Overview: Network and Internet Security

Introduction

Dr. Tushar, Mosaddek Hossain Kamal
Professor (CSE, DU)

Computer Science and Engineering, University of Dhaka,

Jan-June, Academic Year: 2025

CSE804: Network and Internet Security

April 2, 2025

Outline

Course Content

Objective

- Interpret the operational concepts of various network and Internet architectures, applications, protocols security and their design issues.
- Analyze security and user application service performances of the various Internet applications and communication protocols.
- Understand Network Threat and Vulnerability
- Identify and Analyzing Network Log and Security Information and Event management , Endpoint Security
- WAN and Wireless Security assessment and Diagnosis

Course Description

Description Internet architecture, security flaws on the Internet, Attacks on networks: DDOS attacks, reflection attacks, amplification attacks, wireless security, WEP cracking, DNS hijacking, routing attacks, case study: NTP DDOS attack, DDOS attack. Network security at different layers of the OSI and TCP/IP models: firewalls, security protocols (in particular, IPsec, SSL, and Kerberos), Denial of Service (DoS) attacks/ detection/prevention, viruses and worms, DNS, email & Voice Over IP (VoIP) security, wireless infrastructure security. Network Intrusion Detection and Analysis: NIDS/NIPS functionality, Modes and types of NIDS, NIDS/NIPS evidence acquisition, snort rules and alerts, Case study. Formal methods for modeling and analyzing authorization and access control systems. Designing Enterprise systems for Access Control, Authentication and Auditing (AAA): Designing networks on selected protocols to support business operations while maintaining identified levels of network security. Supporting secondary network connectivity (wireless, VPNs, BYOD devices, partner networks, cross-domain and other connectivity types). Designing networks to support Resiliency Management, Business Continuity, Disaster Recovery and other principles to avoid network failures that negatively impact the organization's ability to deliver on its core mission. Methods to prevent, detect and respond to security breaches, including the role of Incident

Overview: Information Security

What is security?

- In general, security is "The quality or state of being secure that is to be free from danger".
- To be protected from adversaries from those
  - those who would do harm, intentionally or otherwise
- A successful organization should have
  - **Physical** security is to protect
    - physical objects, or areas of an organization from unauthorized access and misuse
  - **Personal** Security is to protect
    - individual or group who are authorized to access the organization and its operations
  - **Operations** Security is to protect
    - details of a particular operation or series of activities
  - **Communications** Security is to protect
    - an organization's communications media, technology, and content
  - **Network** security is to protect
    - networking components,connections, and contents
  - **Information** Security is to protect
    - information, critical elements, including the systems and hardware.

Information Security

An Information System is much more than computer hardware. It is the security of entire set:

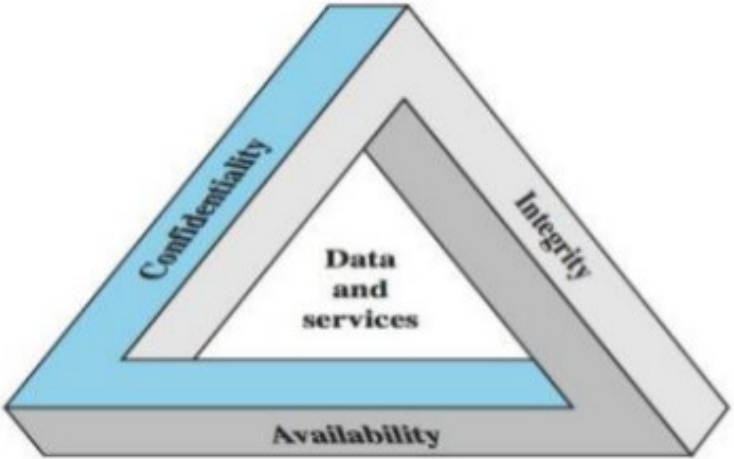
- software, hardware, data, people, and procedures necessary to use information as a resource
- within and outside the organization

Briefly, information security is a work of

- **Securing the component**
  - computer as a subject of attack (compute used as active tools for attack)
  - computer as a object of attack (it is the entity being attack)
- **Security and Access Balancing**
  - Perfect security is not possible
  - Security should be considered a balance between protection and availability
  - Security must allow reasonable access
  - yet protect against threat

Information Security: Components: CIA triangle

C.I.A. triangle is considered the industry standard for security. It is solely based on three components



Components of information security

- **Confidentiality**
  - concealment of information or resources
  - only seen by people who have the right to see it
  - keeping information secret from unauthorized access
- **integrity**
  - refers to the trustworthiness of data or resources
  - preventing improper or unauthorized change
  - ensuring that information remains intact and unaltered
  - includes both the correctness and the trustworthiness of the data
- **availability**
  - ability to use the information or resource desired
  - having access to your information when you need it
  - no person or event is able to block legitimate or timely access to information
  - Information is useless if it is not available
  - In some cases information needs to be changed constantly
    - it must be accessible to those authorized to access it

Information Security

Two additional objectives

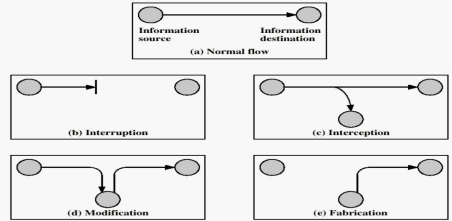
- **Authenticity**
  - being genuine and able to be verified or trust
  - to ensure that the data, transactions, communications or documents are genuine
  - authenticity to validate that both parties involved are who they claim to be
- **Accountability**
  - involves actions of an entity can be traced uniquely
    - nonrepudiation, deterrence, fault isolation, intrusion, detection and prevention
    - one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction
    - Non-repudiation implies one's intention to fulfill their obligations to a contract

Some Common Security Attack

Some common attacks on information security

- **Attacks Threatening Confidentiality**
  - Snooping/Packet Capturaing and Traffic analysis
  - Snooping refers to unauthorized access to or interception of data
  - Traffic analysis: information collected by an intruder by monitoring online traffic
- **Attacks Threatening Integrity**
  - modification, masquerading, replaying and repudiation of information
- **Attacks Threatening Availability**
  - Denial of Service (DOS) attack
  - Make system so busy that it might collapses
  - intercept message sent in one direction such that
    - Sending system believe that other party or message has lost
    - It should be resent

Some Common Security Attack



- **Interruption**: This is an attack on availability
  - Disrupting traffic
  - Physically breaking communication line
- **Interception**: This is an attack on confidentiality
  - Overhearing, eavesdropping over a communication line
- **Modification**: This is an attack on integrity
  - Corrupting transmitted data or tampering with it before it reaches its destination
- **Fabrication**: This is an attack on authenticity
  - Faking data as if it were created by a legitimate and authentic party

Techniques of Information Security

Cryptography!!

- Greek word, means "Secret Writing"

Cryptography is used for information security

- to protect information from unauthorized or accidental disclosure
- Transform usable information to a for that renders
  - unusable by anyone other than an authorized user
  - this process is called encryption
  - original message is known as plain text
  - message sent through channel is referred to as cypher text
- Encrypted information can be transformed back into original usable form
  - known as decryption
  - done by cryptographic key

Cypher Text generation

Types of cypher text

- **Traditional Ciphers**: hiding information from intruders
  - Substitution Ciphers
    - Replace one symbol with another
    - plain text characters are replaced by other characters
  - Transposition Ciphers
    - Does not substitute
    - change the position of the symbols
- **Modern symmetric key cyphers**
  - traditional cypher is no longer secure ??
  - thus, modern symmetric-key ciphers have been developed
  - combination of substitution, transposition and some other complex transformations
  - **Examples**
  - DES: Data Encryption Standard: developed by NIST in 1977;
  - AES: Advanced Encryption Standard: NIST in 2001 (shortcoming of DES)

Asymmetric Key Cryptography

Asymmetric Key Cryptography

- used for confidentiality
- Unlike symmetric key cryptography; distinctive keys are used
- Private key and public key
- A public key encryption is only decrypt by private key

Both symmetric and asymmetric exist in parallel

- In symmetric key cryptography a secret token is shared between two parties
- in asymmetric key cryptography: token is unshared by two parties. creates their own token
- issues are: performance?? Key transfer?? Complement of each other(!!)
- advantage of one compensate the disadvantage of others

Message Integrity

Message Integrity (Hash Function) Message Integrity: Hash Function

- Some occasion we may not need secrecy but need integrity
- Traditionally document integrity is preserved by Fingerprint
- Fringerprint: electronic equivalent are message and digest
- digest: message is passed through a cryptographic hash function
- Hash function create a compressed image of the message – fingerprint
- To check again same function is used on the message and compare

Digital Signature

- Electronic equivalent to the hand written sign
- A document is originated needs his/her signature
- verified signature is the proof of originator
- sender uses a signing algorithm to sign the message
- Receiver applies verification algorithm on message and signature
- private-public key: Sender uses its private key to sign the message
- recipient uses senders public key for the verification of the signature

Authentication and Web Security

Basic Authentication

- Simple user ID and password based authentication
- It limits the user access of specific document/page from the server

SSL (Secure Socket Layer) or TLS

- Originally created by Netscape.
- It is implemented in world wide web
- Confidentiality using symmetric key
- authentication through public key identification and verification
- and connection reliability through integrity checking
- SSL is a handshaking, first authenticate and then transfer of encryption key
- Client public key is verified by CA(certified authority)'s public key
- SSL is obsolete, terms are used commercially, now TLS (Transport layer protcol)

Distributed Authentication & IPSEC

KERBEROS

- authentication (network wide) protocol, confidentiality, integrity
- entirely symmetric key cryptography
- Authentication server issues ticket for client to access a service
- Two types of ticket and life time
- Login session (single access) based ticket & long term ticket (multiple access)
- KDC -key distribution center

IPSEC (Protecting IP)

- Internet Standard to ensure secure private communication over IP
- Developed by IPSEC working group of IETF
- Implements network layer security
- it facilitates direct connectivity between two sensitive node through untrusted network

IPSEC (contd.)

Relation between sender and receiver is identified by

1. Security Parameter Index (SPI)
2. IP Destination address (IP of the destination SA, can be a host, a firewall or a router)
3. Security Protocol Identifier (ESP or AH) SPI + IP destination address uniquely identifies a particular Security Association
4. Authentication Header (AH) provides integrity and authentication without confidentiality
5. Transport Mode AH authenticates the IP payload and selected portions of the IP header
6. tunnel mode AH authenticate entire inner IP packet and othe portion of header

Primary Types of Network Security

- **Firewall**
  - Foundation of the most security setup
  - Create various types of barrier between traffic flows
- **Access Control**
  - Check All entry request
  - Authenticaion and Authorization !!
  - Policies each user privileges
- **Application Security**
  - Proper Configuration of the application
  - Application Code ??? VAPT !!
- **Data Loss Prevension**
  - Protect and security for critical data
  - Recent DU data loss incedent
- **Malware Protection**
- **Web Application**
  - Web Applicateion Gateway for traffic filtering
  - Web Application Firewall
- **Email Security**
- **Use IPS, IDS, VPN and etc**
- **Machine Learning and NBA**

Access Control: Firewall

Access Control: **Firewall**

- Packet Filter
- Application Gateway
- Firewall isolate a organization internal network from a large network
- Allow some packet to pass, block other
- Firewall commonly operates at IP level
- check each IP packet against filter rule
- Address translation (NAT)

Next Generation Firewall

NG Firewall

- Filters packets on application data
- also TCP/UDP packet
- Objective of security in every OSI layer
- Improved detection of encrypted applications and intrusion prevention service
- Traditional firewall rely on IP and Port based filtering which is not work for many application like web application using port 80
- Lead to development of an identity based security

Machine Learning in Security

SIEM – Security information and event management

- Log based discovery
- Collecting log database from several systems (system log level)
- Run machine learning or intelligent algorithm to discover any vulnerability
- provide real-time analysis of security alerts generated by application and network hardware
- The main process are: Data aggregation, Correlation, Alert generation, Dashboard, Compliance, Retention, Forensic analysis

NBA – Nework Behavior Analyzer

- Discovery vulnerability from moving packet in the network
- most system uses signature based approach to detect threat
  - Monitors the pattern in the network
  - Look for patterns in the network which match their signature database
- using machine learning to identify new treats and vulnerability which does not have signature