NTNU Department of Information Security and Communication Technology

TTM4135 Applied Cryptography and Network Security
Semester Spring, 2023

Exercises for TLS 1.3, IPsec and Secure mail

QUESTION 1

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

(a) 0-RTT protocols;
(b) host-to-host, gateway-to-gateway and host-to-gateway IPsec architectures;
(c) IPsec transport mode and tunnel mode
(d) Domain Keys Identified Mail (DKIM)
(e) OpenPGP
(f) Signal protocol

QUESTION 2

Compare the handshake protocols in TLS 1.2 and TLS 1.3 as shown on slide 8 of Lecture 15. The client is not permitted to send application data before it receives the finished message from the server.

(a) How much longer must the client wait before sending application data in TLS 1.2 compared with TLS 1.3?

(b) What attacks are possible in TLS 1.2 if the client could send application data in Phase 3 after its own finished message?

QUESTION 3

Compare IPsec in host-to-gateway architecture with TLS. Consider the following scenarios and discuss which would be most suitable to provide security in each case.

(a) You have two applications on your server which you want to secure with independent keys and different security services.

(b) You want to secure a server which has a number of applications and you may want to add new applications in the future without changing the security settings.

QUESTION 4

Three possible ways to combine encryption and MACs are:

- encrypt first and apply the MAC to the ciphertext;
- apply the MAC first and encrypt plaintext and MAC together;
- apply the MAC and encrypt the plaintext separately.

cont/...

Which of these is used in the TLS Record Protocol (up to version 1.2) and which is used in the ESP protocol of IPsec? Why is the third not suitable in general? (Remember that the purpose of a MAC is only to provide authentication/integrity and not confidentiality.)

QUESTION 5

Explain why the lack of interaction in email delivery prevents the possibility to achieve forward secrecy for secure email. Is there a way that forward secrecy could be approximated for email?

QUESTION 6

In hybrid encryption, such as used in PGP, is it better to have the public key encryption or the symmetric key encryption to be the stronger of the two?

QUESTION 7

End-to-end security and link security are two ways of providing network security. What are some of the advantages and disadvantages of each? What protocols, or configurations, are available to provide each of these types of security in (i) email (ii) IPsec?

QUESTION 8

The messaging protocol Signal uses pre-computed Diffie-Hellman keys to protect the *first* communicated message in any conversation. A client A pre-computes many $t_i = g^{x_i}$ values which are stored on the Signal server. When another client B starts a new conversation with A:

- B is given a previously unused pre-computed key of A, $t_i = g^{x_i}$, and then t_i is deleted from the server;
- B chooses an ephemeral Diffie–Hellman private key x_B;
- B computes a message key k as a hash of $g^{x_i x_B}$;
- B sends the first message to A protected by k and also sends g^{x_B};
- When A receives the message, she uses x_i to recompute k and recover the first message and then deletes x_i.
- For the next message A computes a new ephemeral Diffie–Hellman value which she combines with g^{x_B} to form the next message key.

Since the number of new conversations that will be started is not predictable, Signal has a fallback mechanism to use the last available pre-computed key for many conversations until the supply of pre-computed keys is replenished. Signal suggests keys be replenished once a week, or once a month.

Discuss how this process influences forward secrecy for the first message in each conversation. Include a discussion of whether the pre-computed values should be classed as long-term or ephemeral keys.