GRADAMIC

B.Tech-2nd Year
Session 2023-24
Odd/Even Semester

Dr. A. P. J. Abdul Kalam Technical University
Lucknow, Uttar Pradesh

CYBER SECURITY

(BCC301 / BCC401/ BCC301H / BCC401H)

app.gradamic.com

UNIT - 2nd

UNIT - II

CYBER CRIME: *Mobile and Wireless Devices-Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era.*

Que 1. Explain the rising importance of mobile and wireless devices.

Ans. The rising importance of mobile and wireless devices can be attributed to several factors, reflecting their profound impact on various aspects of our personal and professional lives.

Here are some key reasons for their growing significance:

1. Ubiquity and Accessibility: Mobile devices have become ubiquitous, and wireless connectivity allows users to access information and services from virtually anywhere.

2. Communication and Connectivity: Mobile devices serve as powerful communication tools, enabling voice calls, text messaging, and a wide range of multimedia applications. The evolution of wireless technologies like 4G and 5G has enhanced data transfer speeds, ensuring seamless connectivity for a variety of applications.

3. Productivity and Remote Work: Mobile devices empower individuals to work remotely and stay productive while on the go. The ability to access emails, documents, and collaboration tools from mobile devices has become essential for professionals and businesses, fostering flexibility and efficiency.

4. E-commerce and Mobile Banking: Mobile devices have revolutionized the way people shop and manage their finances. Mobile e-commerce applications and mobile banking services have become integral parts of daily life, offering convenience and accessibility for transactions and financial management.

5. Education and Learning: Mobile devices have become essential tools for education, allowing students to access learning materials, collaborate with peers, and engage in online courses.

6. Navigation and Location-Based Services: GPS technology integrated into mobile devices has revolutionized navigation and location-based services. Users can easily find directions, discover nearby businesses, and access location-specific information, enhancing convenience and efficiency.

7. Social Connectivity: Social media platforms, which are predominantly accessed through mobile devices, play a significant role in connecting people globally.

Mobile devices facilitate instant communication, sharing of experiences, and real-time updates, fostering a sense of community.

Que 2. Write a short note on the proliferation of mobile and wireless devices.

Ans. ***The proliferation of mobile and wireless devices:***

ϖ The proliferation of mobile and wireless devices represents a transformative trend in modern society, influencing the way we live, work, and connect.

This phenomenon is characterized by the widespread adoption and rapid increase in the use of mobile technologies across diverse demographics and sectors.

ϖ Several key factors contribute to this proliferation. Advances in wireless communication technologies, such as 4G and 5G networks, have significantly enhanced the speed and reliability of data transfer, making mobile devices more appealing and versatile.

ϖ The ubiquity of mobile devices is evident in their diverse applications.

From communication and social interaction to productivity, entertainment, and education, mobile devices have become indispensable tools in our daily lives.

ϖ This proliferation has profound implications for global connectivity and collaboration.

Mobile devices facilitate instant access to information, enable real-time communication, and bridge geographical gaps.

Businesses leverage mobile technologies to enhance productivity, while educational institutions integrate them into learning environments, transforming traditional approaches to education.

Que 3. What do you mean by credit card fraud in the context of mobile and wireless computing?

Ans. ***Following is a breakdown of the impact of cybercrimes on these categories***:

1. Financial losses: Individuals can suffer financial losses through various cybercrimes. Cybercriminals may steal money directly from bank accounts or make unauthorized purchases using stolen financial information.

2. Privacy invasion: Cybercrimes often involve the unauthorized access or theft of personal information, leading to a breach of privacy. This can result in emotional distress and psychological harm.

3. Identity theft: Victims of cybercrimes like identity theft may experience long-term consequences, including damage to their credit scores and difficulties in reclaiming their identities.

4. Emotional distress: Being a victim of cyber bullying, online harassment, or cyber stalking can cause significant emotional distress and mental health issues.

Que 4. Give distinction among the key terms: mobile computing. wireless computing and handheld devices.

Ans.

Term	Description	Characteristics
Mobile computing	Mobile computing refers to the use of computing devices that are not confined to a single physical location. It involves the ability to access and transmit data while on the move.	• Portability • Wireless Connectivity • Versatility
Wireless computing	Wireless computing refers to the use of computing devices that communicate and exchange data without the need for physical cables or wired connections. It focuses on the wireless transmission of data between devices	• Wireless Communication • Flexibility • Scalability
hand-held devices	Handheld devices are a category of portable computing devices that are specifically designed to be held and operated with one or both hands. They are compact, lightweight, and often feature touchscreens or other intuitive interfaces	• Size and Form Factor • Multifunctionality

Que 5. Discuss the present trends in mobility. What are mobility types and their implications?

Ans. Present trends in mobility:

- Mobile computing is entering a new phase offering enhanced usability, faster networking, and a wider range of applications.
- Prominent examples of this trend include Apple's "iPhone" and the Google-driven "Android" phones, with numerous other advancements reinforcing this direction.

- The growing popularity of this intelligent mobile technology has also attracted the attention of attackers, including hackers and crackers.
- It is essential to pay attention to the evolving trends in mobile computing to appreciate the significance of cybersecurity concerns within this domain.

Mobility types and their implications:

1. User mobility: User mobility refers to the ability of individuals to move physically while maintaining network connectivity and access to services. It involves users accessing network resources from different locations or devices.

Implications:

- **Flexibility:** User mobility allows individuals to work or access services from various locations, which can increase flexibility and productivity
- **Challenges:** Managing security and authentication becomes crucial to ensure that users are granted access only from authorized locations of devices.
- **Data synchronization:** Ensuring that users have access to the same data and services regardless of their location or device requires efficient data synchronization methods.

2. Device mobility: Device mobility refers to the ability of devices (e.g., smartphones, laptops, tablets) to move between different access or networks while maintaining uninterrupted connectivity.

Implications:

- **Seamless connectivity:** Device mobility ensures that users experience continuous network connectivity, even when moving between Wi-Fi networks, cellular networks, or other access points.
- **Handoff mechanisms:** Implementing efficient handoff mechanisms is essential to ensure a smooth transition between different access points.
- **Quality of Service (QoS**): Maintaining QoS is a challenge, as devices may switch between networks with varying bandwidth and reliability.

3. Session mobility: Session mobility refers to the capability to transfer an ongoing network session from one device or network to another without interruption.

Implications:

- **Seamless handover:** Users can switch devices or networks without losing their active sessions, which is essential for applications like video conferencing.
- **Protocol support:** Implementing protocols like Mobile IP or SIP (Session Initiation Protocol) is necessary to support session mobility.
- **Resource management:** Managing resources, such as IP addresses or server connections, during session handovers is crucial for maintaining the user experience.

4. Service mobility: Service mobility involves the ability to access the same services or applications from different devices or locations.

Implications:

- **Cross-platform compatibility:** Services must be designed to work seamlessly across various devices and platforms to accommodate service mobility.
- **Data accessibility:** Ensuring that users have access to their data and services regardless of the device they use is a key consideration.
- **Cloud-based solutions:** Many services leverage cloud computing to provide consistent access and functionality across different devices and locations.

Que 6. Describe the popular types of attacks against 3G mobile networks.

Ans. Following are the different categories or types of cybercrimes.

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

1. Malware, viruses, and worms: Malware, viruses, and worms are malicious software programs that can infect mobile devices within a 3G network. They are typically designed to compromise device security, steal sensitive data, or disrupt network operations.

2. Denial-of-Service (DoS): Denial-of-Service attacks aim to overwhelm 3G network resources, rendering them unavailable to legitimate users. Attackers flood the network with traffic or exploit vulnerabilities to disrupt services.

3. Overbilling attack: Overbilling attacks involve manipulating 3G network protocols or exploiting vulnerabilities to generate fraudulent billing for data or services, leading to financial losses for users.

4. Spoofed Policy Development Process (PDP): In a spoofed PDP attack, malicious entities impersonate a legitimate device to establish a policy context in a 3G network. This allows unauthorized access to network resources.

5. Signalling-level attacks: Signalling-level attacks target the communication protocols used in 3G networks to establish and manage connections. Attackers manipulate these protocols to disrupt services or intercept communication.

Que 7. Discuss credit card frauds in mobile and wireless computing era. Give some tips to prevent credit card frauds.

Ans. ***Credit card frauds in mobile and wireless computing era:***

- Emerging trends in cybercrime related to mobile computing include mobile commerce (MCommerce) and mobile banking (M-Banking).
- The prevalence of credit card fraud is on the rise due to the increasing power and decreasing prices of mobile hand-held devices, making these gadgets readily available to almost anyone.

- Mobile credit card transactions have become commonplace, with new technologies merging affordable mobile phone capabilities and point-of- sale (POS) terminal functionalities.
- The contemporary era is characterized by "mobile computing." emphasizing the ability to compute anywhere and anytime.
- Credit card companies typically assist consumers in resolving identity (ID) theft issues after they occur, but they could further reduce ID fraud by providing consumers with enhanced tools to monitor their accounts and restrict high-risk transactions.

Tips to prevent credit card fraud:

❖ Do's:

1. Sign your card as soon as you receive it.

2. Make photocopies of both sides of your card and store them securely to retain the card number and expiration date in case of card loss.

3. Change the default Personal Identification Number (PIN) received from the bank before initiating any transactions.

4. Maintain vigilance over your card during transactions and ensure its immediate return.

5. Safeguard all receipts for later comparison with your credit card statement.

6. Verify the authenticity of a website before providing your card details.

7. Notify your bank promptly in the event of card loss and report it to the police if necessary.

❖ Don'ts:

1. Avoid storing your card number and PINs in your cell phone.

2. Refrain from lending your cards to anyone.

3. Never leave cards or transaction receipts lying unattended.

4. Do not sign a blank receipt; if the transaction details are unclear, request another receipt to verify the amount.

5. Avoid writing your card number or PIN on a postcard or the outside of an envelope.

6. Do not disclose your account number over the phone immediately, unless you are calling a trusted company or your bank.

7. Do not dispose of credit card receipts by simply discarding them into a garbage box or dustbin.

Que 8. What are the different types and techniques of credit card fraud?

Ans. The following are different types and techniques of credit card fraud:

1. Traditional Techniques:

- **ID theft:** Identity theft involves fraudsters stealing personal information, such as a person's name, address, and credit card details, to impersonate the victim and make unauthorized transactions.
- **Financial fraud:** Financial fraud includes a range of fraudulent activities where criminals use stolen credit card information to make unauthorized purchases, cash advances, or transfers of funds. It can involve card-present or card-not-present transactions.

2. Modern Techniques:

- **Triangulation:** Triangulation fraud involves fraudsters creating a complex network of online transactions. They use a stolen credit card to purchase goods from one online store, have those goods shipped to another address, and then resell them through a third-party marketplace.
- **Credit card generators:** Credit card generators are software programs or tools that create fake credit card numbers that may pass initial validation checks, Criminals use these fake numbers to attempt unauthorized transactions.

Que 9. What are the security challenges posed by mobile devices to cybersecurity?

Ans. ***Mobility brings two main challenges to cybersecurity:***

1. On hand-held devices, information is being taken outside the physically controlled environment: This challenge refers to the fact that mobile and hand-held devices, such as smartphones, tablets, and laptops, are inherently portable. Users carry them outside the physically controlled and secure environments typically found in office or home settings.

2. Remote access back to the protected environment is being granted: This challenge relates to the need to provide remote access to corporate networks or protected environments from mobile devices Users require this access to work and access resources while not physically present in the controlled network environment.

Que 10. What are the technical challenges associated with mobile security?

Ans. ***Some well-known technical challenges in mobile security are:***

1. Managing the registry settings and configurations: Mobile devices often rely on configuration settings stored in the registry Managing these settings securely is a challenge, as unauthorized access security.

2. Managing the authentication service security: Ensuring secure authentication services on mobile devices is crucial. Authentication. mechanisms, such as biometrics, PINs, and passwords, must be protected to prevent unauthorized access to the device and associated services.

3. Cryptography security: Cryptography is essential for securing data on mobile devices, particularly during data transmission and storage. 3. Lightweight Directory Access Protocol (LDAP) security: LDAP is often used for directory services in mobile applications. Ensuring the security of LDAP directories is vital to protect user identities and access control.

4. Remote Access Server (RAS) security: RAS systems enable remote access to corporate networks. Securing RAS is crucial to prevent unauthorized access, data breaches, and attacks.

5. Media player control security: Mobile devices often include media players that can access streaming content or local media files. Securing media player controls is essential to prevent vulnerabilities that could be exploited for malicious purposes.

6. Networking application program interface (APD) security: Mobile applications rely on networking APIs to communicate with servers and services. Securing these APIs is essential to prevent data leaks, unauthorized access, and API abuse.

Que.11 What do you understand by authentication services security? Discuss the types of attacks to which mobile devices are subjected to.

Ans. ***Authentication services security:***

1. Authentication services security refers to the measures and practices put in place to ensure that users and devices attempting to access a network, application, or service are legitimate and authorized.

2. It is a fundamental aspect of mobile and wireless security aimed at verifying the identity of users and devices to prevent unauthorized access and protect sensitive information.

3. Authentication services security is crucial for safeguarding sensitive data, protecting networks, and ensuring that only authorized users and trusted devices can access resources and services.

4. It is an essential component of a robust mobile and wireless security strategy.

Types of attacks: Mobile devices are subject to the following types of attacks:

1. Push attacks: Push attacks are malicious actions initiated by external entities or applications to exploit vulnerabilities in a mobile device. These attacks often involve the unauthorized installation of malware, malicious apps, or files onto the device without the user's consent or knowledge.

2. Pull attacks: Pull attacks involve the mobile device actively seeking and downloading malicious content or software from untrusted sources, often without the user's awareness. These attacks occur when a user unknowingly initiates actions that lead to the compromise of their device.

3. Crash attacks: Crash attacks aim to destabilize a mobile device by exploiting software vulnerabilities. Attackers deliberately send malformed or malicious data to the device, causing applications, services, or even the entire operating system to crash.

Que 12. Describe the various types of attacks against mobile/ cell phones.

Ans. Following the various types of attacks against mobile/cell phones:

1. Mobile phone theft: Mobile phone theft occurs when a mobile device is physically stolen by a perpetrator. The theft can happen through snatching, pickpocketing, or burglary. The thief gains unauthorized access to the victim's personal data, contacts, messages, photos, and potentially sensitive information.

2. Mobile viruses: Mobile viruses are malicious software programs specifically designed to infect and disrupt the operation of mobile devices. These viruses can spread through infected apps, downloads, or malicious links. Mobile viruses can compromise device security, steal personal information, send unauthorized messages, or render the device unusable.

3. Mishing: Mishing (Mobile Phishing) is a cyber-attack where attackers use text messages (SMS) to trick users into divulging sensitive information, such as login credentials, account numbers, or personal details.

4. Vishing: Vishing (Voice Phishing) involves attackers using phone calls to impersonate legitimate entities, such as banks or government agencies, to manipulate victims into revealing confidential information or performing certain actions.

5. Smishing: Smishing (SMS Phishing) is a form of phishing where attackers send deceptive SMS messages containing malicious links or prompts to trick users into revealing personal information or installing malware. Smishing can lead to malware infections, identity theft, or unauthorized access to sensitive accounts.

6. Hacking Bluetooth: Hacking Bluetooth involves unauthorized access to a device's Bluetooth connection. Attackers can exploit vulnerabilities to gain control of the device, eavesdrop on communications, or transmit malicious content.

Que 13. What are the various security implications for organizations related to mobile devices?

Ans. The following are various security implications for organizations related to mobile devices:

❖ **Managing diversity and proliferation of hand-held devices:**

- For most organizations, cyber security remains a primary concern.
- Many organizations overlook the long-term importance of maintaining records of mobile device ownership.
- Regardless of whether employees receive devices from the organization, their mobile devices should be registered in the corporate asset register.
- Furthermore, diligent monitoring of these devices is necessary in terms of their usage.
- Upon an employee's departure, it is crucial to revoke both logical and physical access to organizational networks.

- Consequently, company-owned mobile devices should be surrendered to the IT department and, at a minimum, deactivated and thoroughly cleansed.

❖ Unconventional/Stealth storage devices:

- Secondary storage devices, like USB drives, used by employees pose a potential cyber security risk.
- Advancing technology leads to the continual reduction in the size and diversification of these devices.
- Modern storage devices are challenging to detect, presenting a significant security concern for organizations.
- Their compact dimensions enable inconspicuous concealment within bags or on one's person.
- Advisable measures include prohibiting employee usage of these devices, as they can introduce viruses, worms, and Trojans into the organizational network, potentially causing data loss.

❖ Threats through lost and stolen devices:

- This presents a newly emerging cyber security concern.
- Mobile handheld devices are frequently misplaced during people's travels.
- Misplaced mobile devices pose an even greater security threat to corporations.
- The cyber security threat in this scenario is concerning due to the generally inadequate security on mobile devices.
- The value of the handheld device itself is often insignificant compared to the critical content it holds; its loss or theft can jeopardize a company's professional integrity, subjecting it to sabotage, exploitation, or damage.
- Many of these lost devices have wireless access to corporate networks and minimal security, making them a vulnerable point and a significant challenge for security administrators.

Que 14. Discuss what organizations can do toward safeguarding their information systems in the mobile computing paradigm.

Ans. ***Organizations can do following to safeguard their information systems:***

A. Encrypting organizational databases:

1. Hand-held devices now offer access to critical and sensitive data stored in databases, thanks to technological advancements.

2. Protecting the organization's data from loss necessitates encrypting such databases.

3. Typically, two algorithms are employed to implement strong encryption of database files: • The Rijndael algorithm • The Multi-Dimensional Space Rotation (MDSR) algorithm

4. In this context, "strong encryption" implies greater resistance to decryption attempts that can impact performance significantly.

5. Employing either AES or MDSR algorithms for database file encryption renders the database unusable without the key (password).

6. When implementing strong encryption, it's crucial not to store the key on mobile devices.

7. The key is case-sensitive and must be accurately entered to access the database.

8. For enhanced security, there's an option to prompt the user to enter the encryption key via a dialog box displayed by the database server.

9. To safeguard against information theft through mobile devices connecting to corporate databases, additional security measures can be implemented, including a server-controlled self-destruct policy.

B. Including mobile devices in security strategy:

1. The responsibility for addressing cyber security threats stemming from improper access to organizational data by mobile-device-using employees falls squarely on the shoulders of IT departments.

2. Encrypting corporate databases doesn't mark the conclusion of security measures.

3. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse.

4. There exist technologies capable of adequately securing mobile devices, which suffice for the majority of organizations.

Que 15. Discuss the importance of security policies relating to mobile computing devices.

Ans. Security policies for mobile computing devices are crucial in today's interconnected and mobile-driven world. As smartphones, tablets, and other portable devices become increasingly integral to both personal and professional aspects of our lives, the need for robust security measures becomes more pronounced.

Here are several reasons highlighting the importance of security policies for mobile computing devices:

1. Data Protection: Mobile devices often store sensitive and confidential information, including personal data, financial details, and business-related information. Security policies help safeguard this data from unauthorized access, ensuring the privacy and protection of individuals and organizations.

2. Network Security: Mobile devices often connect to various networks, including public Wi-Fi, which can pose security risks. Security policies guide users on secure network practices, such as using virtual private networks (VPNs) and avoiding unsecured networks, to protect against eavesdropping and man-in-the middle attacks.

3. Malware and Phishing Protection: Mobile devices are susceptible to malware and phishing attacks, which can compromise data and system integrity. Security policies guide users on safe browsing practices, using reputable app stores, and installing security software to mitigate these threats.

4. Awareness and Training: Security policies are crucial in educating employees about potential risks and best practices for mobile security. Regular training programs help foster a securityconscious culture within organizations, reducing the likelihood of human error leading to security incidents.

5. Device Loss or Theft: Mobile devices are easily lost or stolen, putting sensitive information at risk. Security policies often include measures like remote wipe capabilities, encryption, and tracking features to mitigate the impact of device loss and prevent unauthorized access to stored data.

Que 16. Give the operating guidelines for implementing mobile device security policies.

Ans. ***Following are the operating guidelines for implementing mobile device security policies:***

1. Assess whether organizational employees require the use of mobile computing devices.

2. Deploy additional security technologies such as robust encryption, device passcodes, and physical locks.

3. Standardize both the mobile computing devices and the associated security tools used in conjunction with them.

4. Formulate a dedicated framework for the utilization of mobile computing devices.

5. Maintain an inventory to track who is using which types of devices.

6. Institute patching protocols for software on mobile devices.

7. Label the devices and register them with an appropriate service.

8. Establish procedures for disabling remote access to any mobile device.

9. Eradicate data from computing devices that are not in active use.

10. Offer education and awareness training to personnel utilizing mobile devices.