19ITOC1004 – Cyber Law and Information Security

Unit II – Cybercrime: Mobile and Wireless Devices

CO2: Describe the cyber-attacks on mobile and wireless devices

LO1:To learn about Mobile and wireless devices

SO1:Discuss about trends in mobility.

Prepared by

G. Keerthika

AP/IT

Unit II
Cybercrime: Mobile and Wireless Devices

Mobile and Wireless Devices - Trend mobility - Authentication Service Security - Attacks on Mobile Phones - Mobile Devices: Security Implications for Organizations – Organizational Measurement for Handling Mobile – Organizational Security Policies and Measures in Mobile Computing Era – Laptops..

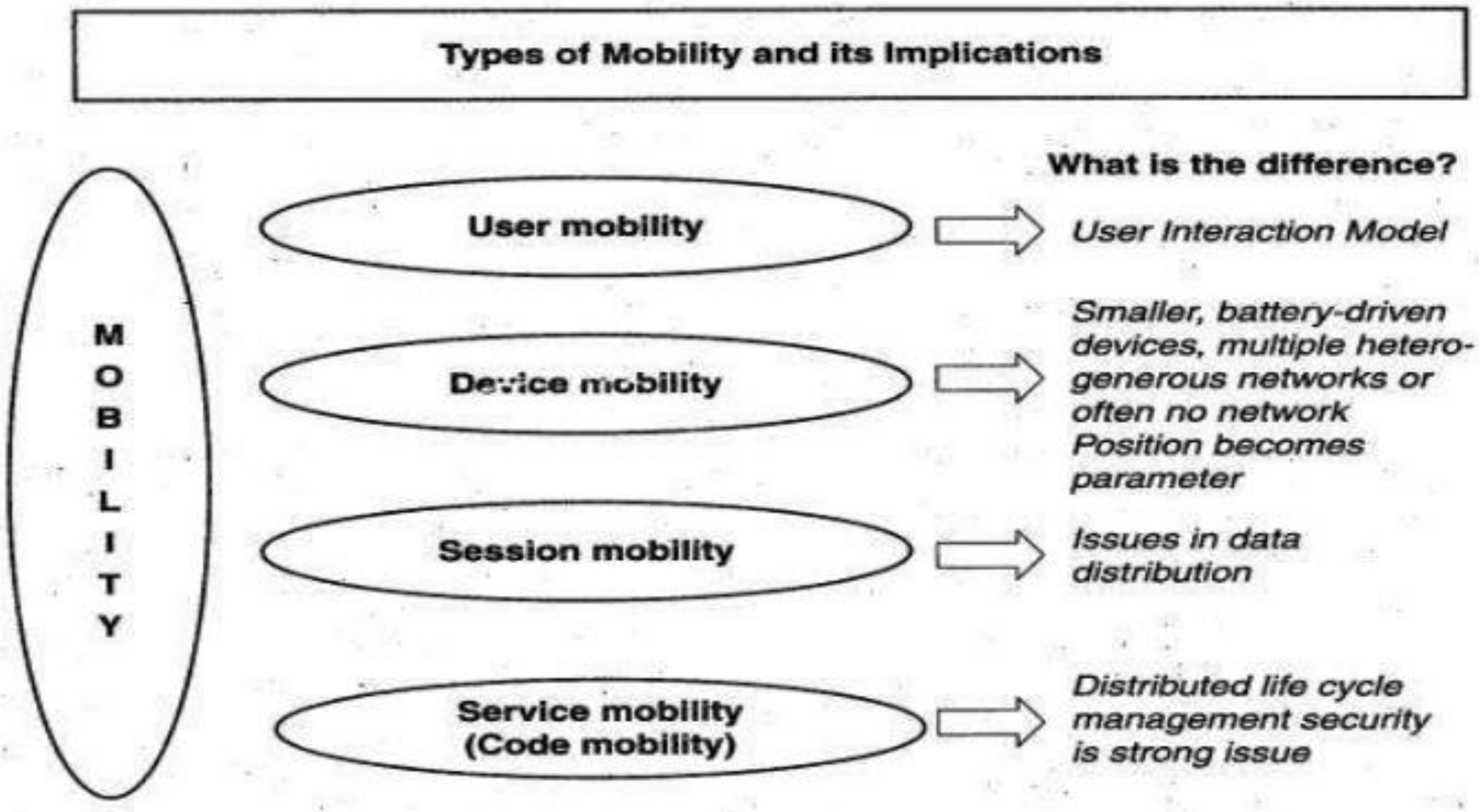
Mobile and Wireless Devices

- Every day, mobile devices are lost, stolen, and infected.
- Mobile devices can store important business and personal information and are often be used to access University systems, email, banking.

Trends in Mobility:

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

Figure:



Types of Mobility and its Implications

What is the difference?

M O B I L I T Y

User mobility → User Interaction Model

Device mobility → Smaller, battery-driven devices, multiple heterogenerous networks or often no network Position becomes parameter

Session mobility → Issues in data distribution

Service mobility (Code mobility) → Distributed life cycle management security is strong issue

Figure: Mobility types and implications

Trends in Mobility(cond..)

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

Types of attacks against 3G mobile networks

1. Malwares, viruses and worms:

- Although many users are still in the transient process of switching from 2G,2.5G2G,2.5G to 3G,3G.
- It is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices.

Few examples of malware(s) in mobile devices

Skull Trojan: I targets Series 60 phones equipped with the Symbian mobile OS.

Cabir Worm: It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology.

The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.

Mosquito Trojan: It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.

Brador Trojan: It affects the Windows CE OS by creating a svchost. exe file in the Windows start-up folder which allows full control of the device.

This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.

Lasco Worm: It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

Types of attacks against 3G mobile networks (contd…)

2. Denial-of-service (DoS): The main objective behind this attack is to make the system unavailable to the intended users.

- Virus attacks can be used to damage the system to make the system unavailable.
- Presently, one of the most common cyber security threats to wired Internetservice providers (iSPs) is a distributed denial-of-service (DDos) attack .
- DDoS attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

Types of attacks against 3G mobile networks (contd…)

3. Overbilling attack: Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes.

In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct

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

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

Dr. MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution (Since 2011)

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003 Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit II – Cybercrime: Mobile and Wireless Devices

CO2: Describe the cyber-attacks on mobile and wireless devices

LO1:To learn about Mobile and wireless devices

SO2:Disscuss about authentication service security.

Prepared by
G. Keerthika
AP/IT

Unit II
Cybercrime: Mobile and Wireless Devices

Mobile and Wireless Devices - Trend mobility - Authentication Service Security - Attacks on Mobile Phones - Mobile Devices: Security Implications for Organizations – Organizational Measurement for Handling Mobile – Organizational Security Policies and Measures in Mobile Computing Era – Laptops..

Authentication Service Security

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

Authentication Service Security (contd…)

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

Attacks on Mobile-Cell Phones:

Mobile Phone Theft:

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

CO2: Describe the cyber-attacks on mobile and wireless devices

LO2:To learn about attacks on mobile devices.

SO1:Discuss about attacks on mobile phones and mobile devices.

Attacks on Mobile-Cell Phones:

The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million.

- The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito.
- This virus sent SMS text messages to the organization without the users' knowledge.

Attacks on Mobile-Cell Phones

2. Enough functionality:

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

3. Enough connectivity:

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

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit II – Cybercrime: Mobile and Wireless Devices

CO2: Describe the cyber-attacks on mobile and wireless devices

LO2:To learn about attacks on mobile devices.

SO2: Summarize about security implications for organization.

Prepared by

G. Keerthika

AP/IT

Unit II
Cybercrime: Mobile and Wireless Devices

Mobile and Wireless Devices - Trend mobility - Authentication Service Security - Attacks on Mobile Phones - Mobile Devices: Security Implications for Organizations – Organizational Measurement for Handling Mobile – Organizational Security Policies and Measures in Mobile Computing Era – Laptops..

Security Implications for Organizations

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

An insider threat

- An insider threat is defined as “the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other ‘trusted’ individuals.”
- Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of “insiders” such as:

1. A malicious insider is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrity and/or availability.

2. A careless insider can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.

3. A tricked insider is a person who is “tricked” into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via “pretexting” (known as social engineering).

Insider Attack Example 1: Heartland Payment System Fraud

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

Privacy - four key dimensions

Cybercrimes take place due to weakness of cyber security practices and "privacy" which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

1.**Informational/data privacy:** It is about data protection, and the users' rights to determine how, when and to what extent information about them is communicated to other parties.

2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.

3. **Communication privacy:** This is as in networks, where encryption of data being transmitted is important.

4. **Territorial privacy:** It is about protecting users' property for example, the user devices from being invaded by undesired content such as SMS or E-Mail/Spam messages.

Information threats to organizations

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

1. Industrial espionage: There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.

2. IP-based blocking: This process is often used for blocking the access of specific IP addresses and/or domain names.

3. IP-based "cloaking": Businesses are global in nature and economies are interconnected.

4. Cyberterrorism: "Cyberterrorism" refers to the direct intervention of a threat source toward the organization's website.

Confidential information leakage: "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solutions

Security and privacy implications from cloud computing

- Cloud computing is one of the top 10 Cyber Threats to organizations. There are data privacy risks through cloud computing.
- Organizations should think about privacy scenarios in terms of “user spheres”.

1. User sphere:

- Here data is stored on users’ desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc.
- Organization’s responsibility is to provide access to users and monitor that access to ensure misuse does not happen.

2. Recipient sphere:

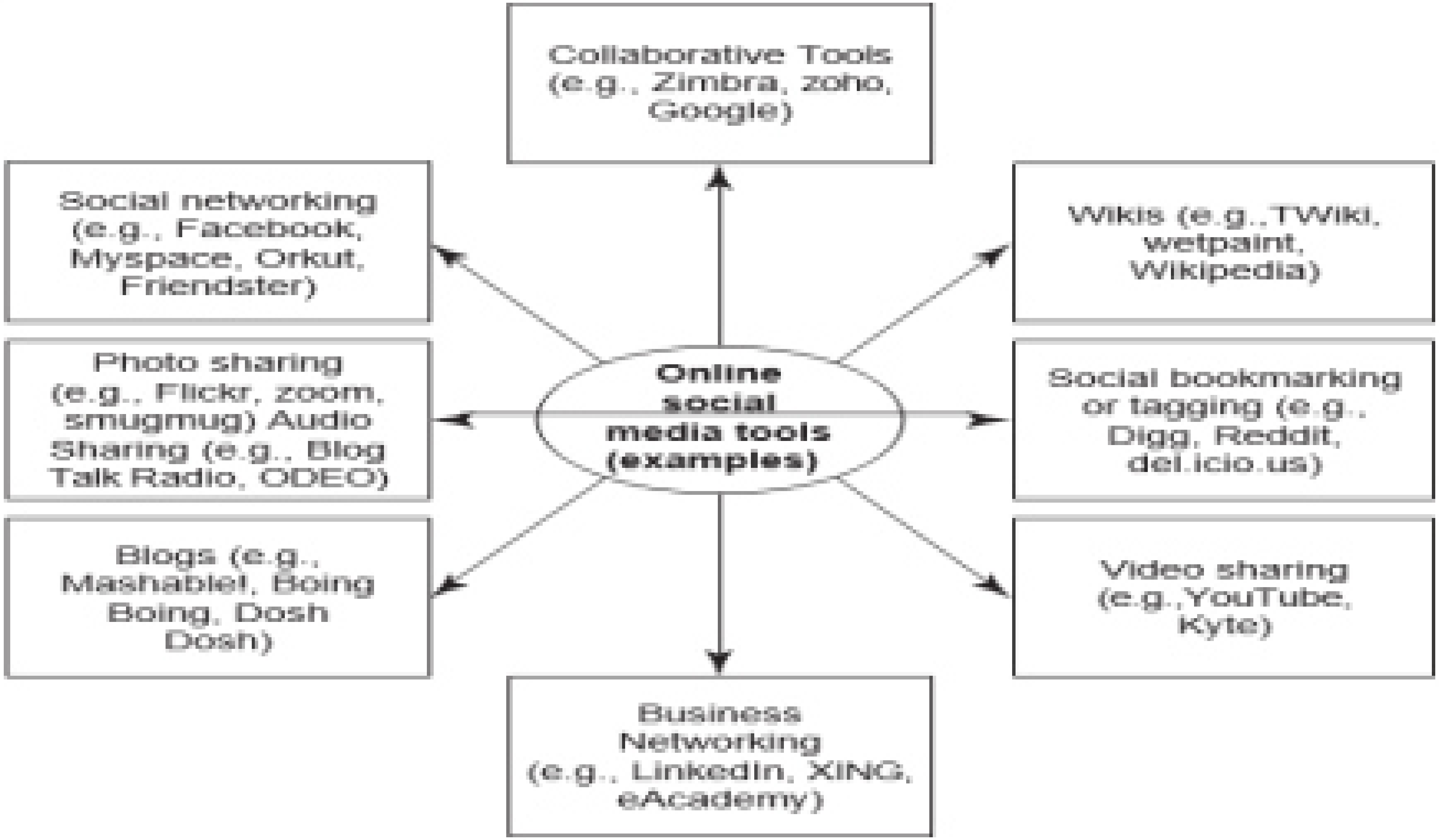
- Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data.
- Organizations responsibility is to minimize users privacy risk by ensuring unwanted exposure of personal data of users does not happen

3. Joint sphere:

- Here data lies with web service provider’s servers and databases. This is the in between sphere where it is not clear to whom does the data belong.
- Organization responsibility is to provide users some control over access to themselves and to minimize users futures privacy risk.

Social Media Marketing: Security Risks and Perils for Organizations

Social media marketing has become dominant in the industry.



Online social media tools (examples)

Collaborative Tools (e.g., Zimbra, zoho, Google)

Social networking (e.g., Facebook, Myspace, Orkut, Friendster)

Wikis (e.g.,TWiki, wetpaint, Wikipedia)

Photo sharing (e.g., Flickr, zoom, smugmug) Audio Sharing (e.g., Blog Talk Radio, ODEO)

Social bookmarking or tagging (e.g., Digg, Reddit, del.icio.us)

Blogs (e.g., Mashable!, Boing Boing, Dosh Dosh)

Video sharing (e.g.,YouTube, Kyte)

Business Networking (e.g., Linkedin, XING, eAcademy)

FIG: Social Media Marketing Tools

Usage of social media sites by large business-to-business (B2B) organizations shows the following:

1. Facebook is used by 37% of the organizations.

2. LinkedIn is used by 36% of the organizations.

3. Twitter is used by 36% of the organizations.

4. YouTube is used by 22% of the organizations.

5. My Space is used by 6% of the organizations.

Understanding Social Media Marketing

- Most professionals today use social technologies for business purposes.
- Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development.
- Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.

2. To increase traffic to their website coming from other social media websites by using Blogs and social and business-networking.

3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.

4. To build credibility by participating in relevant product promotion forums and responding to potential customers’ questions immediately.

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

Other tools used by organizations

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

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit II – Cybercrime: Mobile and Wireless Devices

CO2: Describe the cyber-attacks on mobile and wireless devices

LO3: Describe about Organizational Measurement for Handling Mobile

SO1: Explain about Organizational Security Policies and Measures in Mobile Computing Era

Prepared by
G. Keerthika
AP/IT

Unit II
Cybercrime: Mobile and Wireless Devices

Mobile and Wireless Devices - Trend mobility - Authentication Service Security - Attacks on Mobile Phones - Mobile Devices: Security Implications for Organizations – Organizational Measurement for Handling Mobile – Organizational Security Policies and Measures in Mobile Computing Era – Laptops..

Organizational security Policies and Measures in Mobile Computing Era

- Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think.
- People have grown so used to their hand-helds they are treating them like wallets.
- For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their-hand-held devices.

Organizational security Policies and Measures in Mobile Computing Era (Contd...)

- One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices

- Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, evealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information

Operating Guidelines for Implementing Mobile Device Security Policies

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

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

2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used.

Most mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks.

Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.

Operating Guidelines for Implementing Mobile Device Security Policies (contd...)

3. Standardize the mobile computing devices and the associated security tools being used with them.

As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.

4. Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.

5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.

Operating Guidelines for Implementing Mobile Device Security Policies (contd…)

6. Establish patching procedures for software on mobile devices.

This can often be simplified by integrating patching with syncing or patch management with the centralized

7. Provide education and awareness training to personnel using mobile devices.

People cannot be expected to appropriately secure their information if they have not been told how

Organizational Measurement for Handling Mobile

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

Organizational Measurement for Handling Mobile

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

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit II – Cybercrime: Mobile and Wireless Devices

CO2: Describe the cyber-attacks on mobile and wireless devices

LO3: Describe about Organizational Measurement for Handling Mobile

SO2:Discuss about laptop in cybercrime and its handling procedures.

Prepared by
G. Keerthika
AP/IT

Unit II
Cybercrime: Mobile and Wireless Devices

Mobile and Wireless Devices - Trend mobility - Authentication Service Security - Attacks on Mobile Phones - Mobile Devices: Security Implications for Organizations – Organizational Measurement for Handling Mobile – Organizational Security Policies and Measures in Mobile Computing Era – Laptops.

Laptops

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

Laptops

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

Physical Security Countermeasures

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

1. Cables and hardwired locks

- The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops.
- Kensington cables are one of the most popular brands in laptop security cable.
- These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40%stronger than any other conventional security cables.
- One end of the security cable is fit into the universal securityslot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop.
- These cables come with a variety of options such as number locks, key locks and alarms

2. Laptop safes:

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

3. Motion sensors and alarms

Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops.

Once these devices are activated, they can be used to track missing laptops in crowded places.

Also owing to their loud nature, they help in deterring thieves.

Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals toa certain range around the laptop.

4. Warning labels and stamps:

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

5. Other measures for protecting laptops are as follows:

- Engraving the laptop with personal details
- Keeping the laptop close to oneself wherever possible
- Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves
- Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop.
- Making a copy of the purchase receipt, laptop serial number and the description of thelaptop
- Installing encryption software to protect information stored on the laptop
- Using personal firewall software to block unwanted access and intrusion
- Updating the antivirus software regularly

5. Other measures for protecting laptops are as follows:

- Tight office security using security guards and securing the laptop by locking it down in lockers when not in use
- Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti theft device;
- Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

Logical or access controls

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

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/ access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handing of removable drives/storage mediums /unnecessary ports.
6. Password protection through appropriate passwords rules and use of Strong passwords.

Logical or access controls

7. Locking down unwanted ports/devices.

8. Regularly installing security patches and updates.

9. Installing antivirus software/firewalls / intrusion detection system (IDSs).

10. Encrypting critical file systems.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You