Stockholm University

Network Security

Introduction to Information Security (IntroSec)

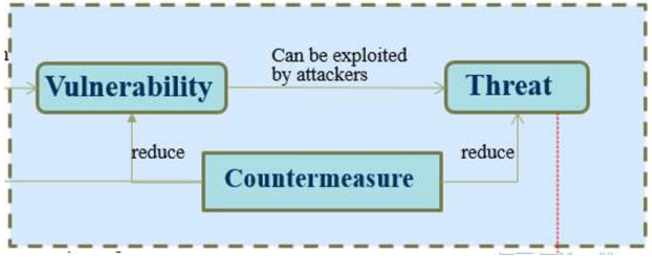
Yuhong Li

Outline

- Vulnerability in networks: why network security?

- Network security threats and attacks
- Network security defenses
- Network security management

- Expected learning outcomes



Vulnerability in Networks

- What is network security
- Factors causing vulnerability of network systems

Network Security

- Computer (incl. system) security: security for information storage and processing， C.I.A. in
  - Hardware, software, data
- Network security: security for the whole procedure of information transmission
  - Information carrier + information processing, transmission, storage, access
  - Distinguish the malicious data from normal information
  - Distinguish between the legal and illegal access
  - Distinguish between the authorized and unauthorized users

Vulnerability of the Network Systems

- Non-technically
  - Network operations
  - Rules of security management
  - Attitude/knowledge of people maintaining and using networks
- Technically, vulnerabilities are caused by
  - Openness of systems and protocols
  - Systems design (faults), implementation (bugs, backdoors)
  - Network maintenance, improper configuration

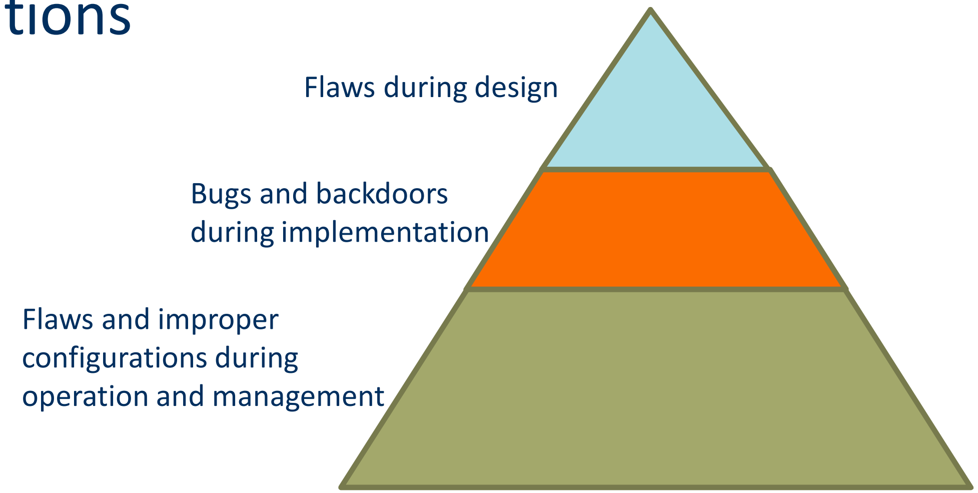
Openness

- Architecture and protocols are open/standardized
  - Originally, connected computers were considered to be trustworthy
  - Now, all kinds of computers and users are connected to Internet ->computers and people using the computers are not trustworthy anymore!
- Resources are open
  - Physical connections, software, tools, are shared -> not trustworthy

⇨ The network systems is vulnerable!

Operations and Maintenance

- Congestion, disconnection of networks (->availability)
  - Mistakes in design, implementation
  - Wrong configurations



Flaws during design

Bugs and backdoors
during implementation

Flaws and improper
configurations during
operation and management

Everything can be a target

- Threats and attacks may come from everywhere!
  - Openness (interdependencies) allow attacker’s goal to be met in any numbers of ways
  - Attacker’s options can be both hardware and software, e.g.,
    - Protocols, routers, applications, OS, Internet bandwidth, firewalls, servers, etc.

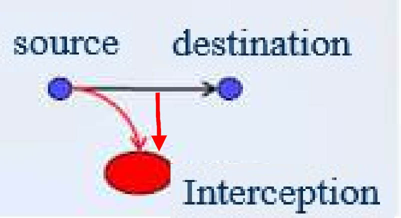
Threats and Attacks

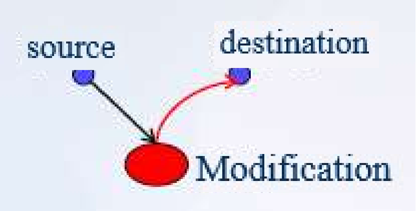
- Passive and active attacks
- Means of performing network attacks
- Typical threats and their relationship

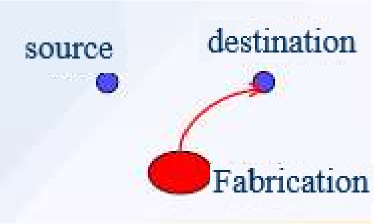
Basic Types of Threats

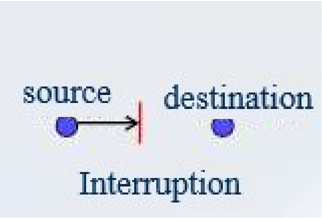
- Interception, or unauthorized viewing
  - Eavesdropping, wiretapping
- Modification, or unauthorized change
  - Sequencing, substitution, insertion
- Fabrication, or unauthorized creation
  - replay
- Interruption, or preventing authorized access
  - DoS to routers, ports, servers

- Attacks: passive and active









Passive Attacks

- Goal is to obtain information that is being transmitted
  - For example, eavesdropping (listening) and snooping (monitor and analysis), attempt to learn or make use of information from the network but do not affect system resources.
- Two types of passive attacks:
  - The release of message contents: monitors e-mails, web usage, interactive services
    - For example: dsniff (webpsy, urlsnarf…)
  - Traffic analysis: to look at communication patterns between entities in a system. Who? When? How long?
    - For example: Tcpdump, Wireshark -> packet size, frequency

Active Attacks -I

- The goal is to destroy or disrupt a system or function.
- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
  - The goal of defense is to detect attacks and to recover from any disruption or delays the caused by them

Active Attacks -II

- Man-in-the-middle attack (MITM): content is modified to deceive two ends into believing they are communicating directly
- Replay: intercept and reuse legitimate data
- Modification of messages: Some portion of a legitimate message is altered
- Denial of service (DoS/DDoS): Prevents or inhibits the normal use or management of communications resources
- Masquerade/spoof/impersonate: Take place when one entity pretends to be a different entity
- Passwords/vulnerabilities cracking

Examples of Network Attacks

- Land Attack
- ICMP Redirect
- Smurf
- Winnuke (for win95/NT)
- Fraggle
- TCP Flag attack
- Ping of Death
- IP Fragment attack (teardrop attack)
- ICMP unreachable
- Traceroute attack

Network Malwares

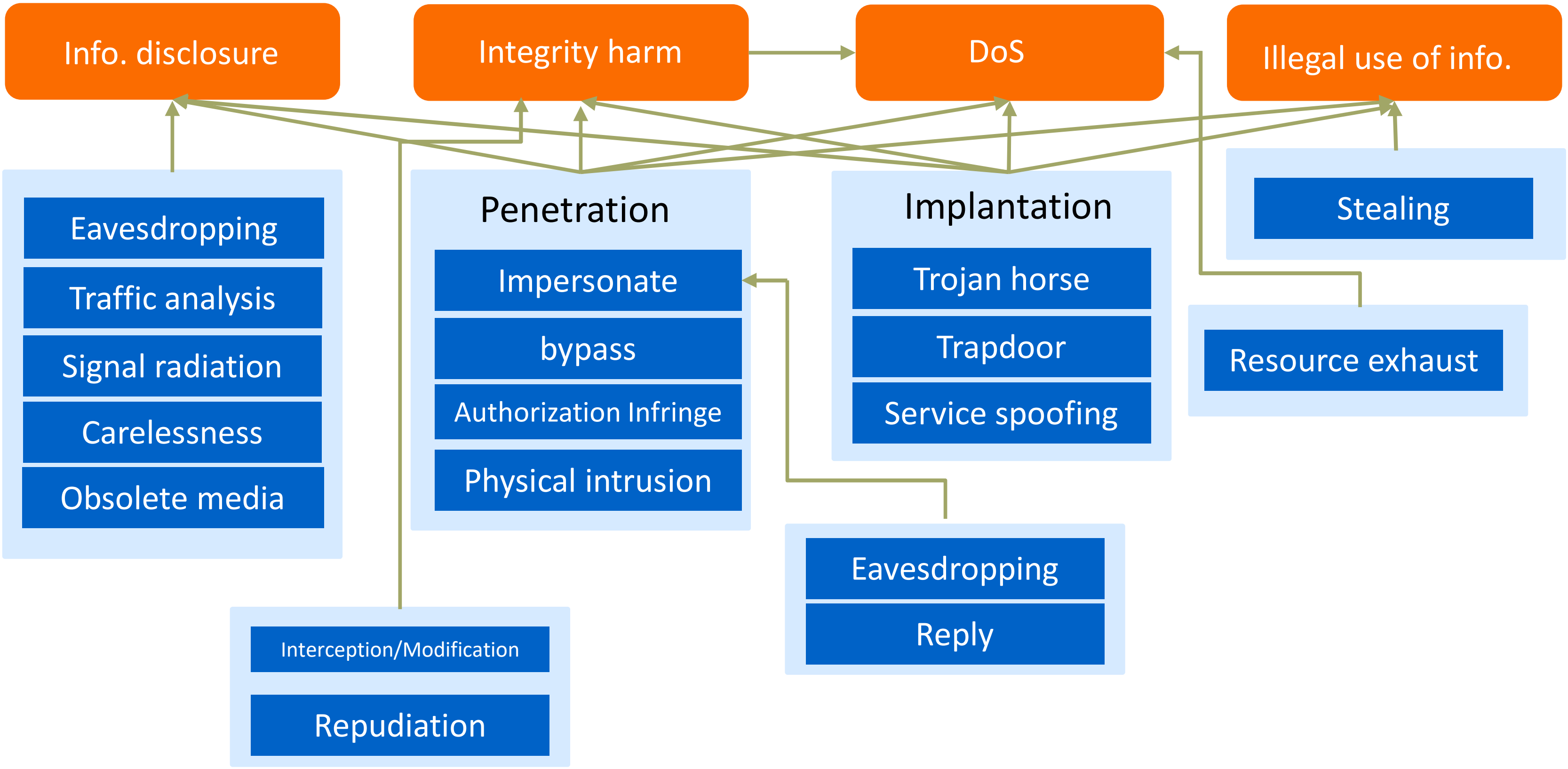
- Virus: replicate through emails! Backdoor: reserved by programmers
- Worm: spreads copies of itself through a network, bot
- Trojan horse: hidden in attached files of email, web pages…
- Harmful scripts: integrated in the web pages (Jave Applets, VBScript, JavaScript)
- Spams

Means of Performing Network Attacks

- Network invisibility
  - IP spoofing, MAC spoofing, NAT, hiding agents (CCProxy, Squid, SocksCaps64, Proxychains), Zombie
- Network scanning
  - Port scanning, type &version scanning (telnet, rpcinfo, Metasploit, Nmap), vulnerability scanning (OpenVAS), weak password scanning, Web vulnerability scanning(Nikto, VEGA, Accunetix, Appscan), system configuration scanning (Lynis , Auditd) etc.
- Backdoors and log cleaning (msfvenom, backdoor_factory, wtmpclean, Logstramper)

Typical Threats and Their Relationship

Stockholm University



Major Treats in Practice

- An investigation results of sampling more than 3000 cases (order according to the occurred frequencies)
  - Authorization infringe
  - Spoofing
  - Bypass
  - Trojan horse/trapdoor
  - Obsolete media

Countermeasures

- Cryptography
- Firewall
- Intrusion detection system
- Security management

Countermeasures

- Goal – C.I.A.
  - Confidentiality: wiretapping, eavesdropping
  - Integrity: data corruption
  - Availability: DoS (denial of service)

Protections

- Cryptography for networks
- Firewalls
- Intrusion detection and prevention systems
- Managing network security, secure information and event management
- Malicious code detection and killing
- Vulnerability scanning

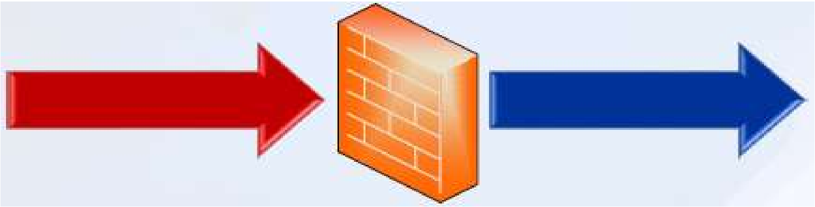
Cryptography

- Link by link and end-to-end encryption

- Layer 3
  - Onion routing
  - IPsec
- Layer 4-Layer 7: SSL, SSH, TLS, HTTPS

Firewall

- In the middle of the secure and insecure networks
- Hardware + software
- Filter the traffic
- Only the permitted traffic can pass
- But, cannot protect the internal attacks



- Security policy: what traffic can or cannot pass through the firewall

1 All the traffic to/from the internal network must pass through the firewall

2 Only the authorized traffic can pass through the firewall

3 The firewall itself is immune to the attacks

Types of Firewalls

Working place

- Packet-filtering firewall
- Circuit-level firewall
- Application-level firewall

Design architectures

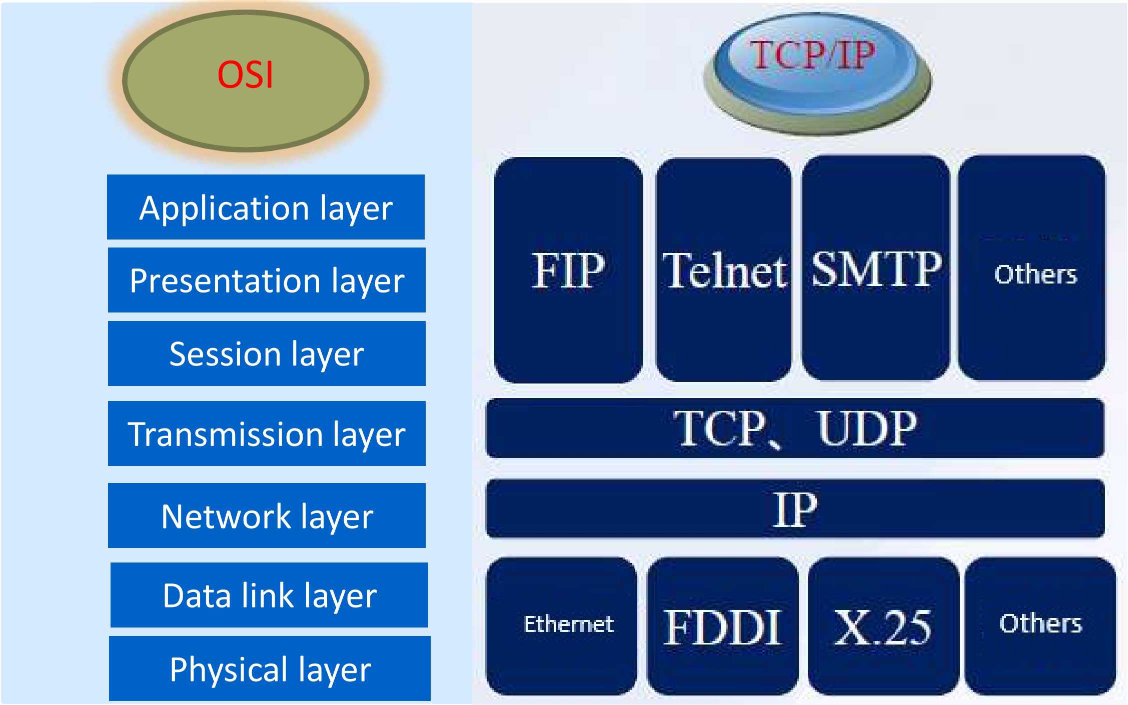
- Static packet filtering
- Dynamic packet filtering
- Circuit-level gateway
- Application-level gateway
- Stateful inspection
- Proxy
- Physical isolation

Firewalls and OSI Model

Application-level gateway

Circuit-level gateway

Packet filter



OSI

Application layer

Presentation layer

Session layer

Transmission layer

Network layer

Data link layer

Physical layer

TCP/IP

FIP

Telnet

SMTP

Others

TCP、UDP

IP

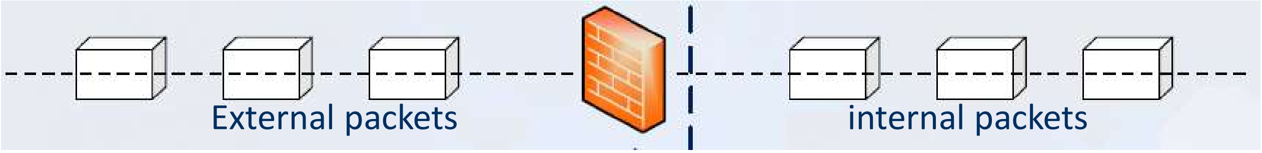
Ethernet

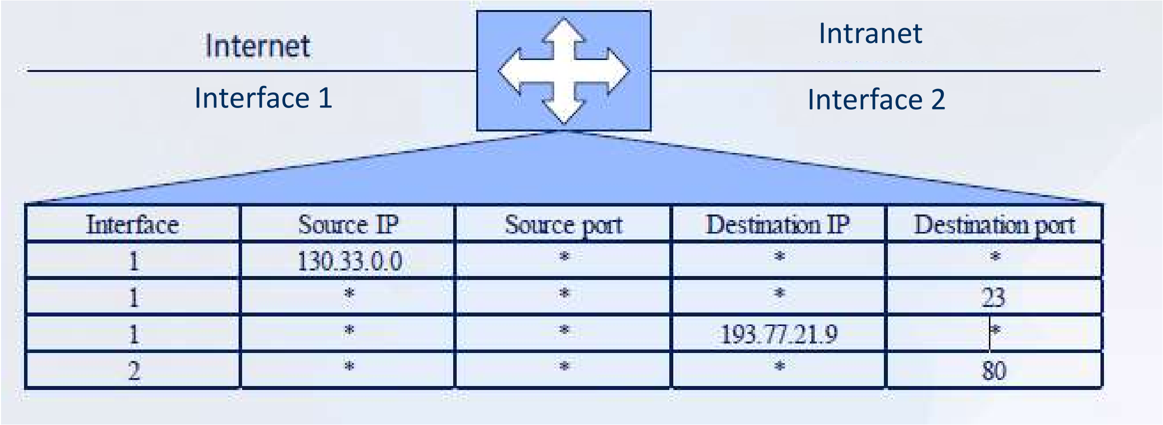
FDDI

X.25

Others

Static Packet-Filtering Firewall



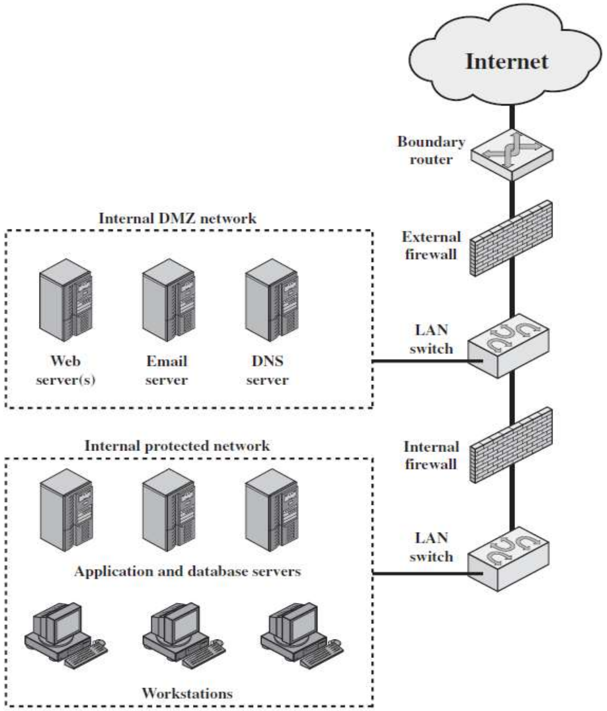


Interface	Source IP	Source port	Destination IP	Destination port
1	130.33.0.0	*	*	*
1	*	*	*	23
1	*	*	193.77.21.9	*
2	*	*	*	80

Actions：deny

Firewall Examples

- Packet-filtering firewall
- DMZ (demilitarized zone)
- NAT (Network Address Translation)

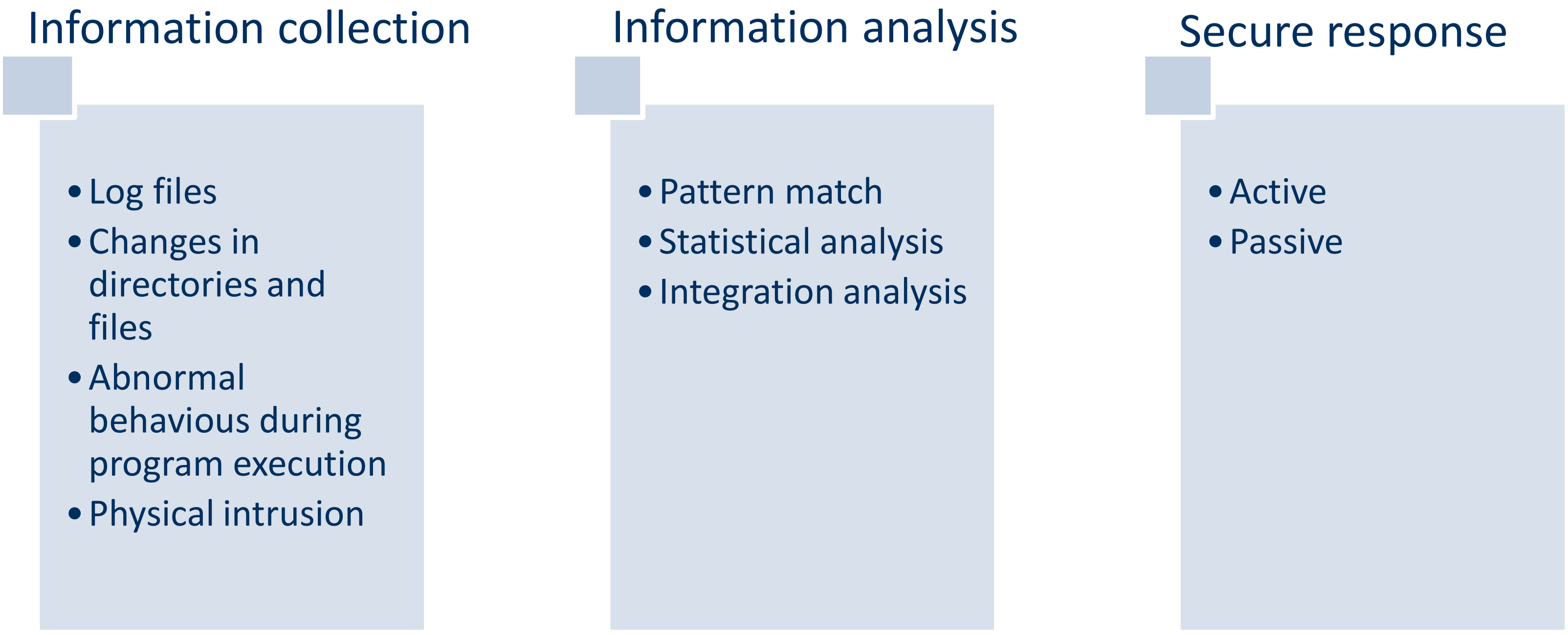


Intrusion Detection

- Intrusion
  - Illegally gain access to a system
  - Collect system’s information (by using system’s vulnerabilities)
  - Destroy the system
- Intrusion detection
  - Detect the unauthorized access
  - Monitor the running states of the system, keep the C.I.A.
  - Identify the attacks to the computer networks or systems.

Tasks of Intrusion Detection System

Stockholm University



Information collection

- Log files
- Changes in directories and files
- Abnormal behavious during program execution
- Physical intrusion

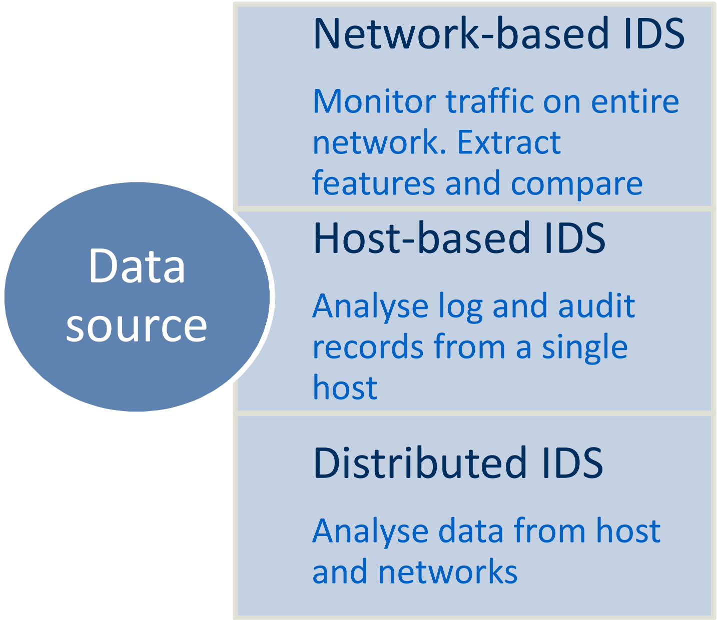
Information analysis

- Pattern match
- Statistical analysis
- Integration analysis

Secure response

- Active
- Passive

Types of IDS



Data source

Network-based IDS

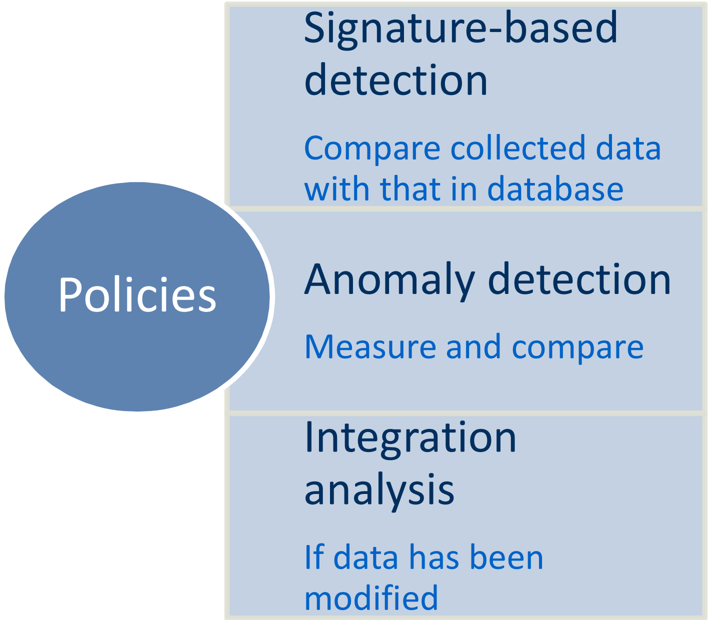
Monitor traffic on entire network. Extract features and compare

Host-based IDS

Analyse log and audit records from a single host

Distributed IDS

Analyse data from host and networks



Policies

Signature-based detection

Compare collected data with that in database

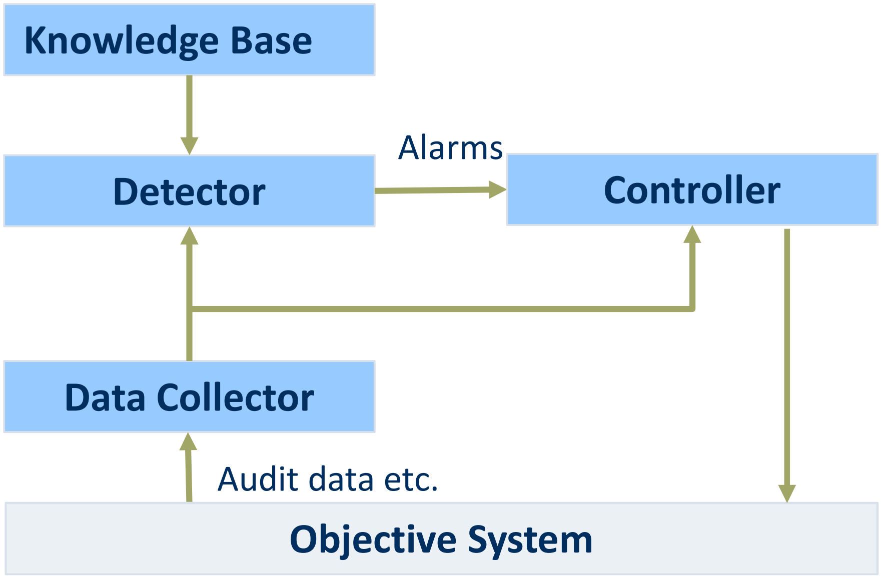
Anomaly detection

Measure and compare

Integration analysis

If data has been modified

General IDS Model



Network Management

- Availability
  - Promote fair use of resources
  - Block a malicious traffic flows
- Functions
  - Monitor network performance and adjust configurations if necessary
  - Collect status indications from a range of products, including firewalls, IDSs, routers, load balancers

Typical methods

- Capacity planning
- Load balancing
- Network tuning: e.g., rate limiting
- Network addressing
- Shunning
- Blacklisting and sinkholing

Network security is a system

- Defense-in-depth
  - Consider mitigation of different threat categories
  - Use various threat mitigation techniques: protect, detect, deter, recover, and transfer
  - A collection of a network-connected devices, technologies, and best practices that work in a complementary ways to provide security

Expected Learning Outcomes of Network Security

- Understand the scope of network security and the security goals
- Understand the factors causing network vulnerability
- Understand the major techniques of network attacks and describe the major network attacks (e.g., DoS/DDoS, MITM, replay, spoofing)
- Understand the major network defense techniques and describe how they can protect networks
  - Firewall (Statistic packet filtering, Circuit-level gateway, Application-level gateway)
  - IDS (Signature-based, anomaly-based detection)
- Explain and reason some terms: onion routing, DMZ, NAT, shunning, sinkholing

END