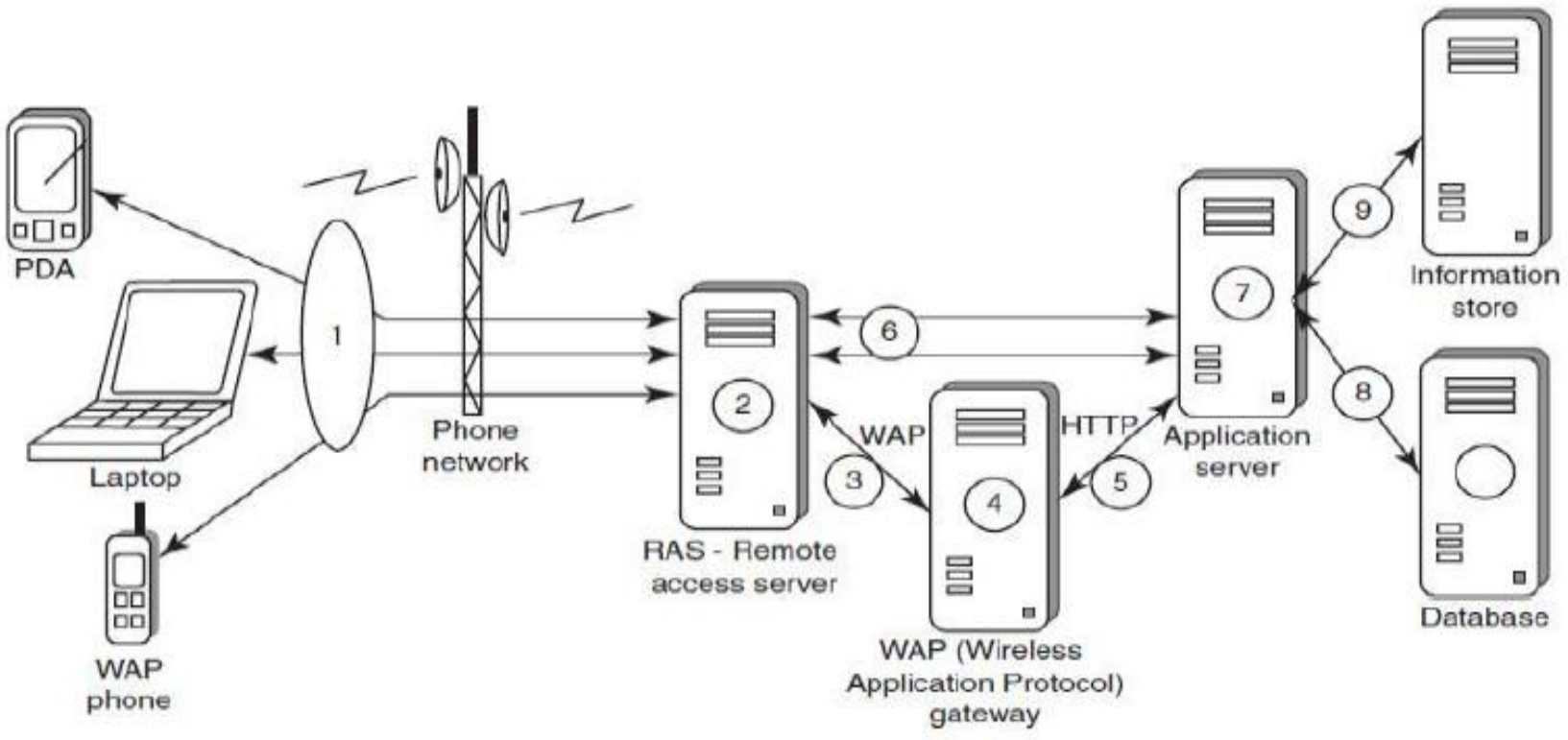


Figure: Communication from mobile client to organization information store.

RAS SECURITY FOR MOBILE DEVICES



- Another threat comes from the practice of port scanning:
- First, attackers use a domain name system (DNS) server to locate the IP address of a connected computer. A domain is a collection of sites that are related in some sense.
- Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls.
- For instance, File Transfer Protocol (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by the attackers.
- Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID.
- A personal firewall on a pocket PC or Smartphone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection

MEDIA PLAYER CONTROL SECURITY



- Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the “music gateways.” 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. For example, in the year 2002, Microsoft Corporation warned about this.
- 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.
- 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.

NETWORKING API SECURITY FOR MOBILE COMPUTING APPLICATIONS



- 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.
- Furthermore, with the advent of Web services and their use in mobile computing applications, the API becomes an important consideration.
- Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications
- 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).
- Technological developments such as these provide the ability to significantly improve cybersecurity of a wide range of consumer as well as mobile devices. Providing a common software framework, APIs will become an important enabler of new and higher value services.

ATTACKS ON MOBILE/CELL PHONES



Mobile Phone Theft

- Mobile phone has transformed from being a luxury to a bare necessity.
- Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users.
- Theft of mobile phones has risen dramatically over the past few years.
- Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims.
- "Contact List" and "Personally Identifiable Information (PII)" really matter when mobile phones are lost.
- After PC, the criminals‘ target has been cell phones due to the following reasons:
  - availability of internet using cell phones.
  - increasing demand for Wi-Fi zones in the metropolitans and
  - extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

ATTACKS ON MOBILE/CELL PHONES



- **Tips to Secure your Cell/Mobile Phone from being Stolen/Lost:**
- Ensure to note the following details about your cell phone and preserve it in a safe place
  - Your phone number;
  - the make and model
  - color and appearance details
  - PIN and/or security lock code
  - IMEI number.

ATTACKS ON MOBILE/CELL PHONES



The International Mobile Equipment Identity (IMEI)

- It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number one can be obtained by entering *#06# from the keypad.
- The IMEI number is used by the GSM network to Identify valid devices and therefore con be used to stop o stolen phone from accessing the network In that country. For example. if a mobile phone is stolen. the owner con call his or her service provider and instruct them lo "lock" the phone using its IMEI number This will help to stop the usage or phone in that country. even if a SIM is changed.

ATTACKS ON MOBILE/CELL PHONES



- 1. Add a security mark on your cell phone. Use permanent marker and print your alternate contact number and short address on your cell phone instrument as well as on battery. In case someone finds your handset it is easier to contact you if the finder of your cell phone would like to return it to you.
- 2. Set a password and ensure the password is strong enough so that a finder of your cell phone cannot easily guess it.
- 3. In case of loss or your cell phone. register a complaint with cell phone service provider immediately using your IMEI number. to enable your service provider to block your cell phone and your account details. Preserve on the details or launched complaints. that is obtain confirmation in writing from your service provider that your phone has been disabled.
- 4. In case of loss of your cell phone, register a complaint at the police station and obtain FIR. Preserve all the details for launched complaints. i.e. FIR report.

ATTACKS ON MOBILE/CELL PHONES



- 5. Keep an eye on your phone while traveling. During the security check at the airport security, ensure to retrieve your cell phone immediately once It enters the x-ray machine - criminals often steal phones during these vulnerable seconds.
- 6. Keep Wi-Fi and Bluetooth OFF when it is not required to be in use. Airports. coffee shops, hotels and all other public places wherever free Wi-Fi zone is available criminals always have an eye to seek the vulnerability to steal information.
- 7. Periodic backup is important and especially if you are traveling, backup before traveling is necessary. It takes only few minutes to take backup but it is always helpful in case you lose your cell phone during traveling.
- 8. Do not forget to apply all the updates for cell phone software/firmware, received from manufacturers, which are routinely provided to update vulnerabilities fixes.
- 9. Only download applications from reputable sources - specific care should be taken while downloading plug-in applications on the cell phone. It is always advised to use the recommendations provided by cell phone manufacturers' to download directly from the Web.

ATTACKS ON MOBILE/CELL PHONES



- Install antitheft software on your cell phone
  - GadgetTrak
  - Back2u
  - Wavesecure
  - F-Secure
- The following factors contribute for outbreaks on mobile devices:

  1. Enough target terminals: The first Palm OD virus was seen after the number of Palm OS devices reached 15million. The 1st 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 user's knowledge.

  2. Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data & 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

ATTACKS ON MOBILE/CELL PHONES



Mobile Viruses:

- A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it.
- 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.
- 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.
- Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS.
- Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones
- MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

ATTACKS ON MOBILE/CELL PHONES



- 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.

ATTACKS ON MOBILE/CELL PHONES



Mishing

- Mishing is a combination of mobile and Phishing. Mishing attacks are attempted using mobile phone technology.
- 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.
- A typical Mishing attacker uses call termed as Vishing or message (SMS) known as Smishing.
- Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
- Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

ATTACKS ON MOBILE/CELL PHONES



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:
  - ID theft
  - Purchasing luxury goods and services
  - Transferring money/funds
  - Monitoring the victims' bank accounts
  - Making applications for loans and credit cards

ATTACKS ON MOBILE/CELL PHONES



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: Text is being messaged in Mobile.

3. Voicemail: Here, Victim is forced to call on the provided phone number, once he/she listens to voice mail.

4. Direct phone Call: Following are the steps detailing on how direct phone call works

   • The criminal gathers cell/mobile phone numbers located and steals mobile phone numbers after accessing cellular company.

   • The criminal often uses a dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.

ATTACKS ON MOBILE/CELL PHONES



- 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.
- The message instructs the victim to call one phone number immediately.
- The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.
- 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 gain additional details such as date of birth, credit card expiration date, etc.

ATTACKS ON MOBILE/CELL PHONES



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 your 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”.

ATTACKS ON MOBILE/CELL PHONES



How to Protect 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. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.
- 5. Report incidents: Report Vishing calls to the nearest cyber police cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

ATTACKS ON MOBILE/CELL PHONES



- **Smishing**
- Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from “SMs phISHING”. SMS – Short Message Service – is the text messages communication component dominantly used into mobile phones.
- SMS can be abused by using different methods and techniques other than information gathering under cybercrime. Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. The popular technique to “hook” the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI. Smishing works in the similar pattern as Vishing

ATTACKS ON MOBILE/CELL PHONES



Pretexting

- It is also a form of social engineering, wherein a pretexter hides his/her purpose and/or identity to get the personal information/sensitive data about another individual. For example. the pretexter may claim his/her affiliation with a survey agency, financial institute or bank. Usually victims are targeted over the phone and enticed to reveal their information or perform on action.

Sexting

- It is the practice of sending sexually explicit text messages and photos over the cell phone. It is becoming an increasingly hot topic both in schools/colleges and in the workplace.

VoIP Spam

- VoIP Spam is the proliferation of unwanted. automatically dialed and prerecorded phone calls using VoIP. Some pundits hove token to referring to it as "Spam over Internet telephony" (SPIT).

ATTACKS ON MOBILE/CELL PHONES



How to Protect from Smishing Attacks:

- 1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
- 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. 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. Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

- **SMS Blocker:** smsBlocker is powered with a unique intuitive algorithm to detect and block Spam SMS automatically. However. mobile user can also customize the filtering levels as per his/her own privacy requirements.

ATTACKS ON MOBILE/CELL PHONES



Hacking Bluetooth:

- Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile device. Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication. The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.
- The attacker installs special software [Bluetooth hacking tools] on a laptop and then installs Bluetooth antenna. Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

ATTACKS ON MOBILE/CELL PHONES



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 is a GUI-based utility for finding discoverable and hidden Bluetooth enabled 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 ON MOBILE/CELL PHONES



- Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.
  - **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 (within 10-m radius), Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.
  - **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.
  - **Bluebugging:** It allows attackers to remotely access a user's phone and use its features without user's attention.
  - **Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo.
- Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking.