Telematics 10

Chapter 10
Network Security

Network Security: Overview

- Introduction:
  - Threats in Communication Networks
  - Security Goals & Requirements
  - Safeguards
- Fundamentals of Security Technology:
  - Symmetric & asymmetric cryptography
  - Detection of message modifications
  - Cryptographic protocols
- Network Security Examples:
  - Integration of Security Services into Network Architectures
  - IPSec
  - Firewalls

What is a Threat in a Communication Network?

- Abstract Definition:
  - A *threat* in a communication network is any possible event or sequence of actions that might lead to a violation of one or more *security goals*
  - The actual realization of a threat is called an *attack*
- Examples:
  - A hacker breaking into a corporate computer
  - Disclosure of emails in transit
  - Someone changing financial accounting data
  - A hacker temporarily shutting down a website
  - Someone using services or ordering goods in the name of others
- What are security goals?
  - Security goals can be defined:
    - depending on the application environment, or
    - in a more general, technical way

Security goals depending on the application environment 1

- Banking:
  - Protect against fraudulent or accidental modification of transactions
  - Identify retail transaction customers
  - Protect PINs from disclosure
  - Ensure customers privacy
- Electronic trading:
  - Assure source and integrity of transactions
  - Protect corporate privacy
  - Provide legally binding electronic signatures on transactions
- Government:
  - Protect against disclosure of sensitive information
  - Provide electronic signatures on government documents

Security goals depending on the application environment 2

- Public Telecommunication Providers:
  - Restrict access to administrative functions to authorized personnel
  - Protect against service interruptions
  - Protect subscribers privacy
- Corporate / Private Networks:
  - Protect corporate / individual privacy
  - Ensure message authenticity
- All Networks:
  - Prevent outside penetrations (who wants hackers?)
- Sometimes security goals are also called *security objectives*

Security Goals Technically Defined

- *Confidentiality:*
  - Data transmitted or stored should only be revealed to an intended audience
  - Confidentiality of entities is also referred to as *anonymity*
- *Data Integrity:*
  - It should be possible to detect any modification of data
  - This requires to be able to identify the creator of some data
- *Accountability:*
  - It should be possible to identify the entity responsible for any communication event
- *Availability:*
  - Services should be available and function correctly
- *Controlled Access:*
  - Only authorized entities should be able to access certain services or information

Threats Technically Defined

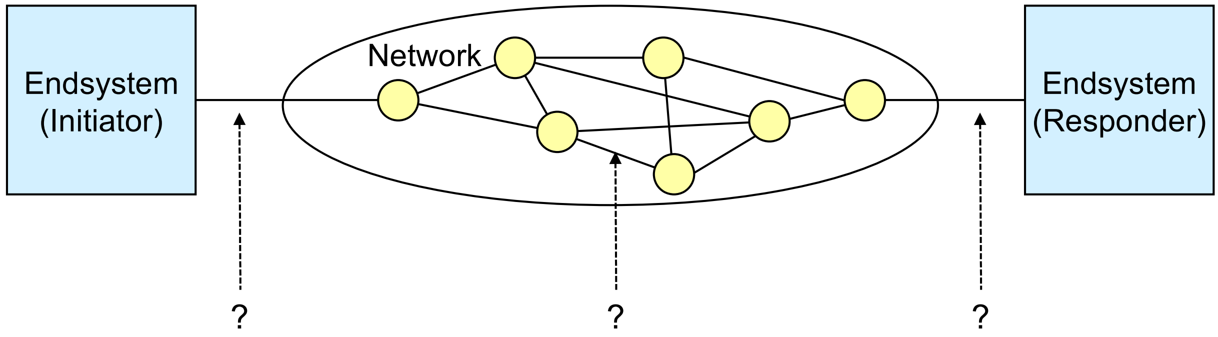
- *Masquerade:*
  - An entity claims to be another entity
- *Eavesdropping:*
  - An entity reads information it is not intended to read
- *Authorization Violation:*
  - An entity uses a service or resources it is not intended to use
- *Loss or Modification of (transmitted) Information:*
  - Data is being altered or destroyed
- *Denial of Communication Acts (Repudiation):*
  - An entity falsely denies its' participation in a communication act
- *Forgery of Information:*
  - An entity creates new information in the name of another entity
- *Sabotage:*
  - Any action that aims to reduce the availability and / or correct functioning of services or systems

Threats and Technical Security Goals

Technical Security Goals	General Threats						
	Masquer-ade	Eaves-dropping	Authori-sation Violation	Loss or Mo-dification of (transmitted) information	Denial of Communi-cation acts	Forgery of Infor-mation	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x
Controlled Access	x		x			x	

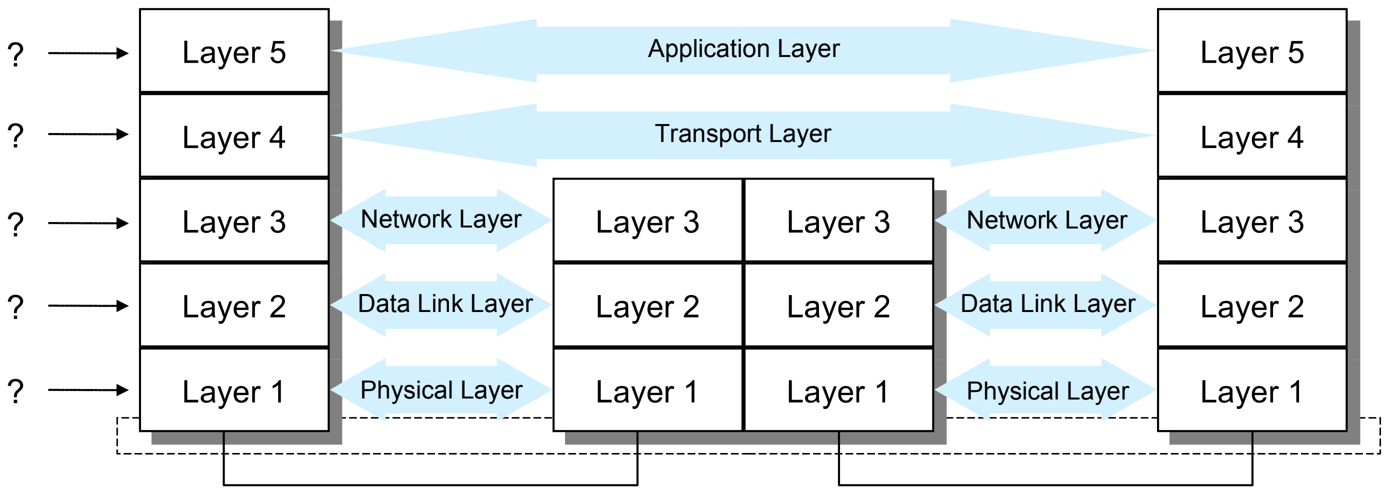
These threats are often combined in order to perform an attack!

Security Analysis of Layered Protocol Architectures 1



Dimension 1: At which interface does the attack take place?

Security Analysis of Layered Protocol Architectures 2



Dimension 2: In which layer does the attack take place?

Attacking Communications on the Message Level

- Passive attacks:
  - Eavesdropping
- Active attacks:
  - Delay of PDUs (Protocol Data Units)
  - Replay of PDUs
  - Deletion of PDUs
  - Modification of PDUs
  - Insertion of PDUs
- Successful launch of one of the above attacks requires:
  - There are no detectable side effects to other communications (connections / connectionless transmissions)
  - There are no side effects to other PDUs of the same connection / connectionless data transmission between the same entities
- A security analysis of a protocol architecture has to analyse these attacks according to the architecture's layers

Safeguards Against Information Security Threats 1

- *Physical Security:*
  - Locks or other physical access control
  - Tamper-proofing of sensitive equipment
  - Environmental controls
- *Personnel Security:*
  - Identification of position sensitivity
  - Employee screening processes
  - Security training and awareness
- *Administrative Security:*
  - Controlling import of foreign software
  - Procedures for investigating security breaches
  - Reviewing audit trails
  - Reviewing accountability controls
- *Emanations Security:*
  - Radio Frequency and other electromagnetic emanations controls

Safeguards Against Information Security Threats 2

- *Media Security:*
  - Safeguarding storage of information
  - Controlling marking, reproduction and destruction of information
  - Ensuring that media containing information are destroyed securely
  - Scanning media for viruses
- *Lifecycle Controls:*
  - Trusted system design, implementation, evaluation and endorsement
  - Programming standards and controls
  - Documentation controls
- *Computer Security:*
  - Protection of information while stored / processed in a computer system
  - Protection of the computing devices itself
- *Communications Security:* (the main subject of this lecture)
  - Protection of information during transport from one system to another
  - Protection of the communication infrastructure itself

Communications Security: Some Terminology

- Security Service:
  - An abstract service that seeks to ensure a specific security property
  - A security service can be realised with the help of cryptographic algorithms and protocols as well as with conventional means:
    - One can keep an electronic document on a floppy disk confidential by storing it on the disk in an encrypted format as well as locking away the disk in a safe
    - Usually a combination of cryptographic and other means is most effective
- Cryptographic Algorithm:
  - A mathematical transformation of input data (e.g. data, key) to output data
  - Cryptographic algorithms are used in cryptographic protocols
- Cryptographic Protocol:
  - A series of steps and message exchanges between multiple entities in order to achieve a specific security objective

Security Services – Overview

- *Authentication*
  - The most fundamental security service which ensures, that an entity has in fact the identity it claims to have
- *Integrity*
  - In some kind, the “small brother” of the authentication service, as it ensures, that data created by specific entities may not be modified without detection
- *Confidentiality*
  - The most popular security service, ensuring secrecy of protected data
- *Access Control*
  - Controls that each identity accesses only those services and information it is entitled to
- *Non Repudiation*
  - Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred

Cryptology – Definition and Terminology

- *Cryptology:*
  - Science concerned with communications in secure and usually secret form
  - The term is derived from the Greek *kryptós* (hidden) and *lógos* (word)
  - Cryptology encompasses:
    - *Cryptography* (*gráphein* = to write): the study of the principles and techniques by which information can be concealed in *ciphertext* and later revealed by legitimate users employing a secret key
    - *Cryptanalysis* (*analýein* = to loosen, to untie): the science (and art) of recovering information from ciphers without knowledge of the key
- *Cipher:*
  - Method of transforming a message (plaintext) to conceal its meaning
  - Also used as synonym for the concealed *ciphertext*
  - Ciphers are one class of cryptographic algorithms
  - The transformation usually takes the message and a *(secret) key* as input

(Source: Encyclopaedia Britannica)

Cryptographic Algorithms

- For network security two main applications of cryptographic algorithms are of principal interest:
  - *Encryption* of data: transforms plaintext data into ciphertext in order to conceal its' meaning
  - *Signing* of data: computes a *check value* or *digital signature* to a given plain- or ciphertext, that can be verified by some or all entities being able to access the signed data
  - Some cryptographic algorithms can be used for both purposes, some are only secure and / or efficient for one of them.
- Principal categories of cryptographic algorithms:
  - *Symmetric cryptography* using 1 key for en-/decryption or signing/checking
  - *Asymmetric cryptography* using 2 different keys for en-/decryption or signing/checking
  - *Cryptographic hash functions* using 0 keys (the "key" is not a separate input but "appended" to or "mixed" with the data).

Important Properties of Encryption Algorithms

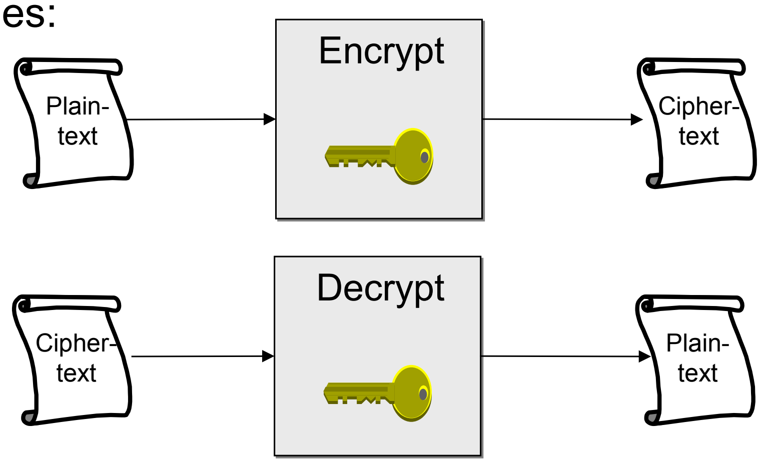
Consider, a sender is encrypting plaintext messages P_1, P_2, ... to ciphertext messages C_1, C_2, ...

Then the following properties of the encryption algorithm are of special interest:

- *Error propagation* characterizes the effects of bit-errors during transmission of ciphertext to reconstructed plaintext P_1', P_2', ...
  - Depending on the encryption algorithm there may be one or more erroneous bits in the reconstructed plaintext per erroneous ciphertext bit
- *Synchronization* characterizes the effects of lost ciphertext data units to the reconstructed plaintext
  - Some encryption algorithms can not recover from lost ciphertext and need therefore explicit re-synchronization in case of lost messages
  - Other algorithms do automatically re-synchronize after 0 to n (n depending on the algorithm) ciphertext bits

Symmetric Encryption

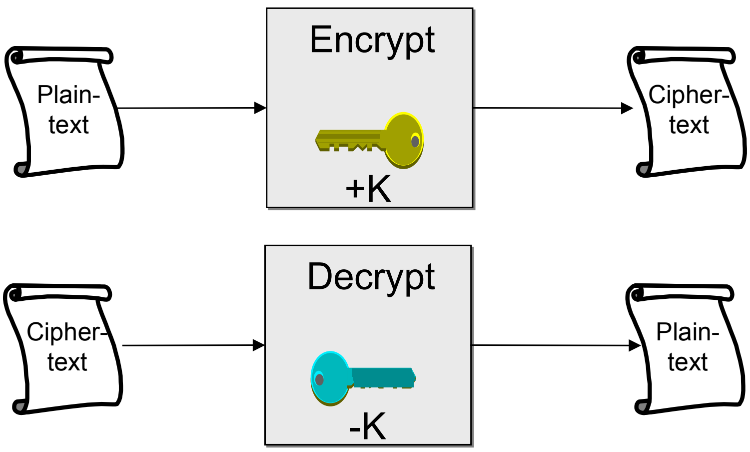
- General description:
  - The same key $K_{A,B}$ is used for enciphering and deciphering of messages:



- Notation:
  - If *P* denotes the plaintext message $E(K_{A,B}, P)$ denotes the ciphertext and it holds $D(K_{A,B}, E(K_{A,B}, P)) = P$
  - Alternatively we sometimes write $\{P\}_{K_{A,B}}$ for $E(K_{A,B}, P)$
- Examples: DES, 3DES, IDEA, AES, RC4, ...

Asymmetric Cryptography (1)

- General idea:
  - Use two different keys $-K$ and $+K$ for encryption and decryption
  - Given a random ciphertext $c = E(+K, m)$ and $+K$ it should be infeasible to compute $m = D(-K, c) = D(-K, E(+K, m))$
    - This implies that it should be infeasible to compute $-K$ when given $+K$
  - The key $-K$ is only known to one entity A and is called A's *private key* $-K_A$
  - The key $+K$ can be publicly announced and is called A's *public key* $+K_A$



Asymmetric Cryptography (2)

- Applications:
  - Encryption:
    - If B encrypts a message with A's public key $+K_A$, he can be sure that only A can decrypt it using $-K_A$
  - Signing:
    - If A encrypts a message with his own private key $-K_A$, everyone can verify this signature by decrypting it with A's public key $+K_A$
  - Attention:
    - It is crucial, that everyone can verify that he really knows A's public key and not the key of an adversary!
- Practical considerations:
  - Asymmetric cryptographic operations are about magnitudes slower than symmetric ones
  - Therefore, they are often not used for encrypting / signing bulk data
  - Symmetric techniques are used to encrypt / compute a cryptographic hash value and asymmetric cryptography is just used to encrypt a key / hash value

Detection of Message Modifications

- Motivation:
  - An *error detection code* over a message enables the receiver to check if a message was altered during transmission
    - Examples: Parity, Bit-Interleaved Parity, Cyclic Redundancy Check (CRC)
  - This leads to the wish of having a similar value called *modification check value* that allows to check, if a message has been modified during transmission
- Realization of modification check values:
  - Cryptographic Hash Functions:
    - These are either combined with asymmetric cryptography to obtain a signed *modification detection code (MDC)* or already include a shared secret mixed with the message
  - Message Authentication Codes:
    - Common message authentication codes (MAC) are constructed from a symmetric block cipher

Cryptographic Protocols

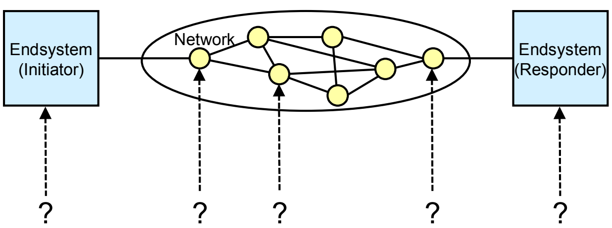
- Definition:

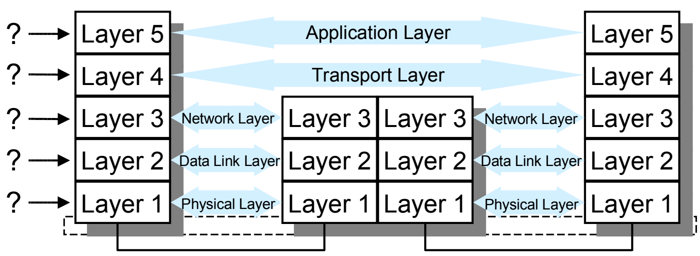
  A *cryptographic protocol* is defined as a series of steps and message exchanges between multiple entities in order to achieve a specific security objective

- Applications of cryptographic protocols:
  - Key exchange
  - Authentication
    - Data origin authentication: the security service, that enables a receiver to verify by whom a message was created and that it has not been modified
    - Entity authentication: the security service, that enables communication partners to verify the identity of their peer entities
  - Combined authentication and key exchange

Security in Networks: What to do where?

- Analogous to the methodology of security analysis, there are *two dimensions* guiding the integration of security services into communications architectures:

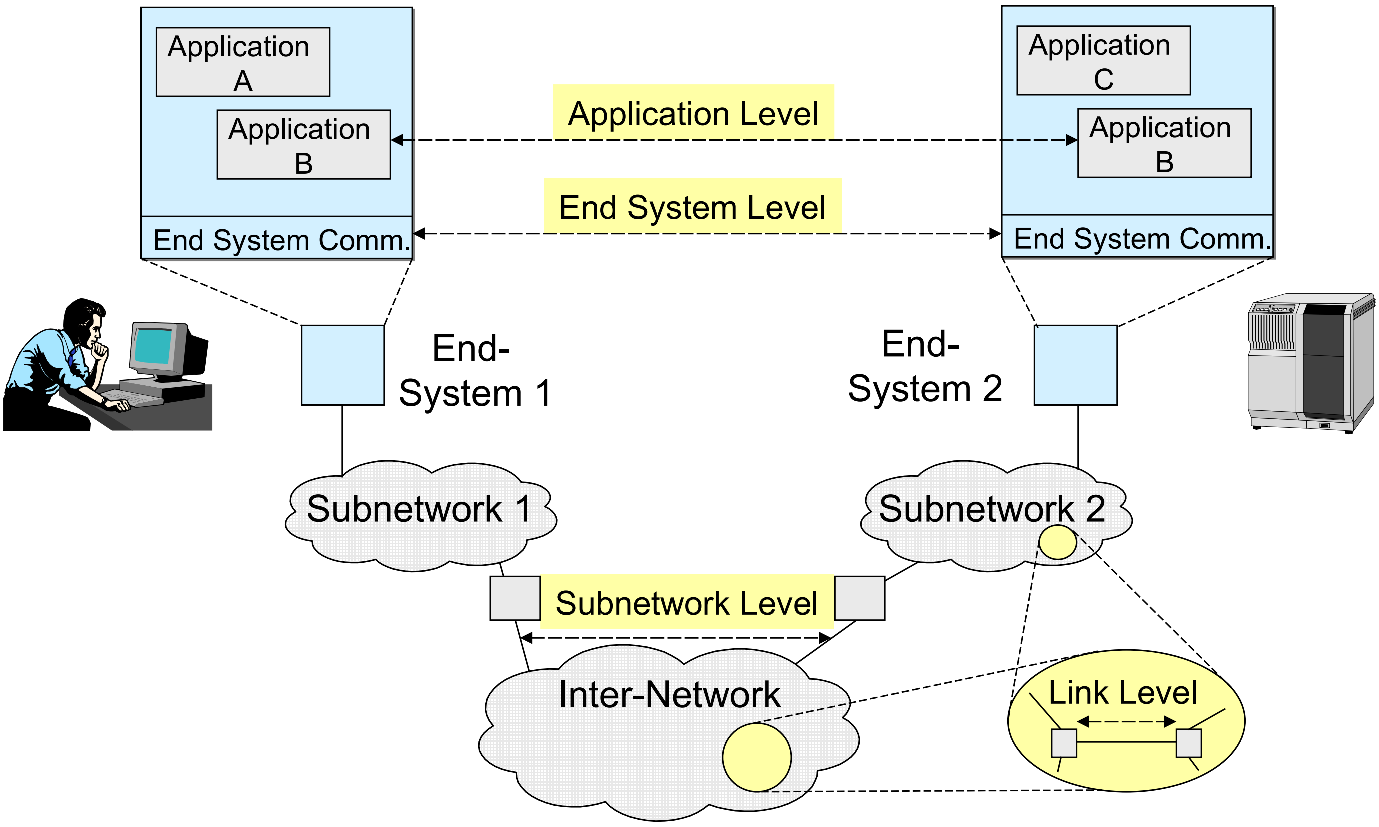




Dimension 1:
Which security service should be realized in which node?

Dimension 2:
Which security service should be realized in which layer?

A Pragmatic Model for Secured & Networked Computing (1)



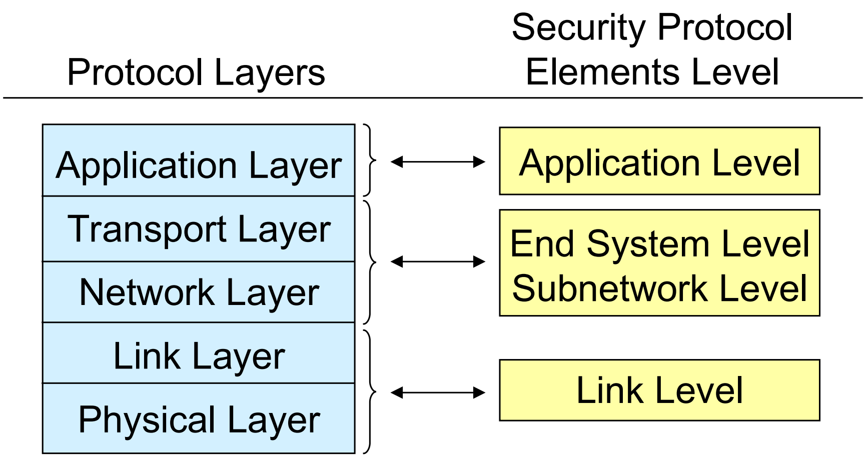
A Pragmatic Model for Secured & Networked Computing (2)

- *Application:*
  - A piece of software that accomplishes some specific task, e.g. electronic email, web service, word processing, data storage, etc.
- *End System:*
  - One piece of equipment, anywhere in the range from personal computer to server to mainframe computer
  - For security purposes one end system usually has one policy authority
- *Subnetwork:*
  - A collection of communication facilities being under the control of one administrative organization, e.g. a LAN, campus network, WAN, etc.
  - For security purposes one subnetwork usually has one policy authority
- *Inter-Network:*
  - A collection of inter-connected subnetworks
  - In general, the subnets connected in an inter-network have different policy authorities

A Pragmatic Model for Secured & Networked Computing (3)

- There are four levels at which distinct requirements for security protocol elements arise:
  - *Application level:*
    - Security protocol elements that are application dependent
  - *End system level:*
    - Provision of protection on an end system to end system basis
  - *Subnetwork level:*
    - Provision of protection over a subnetwork or an inter-network which is considered less secure than other parts of the network environment
  - *Link level:*
    - Provision of protection internal to a subnetwork, e.g. over a link which is considered less trusted than other parts of the subnetwork environment

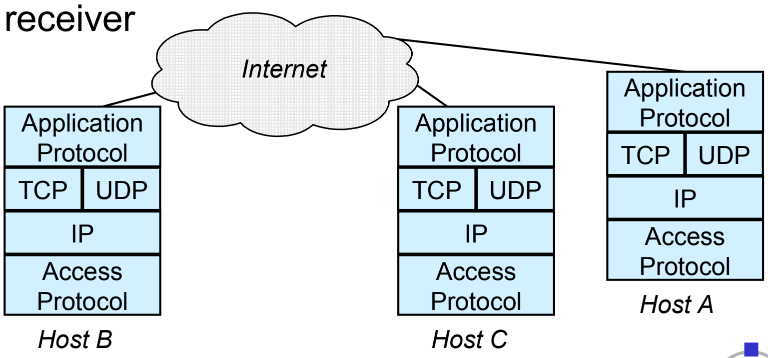
Relationships Between Layers & Requirements Levels



- The relations between protocol layers and the protocol element security requirements levels are not one-to-one:
  - Security mechanisms for fulfilling both the end system and the subnetwork level requirements can be either realized in the transport and / or the network layer
  - Link level requirements can be met by integrating security mechanisms or using “special functions” of the either the link layer and / or the physical layer

Security Problems of the Internet Protocol

- When an entity receives an IP packet, it has no assurance of:
  - *Data origin authentication / data integrity:*
    - The packet has actually been send by the entity which is referenced by the source address of the packet
    - The packet contains the original content the sender placed into it, so that it has not been modified during transport
    - The receiving entity is in fact the entity to which the sender wanted to send the packet
  - *Confidentiality:*
    - The original data was not inspected by a third party while the packet was sent from the sender to the receiver



Security Objectives of IPSec

- IPSec aims to ensure the following security objectives:
  - *Data origin authentication / connectionless data integrity:*
    - It is not possible to send an IP datagram with neither a masqueraded IP source nor destination address without the receiver being able to detect this
    - It is not possible to modify an IP datagram in transit, without the receiver being able to detect the modification
    - *Replay protection:* it is not possible to later replay a recorded IP packet without the receiver being able to detect this
  - *Confidentiality:*
    - It is not possible to eavesdrop on the content of IP datagrams
    - Limited traffic flow confidentiality
- Security policy:
  - Sender, receiver and intermediate nodes can determine the required protection for an IP packet according to a local security policy
  - Intermediate nodes and the receiver will drop IP packets that do not meet these requirements

TELEMATIK Rechnernetze

IPSec: Security Association

- A *security association (SA)* is a simplex "connection" that provides security services to the traffic carried by it
  - Security services are provided to one SA by the use of either AH or ESP, but not both
  - For bi-directional communication two security associations are needed
  - An SA is uniquely identified by a triple consisting of a *security parameter index (SPI)*, an IP destination address, and a security protocol identifier (AH / ESP)
  - An SA can be set up between the following peers:
    - Host ↔ Host
    - Host ↔ Gateway (or vice versa)
    - Gateway ↔ Gateway
  - There are two conceptual databases associated with SAs:
    - The security policy database (SPD) specifies, what security services are to be provided to which IP packets and in what fashion
    - The security association database (SADB)

TELEMATIK Rechnernetze

IPSec: Protocol Modes

- Protocol modes – An SA is always of one of the following types:
  - *Transport mode* can only be used between end-points of a communication:
    - host ↔ host, or
    - host ↔ gateway, if the gateway is a communication end-point
  - *Tunnel mode* can be used with arbitrary peers
- The difference between the two modes is, that:
  - Transport mode just adds a security specific header (+ potential trailer):

IP header	IPSec header	protected data

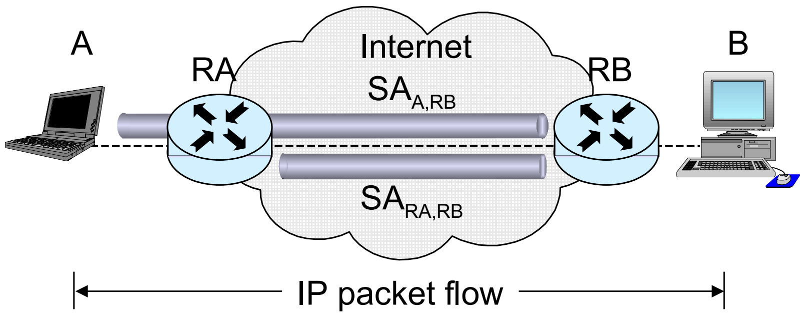
  - Tunnel mode encapsulates IP packets:

IP header	IPSec header	IP header	protected data

  Encapsulation of IP packets allows for a gateway protecting traffic on behalf of other entities (e.g. hosts of a subnetwork, etc.)

IPSec: Nesting of Security Associations

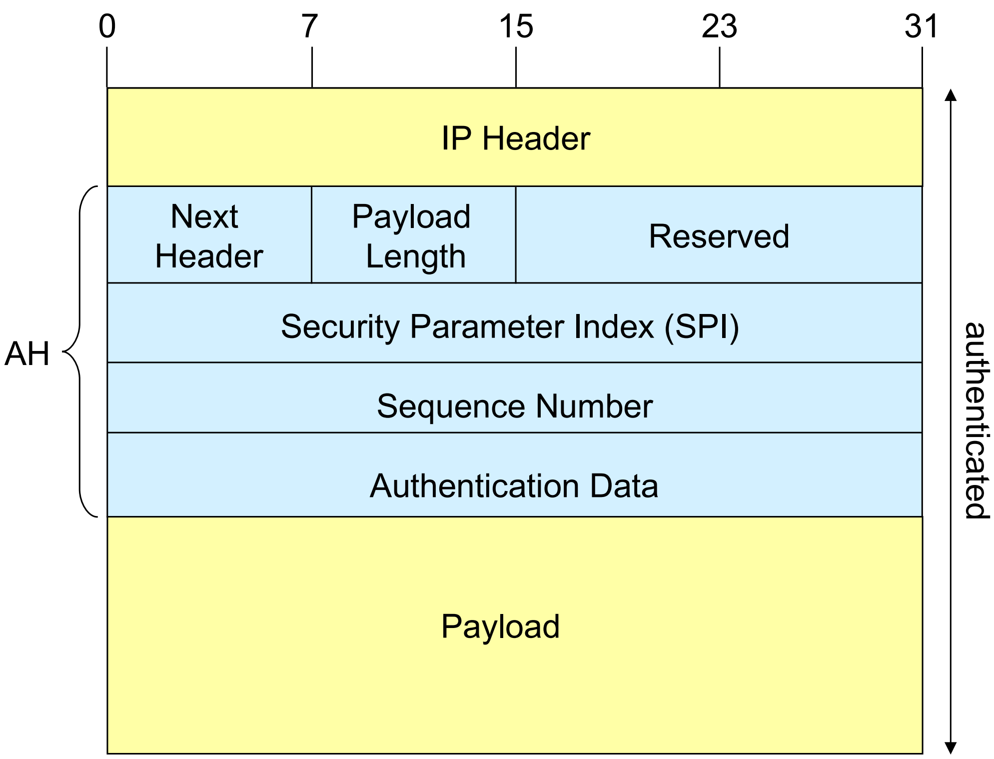
- Security associations may be nested:
  - Example: Host A and gateway RB perform data origin authentication and gateways RA and RB perform subnetwork-to-subnetwork confidentiality



packet structure

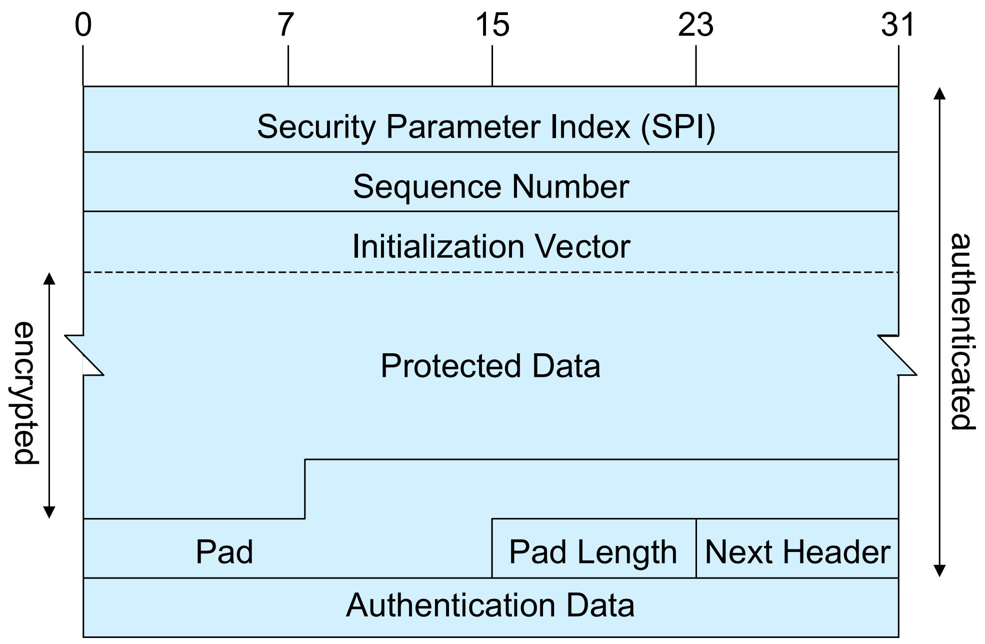
IP header	IPSec header	IP header	IPSec header	IP header	protected data
Src = RA Dst = RB		Src = A Dst = RB		Src = A Dst = B	

IPSec: Authentication Header (AH)



- In tunnel mode the payload constitutes a complete IP packet

IPSec: Encapsulating Security Payload (ESP)



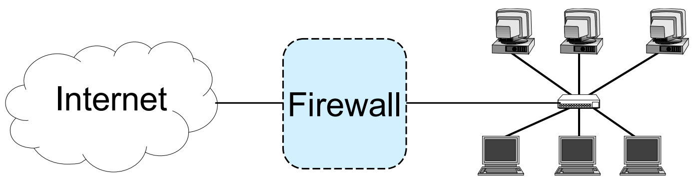
- The ESP header immediately follows an IP header or an AH header
- The next-header field of the preceding header indicates “50” for ESP

IPSec: Establishment of Security Associations

- Prior to any packet being protected by IPSec, an SA has to be established between the two “cryptographic endpoints” providing the protection
- SA establishment can be realized:
  - Manually, by proprietary methods of systems management
  - Dynamically, by a standardized authentication & key management protocol
  - Manual establishment is supposed to be used only in very restricted configurations (e.g. between two encrypting firewalls of a VPN) and during a transition phase
- IPSec defines a standardized method for SA establishment:
  - *Internet Security Association and Key Management Protocol (ISAKMP)*
    - Defines protocol formats and procedures for security negotiation
  - *Internet Key Exchange (IKE)*
    - Defines IPSec’s standard authentication and key exchange protocol

Internet Firewalls

- In building construction, a firewall is designed to keep a fire from spreading from one part of the building to another
- A network firewall, however, can be better compared to a moat of a medieval castle:
  - It restricts people to entering at one carefully controlled point
  - It prevents attackers from getting close to other defenses
  - It restricts people to leaving at one carefully controlled point
- Usually, a network firewall is installed at a point where the protected subnetwork is connected to a less trusted network:
  - Example: Connection of a corporate local area network to the Internet



  - Basically firewalls realize access control on the subnetwork level

Firewalls: Terminology (1)

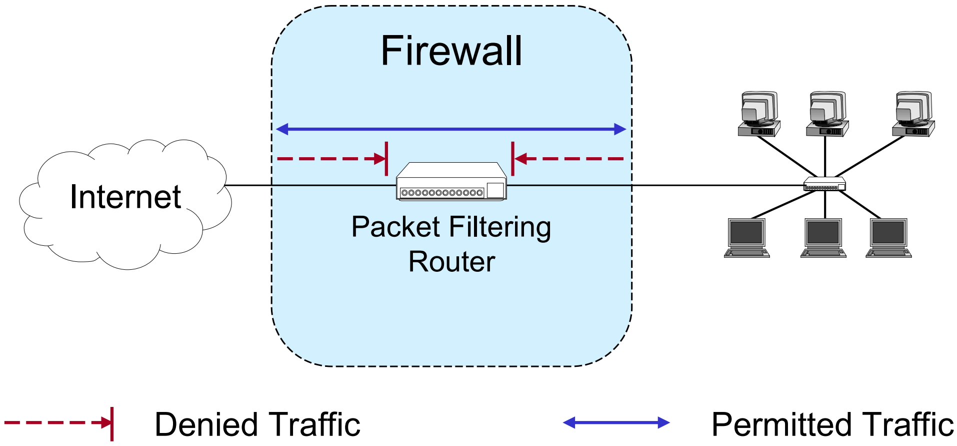
- *Firewall:*
  - A component or a set of components that restricts access between a protected network and the Internet or between other sets of networks
- *Packet Filtering:*
  - The action a device takes to selectively control the flow of data to and from a network
  - Packet filtering is an important technique to implement access control on the subnetwork-level for packet oriented networks, e.g. the Internet
  - A synonym for packet filtering is *screening*
- *Bastion Host:*
  - A computer that must be highly secured because it is more vulnerable to attacks than other hosts on a subnetwork
  - A bastion host in a firewall is usually the main point of contact for user processes of hosts of internal networks with processes of external hosts
- *Dual homed host:*
  - A general purpose computer with at least two network interfaces

Firewalls: Terminology (2)

- *Proxy:*
  - A program that deals with external servers on behalf of internal clients
  - Proxies relay approved client requests to real servers and also relay the servers answers back to the clients
  - If a proxy interprets and understands the commands of an application protocol it is called an *application level proxy,* if it just passes the PDUs between the client and the server it is called a *circuit level proxy*
- *Network Address Translation (NAT):*
  - A procedure by which a router changes data in packets to modify the network addresses
  - This allows to conceal the internal network addresses (even though NAT is not actually a security technique)
- *Perimeter Network:*
  - A subnetwork added between an external and an internal network, in order to provide an additional layer of security
  - A synonym for perimeter network is *de-militarized zone (DMZ)*

Firewalls: Architectures (1)

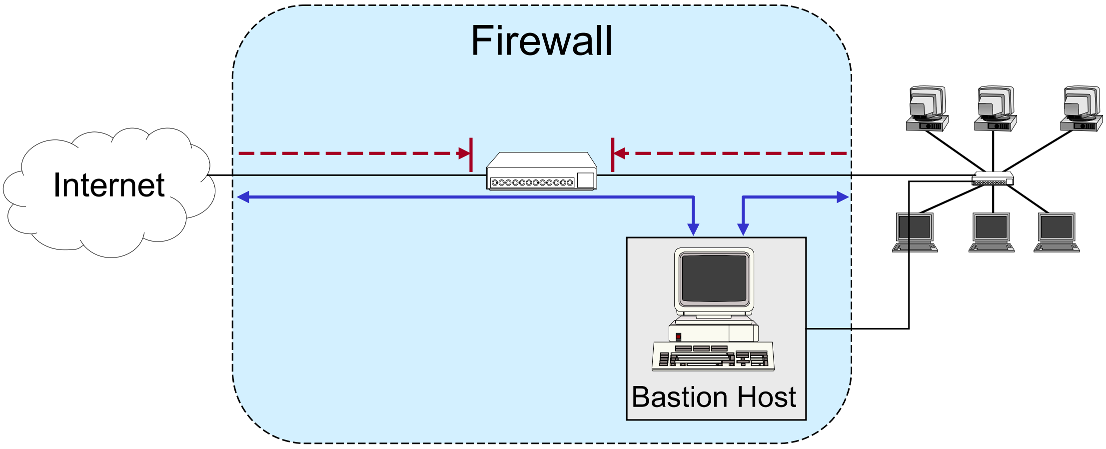
The Simple Packet Filter Architecture



- The most simple architecture just consists of a packet filtering router
- It can be either realized with:
  - A standard workstation (e.g. Linux PC) with at least two network interfaces plus routing and filtering software
  - A dedicated router device, which usually also offers filtering capabilities

Firewalls: Architectures (2)

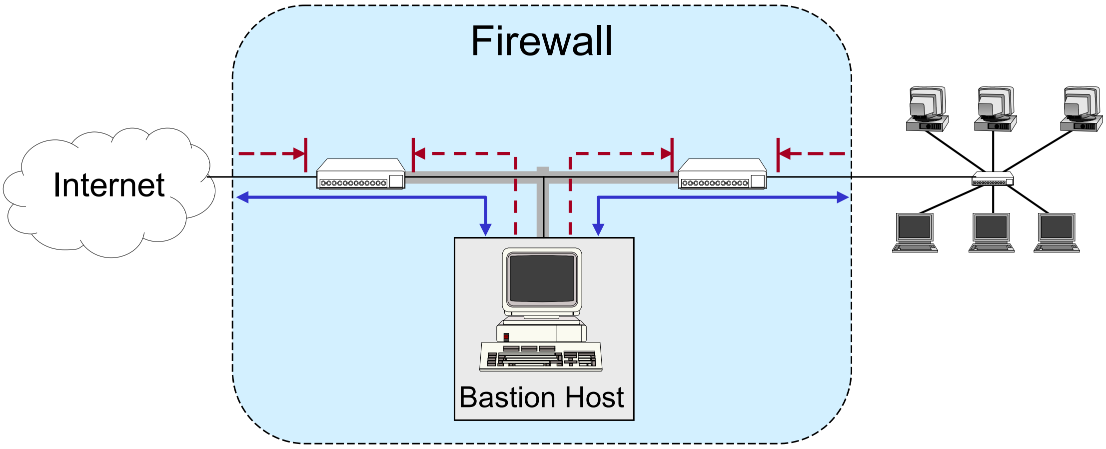
The Screened Host Architecture



- The packet filter:
  - Allows permitted IP traffic between the screened host and the Internet
  - Blocks all direct traffic between other internal hosts and the Internet
- The screened host provides proxy services:
  - Despite partial protection by the packet filter the screened host acts as a bastion host

Firewalls: Architectures (3)

The Screened Subnet Architecture



- A perimeter network is created between two packet filters
- The inner packet filter serves for additional protection in case the bastion host is ever compromised:
  - For example, this avoids a compromised bastion host to eavesdrop on internal traffic
- The perimeter network is also a good place to host a publicly accessible information server, e.g. a www-server

Firewalls: Packet Filtering

- What can be done with packet filtering?
  - Theoretically speaking everything, as all information exchanged in a communication relation is transported via packets
  - In practice, however, the following observations serve as a guide:
    - Operations that require quite detailed knowledge of higher layer protocols or prolonged tracking of past events are easier to realize in proxy systems
    - Operations that are simple but need to be done fast and on individual packets are easier to do in packet filtering systems
- Basic packet filtering enables to control data transfer based on:
  - Source IP Address
  - Destination IP Address
  - Transport protocol
  - Source and destination application port
  - Potentially, specific protocol flags (e.g. TCP's ACK- and SYN-flag)
  - The network interface a packet has been received on

Firewalls: An Example Packet Filtering Ruleset

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Bastion	TCP	>1023	25	Any	Permit
B	Outbound	Bastion	External	TCP	25	>1023	Yes	Permit
C	Outbound	Bastion	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Bastion	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

- This ruleset specifies, that incoming and outgoing email is the only allowed traffic into and out of a protected network:
  - Email is relayed between two servers by transferring it to an SMTP-daemon on the target server (server port 25, client port > 1023)
  - Rule A allows incoming email to flow to the bastion host and rule B allows the bastion hosts acknowledgements to exit the network
  - Rules C and D are analogous for outgoing email
  - Rule E denies all other traffic

If you would like some more...

- There is a whole course on network security during the fall term:

1. Introduction & Terminology
2. Basics of cryptography
3. Symmetric cryptography
4. Asymmetric cryptography
5. Modification check values
6. Random number generation
7. Cryptographic protocols
8. Secure Group Communications
9. Access control
10. Integrating security services into communication architectures
11. Security protocols of the data link layer
12. The IPSec architecture for the Internet Protocol
13. Security protocols of the transport layer
14. Security aspects of mobile communications
15. Security of wireless local area networks
16. Security of GSM and UMTS networks

http://www.tu-ilmenau.de/fakia/networksecurity.html

Network Security Bibliography

[Amo94] E. G. Amorosi. *Fundamentals of Computer Security Technology.* Prentice Hall. 1994.

[Cha95] Brent Chapman and Elizabeth Zwicky. *Building Internet Firewalls.* O'Reilly, 1995.

[For94b] Warwick Ford. *Computer Communications Security - Principles, Standard Protocols and Techniques.* Prentice Hall. 1994.

[Gar96] Simson Garfinkel and Gene Spafford. *Practical Internet & Unix Security.* O'Reilly, 1996.

[Men97a] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press Series on Discrete Mathematics and Its Applications, Hardcover, 816 pages, CRC Press, 1997.

[Sch96] B. Schneier. *Applied Cryptography Second Edition: Protocols, Algorithms and Source Code in C.* John Wiley & Sons, 1996.

[Sch03] G. Schäfer, M. Roßberg. Netzsicherheit. 2. aktualisierte und erweiterte Auflage, dpunkt.verlag, 646 Seiten, 49.90 Euro, 2014.

[Sta98a] W. Stallings. *Cryptography and Network Security: Principles and Practice.* Hardcover, 569 pages, Prentice Hall, 2nd ed, 1998.

[Sti95a] D. R. Stinson. *Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)*. Hardcover, 448 pages, CRC Press, 1995.