Lecture 1: Network Security

1. The Problem of Network Security:

Attackers only need one weak point.

Defenders must protect all points.

2. Attacks by Network Layers (OSI Model):

Application Layer:

Phishing, Email spoofing, Modem hijacking, DNS poisoning.

Transport Layer:

Denial of Service (DoS), Connection hijacking.

Network Layer:

IP spoofing, Routing attacks.

Link Layer:

Broadcast storms, MAC address spoofing.

3. Attack Enhancement:

Distributed DoS (DDoS) using botnets, hard to trace and protect.

Host fingerprinting: identify systems to target (attack).

4. Protection Methods:

Application Layer:

Secure Email (S/MIME, PGP).

HTTPS (TLS for web).

Secure DNS (DNSSECURITY).

Transport Layer:

Transport Layer Security (TLS)/Secure Sockets Layer(SSL): **Encrypts app data.**

Simple Authentication and Security Layer(SASL): **Authentication in open connections. e.g., in secure SMTP.**

Randomized Initial Sequence Number (ISNs): **to prevent hijacking.**

Network Layer:

Virtual Private Network (VPNs): **Secure tunnel over the Internet.**

IPSec(sublayer): **AH (auth Header), ESP (encryption), SA (security associations).**

Link Layer:

WiFi: **WEP (weak), WPA (better), WPA2 (best).**

Use secure methods beyond WiFi.

Filtering switches prevent spoofing.

5. Firewalls:

Firewall: **All traffic must pass through.**

Network Address Translation (NAT): **Only open ports receive data.**

Honeypot: **Fake system to catch attackers.**

6. Hacking Phases:

1. Reconnaissance: **Info gathering.**

2. Scanning: **Find open ports and devices.**

3. Gaining Access: **Sniffing, spoofing, cracking.**

7. Types of Attacks:

Eavesdropping, Traffic analysis, Footprinting.

DoS, Spoofing, Message modification, Packet replay, Man-in-the-middle, SQL injection.

8. Botnets:

Zombies controlled remotely.

Used for spam, DDoS, hosting illegal content.

9. Defense in Depth:

Use multiple layers: **routers, firewalls, Intrusion Detection System(IDS), VPNs, strong policies.**

Bastion Host: **Highly secured system.**

10. Filters:

Route Filter: **Verifies IPs.**

Packet Filter: **Checks headers.**

Content Filter: **Checks message content.**

11. Data Privacy Concepts:

Confidentiality: **Keep info secret (encryption).**

Authenticity: **Verify sender (digital signatures).**

Integrity: **Ensure unmodified data (hashing).**

Non-repudiation: **Can't deny sending (signatures).**

Lecture 2: Cyber

Cybercrime: **cybercrime is a fast-growing area of crime using Internet and computers.**

Cybercrime's areas:

1.**Attacks against computer hardware and software.**

2. **Financial crimes and corruption.**

3.**Crimes against children.**

Cybercrimes Against individuals:

1.**Email spoofing.**

2.**Fraud.**

3.**Phishing.**

4.**Cyber stalking.**

5.**Hacking computers.**

Cybercrimes Against society:

1.**Polluting the youth through indecent exposure.**

2.**Trafficking financial crimes.**

3.**Sale of illegal articles.**

4.**Online gambling.**

Cybercrimes Against government & organizations:

1.**Cyber terrorism.**

2.**Distribution of pirated software.**

3.**Unauthorized control/access. over computer system.**

4.**Possession of unauthorized information.**

5.**Forgery.**

Cyber Security: **Involves protection of sensitive personal and business information through prevention, detection and response to different online attacks.**

Cyber Forensics: Computer Forensics, is the application of scientifically proven methods to gather, process, interpret, and to use digital evidence to provide a conclusive description of cyber-crime activities.

Cyber Law: **Any laws relating to protecting the internet and other online communication technologies.**

Needs for cyber law:

1.**Integrity and security information**

2.**Security of Government Data**

3.**Intellectual property rights**

4.**Privacy and confidentially of information**

5.**Legal status of online Transactions**

to become a safe from cybercrime needs to:

1.**Avoid using peer to peer programs.**

2.**Avoid downloading unnecessary applications and freeware.**

3.**Do not open suspicious files/emails.**

Lecture 3: Dark Web

Internet, Dark Web and Deep Web:

The Internet**: This is the easy one. It's the common Internet everyone uses.**

The Deep Web: **Is a subset of the Internet that is not indexed by the major search engines. You have to visit those places directly instead of been able to search for them.**

The dark web: **The dark web is a hidden part of the internet that you can't access with normal browsers or search engines. It's used for privacy and sometimes for illegal activities.**

Search Engines: **Programs that search documents for specified keywords or phrases and returns a list of documents where the keywords were found.**

How search Engines Work:

Uses a spider program to fetch as many webpages as possible ,A program called an indexer then reads these webpages and creates an index, storing the URL and important content of webpage, Each search engine has its own ranking algorithm that returns results based on their relevance to the user's specified keywords or phrases.

Access to Dark web = Access to Information

Lecture 4: Malware

1. What is Malware?

Malware: **Malicious software Used to: Disrupt systems, Steal info Gain, unauthorized access**

Types: **Virus, Worm, Trojan horse, Spyware, Others**

2. Differences Between Virus, Worm, Trojan, Virus:

Virus: **Needs human action to spread., Attaches to files/programs., Doesn't act unless executed.**

Worm: **Spreads on its own., Exploits system features., Can replicate and slow down the system.**

Trojan Horse: **Looks like legit software., Hidden damage or creates a backdoor., Doesn't replicate by itself.**

3. How to Protect Your Computer:

1. **Understand how malware works.**
2. **Use updated antivirus.**
3. **Turn on your firewall.**
4. **Always backup your important files.**

Lecture 5 : Social Engineering & Privacy

What is 'Personal Information'?

Personal information is any data that can identify a person directly or indirectly, especially when combined with other linked information.

Personal Information Online:

Internet Uses: **Communication, Shopping, Banking, social media, Gaming.**

Risks: **Hacking, Scams, Identity Theft, Data Leaks, Malware.**

Safety Tips: **Use strong passwords, shop on secure sites, adjust privacy settings, avoid oversharing, enable two-factor authentication.**

Social Engineering:

Social engineering: **is tricking people into doing things or giving information that helps an attacker.**

A hacker **may use social engineering to gather information for revenge, fun, or profit. They might steal data, access accounts, or commit fraud for financial gain.**

Email: **Used to send phishing or spread malware.**

Social Media: **Impersonation for scams.**

Bank Info: **Enables fraud or theft.**

Business Data: **Used for blackmail.**

Personal Info: **Sold or used for identity theft.**

Gaming Accounts: **Held for ransom.**

Shopping History: **Sold for targeted ads.**

Social Engineering:

Hardware Locks & Security: **Physical measures to keep systems secure and in place.**

Mantraps: **Use ID checks and authentication for access.**

Biometrics: **Identify users by unique traits like fingerprints or retina patterns.**

Alarms: **Alert on unauthorized access or security breaches.**

Principles Behind Social Engineering:

- Authority
- Intimidation
- Consensus/social proof
- Scarcity
- Urgency
- Familiarity/liking.
- Trust

Cyber Aware:

1. **Use a strong and different password for *email accounts.***
2. **Create strong passwords for all accounts**
   (e.g. use three random words) .
3. **Turn on 2-step verification (2SV).**
4. **Save passwords using a browser or a password manager**
5. **Back up data.**
6. **Update devices.**

What is MISINFORMAION?

Misinformation: False or incorrect information.

Purpose: Affect the perception of people.

Problem Overview of social engineering:

social media enables rapid spread of rumors and fake news, making truth hard to verify and causing real-world harm.

Current solution of social engineering:

- **Data Representation**
- **Deep Syntax**
- **Semantic Analysis**
- **Discourse Analysis**
- **Classifiers**

What is Privacy:

Privacy **means control over what others can know about us. It varies by culture and context, and is linked to security and personal space. Courts haven't clearly defined it, and it sometimes conflicts with freedom of expression.**

Privacy is not Data Protection:

Privacy **is about what info people expect to keep private, while data protection focuses on rules for how organizations handle personal data they collect.**

Meaning of Privacy Changes:

Privacy means personal integrity, but its meaning changes by community and technology. Big changes like the Internet reshape privacy, and people often say one thing about privacy online but act differently.

The Internet:

The Internet allows collecting new personal data, helps businesses and governments access and use it, and creates challenges for rules because it crosses countries.

Internet Services redefine Privacy Environment Dramatically:

Cloud computing raises concerns about security and data ownership.
Search engines track our behavior.
Social networks rely on user data collection and analysis.
Mobile internet links usage to location.
The Internet of Things connects devices, revealing a full picture of our lives.

Government use of Data:

E-government means delivering services online using digital IDs for banking, voting, health, etc.

Governments collect lots of data, raising challenges to balance efficient e-services with security and privacy.

Internet is Built and Operated by the Private Sector not a Public Utility:

Many internet services are free because they make money from ads by using our private data.

We give up privacy for free use, often without fully understanding or challenging it, due to complex terms and low public concern.

Economic Growth and Internet:

Economic growth pushes data sharing and cross-border transfers, but businesses need people to trust that sensitive info (like health or financial) stays confidential. Cybersecurity is key to protecting privacy and supporting the internet economy.

Privacy Offline and Online:

Online privacy deserves the same protection as offline privacy. To achieve this, we need strong technical security like encryption and clear legal rules on personal data use and access.

What is the Privacy Agenda?

Personal integrity is the foundation of data protection. Today's business models make us give companies ownership of our data for benefits, often with little regulation. Governments also seek access to this data.

Governments should:

Commit to protecting user privacy and security while balancing freedom of expression. See cybersecurity as protecting users.

Be clear and lawful about surveillance, following international standards and court oversight.

Regulate effectively with proper technical skills.

Companies Should:

Be clear about how data is managed.
Offer simple, fair terms of service.
Promote strong encryption and anonymity to protect privacy.
Disclose government data requests.

Civil Society Role:

Include voices of marginalized groups,
offer new ideas and policies,
and support privacy policies that serve the public interest.

Lecture 6: Phishing Attacks

What is Phishing Attack?

Phishing **uses fake emails, websites, or calls to steal money or personal info. Cybercriminals may use malware, trick you into sharing data, or directly steal information from your device.**

Phishing **is the most common way attackers illegally access systems.**

, phishing **message is designed to trick you.**

Cyber attackers phish for different reasons, but they all phish.:

Criminals: Money, Fraud, Identity Theft.

Intelligence: Sensitive Data, Network Access, Infrastructure.

Hacktivists: Public Web Pages, social media.

Types of Phishing Attack:

Social engineering **uses info from social media—like your name, job, interests, or contacts—to create fake but convincing messages.**
Cybercriminals **use this to trick you more easily.**

1.Link Manipulation: **Phishing often uses fake links that look real, with misspelled URLs or tricky subdomains, to fool users. Previews can help spot them.**

2.Spear phishing: **targets specific people using personal info to seem real. It makes up 91% of phishing attacks.**

3.Clone phishing: **copies a real email but replaces links or attachments with harmful ones, sent from a fake address that looks real.**

4.Voice phishing (vishing): **uses phone calls and social engineering to steal personal or financial info, often for fraud or identity theft.**

Phishing messages are designed to get you to react quickly without thinking too much...:

Sense of urgency, offers of money ,confirmations, odd requests rewards ,it support.

What should I do when I get a phishing email?

Click, Delete, Report

What happens if I click?

Clicking phishing links can steal your info, infect your device, and cause financial loss.

What happens if I delete?

Review Links., Check Accounts., Block Domains., Remove Messages.

Tips to protect yourself from Phishing emails:

1. **Never share passwords via email.**
2. **Don't open unexpected attachments.**
3. **Verify suspicious emails by calling the sender.**
4. **Avoid pop-ups asking for info.**
5. **Hover over links to check their destination.**
6. **Look for https:// before entering info.**
7. **Watch for bad spelling/grammar — it's a red flag!**