SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 1: INTRODUCTION TO NETWORK AND CYBER SECURITY

Topic : Cyber Crime

DEFINITION

- Cybercrime involves criminal activities carried out through computers and the internet, encompassing hacking, malware, identity theft, and online fraud.
- Motivations include financial gain, ideological objectives, and personal vendettas.
- As technology advances, cybercriminals continually adapt, making robust cybersecurity crucial for safeguarding digital assets.

Types of cyber crime

1. **Phishing:** In phishing, attackers deceive individuals into providing sensitive information by disguising as trustworthy entities through fraudulent emails, messages, or websites.
2. **Ransomware:** Ransomware involves malicious software that encrypts a user's files, demanding a ransom for their release, posing significant threats to individuals and organizations' data security.
3. **Identity Theft:** Identity theft occurs when personal information is stolen to impersonate someone else, often for financial gain, leading to fraudulent activities and potential damage to the victim's reputation.
4. **DDoS Attacks (Distributed Denial of Service):** DDoS attacks overwhelm a target's online services by flooding them with traffic, causing disruption or shutdown, illustrating the potential impact of coordinated efforts to cripple digital infrastructures.

Real world examples

1. **WannaCry Ransomware Attack (2017):** A global cyberattack that encrypted data on infected computers, demanding ransom payments in Bitcoin for decryption keys, affecting organizations worldwide.
2. **Equifax Data Breach (2017):** One of the largest data breaches, compromising sensitive personal information of 147 million individuals due to a vulnerability in the company's website software, leading to widespread identity theft concerns.

Real world examples

1. **WannaCry Ransomware Attack (2017):** A global cyberattack that encrypted data on infected computers, demanding ransom payments in Bitcoin for decryption keys, affecting organizations worldwide.
2. **Equifax Data Breach (2017):** One of the largest data breaches, compromising sensitive personal information of 147 million individuals due to a vulnerability in the company's website software, leading to widespread identity theft concerns.

Motive behind cyber crime

- Motivations behind cybercrime include financial gain, ideological motives, political objectives, and revenge.
- Cybercriminals seek to exploit vulnerabilities in digital systems for personal, monetary, or strategic advantages, posing threats to individuals, organizations, and governments.

Cyber Security Challenges

1. **Rapid Technological Advancements:** The swift evolution of technology creates challenges for cybersecurity as cybercriminals exploit new vulnerabilities, necessitating constant adaptation and updates to defense mechanisms.
2. **Skill Gap in the Cybersecurity Workforce:** The shortage of skilled cybersecurity professionals poses a significant challenge, as organizations struggle to find and retain talent capable of defending against increasingly sophisticated cyber threats.

Cyber security Practices

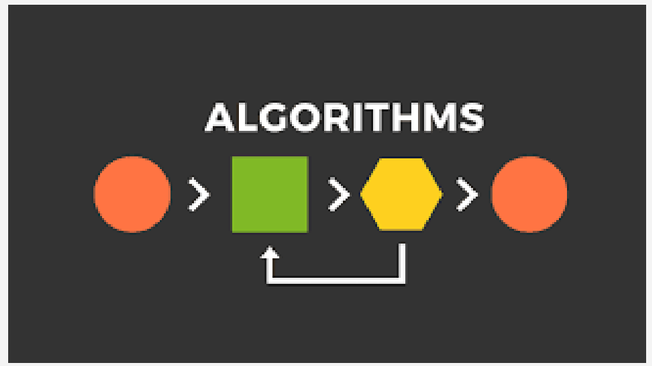
1. **Strong Password Policies:** Implementing robust password protocols, including complex combinations of characters and regular updates, helps safeguard digital accounts from unauthorized access.
2. **Multi-factor Authentication (MFA):** MFA adds an extra layer of security by requiring users to provide multiple forms of identification, such as passwords and unique codes, enhancing protection against unauthorized access and identity theft.

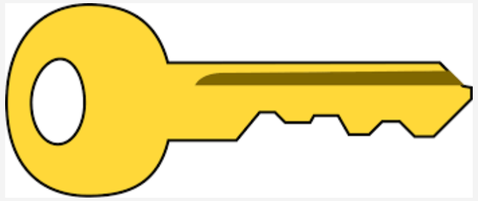
Future Trends in Cybercrime

- Future trends in cybercrime include the increased use of artificial intelligence and machine learning by cybercriminals to create more sophisticated and adaptive attacks.
- Additionally, the rise of quantum computing poses new challenges, potentially enabling cyber threats that can bypass traditional encryption methods.

Four basic tasks in designing a particular security service

- Design a suitable algorithm for the security transformation
- Generate the secret information (keys) used by the algorithm
- Develop methods to distribute and share the secret information
- Specify a protocol enabling the principals to use the transformation and secret information for a security service





References

- William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.
- Behrouz A. Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.