TTM4135 Worksheet 8: TLS, IPsec, Secure Mail and Secure Messaging

Tjerand Silde and Emil August Hovd Olaisen
{tjerand.silde, emil.august.olaisen}@ntnu.no

Spring 2026

1. Review the definitions of the following concepts:
   (a) TLS ciphersuites
   (b) TLS Record protocol
   (c) TLS Handshake protocol
   (d) 0-RTT protocols;
   (e) Host-to-host, gateway-to-gateway and host-to-gateway IPsec architectures;
   (f) IPsec transport mode and tunnel mode
   (g) Domain Keys Identified Mail (DKIM)
   (h) OpenPGP
   (i) Signal protocol

2. 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.
   (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

3. Consider man-in-the-middle (MITM) scenarios with TLS 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?

4. 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 $P_n = D(C_n, K)$?

5. Compare the handshake protocols in TLS 1.2 and TLS 1.3 as shown on in the slides. 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?

6. 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.

7. 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.

   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.)

8. 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?

9. 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?

10. 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

    (a) Email

    (b) IPsec

11. 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.