University of Oslo
INF3510 Information Security
Spring 2016
Workshop Questions and Answers

Lecture 10: Communications Security

Question 1

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

Answer

a. A security protocol is a type of communication protocol combined with cryptographic mechanisms, i.e. it specifies sequence and formats for exchanging messages including cryptographic elements between two or more parties.
b. Typical services provided by security protocols are: Confidentiality, Entity authentication, Data authentication, Data integrity, Key exchange/establishment,
c. Well-known security protocols are: TLS (aka. SSL), IPSec, Kerberos, SAML used in federated Id Man., OAuth (Open Authorization) used for access control in online social networks, e-Voting protocols, e-Payment protocols, etc.

Question 2

TLS is an Internet security protocol which actually consists of multiple sub-protocols.

a. Which port is reserved for TLS? Which URL prefix denotes resources using TLS?
b. 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. In the Handshake Protocol the client and server negotiate which 'cipher suite' to use. Why is this negotiation useful? Why is the negotiation a potential security weakness?

Answer

a. Port 443 is reserved for TLS. https is the prefix used for TLS/SSL connections.
b. TLS consists of multiple sub-protocols.
   - The TLS Record Protocol sits above the TCP protocol.
   - The TLS Handshake Protocol, Change Cipher Suite Protocol, and Alert Protocol are application protocols at the same level as HTTP.
c. TLS Handshake Protocol: negotiates crypto parameters, establishes session key and authenticates server (optionally authenticates client).
d. Message confidentiality and message integrity
e. The crypto algorithms negotiated and the key exchanged in the Handshake Protocol are used by the Record Protocol to to protect the data transferred.
f. Client and server might support various cryptographic algorithms, so they need to agree on the strongest common set. A potential weakness is that an attacker can trick the client and/or server into using weaker algorithms than they both support.

Question 3

TLS (previously called SSL) is potentially vulnerable to TLS stripping.

a. What makes websites vulnerable to TLS stripping?
b. Briefly explain how TLS stripping works.
c. What does the acronym HSTS mean?
d. How does HSTS protect against TLS stripping?
e. How do browsers get HSTS policies for websites?
f. How can HSTS policies be removed from a browser?
g. Use a tool for checking the TLS configuration of servers, e.g. https://www.ssllabs.com/ssltest/
   Test your online bank(s) and other secure sites to see of their TLS configuration is secure.

Answer

a. Websites that use both http and https are vulnerable to SSL stripping.
b. SSL stripping involves the user victim, the web server and the Man-in-the-Middle attacker which can intercept traffic, e.g. in an Internet café. The user requests a website through http. The request is intercepted by the attacker which forwards it to the server. The server redirects to https so the attacker connects to the server with https. Data received through https is forwarded to the user through http. The user might respond by sending username and password over http, which are then intercepted and stolen by the attacker.
c. HSTS means http Strict Transport Security
d. Browsers that support HSTS can hold HSTS policies for specific websites which dictates browsers to **only** use https to those websites. When the user requests a website with http, the browser automatically translates it to https. If an attacker tries to trick the browser to connect with http, the browser refuses to connect.
e. Browsers receive HSTS policies in two ways:
   - Predefined when installing browser
   - Through a https connection to websites that support HSTS.
f. HSTS policies in a browser are removed in two ways:
   - The HSTS policy can be defined with an expiry time up to 365 days.
   - The website can change the policy through an https connection.
g. Try e.g. www.dnb.no, www.nordea.no, www.skandiabanken.no, idporten.difi.no, gmail.com, facebook.com

Question 4

Internet Protocol Security (IPSec) is an 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 gateway/router, it strong security to all traffic crossing this boundary. Internal workstations need not be reconfigured.
   - It 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.
   - Message Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. Data integrity is assured by generating a MAC (Message Authentication Code), 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.
   - 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 in tunnel-mode by concealing IP datagram details such as source and destination address.

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 5

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, data encryption does not cover the IP header, so the original IP header is reused with only small changes to some fields.
   - In tunnel mode the entire original packet is encrypted including the original IP header, so a completely new outer IP header created. The inner IP header of the original IP packet carries the ultimate source and destination addresses. The outer IP header contains different 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 6

Suppose that you are responsible for designing a secure Internet banking application. You are tasked with selecting one of three security protocols for the purpose of providing communication confidentiality. Assess the suitability of each protocol below.

- **HTTP Digest Authentication**. Can it support confidentiality? Explain your answer.
- **TLS**. Does this provide confidentiality? What assumptions would you need to make about the client computing environment? Is key management practical?
- **IPSec**. Does this provide confidentiality? What IPSec architecture would be suitable?

Answer

- HTTP Digest Authentication is inadequate for online banking that requires high authentication assurance and confidentiality. It provides no confidentiality.
- TLS provides confidentiality and integrity of data which are the basic required security services. Server authentication is provided through server certificates. Threats can be malicious software on user PCs, which is not a fault of the TLS. SSL stripping can also be a threat if the website does not use HSTS.
- IPSec provides the essential services of confidentiality and data integrity. Host-to-gateway architecture could be used (with the client PC connecting to a bank gateway). It can be argued that the main reason that IPSec is not widely used in this context due to configuration complexity and key management issues. If configuration and key management were transparent to users it could be practical, but currently it is not.

Question 7

a. Explain why people can be tricked to believe a criminal website is their own online bank, despite the connection being secured with TLS and even HSTS which provides strong sever authentication.
b. What is the petname model ?
c. How can petname systems prevent phishing attacks ?
d. What is the difference between syntactic and semantic/cognitive server authentication?
e. Mention disadvantages of using e petname system.

Answer

a. TLS-based server authentication is only syntactical, and offers little meaningful evidence to the user who ultimately decides whether the website is genuine or not. The user must e.g. be able to distinguish between www.bellabs, www.bellabs.com and www.bell-labs.com.
b. The petname model allows users to define a personal petname to represent a global and unique name. This allows the user to easily recognise a globally unique name through the personally defined petname. The petname can be a word, an image or a sound file.
c. Whenever the user accesses a website, the petname system checks whether a petname corresponds to the domain name for that site. If yes, the petname is displayed or played so the user can recognise it. A warning is given if no corresponding petname is found.
d. With syntactic authentication, only the match between the accessed domain name and the domain name in the server certificate is checked. In this case the domain name themafia.com could perfectly well be authentic. In semantic/cognitive authentication, the relying party also applies a policy to check if the domain name is acceptable or as expected. In this case themafia.com would normally not be accepted.
e. The user needs to define petnames for all sites that are accessed with TLS and for which the user wants to have strong authentication assurance. This creates an extra burden, which makes it more difficult to use petname systems.