Collection of Exam Preparation Tasks for the Lecture “Network Security”

Chapter 1: Introduction

1. Explain the difference between safety and security.

Safety Detection and correction of disruptions that have an impact on the stability of operations

In software safety is put at risk by programming mistakes.

Security

Detection and protection against (often specific) attacks

1. Explain the IT security aims confidentiality, integrity, authenticity, availability, non-repudiation, and privacy. Give examples of situations where each aim is at risk and provide measures to ensure that each aim is achieved.

**Confidentiality** Prevention of unauthorized gaining of information

Measures

1.Data encryption

2.Rules for allowed/not allowed information flows

3.Who can access which information or get to know about it

4. Information flow control: Classification of subjects and objects

In particular: confinement problem, i.e. hidden channels, side channels

**Integrity**

Protection against unauthorized and

unnoticed change of data

Measures to ensure data integrity include

1. Rules for allowed/not allowed data changes

Who (subject) can modify a certain object (asset) in which

way (rights) under which conditions?

2. Granting of access and control rights

E.g. r (read), w (write), x (execute) in Unix file systems

3. Isolation: domains, sandboxes, virtual machines

4. Manipulation detection: check sums, digital watermarks

**Authenticity**

Proof of correctness and credibility of an

object’s or subject’s identity

Measures

1. Rules for the assignment of unique identifiers to subjects and objects
2. Passwords, keys, biometry, smart cards, …
3. Not only identifiers, but also attributes that characterize a subject
4. Procedure to proof the correctness of an identity
5. Provisioning and check of certificates, credentials, tokens
6. Challenge/response protocols: Question/answer procedures

**Availability**

Protection against undesired limitations of the use of functionality/services, etc

Short term measures: Rules for recording and surveillance

Record which accesses on which objects happened when under which resource consumption

Specification of thresholds, e.g. for overload

Remark: Rules means an obligation to act on violations (not like grants or forbids)

Longer term measures

Add more resources, redundant structure

**Non-repudiation**

Protection against claims (not) to have done certain actions

Measures: Specification of accountable actions

1.Linking of action with subject who performs the action: (digital) signature

2.Logging of actions and time stamps, log files on operations system level take note of security relevant actions

3.Capture proofs of action (e.g. for forensic analysis)

**Privacy**

Protection of data related to a person

Measures: Rules of data avoidance and data minimization

Specification of the data recording purpose

Data aggregation: k-anonymity procedure

Pseudonym: Identity is known to a trusted third party (“notary”)

Non-traceability: Change of pseudonyms

1. Differentiate between the terms vulnerability, threat, and risk.

Vulnerability A vulnerability in code or protocols enables that security measures in a system are circumvented, changed or manipulated.

Threat Threats result from potential attacks which can be carried out by using one or more vulnerabilities to endanger the IT security aims.

Risk

Risk of a threat is the likelihood of the event and the potential impact. This can be expressed as: risk = likelihood \* impact

Chapter 2: Attacks on Networks

1. Provide examples of attacks on different OSI layers.

OSI 1 physical layer infrastructure damage

OSI 2 data link layer ARP spoofing

OSI 3 network layer IP spoofing

OSI 4 transport layer SYN flooding

OSI 5 application layer XXS

1. Differentiate between ARP spoofing, IP spoofing, and Caller ID spoofing.

ARP spoofing on OSI 2 data link layer router has wrong table to make information flow from

Victim to the attacker

IP spoofing conceal real IP address of attacker to prevent from tracing

Caller ID spoofing

1. How does ARP spoofing in a switched Ethernet network work?

By cheating the router. Attack use IP spoofing to cheat router. Router has table to direct

1. How can DHCP be abused?

Attackers send many IP address requests to local

DHCP server

Use many different spoofed MAC addresses

DHCP pool is limited, no addresses for real users left

1. What is the meaning of a port scan? Is a port scan the real attack?

Port scan is used for attacker to make preparation for DOS

Directly connect to target server

Check ports one by one for service

Scanning is obvious

1. How can a port scan be carried out without making the victim aware of the attacker’s IP address? Explain the steps.
2. Attacker sends SYN segment to an unused port on proxy
3. Proxy replies with RST-ACK segment, attacker gets IP-ID
4. Attacker sends TCP segment containing proxy IP address to target server
5. Target server replies with RST-ACK segment to proxy
6. No reaction of proxy, IP-ID is not increased
7. Attacker sends again a SYN segment to an used port on proxy
8. Proxy replies with RST-ACK segment, IP-ID is increased by 1.

1. How are DDoS attacks typically carried out?

By using bot network to request too much on server

1. Explain what bot nets are and how they are organized. For which purposes can bot nets be used?

Bot net is a number of internet-connected devices, each of which is running one or more bots. A tree structure can be used to organize the bot nets. Botnets can be used to perform distributed denial of-service attack, steal data, send spam and allows the attacker to access the device and its connection.

1. How can the TCP handshake procedure be abused for a DoS attack? Which countermeasures can be taken?

If the target server gets no replay , it will retransmit the SYN-ACK segments. This may consume all resources on a system.

Protection against SYN floods

Resource reservation on server after first SYN

Resource reservation holds for 60s

Five retries lead to connection reestablishment.

Typically clients can initiate several 1000 connections.

Check for address spoofing

1. Explain how a DNS amplification attack works.

Public DNS servers answer DNS requests for anybody in recursive manner

Attacker searches for or prepares DNS Server A with long entries about server Y.

Request to DNS Server Xn about information on server Y which has been put on DNS Server A

Request leads to transfer of large entries to DNS servers Xn

These requests use target IP address as source

Many large answers are sent to target server

Conclusion : Attacker sends small requests to DNS which leads to relatively large answer

1. What is the potential impact if an attacker can place wrong DNS entries on DNS servers? Give an example scenario.

Attacker put wrong DNS entries on request to DNS servers

DNS servers reply with answer of wrong information containing more bits

Request uses target IP address as source

Target server get large amounts of wrong information.

1. What is the difference between viruses, worms and Trojan horses?

**Viruses**

Sequence of commands, requires host program

Cannot run on its own

Self-replication (can spread itself to other host programs)

**Worms**

Program that can run on its own

Does not require a host program

Replicates itself (via network or USB-sticks (with autorun))

**Trojan horse**

Program with unexpected, malicious behavior

Has beneficial usage functionality

Hidden malicious code (e.g. logs keyboard use, sends screenshot, communicates with command&control center)

No self-replication

Infection

Download of useful program with this side effect

Drive-by-download

1. What is ransomware?

Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim’s data or perpetually block access to it unless a ransom is paid.

More advanced malware used a technique to encrypt the victim’s files, making them inaccessible, and demands a ransom payment to decrypt them.

1. Provide a sequence of steps that leads to a Persistent Cross-Site Scripting attack.

Web page has a guest book

Users can leave comments

Attacker does not only enter plain text, but also

JavaScript code

“Nice web page <script type=text/javascript>alert(“but

with XSS problem!”)</script>”

Stored on the server side in DB if not prevented

Delivery of this script code to users on web page

Access

1. How does SQL injection work?

SQL statements unexpected in GUI input fields

Dangerous if not checked

Attacker can try to put database queries

1. Which measures should be taken to protect oneself against XSS or injection?

Cross-Site Scripting (XSS) definition

Aim to execute malicious script code to affect web site users

Typically via JavaScript

Enabled by nearly all browser users

Other contents (HTML, Flash, ActiveX, VBScript) abuse also possible

1. Which methods are possible to detect Spam e-mails?

Method to prevent

1. Ensure you know and trust the sender before opening an email.

2. Check the subject line for common spam topics

3. avoid opening untrusted link

Content-based message encoding

keyword filtering rules

email authentication rules

mail server IP blacklists

domain blacklists for sending domain and email content

1. Explain how a buffer overflow can happen and the potential consequences.

Too long input which is over the predefined length overwrite internal program buffer.

Attacker can use this to manipulate the return address and then execute code from attacker.

For example, attacker can code to start a shell.

1. How can a user become affected by a drive-by-exploit?

User just open a web page and is affected.

Advertisement on web page can be rented. Attacker use advertisement to put malicious javascript code on it. JavaScript or other malware code is delivered together with advertisements.

Attacker collects knowledge which web sites are often used by victims.

Attacker searches for vulnerabilities on these web sites.

A found vulnerable web site is used to redirect the victim to a special site containing exploit code.

1. Cars are often connected to the Internet nowadays. Discuss potential security threats.

Remote unlocking of doors

Takeover of control

1. What is the difference between online analysis and post mortem analysis in IT forensics? Discuss advantages and disadvantages.

Online analysis

Advantages

work on the running system

Many temporary data are available

Disadvantages Further damage may happen

Active malware can occur.

Post mortem analysis

Advantages it is possible to work only with copies of data and leave originals undestroyed.

It allows to repeatedly process the data in different way

Disadvantages it needs many steps to finish the whole work.

Chapter 3: Network Protection

1. What are the reasons why many organizations structure their local area networks by using VLANs?

Separation of broadcast domains to reduce the traffic load

Security(in particular confidentiality) require so far mechanisms on Network Layer(in particular firewall)

1. Explain the difference between port-based VLANs, MAC-based VLANs, and IP-based VLANs.

Port-based VLANs all end systems behind a port belong to the VLAN Port areas are statically

assigned to VLANs

MAC-based VLANS

VLAN construction via end system MAC addresses

Connection of end system to VLAN independent from

switch port

MAC address stays the same

MAC addresses of new end systems have to be

mapped to VLANs

High configuration effort

IP-based VLANs

VLAN construction using Layer 3 addresses

Violation of layering concept!

No transparency concerning used Layer 3 protocols

e.g. different Internet Protocol versions

1. Explain how the rules on a packet filter firewall look like.

Firstly we have key selection criteria to determine “true” and “false”.

Selection criteria includes IP address , port number , protocol ID , SYN/ACK flags, etc.

When we meet with the first true, action determines general behavior after matching.

We can make decision whether packet is forwarded

Allow Rule : forward packet

Deny Rule: drop packet

Reject Rule: drop packet + send ICMP notification back to source.

Packet filtering firewall is the process of passing or blocking packets at a network interface based on source and destination addresses , ports or protocols The process is used in conjunction with packet mangling and Network Address Translation(NAT). Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion.

Packet filtering is done by a program called a packet filter. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides to prevent it from passing or allow it to pass.

1. It should be possible to reach any web server (TCP port 80) in the Internet from an internal network (10.0.1.0/24). To allow for reasonable communication the web servers should be allowed to answer. Provide firewall rules including a default rule for specifying this in a suitable manner.

Packet from internal network(10.0.1.0/24) which is the source address and port number is 80 should be allowed. And packet whose destination address is (10.0.1.0/24) and port number is 80 and source address is arbitrary should also be allowed. Otherwise , other packets should be dropped.

1. Which impact does the order of firewall rules have for the check of packets? How should the rules be ordered?

Firewall rules have a priority order that determines the order in which the rules are applied to network traffic.

Firewall rules are shown as a list on the Rules tab. The rules are applied from top to bottom, and the first rule that matches the traffic overrides all the other rules below. The main principle is to allow only the needed traffic and block the rest. Therefore, the last rule of a firewall profile is the Deny rest rule. It blocks all the traffic that the rules above it do not specifically allow.

Dynamic firewall rules are shown separately as a list on the Activity tab. The priority of the dynamic rules is lower than the priority of normal firewall rules. This means that if a firewall rule denies some traffic, the dynamic rule cannot allow it. However, the priority of the dynamic rules is higher than the priority of the predefined Deny rest rule.

1. A company provides services intended for the public Internet on a few servers. In addition, it operates a set of other computers that do not provide publicly available services. Make a drawing that shows a typical DMZ configuration in this scenario.

Access from outside to DMZ is only allowed for selected services and hosts

Access from outside to inside is in general not allowed

Access from DMZ to inside is in general not allowed

Access from DMZ to outside is in general not allowed

Access from inside to DMZ is not allowed

Access from inside to outside is not allowed

1. Assume that there is a separation between internal network, DMZ and the Internet. Which kinds of connections (initiated from where?) should in general be possible and which ones should be blocked by packet filters?

Access from outside to inside is in general not allowed

Access from outside to DMZ is only allowed for selected services and hosts

Access from DMZ to inside is in general not allowed

Access from DMZ to outside is in general not allowed

Access from inside to DMZ is only allowed for selected services and hosts

Access from inner network to outside is in general allowed

Useful functionality replies are allowed

1. Should servers in a company network be configured to reply to ICMP echo requests? Discuss advantages and disadvantages.

Servers should be configured to reply to ICMP echo requests

Advantages improve the availability of the server

Disadvantage increase the risk of DDOS, DOS

1. In which respect is there a relationship between a firewall and ARP spoofing?

Firewall can be used for preventing ARP spoofing attack by using specific rules on packet filter

1. How should a firewall and a bastion host be configured?

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attack. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

It is hardened in this manner primarily due to its location and purpose, which is either on the outside of a firewall or in a demilitarized zone and usually involves access from untrusted networks or computers.

1. What is the difference between network-based sensors (NIDS) and host-based sensors (HIDS)?

Network-based sensors NIDS

Monitors all network traffic at central network locations

Advantages

It can detect attacks on different hosts in the network

It does not require resources on host

It can be configured as invisible for attackers

Disadvantages

Throughput may be too high to observe all traffic

It can not observe situation on hosts

It can not inspect encrypted communication

Limited knowledge leads to false positives

Host-based sensors HIDS

It runs on a specific host to protect it on application and OS level, sometimes network level

Advantages

It can observe actual influence on system (contrast to NIDS)

Network traffic can possibly be monitored on all layers.

Disadvantages

It has to be installed on every host

Application and OS specific, requires more adaption effort for heterogeneous hosts

It cannot be configured as invisible

It consumes resources on host

There is no information available on parallel attacks on other systems

1. Why is it necessary to run (several) IDS in addition to firewalls?

There are different ways of attack detection by IDS

Some are available in commercial or open source IDS

Others are under test in academia

1. Provide a drawing of a network with a DMZ and show useful locations of HIDS and NIDS.

HIDS host-based IDS

NIDS Network-based IDS

1. What is the meaning of “honeypot” for computer networks? How are honeypots used today?

Traffic from the honeypot is not used for real service use

It is possible to learn how attackers are performing attacks .

1. Which security models do you know? Explain the purpose of the Bell-LaPadula and the Biba model and their rules.

Bell-Lapadula Model aim : ensure data confidentiality

No-read-up No subject S1 from a lower confidentiality class is allowed to read data of a subject S2 belonging to a higher confidentiality class

No-read-down

Biba Model

Chinese Walls Model (Hybrid Model)

1. Distinguish between the terms “verification” and “identification”.

Two authentication methods can be distinguished

Verification user claims to be a certain person

Comparison with reference data used to check it

Identification data from an unknown person is compared with reference data from all persons

1. What is the purpose of MPLS and how is it related to circuit switching and packet switching? How does MPLS impact IP routing?

MPLS is a protocol-agnostic routing technique designed to speed up and shape traffic flows across enterprise wide area and service provider networks.

MPLS tries to combine the benefit of both the above switching technologies. It uses circuit switching within an ISP while packet switching is used within ISP’s.

MPLS requires each router to independently determine a packet’s next hop by inspecting the packet’s destination IP address before consulting its own routing table. This process consumes time and hardware resources, potentially resulting in degraded performance for real-time application such as voice and video.

1. Explain the terms “label edge router”, “label switch router”, “label switched path” and “forwarding equivalence class”.

LER: Label edge router adds and removes labels

LSR: label switch router change labels, work as a switch rather than a router

LSP: label switched path path between LER and LSR or path between LSR and LSR

FEC: Forwarding Equivalence Class It can determine group of IP packets which are forwarded in the same way. It may have a table entry

It is easy to introduce priority.

1. How are the contents of Management Information Bases arranged? Are these objects in the sense of a programming language like Java?

Management Information Base(MIB)

Variable definitions are registered in the ISO registration tree

Nodes are identified by names and IDs

Leaves of the tree represent values in the managed objects

1. What is specific about an SNMP trap message in comparison to the other SNMP messages?

SNMP trap message

SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

The setup on the left shows a network management system that polls information and gets a response. The setup on the right slows an agent that sends an unsolicited or asynchronous trap to the network management system.

1. Which transport protocol is the basis of SNMP? Explain this choice. Are there also disadvantages of this choice?

UDP

Messages can get lost.

1. What is the purpose of the “community string” in SNMP? Discuss it under security aspects.

The “SNMP Community string” is like a user id or password that allows access to a router’s or other device’s statistics.

IP Check Server Monitor sends the community string along with all SNMP requests.

If the community string is correct, the device responds with the requested information

If the community string is incorrect, the device simply discards the request and do not respond.

SNMP community strings are used only by devices which support SNMPv1 and SNMPv2 protocol. SNMPv3 uses username/password and authentication, along with an encryption key.

1. Which are the major differences between the SNMP versions 1, 2 and 3?

SNMP v1 and SNMPv2 contain only limited security mechanisms

There is no encrypted message and no participant authentication

SNMPv1 and SNMPv2 are used for monitoring, but not for administration of managed devices

In SNMPv3 a completely different new architecture is specified

Security in SNMPv3

Authentication via username/password or key

Encryption of Messages using DES (Data Encryption Standard)

Specification of user-based privileges

1. A company network is strongly protected from the outside world. Its internal network should be managed via SNMP. Which version would you recommend?

Use SNMPv1 v2

Only user id and password is required to get information from managed devices.

The traffic in the network for SNMP is smaller than version3.

1. Explain the difference between active and passive network monitoring.

Active network monitoring

Measures the flow of data on your network by ‘injecting’ test traffic into the environment. Active monitoring adds overhead to your networking hardware, and could result in poor performance if used in excess.

Passive network monitoring

Passive network monitoring techniques constantly collect data from the network environment over a period of time, and base their results on historic data. Because it doesn’t pull real-time information from your network hardware, passive monitoring is typically far less resource-intensive than active monitoring. However, passive monitoring is better suited to general measurements over time , and as data.

Conclusion

Active network monitoring injects extra traffic into the network, which may influence the performance of the network.

Passive network monitoring is far less resource-intensive but does not pull real-time information from your network hardware.

Passive monitoring techniques typically require specialized devices in order to measure traffic, so the economy commitment could be higher than that of active monitoring.

Chapter 4: Security Protocols and VPNs

1. Which different kinds of VPNs do you know?

Intranet VPN Site-To-Site VPN

Internal network of company/organization

Central configuration on transition points towards Internet, not on each end system.

Remote Access VPN (End-to-Site) VPN

A Tunnel is configured to link between company domain and mobile employee notebook or home office. Site means company domain. End means devices that is used by individuals.

Extranet VPN

Linking of organizations link between location of other company and company headquarters

Implementation dependent on way of collaboration

Realization using IPsec or SSL/TLS possible

End-To-End VPN

Tunnel is configured between two end points

Configuration on both devices necessary

Highest security level possible due to end-to-end encryption

Realization often using SSL/TLS or SSH

1. What is the difference between symmetric and asymmetric ciphers?

Symmetric ciphers encrypt message with a single key

Asymmetric ciphers encrypt message with different key

1. In which way has the AES algorithm been standardized? Do you regard this as a reasonable way of standardization in case of a security-related algorithm?

Competition was regraded as very good method for algorithm selection afterwards.

Algorithm to be published with details

Worldwide use without license fees

Useful for next 30 years

1. Explain the difference between block ciphers and stream ciphers.

Block ciphers

expects input in specified block length n

message m of length |m| is divided into r blocks of length n

Necessary to fill up last block with additional (random) bits

Stream ciphers encryption of small plain text units

1. What is the difference between electronic code book mode and cipher block chaining?

Electronic code book mode each plain text block is encrypted by the same key on its own

Cipher block chaining each plain text block is XORed with previous cipher text block

1. How can steganography be applied related to images with RGB encoding?

Steganography in pictures

Change least significant bit in RGB color values

1. Explain how a message authentication code is calculated (in general). Which security aims are targeted by using such a code?

To ensure the authenticity of sender

Prerequisite: Alice and Bob have exchanged a secret key beforehand

1. Alice wants to communicate with Bob, Bob wants to be sure that this is really Alice.
2. Bob sends randomly generated bit sequence (challenge) to Alice.
3. Alice uses an algorithm (input: secret key, random sequence received from Bob) and sends result back to Bob(response)
4. Bob compares Alice’s calculation result with his own calculation result (done in parallel)
5. If both are equal, Alice authenticity is verified (she knows the secret key)

1. Which features are important for cryptographic hash functions?

Hash function has the features of a one-way function

It is practically impossible to find any collision. i.e. an arbitrary pair m, m’ where m is not equal to m’ and H(m) = H(m’)

1. Explain the main tasks of a certification authority.

Certificate issuance Generation of data structures and signature

Certification repository Commonly accessible data base of certificates

Certificate revocation Necessary if private key has been stolen

Certificate update Renewal of certificates after expiry

Key generation

Certification history Data base of no longer valid certificates(for investigations)

Notarization CA signs agreements between users

Time stamping CA ties information to dates

Cross certification CA issues certificates about foreign CAs

Attribute certificates Link attributes to an identity(e.g. rights, mandates)

1. Why is it necessary to check for certificate revocation?

Certificate revocation is needed if key is compromised

Certificate revocation lists : List of certificate IDs with dates of invalidity, digitally signed by CA

Requirements on information dissemination

Up-to-date

Complete

Efficient

1. Map the protocols IPsec, SSL/TLS and SSH to the OSI model.

IPsec OSI layer 3

SSL secure sockets layer version 1,2,3 OSI layer 4.5 between transport layer and application layer

TLS Transport Layer Security OSI layer 4

SSH secure shell application layer OSI layer 5

1. Explain the features of AH and ESP in IPsec as well as the difference between the tunnel mode and the transport mode. What does it mean to “tunnel IP packets” in this context?

Authentication Header Protocol to ensure integrity and authenticity, not confidentiality

Cryptographic checksum (hash) calculated for IP packet (options: MD5 ,SHA -1 , SHA-\* , none , …)

Encapsulating Security Payload(ESP) Protocol to ensure confidentiality , integrity and authenticity

Cryptographic checksum like in AH

Symmetric encryption of IP packet or payload

Tunnel mode AH authenticate whole IP packet

ESP encrypts IP header, payload and ESP trailer and authenticate ESP header, IP header , payload and ESP trailer

Transport mode has less IP header

1. What is a replay attack and how is it prevented by IPsec?

A reply attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it , possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a “Man-in-the-middle attack”

AH and ESP are used to prevent reply attack

1. A company has two locations which are connected over the Internet. The company would like to make sure that there are no successful eavesdrops. Provide a useful configuration for this scenario based on IPsec.

use tunnel mode because the payload is encrypted.

1. What is the difference if there is https instead of http in the browser input line?

https means that the data from the input line is encrypted during the process of transmission.

http does not encrypt data during the transmission

1. How are symmetric and asymmetric ciphers combined in the TLS implementation?

SSL and TLS use a combination of symmetric and asymmetric encryption to ensure message privacy. During the SSL or TLS handshake, the SSL or TLS client and server agree an encryption algorithm and a shared key to be used for one session only.

1. Compare IPsec and SSL/TLS by showing commonalities and differences. Discuss also advantages and disadvantages.

Commonalities Client and server authentication

Securing of confidentiality, integrity and authenticity (but on different layers)

Differences

SSL/TLS does not protect IP header (attacks possible)

SSL/TLS can not protect UDP-based traffic (possible with Datagram TLS)

SSL/TLS requires modification of applications

Administrative effort for per user is typically lower for SSL/TLS

Detailed rights management is easier to be realized for SSL/TLS

Conclusions

For single application and frequently changing user population we can use SSL/TLS (e.g. home banking, mobile user)

For multiple application and static user communication we can use user IPsec rather than SSL/TLS

Assessment of IPsec

Advantages

Limitation to IP not an issue due to IP’s dominance, works for all applications

Assurance of confidentiality, integrity and authentication

Disadvantages

Complex IPsec standards and implementations

Effort is needed for tunnel configuration and certification infrastructure

Effort is needed for VPN clients on end systems

Assessment of SSL/TLS

Advantages

In many cases no additional software is required for end users

We have assurance of confidentiality, integrity and authentication from SSL/TLS

Disadvantages

There is no IP header protection

SSL/TLS works only for TCP-based applications

Configuration is needed for each application required

End system protection is needed

certificate trustworthiness is concerned difficult

1. A company has sales people who are often negotiating contracts with the customers during visits at the customer sites. During these negotiations they need to get access to servers within the company. Discuss whether a realization via IPsec or SSL/TLS is preferable.

IPsec and SSL/TLS both have Client and server authentication

Securing of confidentiality, integrity and authenticity( but on different layers)

Strong cryptographic algorithms selectable

1. What is the purpose of the SSH protocol?

Original purpose replace insecure “remote-tools” to execute commands on remote computer

It also can be used for tunneling of applications (port forwarding)

It is useful for small VPNs

Application is enhanced like SFTP, SCP

1. Why is it not sufficient to enable SSL/TLS in an e-mail client to ensure end-to-end confidentiality? What needs to be used instead?

SSL/TLS only has encryption to mail server and from mail server, but not end -to- end, which means that Plain text is on the mail servers and there is no encryption between mail servers

We need https on combination with SSL/TLS so that user can communicate only with encryption up to mail server.