Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

Cryptography and Network Security
Tutorial 3

Nhat Nam Nguyen
nhatnamcse@gmail.com

28/3/2015

Basic Exercises (7pts)

Exercise 1. (0.5pts)

Where exactly does the SSL protocol fit within the TCP/IP protocol stack?

a. At the network layer
b. At the physical layer
c. Between the data link layer and the network layer
d. Between the Transport (TCP) layer and Application Layer

Exercise 2. (0.5pts)

Which of the following provide authentication for an SSL connection?

a. Digital certificates
b. Diphers
c. Secret key
d. IP address

Exercise 3. (1pts)

What is a man-in-the-middle attack? Explain how SSL against man-in-the-middle attack?

Exercise 4. (1pts)

What steps are involved in the SSL Record Layer Protocol?

Exercise 5. (4pts)

Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.

a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.

b. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full cipher-text to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys).

c. Replay Attack: Earlier SSL handshake messages are replayed.

d. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.
e. Password Sniffing: Passwords in HTTP or other application traffic are eaves- dropped.

f. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.

g. IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.

h. SYN Flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the “half-open connection” around for a few minutes. Repeated SYN messages can clog the TCP module.

Advanced Exercises (3pts)

Exercise 6. (3pts)

I connect to my bank using SSL. Answer the following questions:

(1) How does a certificate from the bank protect me from a man-in-the-middle attack? Can an attacker, Trudy, intercept the message, substitute the certificate with her own, and cause me to think that she is the bank? If not, why?

(2) After I receive the certificate, I would like to establish a session key (symmetric key) for the transaction. How can the public-key cryptosystem be used to securely share a session key?

(3) The bank in turn needs to ensure that I am who I claim to be and not an attacker. Thus, I need to authenticate myself to the bank. Explain how such an authentication procedure would occur?

THE END