University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions and Answers

Lecture 9: Communication Security

QUESTION 1

a. What is a security protocol, and what is its purpose?
b. Give examples of services that can be provided by security protocols.

Answer

a. A security protocol is a type of communication protocol which specifies sequence and formats for exchanging messages combined with cryptographic mechanisms.
b. Typical services provided by security protocols are: Authentication, confidentiality, integrity, key establishment, e-voting, secret sharing etc.

QUESTION 2

TLS is a cryptographic services protocol based upon public-key certificates, and is commonly used on the Internet.

a. What port is reserved for HTTP over TLS? What is the prefix for a URL that describes a resource accessible by HTTP over TLS?
b. TLS is designed to secure reliable end-to-end services over TCP. Briefly describe where the TLS operates in the OSI and TCP/IP protocol stacks.
c. Briefly explain the purpose of the TLS Handshake protocol.
d. Identify the security services provided to TLS connections by the TLS Record Protocol.
e. How are the TLS Handshake Protocol and the TLS Record protocol connected?
f. As part of the Handshake Protocol the client and server negotiate which 'cipher suite' to use. In what circumstances is this negotiation useful? Why can this negotiation lead to potential security weaknesses?

Answer

a. 443 and HTTPS
b. TLS operates at the Transport Layer (OSI layer 4) The TLS Record Protocol sits above the TCP protocol.
c. TLS Handshake Protocol: negotiates crypto parameters, establishes session key and authenticates server (optionally authenticates client).
d. Message confidentiality and message integrity
e. The cryptographic algorithms negotiated, and the key exchanged, in the Handshake Protocol are used to protect the data transferred in the Record protocol.
f. The cipher suite negotiation is useful when the end users support different cryptographic algorithms. A potential weakness is that an attacker may alter the protocol messages to try to make a connection employ a weaker authentication mechanism than the strongest one that both endpoints can support.

QUESTION 3

Internet Protocol Security (IPSec) is a framework of open standards for Internet Protocol (IP) networks.

a. Briefly describe three major benefits of using IPSec.
b. Three security services that can be provided by IPSec are: message confidentiality, message integrity and traffic analysis protection. Briefly explain the type of mechanism used to provide each of these services.
c. Briefly describe the three major VPN architectures supported by IPSec. Describe typical application scenarios for each architecture.

Answer

a. Four relevant benefits are mentioned in the slides.
    - If applied at a firewall/router, strong security applies to all traffic crossing this boundary. Internal workstations need not be reconfigured.
    - Is transparent to applications: Operates at layer 3 so applications are not aware of its operation.
    - Can be transparent to end users: System administrator configures IPSec; the end user is not involved.
    - Can provide security for individual users: Can be configured on specific systems.
b. The mechanisms for the respective services are:
    - Message Confidentiality. Protect against unauthorised data disclosure. Accomplished by the use of encryption mechanisms.
    - Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. Provided by concealing IP datagram details such as source and destination address.
    - Message Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.
c. The major VPN architectures are:
    - Gateway-to-Gateway Architecture. Provides secure network communications between two networks. Establish a VPN connection between the two gateways. Network traffic is routed through the IPsec connection, protecting it appropriately. Only protects data between the two gateways. Most often used when connecting two secured networks, such as linking a branch office to headquarters over the Internet. Gateway-to-gateway VPNs often replace more costly private wide area network (WAN) circuits.
    - Host-to-Gateway Architecture. Commonly used to provide secure remote access. The organization deploys a VPN gateway onto its network; each remote access user then establishes a VPN connection between the local computer (host) and the VPN gateway. As with the gateway-to-gateway model, the VPN gateway may be a dedicated device or part of another network device. Most often used when connecting hosts on unsecured networks to resources on secured networks, such as linking travelling employees around the world to headquarters over the Internet.
    - Host-to-Host Architecture. Only model that provides protection for data throughout its transit. Resourceintensive to implement and maintain in terms of user and host management. All user systems and servers that will participate in VPNs need to have VPN software installed and/or configured. Key establishment is often accomplished through a manual process. Typically used for special purpose needs, such as system administrators performing remote management of a single server.

QUESTION 4

Encapsulating Security Payload (ESP) is an IPSec protocol that can be run in two modes: transport mode and tunnel mode.

a. Explain the main difference in packet processing between these two modes.
b. Briefly describe the most typical application scenario for ESP in tunnel mode.
c. Briefly describe an application scenario for ESP in transport mode.
d. Briefly explain the additional security services provided by using ESP in tunnel mode as opposed to using ESP in transport mode.

Answer

a. The differences are explained as follows:
   - In transport mode the data is encrypted without the IP header, and the original IP header is used as the packet header after some fields in the original IP header are changed.
   - In tunnel mode the entire original packet is encrypted and a new outer IP header is used. The inner IP header of the original IP packet carries the ultimate source and destination addresses. The outer IP header may contain distinct IP addresses such as addresses of security gateways.
b. Gateway to Gateway – connecting two branch offices together over the Internet.
c. Remote administrator accessing a local host securely.
d. Avoids traffic analysis – extra confidentiality service.

QUESTION 5

Suppose that you are responsible for designing a secure Internet banking application. You have been asked to consider one of three security protocols for communication confidentiality.

- **HTTP Digest Authentication**. Would this be a suitable choice? Explain your answer.

- **TLS**. Does this provide the required security services? What assumptions would you need to make about the client computing environment?

- **IPSec**. Does this provide the required security services? What IPSec architecture would be suitable? Why is this choice not widely used in practice?

Answer

- HTTP Digest Authentication is definitely not suitable for an application such as Internet banking which requires a high level of security. It provides no confidentiality for user transactions and limited integrity. It is also vulnerable to ‘man-in-the-middle’ attacks.
- TLS provides confidentiality and integrity of data which are the basic required security services. Non-repudiation is not provided since symmetric encryption is used for data integrity (rather than digital signatures). Server authentication is provided and although client authentication is possible it is often not available in practice since there is no global PKI. Therefore client authentication is often provided using a different mechanism such as a shared password. TLS is in fact widely used to provide security for Internet banking. Probably the main threat comes from malicious software on user PCs. This is not a fault of the TLS protocol of course. Malicious software, such as trojan horses, can infect user PCs in many ways. If an operating system has such software installed then it can directly attack the implementation. For example, a ‘keylogger’ can record all input from the

keyboard, which will include user login details, and send these to a pre-determined location.

- IPSec provides the essential services of confidentiality and data integrity, but like TLS does not provide non-repudiation. The additional service of traffic analysis protection is not likely to be particularly useful for Internet banking (unless you really care that an attacker knows when you are communicating with your bank). While a host-to-gateway architecture could be used (with the client PC connecting to a bank gateway) this would not be appropriate on its own since user transactions would then be in clear in the bank network. Therefore a host-to-host architecture would be most appropriate. While there are some potential problems with using IPSec in IP V4 networks and across firewalls, it seems that the main reason that IPSec is not widely used in this context is historical. Most Internet bank users have browsers with TLS (SSL) installed. IPSec is a newer protocol suite. Possibly IPSec may become more popular in Internet banking applications in the future.