Stockholm University

Network Security System and Architecture

Network Security (NETSEC)

Yuhong Li

Outline

- OSI & TCP/IP model and security requirements at each layer
- OSI security architecture
- Network security model
- Network security axioms

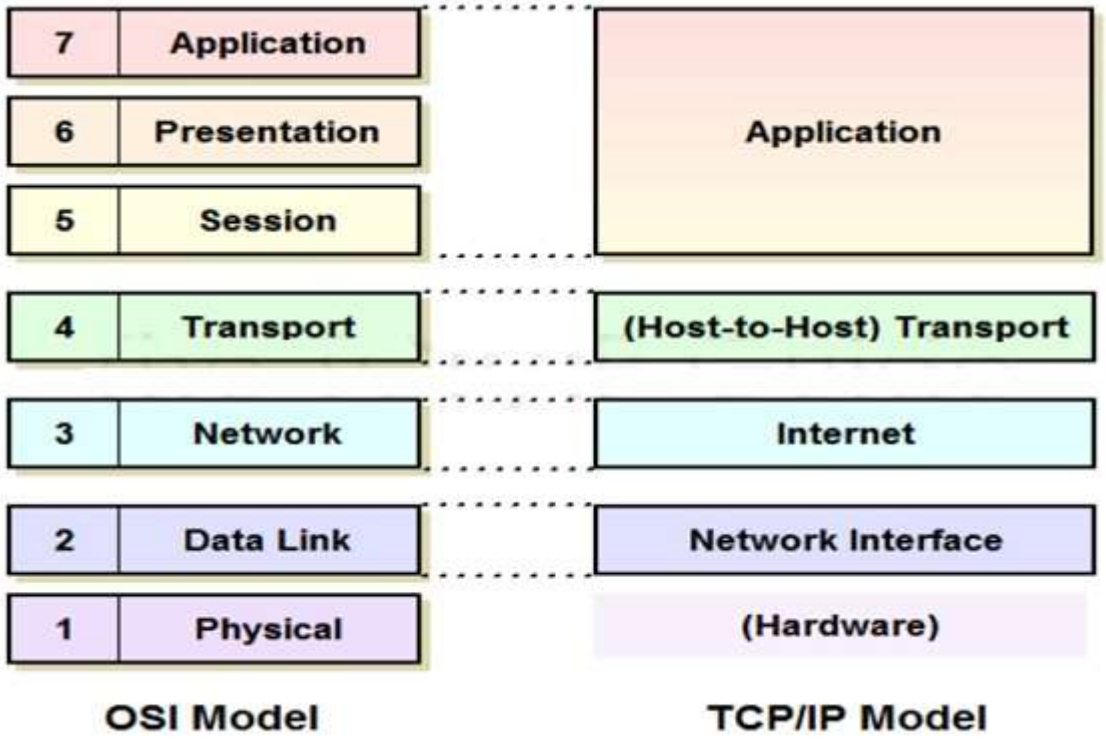
Stockholm University

OSI Network Model and Security Requirements

- Review: OSI model and protocols
- Security problems of OSI model
- Security requirements at each layer

OSI Reference Model and TCP/IP Model

- OSI(Open Systems Interconnection)
  - Session layer
  - Presentation layer

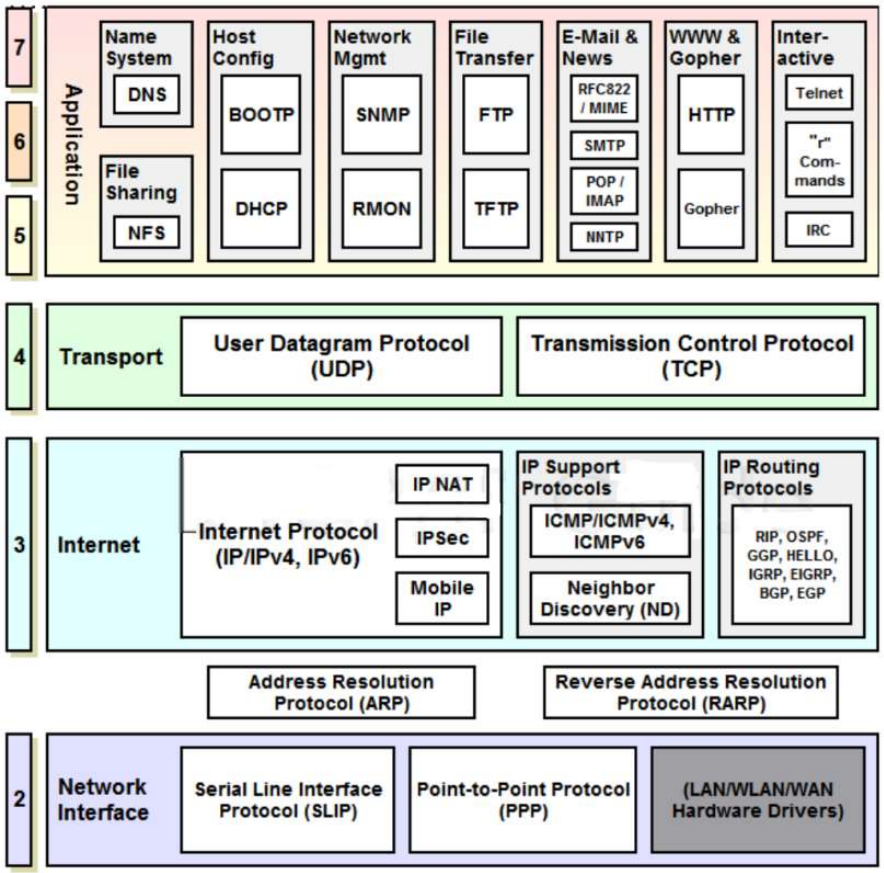


Major Functions at Each Layer

Stockholm University

Layer	Delivery unit	Functions/purposes
Application	Message	High level protocols
Transport	Segment	End-to-end: connection setup, flow control, error control, multiplex
Network	Packet	Addressing and routing: IP supports transmitting packets from any network source on the internetwork and tries to deliver them to the destination regardless of the path each of the packet takes.
Link (Network Interface)	Frame	Hop-by-hop flow control and error control: makes it possible for the packets to cross the physical links from one device to another directly connected device (WANs, LANs)
Physical	Bit stream	Physical and electrical specifications for devices. Devices that operates here are connectors, cabling, NICs…

Protocols


7
6
5
Application
Name System
DNS
File Sharing
NFS
Host Config
BOOTP
DHCP
Network Mgmt
SNMP
RMON
File Transfer
FTP
TFTP
E-Mail & News
RFC822 / MIME
SMTP
POP / IMAP
NNTP
WWW & Gopher
HTTP
Gopher
Inter-active
Telnet
"r" Com-mands
IRC
4
Transport
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
3
Internet
Internet Protocol (IP/IPv4, IPv6)
IP NAT
IPSec
Mobile IP
IP Support Protocols
ICMP/ICMPv4, ICMPv6
Neighbor Discovery (ND)
IP Routing Protocols
RIP, OSPF, GGP, HELLO, IGRP, EIGRP, BGP, EGP
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
2
Network Interface
Serial Line Interface Protocol (SLIP)
Point-to-Point Protocol (PPP)
(LAN/WLAN/WAN Hardware Drivers)

Successes and problems of Internet

Stockholm University

- Global digitalization
  - Digitalization of important information:
    - Personal information, enterprise and industrial information, governmental information
  - Important services and applications are network-based
    - Web-based application (E-business, E-government, …), military, national defense
- Techniques making Internet successful
  - Unified and efficient TCP/IP protocols
  - Layered architecture
  - Various transmission techniques
  - Internet core, educational and research network (GEANT, GEANT2, GENI, CERNET, …)
  - Openness
- Problems
  - Quality of service
  - Management
  - **Security**
  - …

Security problems in Internet-1

Stockholm University

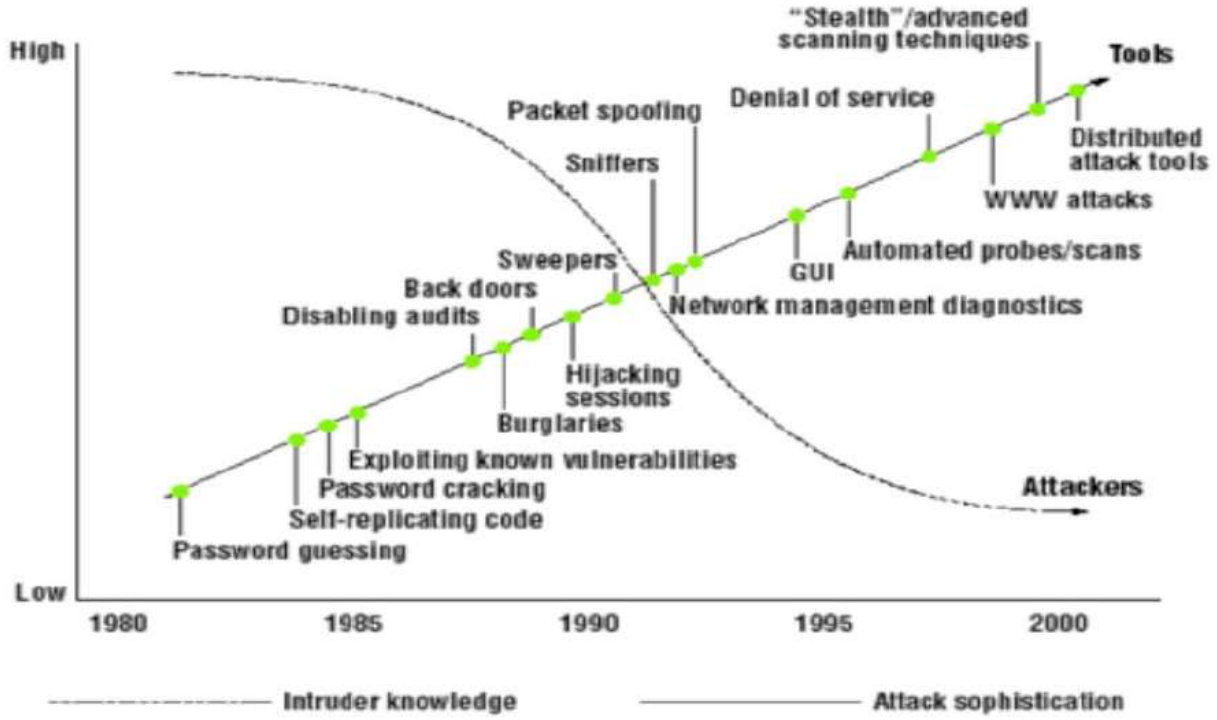
- Exchange of users' social information is becoming more and more dependent on Internet
  - Most users lack knowledge and experiences about computers, networks and security
- TCP/IP architecture
  - Unencrypted transmission -> eavesdropping, falsified, spoofing
  - Openness -> big opportunities to attackers
- Design faults and security vulnerabilities in systems, protocols, applications, configurations
  - Used by attackers

Security problems in Internet -2

Stockholm University

- Internal reasons: security problems in each layer of TCP/IP
  - IP layer: no authentication and encryption mechanisms
    -> IP spoofing
  - TCP/UDP layer: three-way handshake
    -> TCP connection may be spoofed, intercepted, utilized
    -> UDP: IP source routing, flooding
  - Application layer:
    -> No authentication, access control, integrity, encryption etc.
    -> No security mechanisms in the applications: Web, Finger, FTP, Telnet, E-mail, DNS, SNMP…
- External reasons: intruders with various purposes
  - Political, economical, business, personal
  - Hackers, malicious programs
  - **Open-source codes and tools for attacks and anti-attacks in Internet!**

Intruder knowledge vs. attack sophistication

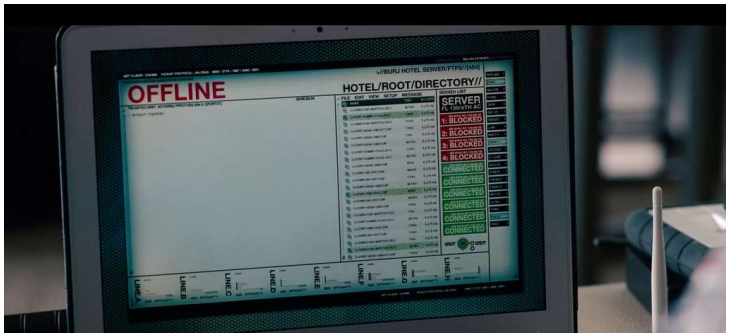


Typical threats to TCP/IP

Stockholm University

- Physical layer
  - Steal, insert, delete, etc., normally devices are needed
- Datalink layer
  - Easy to listen to the data (promiscuous mode)
- Network layer
  - IP spoofing, attacks to the security holes at the network layer
- Transport layer
  - Attacks to the security holes at the transport layer
  - Aiming at header, protocol, traffic,
- Application layer
  - All kinds of threats, aiming at authentication, access control, integrity, confidentiality

Physical layer security



- Security of the physical environment: transmission lines, devices, computer rooms
  - Steal: information >>machine
  - Fire prevention, thunder and lightening prevention
  - Static electricity
  - Prevention from electromagnetic leak
    - Radiation and conduction

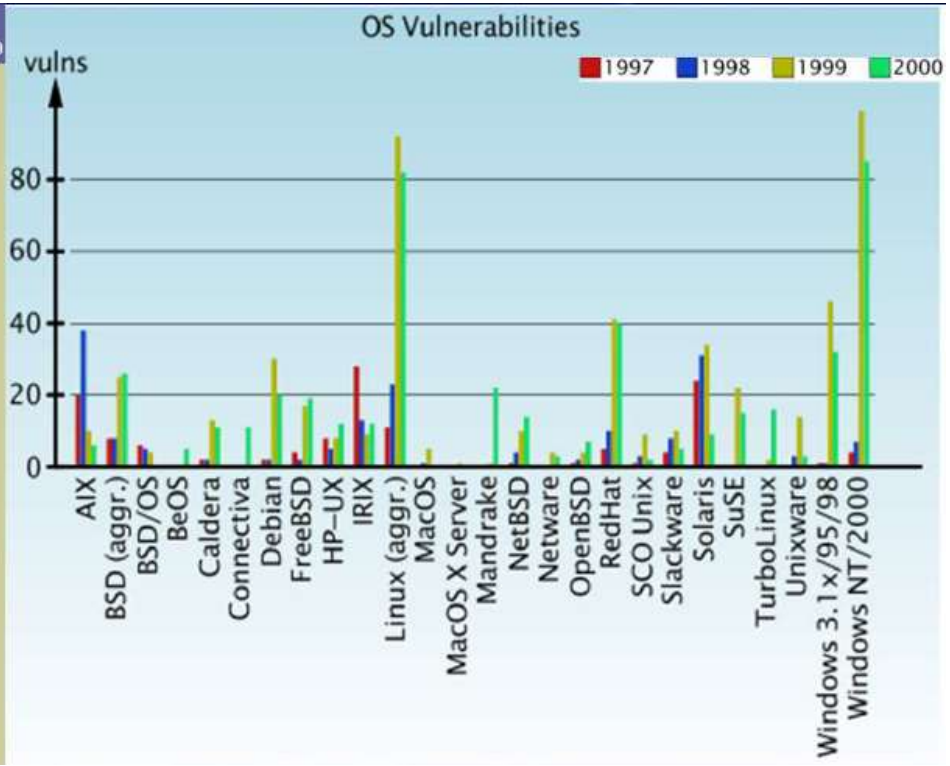
(OS) System security

Stockholm University

- OS security is the basis of computers and the whole networks
- Security holes
  - Faults in design and development
  - Security announcements from OS providers -> update in time
- Wrong configurations
  - Dependent on applications and environment
  - Tools: in accordant with the predefined security policies
- Viruses and worms
  - Protection, check, kill
  - E.g., Microsoft SMB remote codes execution hole: CVE-2017-0144, Microsoft announced an update: in Mar. 2017; but cracked, Ransomware attack in April 2017!

Vulnerability statistics

Number of OS Vulnerabilities by Year				
OS	1997	1998	1999	2000
AIX	20	38	10	6
BSD (aggr.)	8	8	25	26
BSD/OS	6	5	4	0
BeOS	0	0	0	5
Caldera	2	2	13	11
Connectiva	0	0	0	11
Debian	2	2	30	20
FreeBSD	4	2	17	19
HP-UX	8	5	8	12
IRIX	28	13	9	12
Linux (aggr.)	11	23	92	82
MacOS	0	1	5	0
MacOS X Server	0	0	1	0
Mandrake	0	0	1	22
NetBSD	1	4	10	14
Netware	0	0	4	3
OpenBSD	1	2	4	7
RedHat	5	10	41	40
SCO Unix	1	3	9	2
Slackware	4	8	10	5
Solaris	24	31	34	9
SuSE	0	0	22	15
TurboLinux	0	0	2	16



www.securitiyfocus.com (2000)

Network layer security

- Authentication
  - Confirm identity (users, machines, packets' source)
  - Whether has access and use right to certain resources
- Access control
  - Prevent illegal users from entering the protected network resources
  - Prevent legal users from using unauthorized network resources
- Confidentiality and integrity of transmitted data
- Routing system's security
  - OS of routing devices, e.g., configurations
  - Transmission of routing information
- Intrusion detection
  - Collect and analyse network behaviors, security logs etc.
  - Check if there are any potential attacks (break security policies, or being attacked)
  - Real time protection against internal and external attacks
- Anti-virus techniques
  - Obtain information from the collected information
  - Process in the server, send solution to each client
  - Real time data collection, analysis and processing

Application layer security

Stockholm University

- Web security
  - Web services are based on HTTP ->not encrypted
  - HTTP/HTTPS: stateless protocol -> ID spoofing is easy
  - Vulnerability of web programs -> SQL injection, XSS etc.
- DNS security
  - DSN spoofing

  ->against DoS attack: backup DNS server, least privilege, least service, limited domain
- Email system security
  - Direct attacks: steal passwords, intercept email content, falsify email content, spams
  - Indirect attacks: malicious code in attachments, phishing with forged web pages and links

Summary -network security requirement

Stockholm University

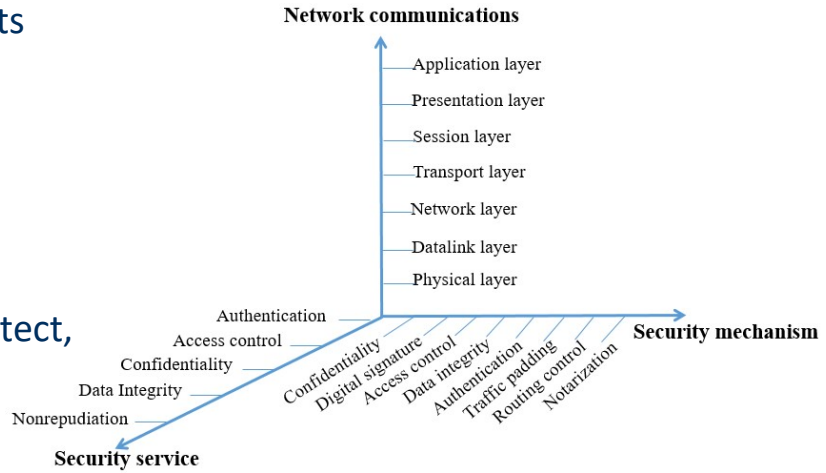
- Any single technique cannot solve the network security problems efficiently
  - Security functions at each layer
  - The functions must be coordinated
- Impossible to design a network security system suitable to all networking environments
  - The network security system must be combined with applications and application systems

OSI Security Architecture

- Security attacks
- Security mechanisms
- Security services

The OSI Security Architecture

- ITU-T Recommendation X.800, *Security Architecture for OSI*
  - Vendors: develop security features for their products and services
  - Managers: organize the task of providing security
- Focuses on security attacks, mechanisms, and services
  - **Security attack:** Any action that compromises the security of information owned by an organization.
  - **Security mechanism:** A **process** (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
  - **Security service:** A processing or communication **service** that enhances the security of the data processing systems and the information transfers of an organization.
    - intended to counter security attacks: use one or more security mechanisms to provide the service.



Security Attacks

Stockholm University

- An intelligent/a deliberate attempt (choice of a method or technique) to
  - violate the security policy of a system
  - bypass security services
  - compromises the security of information
- Can be active or passive

Specific Security Mechanisms

Stockholm University

- Security mechanism: a **process** designed to detect, prevent, or recover from a security attack

Authentication exchange: to ensure the identity of an entity by means of information exchange.

Access control: enforce access rights to resources.

Digital Signature: Allows a recipient to prove the source and integrity of data

Data integrity: to assure the integrity of a data unit or stream of data units

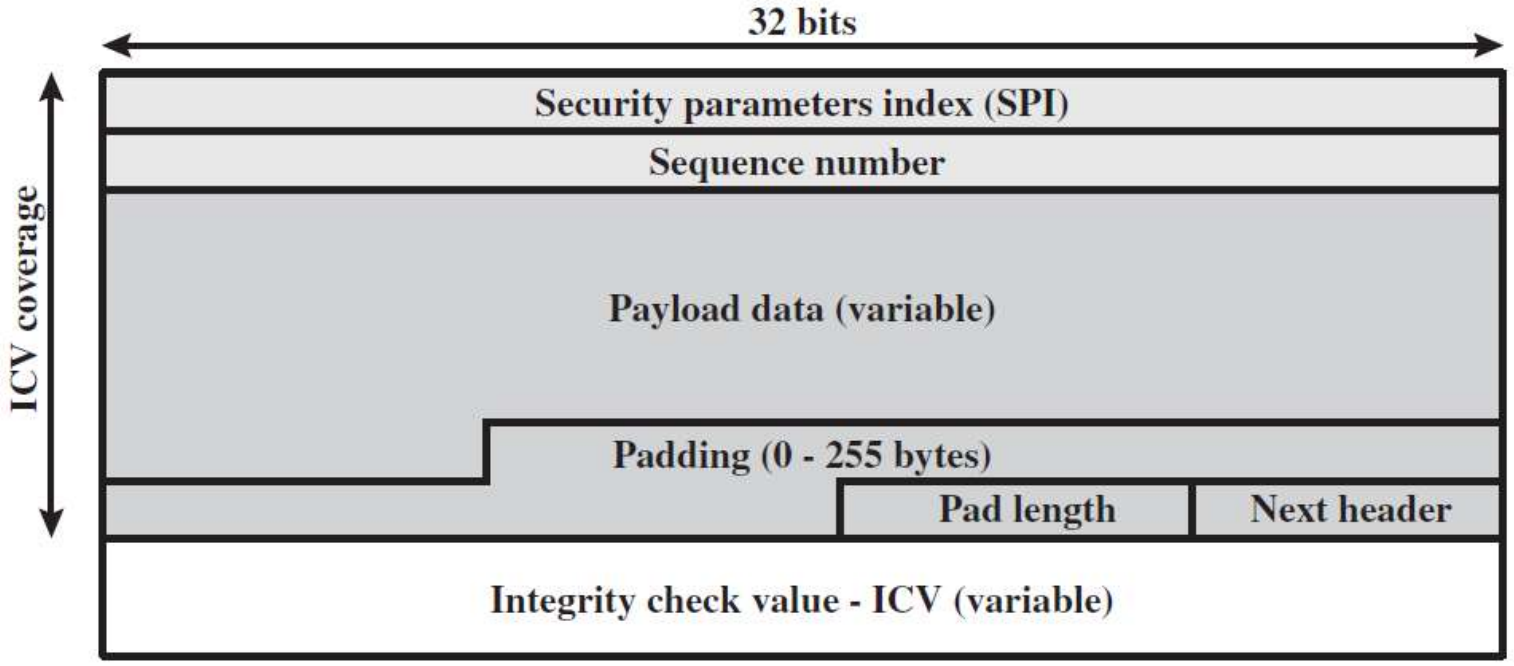
Encipherment: Use of mathematical algorithms to transform data into a form that is not readily intelligible

Traffic Padding: Hides traffic by insertion of bits into gaps in a data stream to mitigate traffic analysis attempts

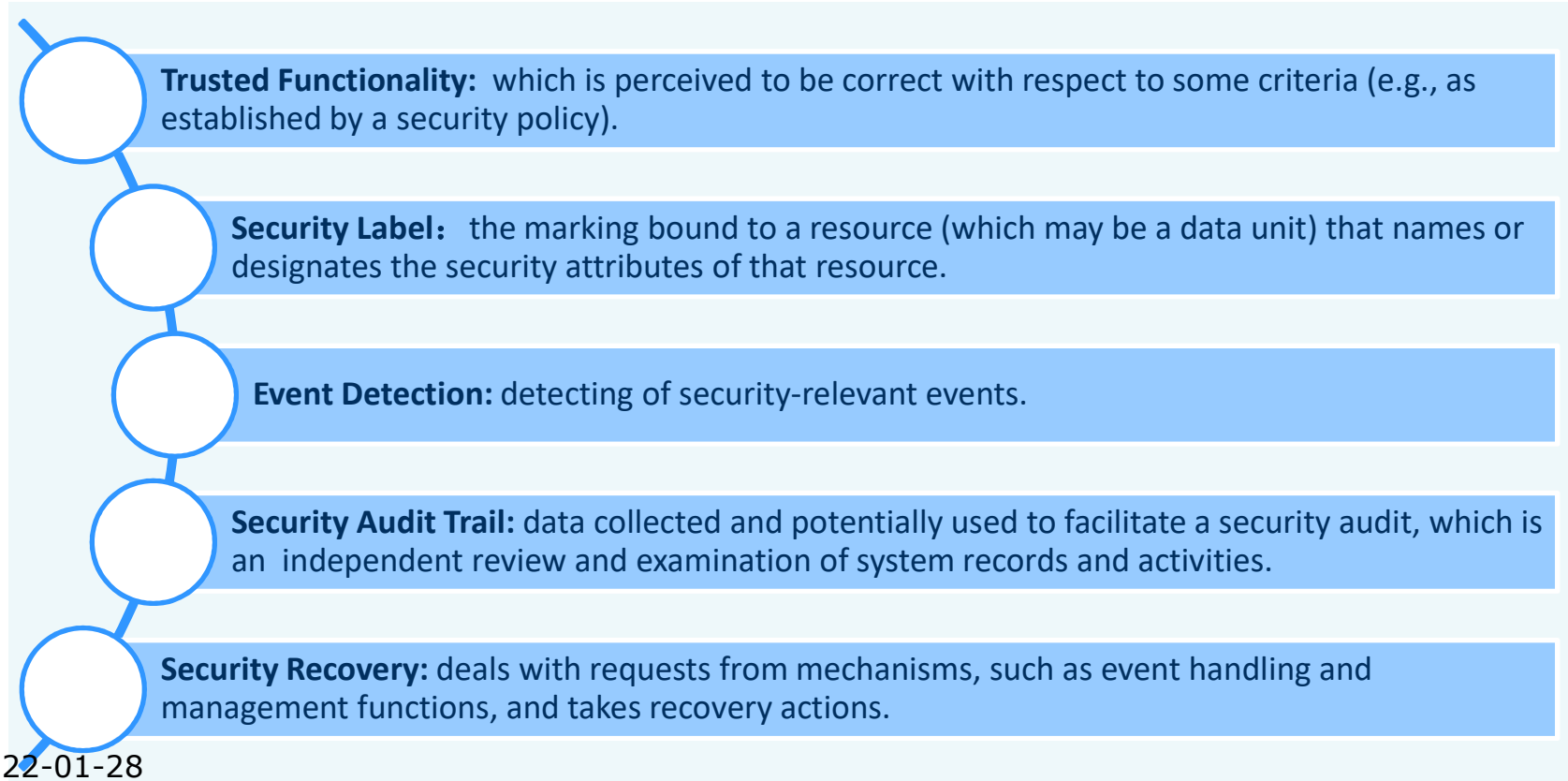
Routing control: enable selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization: The use of a trusted third party to assure certain properties of a data exchange.

Example – security mechanisms used in IPsec ESP



Pervasive Security Mechanisms



Security Service

Stockholm University

- Security service
  - Implements security policies and is implemented by using one or more security mechanisms.
- ITU X.800 defines a security service ”as a service which ensures **adequate security** of the systems or of data transfers”.
- ITU divides security services into 5 categories:
  - Authentication
  - Access Control
  - Data Confidentiality
  - Data Integrity
  - Nonrepudiation

Authentication

Stockholm University

- Concerns assuring that a communication is authentic
  - The recipient of the message (connectionless) is assured that the message came from the source that it claims to be
  - For connection-oriented communication, all entities are assured that the connection is not interfered by unauthorized party
    - At connection initiation – both entities are authentic
    - For ongoing interactions, no third party are involved

Access Control

Stockholm University

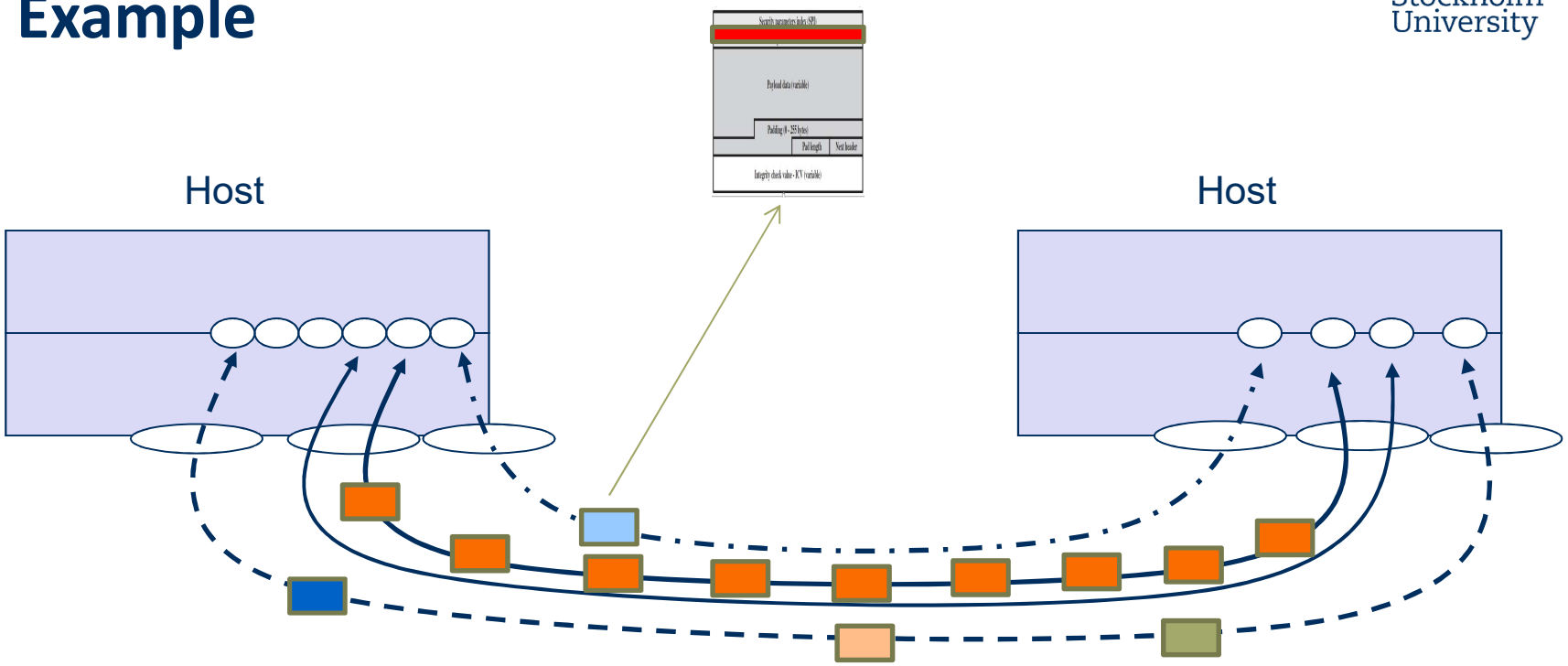
- The ability to limit and control the access to host systems and applications via communications links
  - Each entity must be identified or authenticated, so that access rights can be tailored to the individual
  - Resources: when, what type of resources, for how long

Confidentiality

Stockholm University

- The protection of transmitted data from unauthorized disclosure (from passive attacks).
- Several levels of protection can be identified
  - Confidentiality service: protects all user data transmitted between two users over a period of time
  - Traffic flow confidentiality: protect the information from traffic analysis (source and destination, frequency, length)
  - Connection confidentiality: protect all user data on a connection
  - Connectionless confidentiality: protection of all user data in a single data block
  - Selective field confidentiality: protection of selected data field in a single data block or on a connection

Example



connectionless

connection-oriented

Data Integrity

Stockholm University

- Can apply to a stream of messages, a single message, or selected fields within a message
  - Connection-oriented integrity: data belonging to the connection, **no duplication, insertion, modification, reordering, or replays**
    - Connection Integrity with Recovery
    - Connection Integrity without Recovery
    - Selective-Field Connection Integrity: selected field of a data block within a connection
  - A connectionless integrity: individual messages, **generally** provides protection against message **modification only**
    - Connectionless Integrity: plus a limited form of replay
    - Selective-Field Connectionless Integrity

Non-repudiation

Stockholm University

- Prevents either sender or receiver from denying a transmitted message
  - Origin: a message was sent by the specified party
  - Destination: a message was received by the specified party

Availability

Stockholm University

- 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*

Relationship Between Security Services and Mechanisms

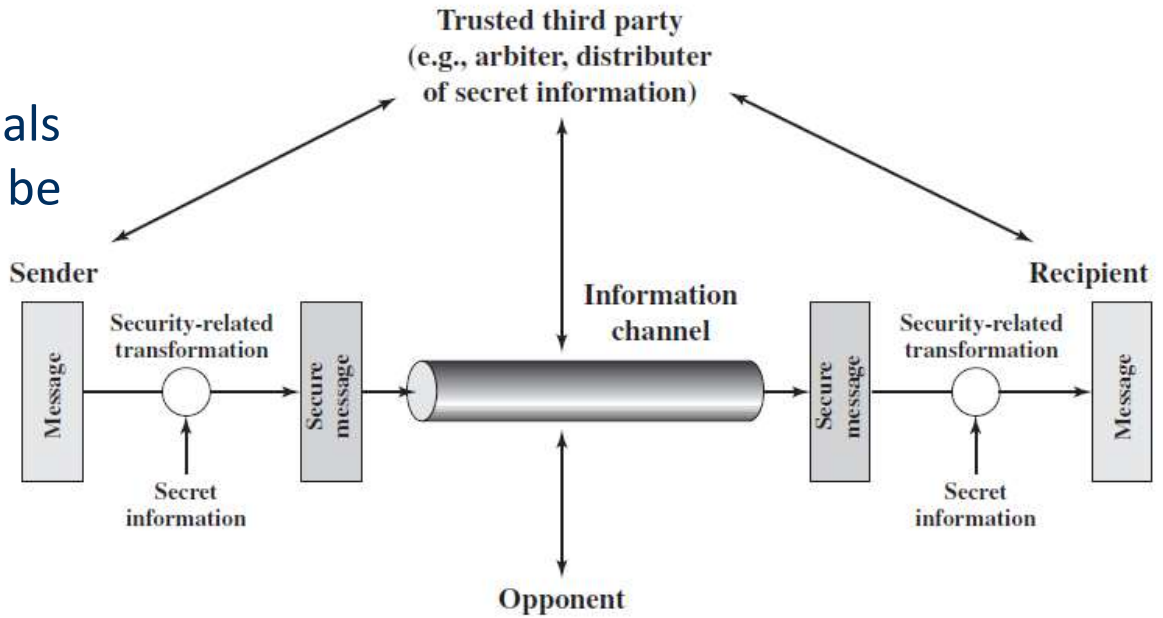
Stockholm University

	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer Entity Authentication	Y	Y			Y			
Data-Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic-Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Network Security Model

Basic Model for Network Security

- A security-related transformation on the information to be sent.
- Some secret information shared by the two principals
- A trusted third party may be needed to achieve secure transmission.



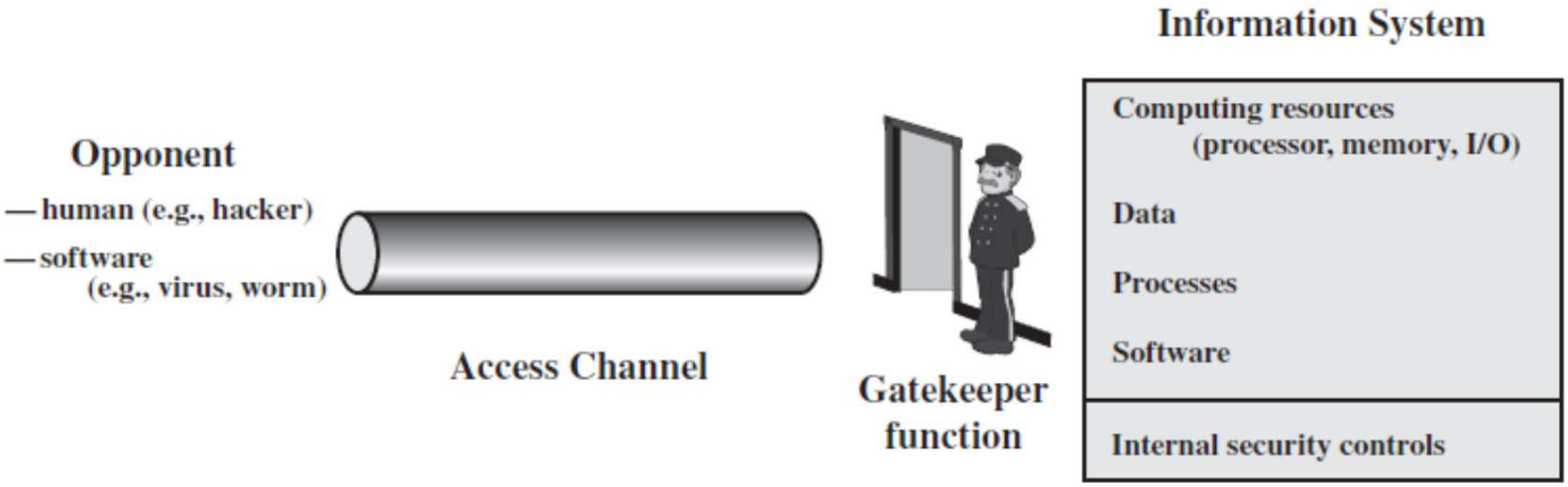
Basic Tasks in Designing Security Service

Stockholm University

1. Design an algorithm for performing the security-related transformation: an opponent cannot defeat.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Network Access Security Model

- A gatekeeper function.
- Internal security controls



Stockholm University

Network Security Axioms

- Discussions about system security
- Network security axioms

Network Security is a System

Stockholm University

- Need complementary technology that applies to specific threat pattern: defense-in-depth
  - Consider mitigation of different threat categories
  - Use various threat mitigation techniques: protect, detect, deter, recover, …
  - A collection of a network-connected devices, technologies, and best practices that work in a complementary ways should be used

System security and operation efficiency

Stockholm University

- Contradictory to each other
  - Security mechanisms and services occupy system resources
  - Improve cost of management

  ->Reduce the efficiency for serving normal users
- Network security techniques must reduce the effect to network operations
- Trade off between cost/efficiency and security when designing systems
  - Key services
  - requirements

Assessment to system security

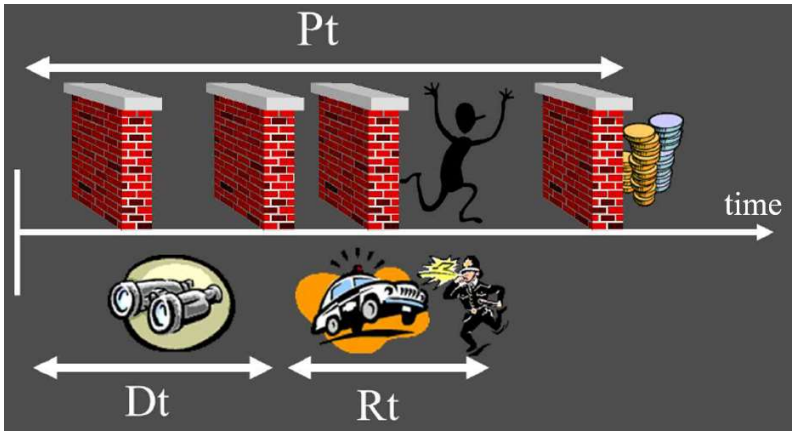
- How to assess if a system secure or not?
  - No absolute security solutions
  - Relative system security
  - No uniform criteria for assessing the system security
    - System environment and applications should be considered
- A secure system should satisfy

  $Pt > Dt+Rt$

  Pt: protection time

  Dt: detection time

  Rt: response time



Network Security Axioms -1

Stockholm University

1. Business priorities must come first
   - There is a relationship between business objectives, the security policy, and security design
2. Network security promotes good network design
   - Thinking about network security after designing the network impacts the network design
   - Considering security from the beginning promotes good network design
3. Everything is a target
   - Interdependencies allow attacker's goal to be met in any numbers of ways
   - Attacker's options
     - protocols, routers, applications, OS, Internet bandwidth, firewalls, servers, etc.

Network Security Axioms -2

4. Everything is a weapon
   - Attacker performs multiple steps to execute an attack
   - An attacker gains additional weapon at each step in order to reach his goal
5. Strive for operational simplicity
   - Respond to the threats you encounter in an easy and obvious way
   - Constantly evaluate the level of complexity to ensure that your security is simple to deploy and straightforward to maintain
   - Human error is one of the biggest root causes of configuration problems

Network Security Axioms -3

Stockholm University

We have a firewall so we are safe…

6. Good network security is predictable
   - Security is only as good as the weakest link, questions to ask
     - What role each technology in your system will play?
     - What are the technological limitations
     - Is there additional technologies in your system that help secure against the same threats
   - Understanding the strength and weaknesses of your security system help to deal with new threats
     - You can quickly decide whether your existing system will deal with the problem adequately
7. Avoid security through obscurity, some examples
   - Rely on the firewall performing its access control function properly
   - Patch discovered threats or attacks quickly
   - Keep system design confidential

Network Security Axioms -4

Stockholm University

- Least privilege
  - For any subject (users, administrators, programmers, systems)
- Defense “vertically”
  - Multiple mechanisms and methods for backup and redundancy
  - Network security +host security+ staff/person security
- Defense diversely
  - Different defensing systems
  - Different configurations
- Default policies-> rejected or permitted

Expected learning outcomes

Stockholm University

- Understand the security problems and requirements of networks (Internet)
- Describe the OSI security architecture
- Describe and apply the network security model (including the network access security model)
- Understand the network security axioms

Thank you!