Stockholm University

Introduction to Network Security

Network Security (NETSEC)

Yuhong Li

2022-01-25

Outline

- Network security definition and objectives
- Network security threats and attacks
- Challenges of network security
- Research content of network security
- Organization of the content of lectures

Network Security Definition and Objectives

- Development of information security
- Definition of Network Security
- Objectives of Network Security

Development of information security

- Communication security phase
  - Solve security problems (confidentiality) for data transmission

  -> cryptography
- Computer system security phase
  - Solve the security problems of computer systems for information storage and processing

  -> access control according to the security level of visitors and information
- Network system security phase
  - Solve the security problems for storing and transmitting information in networks
  - Provide an entire information security solution: protect, detect, response, and recover
- Internet of Things (IoT) security phase
  - Security guarantee to IoT, future direction

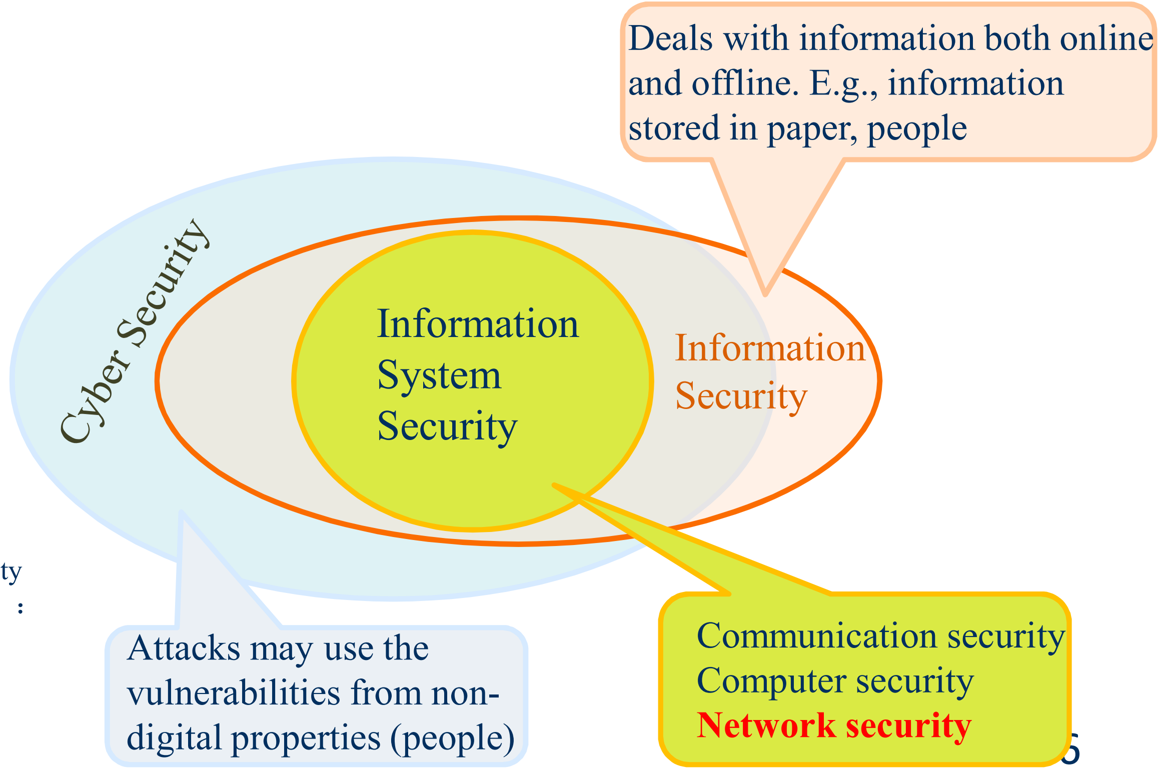
Computer Security vs. Network Security

- Computer security (by NIST):
  - The protection afforded to an **automated information system** in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.
    - C.I.A. of the computer system
    - C.I.A. of computer system resources: hardware, software, firmware, information/data, and communications
- Network security
  - Distributed computer systems
    - using networks and communication facilities to carry data between computers and computers.
  - Measures to deter, prevent, detect, and correct security violations that **involve** the transmission of information.
    - Computer security
    - Special focuses

Information Security, Computer Security, Cyber Security …

- The terms comes from different understandings at different periods
- Different realms, focuses
- Different classifications from different organizations
- One opinion:

Von Solms R, Van Niekerk J. From Information Security to Cyber Security[J]. Computer & Security. 2013（38）：97-102.



Deals with information both online and offline. E.g., information stored in paper, people

Cyber Security

Information System Security

Information Security

Attacks may use the vulnerabilities from non-digital properties (people)

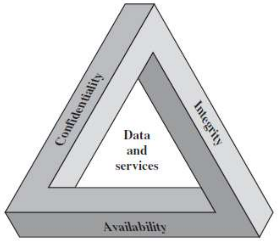
Communication security
Computer security
Network security

Network Security Objectives

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Controllability

Security Objectives -1

- Confidentiality
  - Data confidentiality: not made available or disclosed to unauthorized individuals.
    - Only the sender and the specified receiver
    - Can only collect and store information related to them
  - Privacy: what information may be collected and stored, to whom and by whom that information may be disclosed
- Integrity
  - Data integrity: information and programs are changed only in a specified and authorized manner; **data source** have not been changed.
    - Delete, modify, falsify, insert; derange, **replay**
  - System integrity: free from deliberate or inadvertent unauthorized manipulation of the system.
- Availability: systems work promptly and service is not denied to authorized users.
  - Network connections should not be interrupted
  - Network services should not be denied: DNS, servers, etc.
  - Normal operation of the networks should not be disrupted;

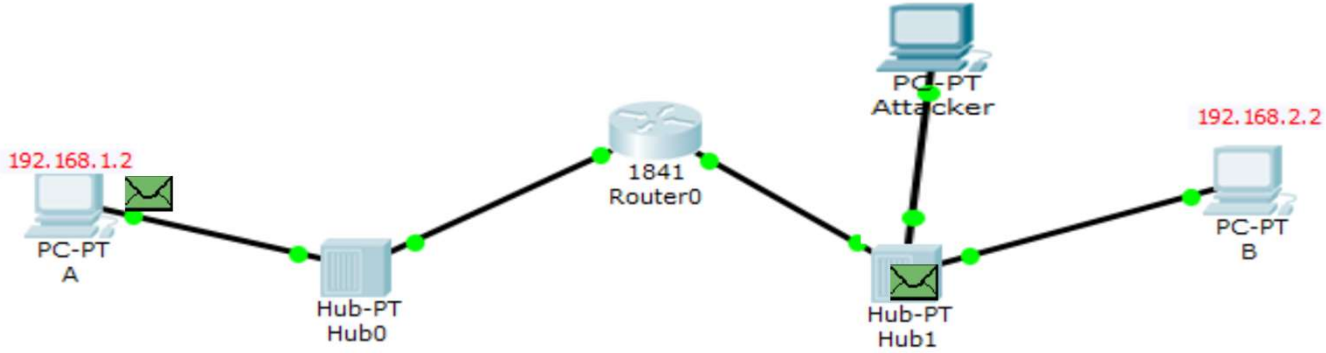


Security Objectives -2

- Non-repudiation: all involved parties cannot deny
  - Authenticate the identities of all involved parties
  - All the parties must have proofs
- Controllability, on
  - data transmission
    - Only the allowed entities, in a specified way to use the allowed resources
    - Information flowing, information content
  - Provide audit and tracing measures

Confidentiality

Anywhere on the transmission path can be inserted a monitoring device, how to prevent confidentiality?



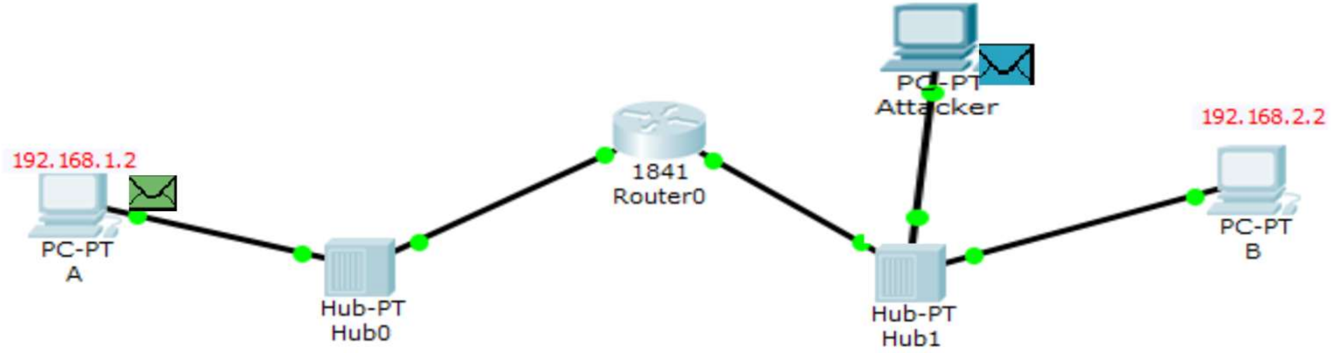
- Encrypt each datagram
- Encrypt the whole “channel”: session, connection, flow

Confidentiality

- Several levels of protection can be identified
  - Encrypt each datagram
  - Encrypt the whole “channel”: session, connection, flow
- Encryption cannot prevent interception
  - Suitable ID and authentication mechanism -> who reads the transmitted data
- Data transmission at both ends： traffic confidentiality
  - Including protection from traffic analysis (source and destination, frequency, length)

Integrity

An attack may intercept and modify a datagram on the transmission path, but both the sender and the receiver don’t know

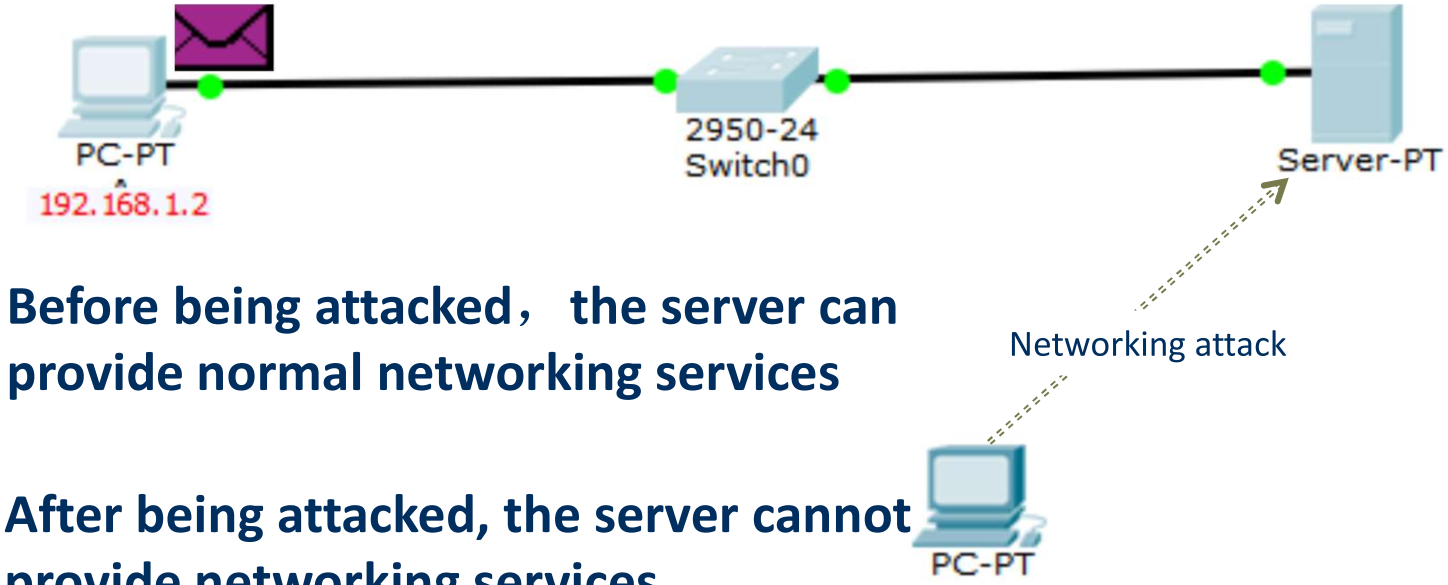


The sender can make a message digest, binding message content and sender id

Data Integrity

- Can apply to a stream of messages, a single message, or selected fields within a message
  - Connection-oriented integrity service deals with a stream of messages (datagrams) and assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays
  - A connectionless integrity service deals with individual messages without considering any larger context, and generally provides protection against message modification only

Availability



Networking attack

Attacking machine

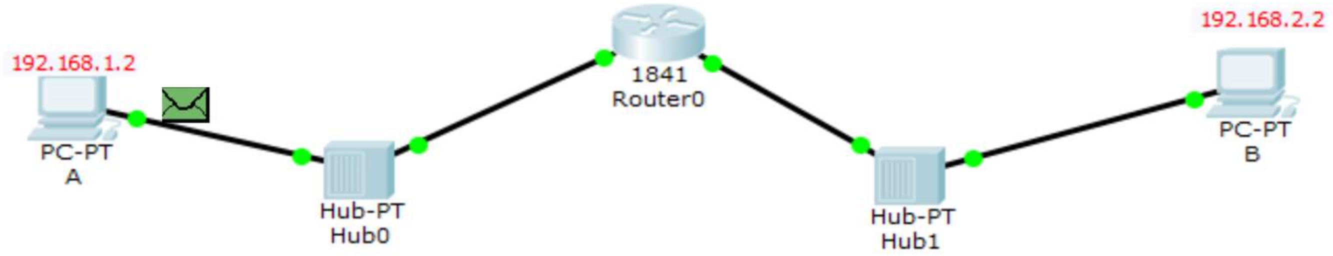
Before being attacked， the server can provide normal networking services

After being attacked, the server cannot provide networking services

Availability

- A system or system resource is accessible and usable upon demand by an authorized entity, according to performance specifications for the system
  - A system is available if it provides services according to the system design whenever legitimate users request them
- A property to be associated with other services
- Availability service
  - Addresses denial-of-service attacks
  - Depends on other security services/mechanisms such *as access control*

Non-repudiation



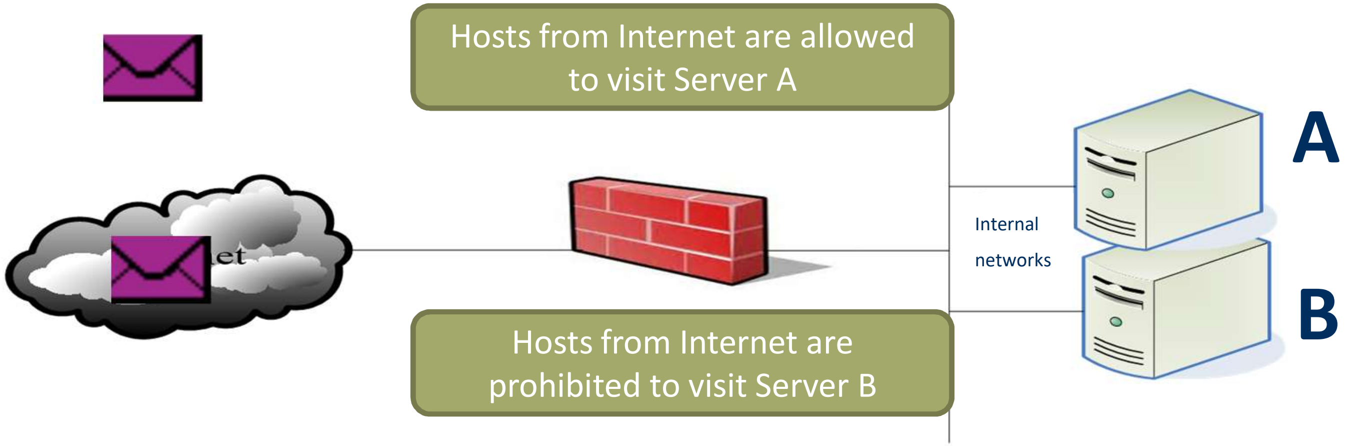
- B may be dishonest: what I received is 🟦 , not 🟩

- A may be dishonest too:
  - I did not send 🟩 to B at all.
  - what I sent to B is 🟦 , not 🟩

Non-repudiation

- Prevents either sender or receiver from denying a transmitted message
  - When a message is sent, the receiver can prove that the alleged sender in fact sent the message
  - When a message is received, the sender can prove that the alleged receiver in fact received the message

Controllability



Hosts from Internet are allowed to visit Server A

Hosts from Internet are prohibited to visit Server B

Summary

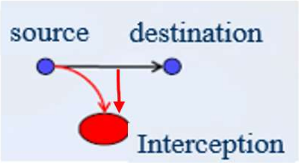
- Network security is closely related to computer security
  - General objectives
  - Protected objects
- Focuses are different
- Need to consider carefully
  - Networking environment
  - Data transmission characteristics or techniques

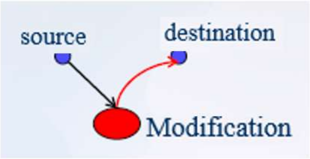
Network Security Threats and Attacks

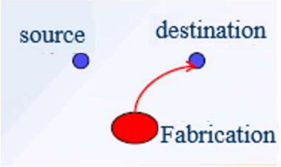
- Classification of threats and attacks
- Malicious codes
- Remote intrusions
- Masquerade
- DoS/DDoS
- Data snooping/eavesdropping and modification

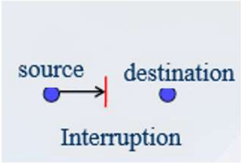
Classification of threats and attacks – attacking means

- According to the attacking means, 4 types
  - 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, file system









Classification of threats and attacks – attacking behaviors

- According to the attacking behaviors
  - Passive attacks: the goal is to obtain information that is being transmitted
    - Does not affect system resources.
    - Learn or make use of information from the system
  - Active attacks: actively harm the system
    - Obtaining user or system information is one step of active attack.

Passive Attacks

- Two types:
  - Release of message contents: monitors e-mails, telephone conversation
    - Eavesdropping (listening)
  - Traffic analysis: looks at communication patterns between entities in a system. Who? When? How long?
    - Packet size, frequency
    - Tcpdump, Wireshark
- Difficult to detect
  - If detected, easy to stop
  - precautions

Active Attacks

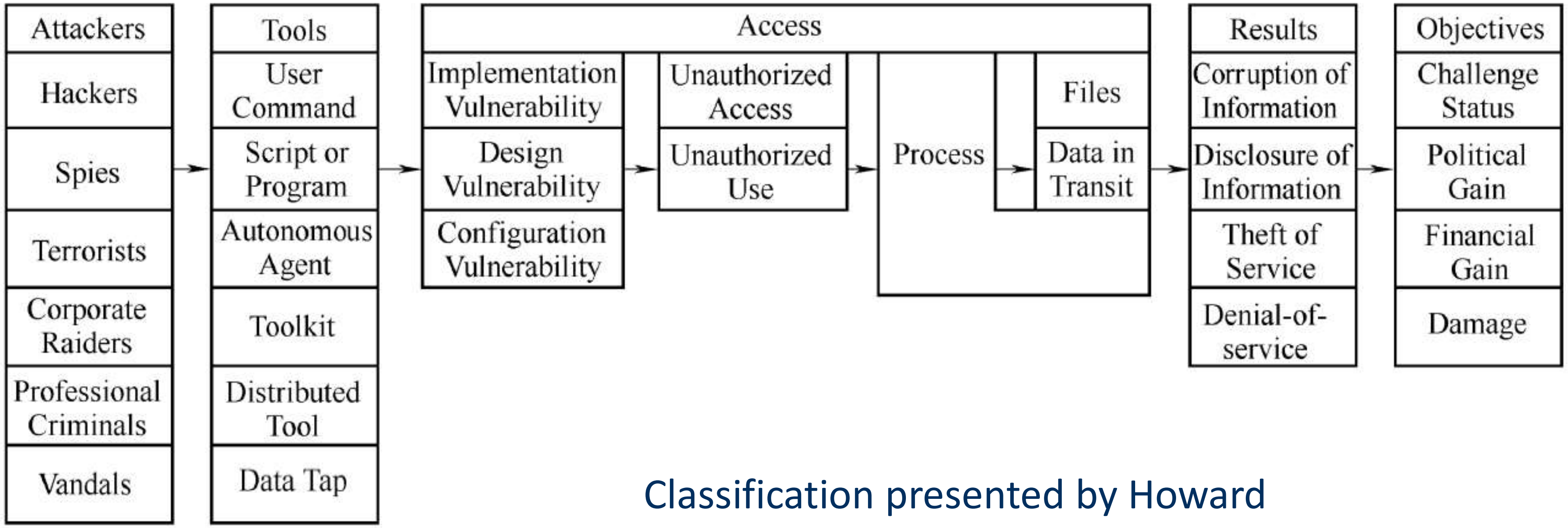
- Involve some modification of the data stream or the creation of a false stream
- Types of active attacks
  - Masquerade/spoof/impersonate: Takes place when one entity pretends to be a different entity.
  - Replay: Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
  - Modification of messages: Some portion of a legitimate message is altered
  - Denial of service: Prevents or inhibits the normal use or management of communications resources
  - Interruption, or preventing authorized access to routers, ports, servers
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
  - To detect attacks and to recover from any disruption or delays caused by them

Other classification methods

- Classification criteria
  - Acceptability, non-ambiguity, sigmacompleteness, mutual exclusiveness, reproducibility, availability, adaptability, atomicity etc.
- According to experiences and terminology:
  - Icove: virus and worms, unauthorized copy, session hijacking, logic bomb, trapdoor, Trojan, hidden channel, …
  - Cohen: Trojan, impersonating, network detection, time bomb, …
- According to single attribute: passive/active; interception/modification/fabrication/interruption…

1. Icove D, Seger K, Vonstorch W, Compter Crime, a crime-fighter's handbook: O'Reilly and Associates, Inc., 1995
2. Cohen F, Information system attacks: a preliminary classification scheme. Computers and security, 1997,16(1), 29-46

Classification of threats and attacks – multiple attributes 1

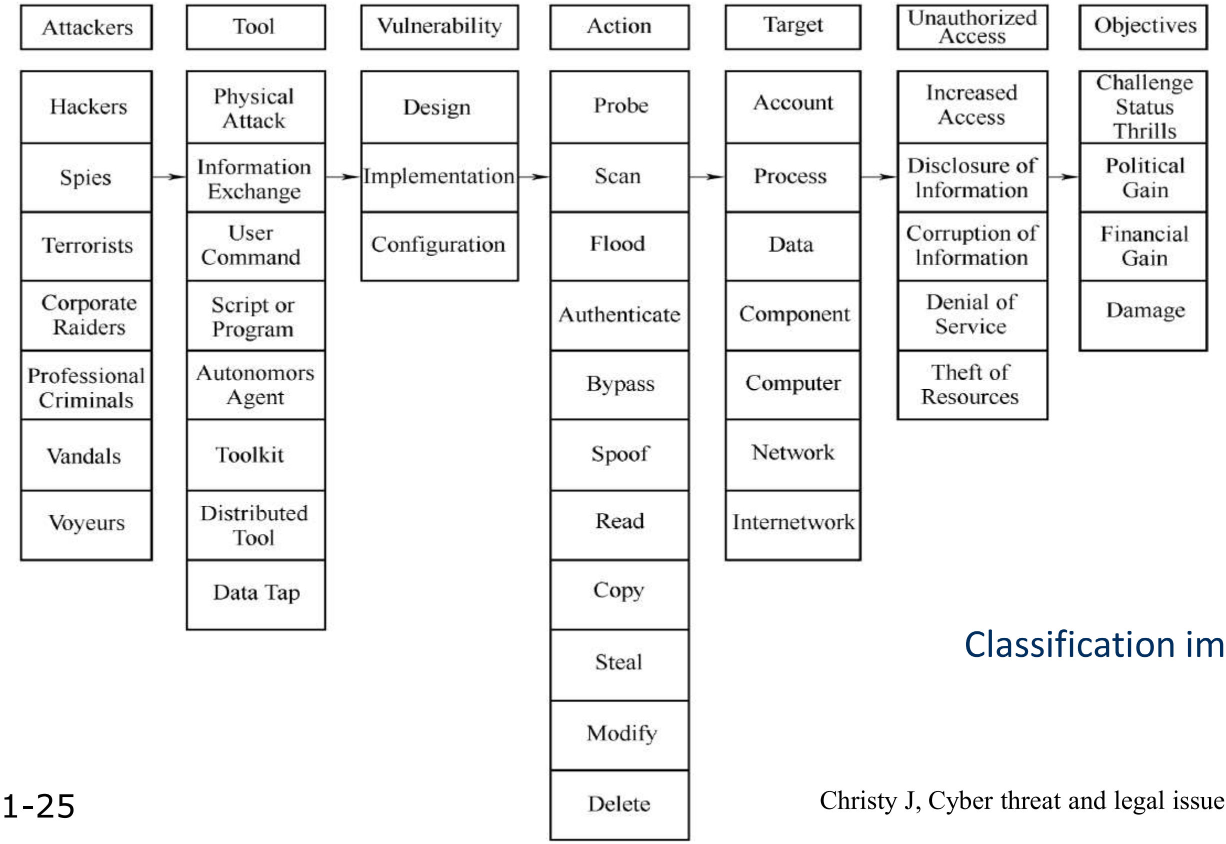


Attackers	Tools	Access				Results	Objectives
Hackers	User Command	Implementation Vulnerability	Unauthorized Access	Process	Files	Corruption of Information	Challenge Status
Spies	Script or Program	Design Vulnerability	Unauthorized Use		Data in Transit	Disclosure of Information	Political Gain
Terrorists	Autonomous Agent	Configuration Vulnerability				Theft of Service	Financial Gain
Corporate Raiders	Toolkit					Denial-of-service	Damage
Professional Criminals	Distributed Tool						
Vandals	Data Tap						

Classification presented by Howard

[1] Howard J, An analysis of security incidents on the Internet, West Lafayette, Carnegie Mellon University, 1997

Classification of threats and attacks – multiple attributes 2

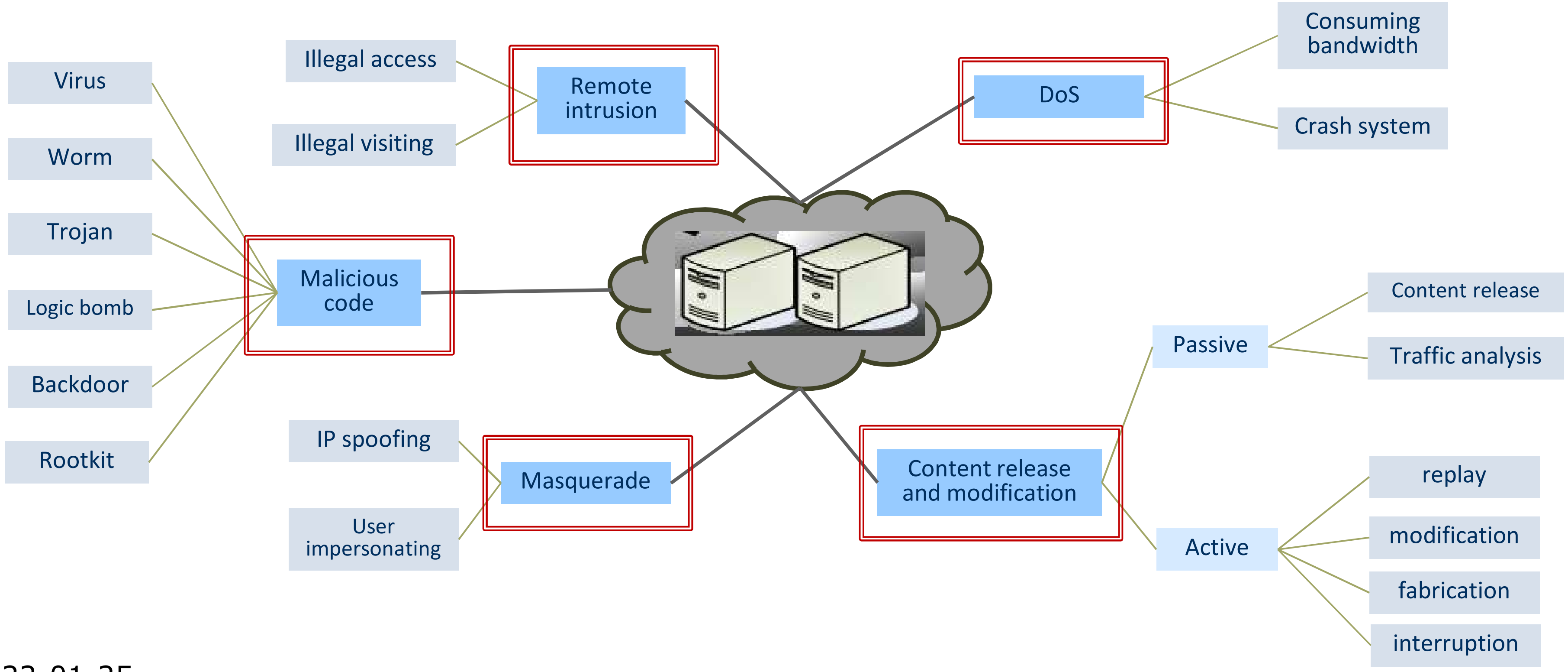


Attackers	Tool	Vulnerability	Action	Target	Unauthorized Access	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge Status Thrills
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomors Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

Classification improved by Christy

Christy J, Cyber threat and legal issues, shadowcon Conference, 1999.

Network security threats and attacks



2022-01-25

Malicious code

- Computer virus: replicate itself into other executable code, when the infected code is executed, the virus also executes.
- Worm: can run independently, and can propagate a complete working version of itself onto other hosts on a network.
- Trojan horse: appears to have a useful function, but also has a hidden and potentially malicious function
- Logic bomb: inserted into software by an intruder; lies dormant until a predefined condition is met;
- Backdoor: bypasses a normal security check; may allow unauthorized access to functionality.
- Rootkit: Set of hacker tools used after attacker has broken into a computer system and gained root-level access
- Malicious scripts: with the purpose of harm and destroy systems or systems' functions

Remote intrusion

- Remote attacking
  - Illegal access: connect to the internal network, and gain the access right to the internal resources (like internal person)
  - Illegal use: use the resources through remote login or hacking tools
- Intruder
  - Hacker
    - proficient in networks, systems, peripherals, software and hardware
    - Spirit of free, innovation, anti-traditions, cooperate
  - Cracker
    - Destroy the system security with evil intentions

Deny of Service (DoS/DDoS)

- Make the target host or system stop providing (or cannot provide enough) services or resources
  - Storage, cache, processes, network bandwidth
- Consuming network bandwidth and resources
  - Land Attack, ICMP Redirect, Smurf, SYN flooding, UDP flooding…
- Braking down the system by making use of vulnerability
  - E.g., buffer overflow

Masquerade

- IP spoofing
  - Use legitimate or non-existing IP address as source address
- User impersonating
  - User identity
  - Social engineering
  - Make use of other users’ identity

Challenges of Network Security and Research Contents

- Challenges of network security
- Research contents
- Contents of the lectures

Security Challenges -1

- Security is not simple
  - Requirements are straightforward and self-explanatory
  - Complex mechanisms are needed to meet the requirements, understanding them maybe not easy
- In developing a particular security mechanism, potential attacks need to be considered.
  - Successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
- The procedures used to provide particular services are often counterintuitive.
  - A security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed.
  - It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense

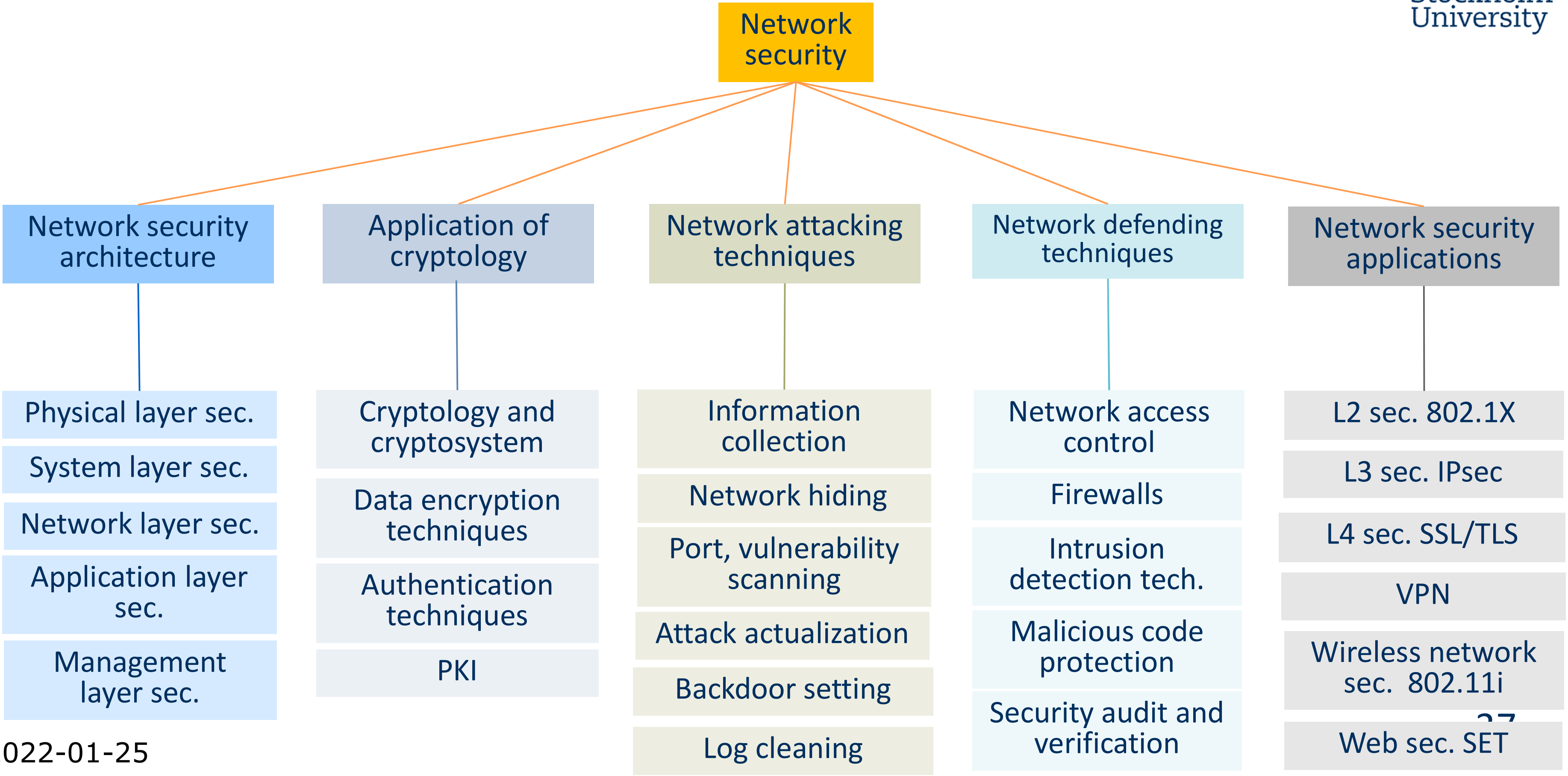
Security Challenges -2

- Necessary to decide where to use designed security mechanisms
  - physical placement (where in a network are certain security mechanisms needed)
  - logical placement (what layers of an OSI architecture should the mechanisms be placed)
- Security mechanisms
  - involve more than a particular algorithm or protocol
    - require that participants possess some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information
- Security is essentially a battle between a perpetrator who tries to find holes and the designer or administrator who tries to close them

Security Challenges -3

- Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.
- Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
- Many users (and even security administrators) view strong security as a hindrance to efficient and user-friendly operation of an information system or use of information
- Users and system managers perceive little benefit from security investment until a security failure occurs.

Research contents of network security



Network security

Network security architecture

- Physical layer sec.
- System layer sec.
- Network layer sec.
- Application layer sec.
- Management layer sec.

Application of cryptology

- Cryptology and cryptosystem
- Data encryption techniques
- Authentication techniques
- PKI

Network attacking techniques

- Information collection
- Network hiding
- Port, vulnerability scanning
- Attack actualization
- Backdoor setting
- Log cleaning

Network defending techniques

- Network access control
- Firewalls
- Intrusion detection tech.
- Malicious code protection
- Security audit and verification

Network security applications

- L2 sec. 802.1X
- L3 sec. IPsec
- L4 sec. SSL/TLS
- VPN
- Wireless network sec. 802.11i
- Web sec. SET

Organization of the Lectures

- **1st week:**
  - L1: course introduction + introduction of network security
  - L2: network security architecture + application of cryptograph (PKI+ MAC)
- **2nd week: network attacking techniques**
  - L3: information collection, network hiding, port, vulnerability scanning (preparations)
  - L4: attack actualization, backdoor setting, log cleaning (attack & processing afterwards)
- **3rd week: network defending techniques**
  - L5: Firewall
  - L6: Intrusion detection
- **4th week: network security applications**
  - L7: IPsec + Transport level security
  - L8: Wireless security

Thank you!