UNIT-1

definiton + scope System Security refers to the processes and methodologies involved in keeping information confidential, available, and ensuring its integrity. It encompasses the protection of all types of computer systems against intrusion, theft, damage, and unauthorized access.

```
physical security, application security, network security, operational
security, and end-user education
```

evolution **Summary: Evolution of Cybersecurity Challenges Over Decades**

- **1970s:** Physical access attacks, basic user authentication, lack of encryption. Defense: Password policies, access controls.
- **1980s:** Rise of malware, viruses, worms, network-based attacks, social engineering. Defense: Antivirus, intrusion detection, firewalls, user education.
- **1990s:** Expansion of the internet, phishing attacks, DDoS attacks, wireless network insecurities. Defense: User education, anti-phishing tools, network improvements.
- **2000s:** Web application insecurities - SQL injection, XSS, CSRF. Defense: Input validation, Web Application Firewall, anti-CSRF tokens.
- **2010s:** Mobile security, cloud challenges, insider threats. Defense: MFA, encryption, user behavior monitoring.
- **2020s:** AI/ML integration, IoT insecurities - data encryption, model explainability, bias. Defense: TLS for IoT, explainability techniques, regular AI model audits.

importance protection of confidential info maintaining business continuity trust and reputation preventing financial loss

threats and vulnerabilities malware phishing DoS MITM attacks insider attacks

```
vulnerabilities are weaknesses or gaps in a security program that can be
exploited by threats to gain unauthorized access to an asset.
Vulnerabilities can exist due to unpatched software, insecure system
configurations, weak passwords, or flawed programming in applications.
Regular vulnerability assessments and remediation are critical components
of a robust system security strategy.
```

impacts of security breaches financial loss reputation damage operational disruption loss of intellectual property emotional and psychological impact

Definitions

- computer sec
  - generic name for collection of tools to protect data
- net sec
  - measures to protect data during transmission
- internet sec
  - measures to protect data during their transmission over an interconnection of networks
- OSI security

Info security

- aspects
  - attack
    - action compromising security of info
  - mechanism
    - detect, prevent or recover from attack
  - sevice
    - to enhance sec of data processing sys and info transfers

> threat and attack are used interchangeably

attacks

- types of attacks
  - passive
    - traffic analysis
  - active
    - masquerade
    - replay
    - modifying message content
    - DoS
- classification
  - interruption - attack on availability
  - interception - attack on confidentiality
  - modification - attack on integrity
  - fabrication - attack on authenticity

CIA triad

security mechanism

- to detect, prevent and recover from attack
- employs cryptographic techniques
- specific sec mech
  - encipherment
  - digi sign
  - access controls
  - traffic padding
  - routing control
- pervasive sec mech

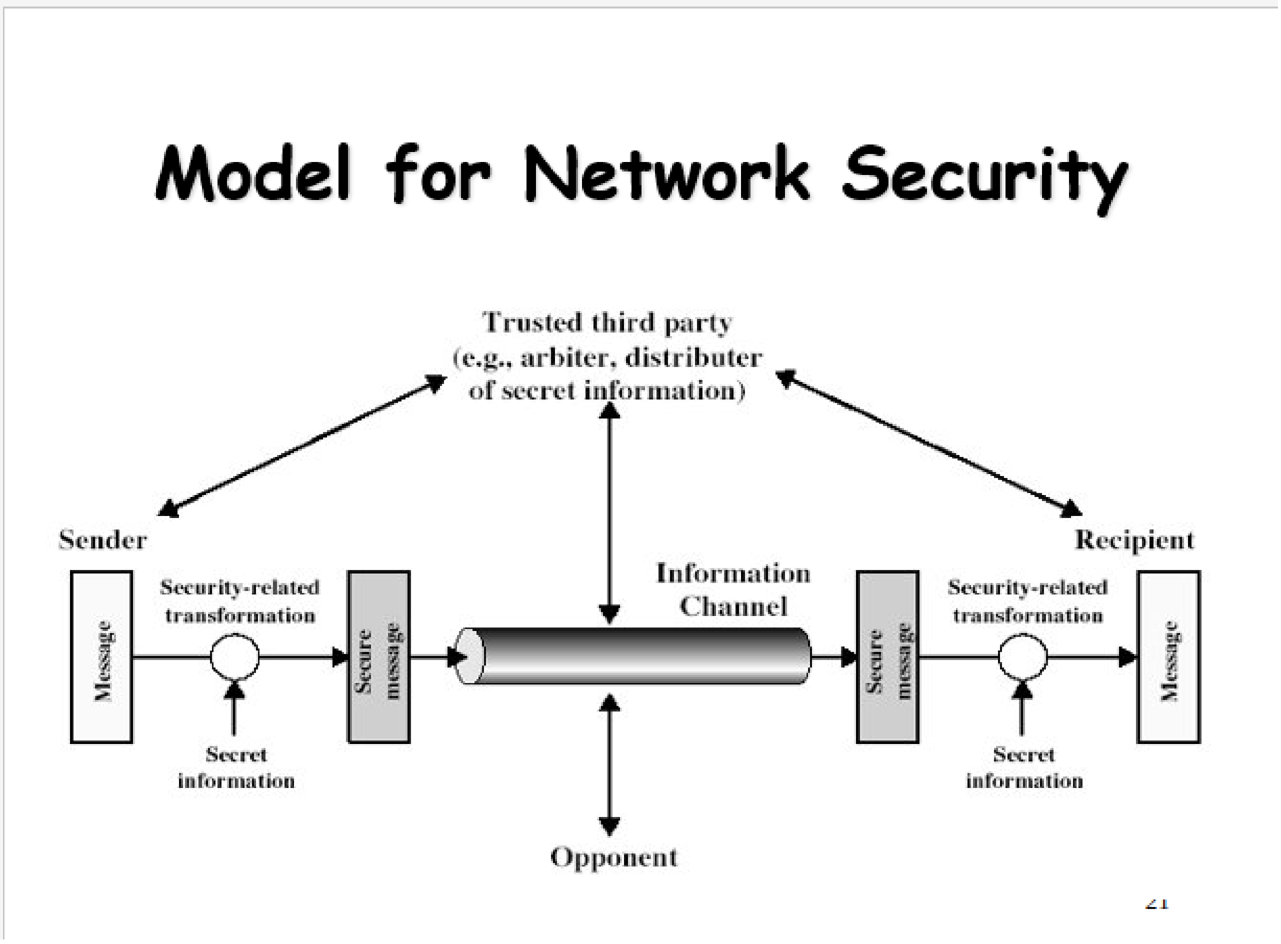
  - event detection
  - sec audit trails
  - sec recovery

security services

- provided by protocol layer of communicating open systems to ensure adequate security of sys or data transfers
- must provide
  - confidentiality
  - authentication
  - integrity
  - non-repudiation
  - access control
  - availability

model for net sec

- design a suitable algo for sec tranformation(encryption/decryption)
- gen secret info(keys) for the algo
- dev methos to distribute and share the secret info
- protocl to enable principals to use transformation and secret info for a sec service


Model for Network Security
Trusted third party (e.g., arbiter, distributer of secret information)
Sender
Recipient
Message
Security-related transformation
Secure message
Secret information
Information Channel
Secure message
Security-related transformation
Message
Secret information
Opponent
21

model for network access security

- authentication
  - to identify users

- authorization
    - ensure only authorized users access designated info or resources

methods of defense

- encryption
- S/W controls
    - limit access in a DB/OS
    - protect each user from other users
- H/W controls
    - smartcard
- policies
    - change passwords frequently
- phy controls

internet standards

- 3 orgs
    - IAB
    - IETF
    - IESG
- RFC - formal standards doc developed in working groups within the IETF

Zero Trust Sec

- IT sec model where strict ID verification for each person and device trying to access resources on a priv net is performed
- shifts sec from a perimeter-centric model to a resource and indentity-centril model

---

principles

- ensure all resources are accessed securely
- least privilege strategy
- inspect and log all traffic
- ensure all components support APIs for event and data exchange

platform requirements

- IAM(identity access management)
    - MFA for auth
    - least privilege access
- net sec
    - micro-segmentation - break net into smaller zones to limit lateral mvmt of threats
- data sec
    - enc - end-to-end enc for data in transit and at rest
    - DLP(data loss prevention) - to monitor and prevent unauth access, use and transimission of sensitive data
- app sec
    - secure coding practices - apps are dev with sec in mind

    - Web app firewalls
- cloud sec
    - use CASB(cloud access sec broker) to enforce sec policies and monitor activity in cloud env
- security analytics
    - log management and real-time analysis of sec events
- training and awareness
    - for employees to enhance their awareness of security best practices and potential threats

threats

- insider threats
    - abuse auth access to compromise data/sys
- credential theft
    - phishing, keylogging, etc. to steal user creds
- malware and ransomware
    - malware and ransomeware can be introduced via compromised endpoints or external sources
- data exfiltration
    - steal sensitive data and transfer it outside the network
- zero-day exploits
    - exploit vulnerabilites not yet known to the vendor
- misconfigs
    - misconfigs in firewalls, access controls, etc. can create vulnerabilites that attackers can exploit
- supply chain attacks
    - inject malicious code into S/W or H/W components and impact the trustworthiness of the entire sys
- social engineering
    - can lead to leaking of sensitive info

implementation

- identify and classify assets within a net
- create a zero trust arch
    - no inherent trust
    - least privilege and micro-segmentation
- implement MFA
- micro-segmentation
- device trustworthiness checks
    - implement cehcks to to ensure trustworhtiness of devices before granting access
- continuous monitoring
- data enc
- cloud security
    - using CASB
- user and device identity mgmt
- firewalls and secure web gateways(SWG)
- regular audits and assessments

models

- ZTX model
  - workload sec
  - net sec
  - device sec
  - data sec
- NIST arch
  - ID mgmt
  - continuous monitoring
  - least privilege access
- Google's BeyondCorp
  - user and device ID verification rather than net location
  - use of context-aware access controls
- zero trust sec model by Palo Alto
  - user and device ID mgmt
  - least privilege access
  - micro-segmentation
- CIS arch
  - continuous monitoring
  - least privilege access
  - strong auth