NTNU Department of Information Security and Communication Technology

TTM4135 Applied Cryptography and Network Security
Semester Spring, 2023

Worksheet 7: key establishment and TLS (Lectures 13 and 14)

QUESTION 1

Review the definitions of the following concepts. They are things that you would be expected to know in the exam.

(a) key predistribution;
(b) session key distribution;
(c) key agreement;
(d) Kerberos;
(e) TLS ciphersuite;
(f) TLS record protocol and TLS handshake protocol.

QUESTION 2

Discuss the advantages and disadvantages of using key predistribution, session key distribution and key agreement protocols in the following scenarios:

- a corporate network such as NTNU's Intranet;
- a small company or domestic environment;
- Internet communications (e.g. HTTPS, secure email).

QUESTION 3

A potential attack on key establishment protocols is where the attacker makes one party A believe that the session key is shared with B but B believes that the same key is shared with C. This is called an *unknown key share attack*.

- Why might this situation be a serious security problem, even if the attacker does not obtain the key
- Why does use of a key derivation function, including the identities of the parties, prevent this attack?

QUESTION 4

Consider the following ciphersuite specifications for TLS. What do each of them mean? Comment on the security of each of the choices regarding: choice of algorithms; key length; forward secrecy.

cont/...

(a) TLS_RSA_WITH_RC4_128_MD5

(b) TLS_RSA_WITH_NULL_SHA

(c) TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

(d) TLS_DHE_DSA_WITH_AES_256_CBC_SHA256

(e) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

(f) TLS_CHACHA20_POLY1305_SHA256

QUESTION 5

Consider MITM scenarios with TLS (like Superfish) in which a root certificate is added to the client machine.

(a) What are scenarios in which such a MITM may be regarded as legitimate?

(b) How might a root certificate get added to a machine in practice?

(c) In what sense are these scenarios always bad for security, no matter how they are implemented?

QUESTION 6

This question illustrates *padding oracle attacks* on TLS. TLS uses padding on plaintexts with CBC mode encryption for block ciphers (like AES). Padding works by adding at least one byte. The padding is the representation of the number of padding bytes (padding length) preceded by that same value repeated for that number of bytes. Thus possible padding is "00" or "01 01" or "02 02 02" or .... In this question assume that the receiver always outputs an error if the padding is incorrect, and this error explicitly states that a padding error occurs.

(a) How will this padding be checked and correctly removed by the receiver?

(b) What happens if the last byte of the block $n-1$, C_{n-1}, of a n-block CBC ciphertext is altered? In what circumstances will the padding in the decryption of the last block, C_n, be correct? (Write an equation for the case when there is one byte of padding.)

(c) Use the above observation to show how a padding oracle attack works to find one byte of the plaintext. How many attempts are required in order to guarantee finding that byte?

(d) How can this attack then be extended to obtain all bytes in $P_n = D(K, C_n)$?