Cybersecurity

CS202 Lecture 25

Lecture Outline

Section 1: Introduction

1. **Definition** of Cybersecurity
2. **CIA Traid** (Confidentiality, Integrity, and Availability)
3. **Importance** of Cybersecurity
4. **Brief History** of Cybersecurity

Section 2: Threat Landscape

1. **Types of Threats:**
   - Malware (Viruses, Worms, Trojans)
   - Phishing and Social Engineering
   - Ransomware
   - Denial of Service (DoS) and Distributed Denial of Service (DDoS)
2. **Threat Actors:**
   - Script Kiddies
   - Hackers
   - Cybercriminals
   - Nation-State Actors
   - Insider Threats
3. **Common Attack Vectors:**
   - Email
   - Web
   - Network
   - IoT Devices

Lecture Outline

Section 3: Cybersecurity Fundamentals

1. Authentication, Authorization, and Accounting (AAA)
2. Encryption: Types (symmetric, asymmetric), Uses (data at rest, data in transit)
3. Password management and password policies

Section 4: Security Controls and Measures

1. Firewalls and network segmentation
2. Intrusion Detection/Prevention Systems (IDS/IPS)
3. Endpoint security: Antivirus software, Endpoint Detection and Response (EDR)
4. Identity and Access Management (IAM)
5. Backup and disaster recovery

Section 5: Best Practices and Future Directions

1. Cybersecurity hygiene: Software updates, Patch management, Regular backups
2. Emerging trends: AI/ML, Cloud security, IoT security
3. Careers in cybersecurity

Section 4: Security Controls and Measures

Endpoint Security – Antivirus Software

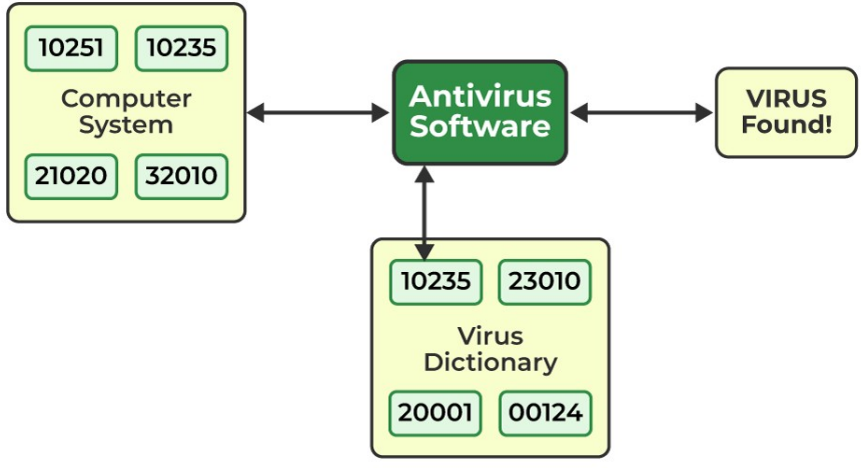
- Scans and removes malicious software

Detects threats like:

- Viruses, trojans, ransomware

Best practices:

- Regular updates
- Real-time scanning



- Antivirus software is a fundamental endpoint security tool, designed to detect and remove threats like viruses, trojans, and ransomware.
- Keeping antivirus software updated ensures it can recognize and neutralize the latest threats.

Backup and Disaster Recovery – Overview

- **Importance:** Mitigates impact of cyberattacks
- Backups and disaster recovery plans are critical for mitigating the impact of incidents like ransomware attacks or natural disasters.
- Regular backups ensure data is recoverable, while a Disaster Recovery Plan (DRP) outlines procedures for restoring operations quickly and minimizing downtime.

Section 5: Best Practices and Future Directions

Cybersecurity Hygiene – Essentials

Software Updates:

- Keep all software and systems up to date
- Address vulnerabilities proactively

Patch Management:

- Automate patch distribution where possible
- Apply critical patches promptly

Regular Backups:

- Test backups for reliability
- Store copies offsite or in the cloud

Emerging Trends – AI and ML in Cybersecurity

Uses in cybersecurity:

- Threat detection and analysis
- Predicting and mitigating attacks

Challenges:

- Adversarial AI: Attackers leveraging AI
- Over-reliance on automated systems

Emerging Trends – Cloud Security

- As organizations migrate to the cloud, securing cloud environments becomes critical.
- The shared responsibility model requires both providers and users to ensure security.
- Key practices include encrypting cloud data, maintaining secure configurations, and enforcing access controls.

Emerging Trends – IoT Security

- Rapid adoption of IoT devices creates vulnerabilities

Risks:

- Weak default credentials
- Lack of updates

Mitigations:

- Secure device configurations
- Network segmentation for IoT devices

Careers in Cybersecurity – Overview

- Growing demand for cybersecurity professionals

Key roles:

- Security analyst
- Ethical hacker/penetration tester
- Incident responder
- Security architect

Skills in demand:

- Risk assessment
- Incident response
- Cloud and network security

Cybersecurity Essentials

Salient Features of Firewall, Honeypot,
Significant Cyberattacks, Digital Forensics,
Cryptography, Ethical Implication of Technology

Salient Features of a Firewall

- **Packet Filtering:** Monitors and controls network traffic
- **Stateful Inspection:** Tracks the state of active connections
- **Proxy Functionality:** Acts as an intermediary between users and resources
- **Network Address Translation (NAT):** Hides internal IP addresses
- **Application Layer Filtering:** Inspects data packets for specific application vulnerabilities
- **Intrusion Detection and Prevention (IDP):** Detects and mitigates threats in real-time
- **Custom Rules Configuration:** Allows tailored security policies

Honeypot in Cybersecurity

Definition: A decoy system designed to attract and analyze cyber attackers

Purpose:

- Understand attacker methods
- Divert attackers from critical systems
- Strengthen defense mechanisms

Types of Honeypots:

1. **Research Honeypots:** Study attack trends
2. **Production Honeypots:** Protect live environments

Public Key Infrastructure (PKI)

Process:

1. Sender encrypts data with the recipient's public key
2. Recipient decrypts data with their private key

Applications:

1. Digital signatures
2. Secure email communication
3. Online transactions

Practical Examples

1. **Firewalls:**
   - Example: Cisco ASA Firewall preventing unauthorized access to a university network
2. **Privacy Intrusion:**
   - Case Study: Facebook-Cambridge Analytica scandal
3. **Honeypot:**
   - Example: Using a honeypot to study ransomware behavior

Significant Cyberattacks

Microsoft Exchange Hack (2021):

- A Chinese hacking group exploited vulnerabilities in Microsoft Exchange, affecting over 30,000 organizations, including government entities and corporations

Ransomware Impact on Healthcare:

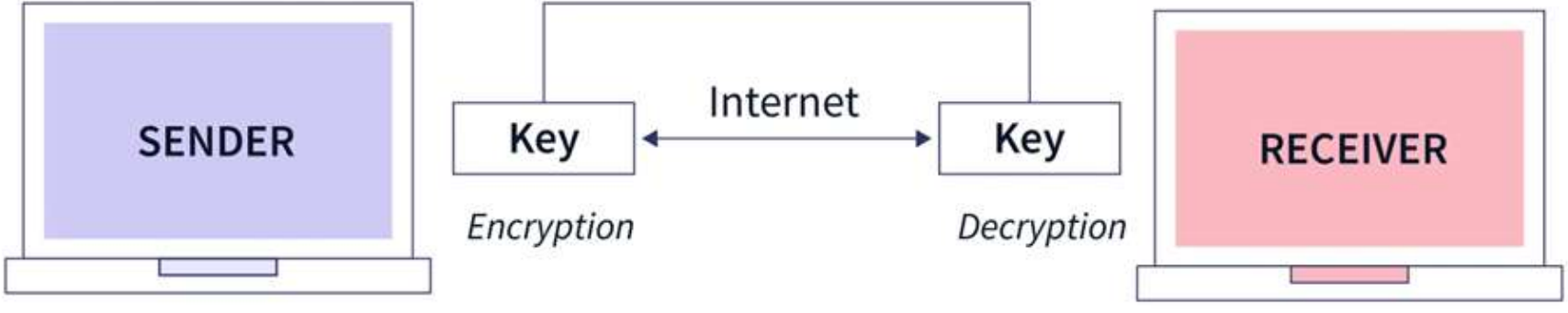
- A reported ransomware attack allegedly caused the first fatality attributed to cybercrime, when delayed access to hospital systems led to a newborn's death

Digital Forensics

- Identifying, acquiring, processing, analysing, and reporting on data stored electronically
- Evidence collected from electronic devices such as computers, smartphones, remote storage, and unmanned aerial systems
- Useful in a variety of contexts, including criminal cases, internal investigations, data breaches, and litigation

Cryptography

- A cybersecurity tool that protects sensitive information by encoding it so that only authorized users can read it
- Used to secure data in transit, prevent unauthorized access, and protect against cyber threats
- Ensures confidentiality by encrypting sent messages using an algorithm with a key only known to the sender and recipient
- A common example of this is the messaging tool WhatsApp, which encrypts conversations between people to ensure they cannot be hacked or intercepted



Ethical Implication of Technology

Privacy Invasion:

- Monitoring personal data, raising privacy concerns
- Organizations may justify surveillance in the name of security

- **Example:** Governments using programs like PRISM for mass surveillance raised concerns about the ethical boundaries of cybersecurity efforts

Ethical Implication of Technology

Misuse of Cybersecurity Tools:

- Tools intended for security can be exploited for malicious purposes
- Hackers can use legitimate software for harmful activities

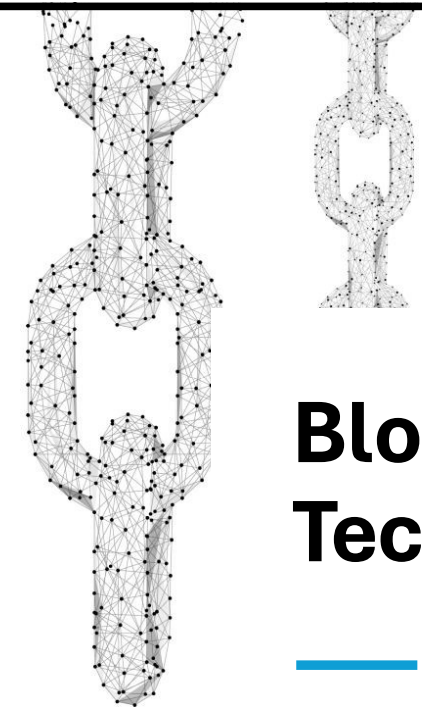
- **Example:** Tools like Wireshark has been used for unauthorized breaches, demonstrating the dual nature of cybersecurity tools

Ethical Implication of Technology

Bias in Security Algorithms:

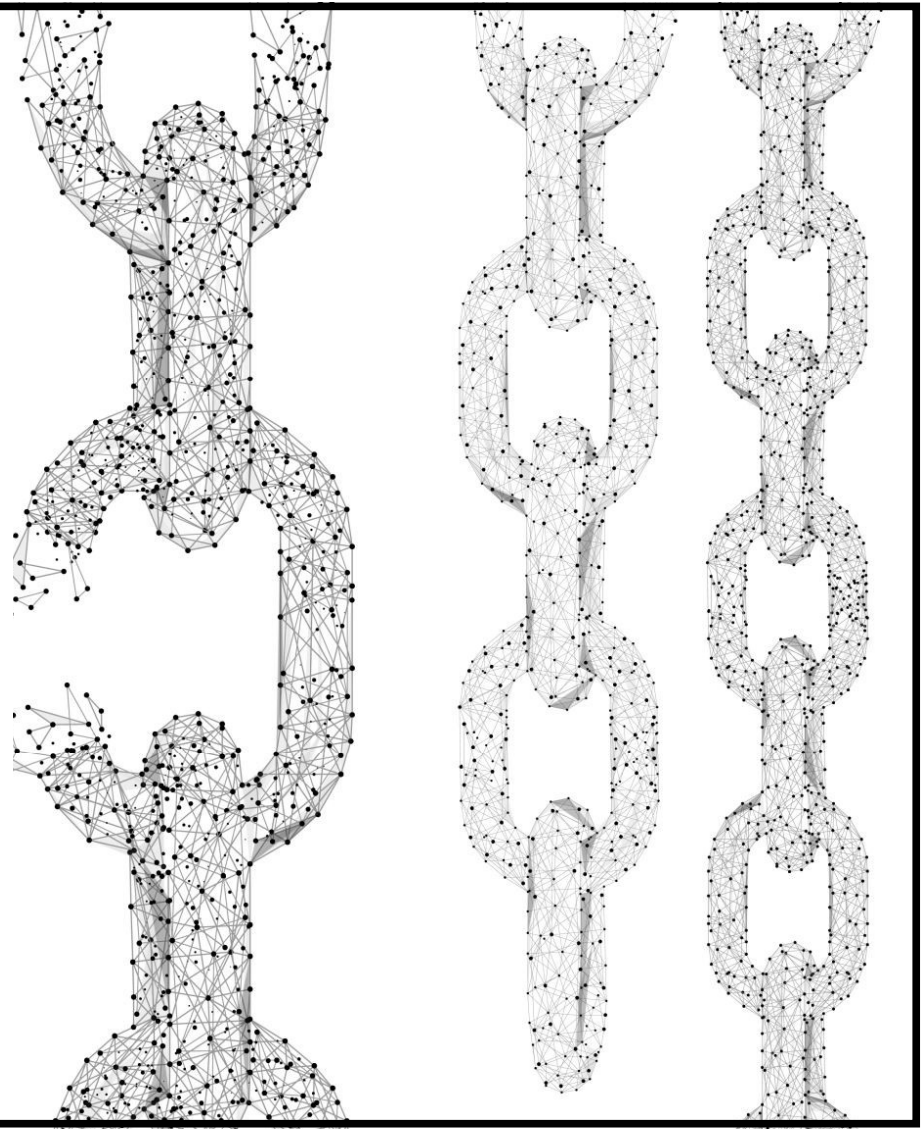
- AI systems used in cybersecurity can inherit biases from training data
- This can lead to unfair or discriminatory practices

- **Example:** Algorithms disproportionately flag emails from non-English-speaking countries, creating ethical dilemmas and impacting specific groups unfairly



Blockchain Technology

A **decentralized** network - constituted by a distribution of functions, powers, people away from a central location or authority



Key Features of Blockchain

1. **Decentralization:**
   - Data is distributed across a peer-to-peer network without a central authority
   - Ensures robustness and reduces single points of failure
2. **Immutability:**
   - Once recorded, data cannot be altered or deleted
   - Provides tamper-proof records for trust and reliability
3. **Transparency:**
   - Transactions are visible to all participants, promoting accountability
   - Public blockchains allow anyone to verify transactions
4. **Security:**
   - Secures data using cryptography (e.g., hashing, digital signatures)
   - Decentralization reduces vulnerability to attacks
5. **Consensus Mechanisms:**
   - Ensures agreement among nodes to validate transactions
   - Common mechanisms include Proof of Work (PoW) and Proof of Stake (PoS)

Additional Features

6. **Smart Contracts:**
   - Self-executing contracts with automated processes
   - Reduces intermediaries and enhances efficiency
7. **Traceability:**
   - Provides a complete history of all transactions
   - Useful for supply chains and verifying product authenticity
8. **Anonymity and Privacy:**
   - Cryptographic addresses ensure user privacy
   - Balances anonymity with traceability for compliance
9. **Scalability and Interoperability:**
   - Emerging focus on handling larger transaction volumes
   - Interconnectivity between different blockchain networks

Decentralization: Real-World Applications

- **Example:** Bitcoin operates without a central authority for peer-to-peer transactions

- **Applications:**
  - **Cryptocurrencies:** Ethereum, Litecoin
  - **DeFi:** Platforms like Aave for decentralized lending and borrowing

Immutability: Real-World Applications

- **Example:** Data stored on Ethereum cannot be altered after being recorded

- **Applications:**
  - **Healthcare Records:** Medicalchain for secure patient data storage
  - **Voting Systems:** Voatz for tamper-proof election processes

Transparency: Real-World Applications

- **Example:** Walmart uses blockchain to track food products from farm to shelf

- **Applications:**
  - **Retail:** Ensuring quality in supply chains
  - **Charity:** GiveTrack for tracking donations

Security: Real-World Applications

- **Example:** Ripple protects international transactions with blockchain security

- **Applications:**
  - **Banking:** JPMorgan's Quorum blockchain
  - **Cybersecurity:** Guardtime for government data integrity

Consensus Mechanisms: Real-World Applications

- **Example:** Bitcoin uses Proof of Work (PoW) for transaction validation

- **Applications:**
  - **Energy Management:** Power Ledger for decentralized energy trading
  - **Gaming:** Axie Infinity for secure in-game assets

Smart Contracts: Real-World Applications

- **Example:** Ethereum pioneered smart contracts in decentralized applications

- **Applications:**
  - **Insurance:** Etherisc for automated claims processing
  - **Real Estate:** Propy for reducing property transaction paperwork

Traceability: Real-World Applications

- **Example:** IBM Food Trust tracks food items from source to consumer

- **Applications:**
  - **Pharmaceuticals:** PharmaLedger ensures authentic medications
  - **Luxury Goods:** Everledger tracks diamonds for conflict-free sourcing

Anonymity and Privacy: Real-World Applications

- **Example:** Monero provides privacy-focused cryptocurrency transactions

- **Applications:**
  - **Finance:** Zcash for anonymous payments
  - **Healthcare:** MediBloc for secure medical data sharing

Scalability and Interoperability: Real-World Applications

- **Example:** Polkadot connects multiple blockchains for seamless data sharing

- **Applications:**
  - **Supply Chain:** Chainlink integrates external data with blockchain
  - **IoT:** IoTeX connects smart devices securely

Summary – Blockchain

1. Blockchain’s features include decentralization, immutability, transparency, and security
2. These features are driving innovation across industries like finance, healthcare, and supply chain
3. Real-world applications demonstrate the transformative power of blockchain technology


The End.