ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

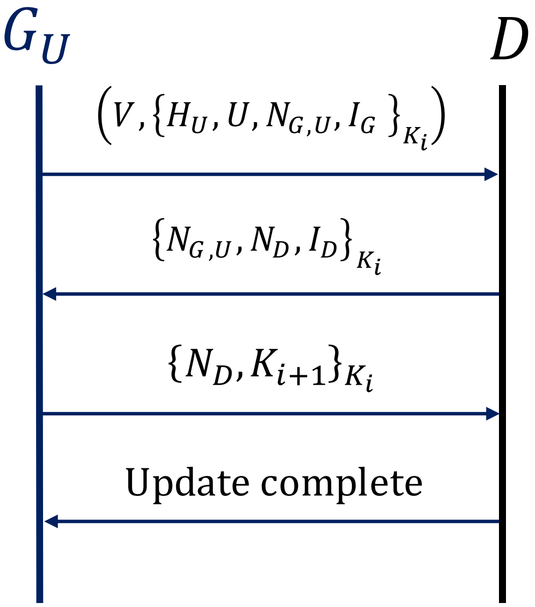
Homework 5, 85 pts.

Due Friday Sept. 19 prior to 11:55pm

(please turn in homework electronically on Canvas)

As always this semester, you are required to solve any and all homework questions alone.

1) (30 pts.) You have a teammate Alex who proposes the following update protocol with a symmetric key K_i held by both the updating organization G_U and the device D. Note that a new symmetric key K_{i+1} is communicated for the next update.


G_U
D
$\left(V, \{H_U, U, N_{G,U}, I_G\}_{K_i}\right)$
$\{N_{G,U}, N_D, I_D\}_{K_i}$
$\{N_D, K_{i+1}\}_{K_i}$
Update complete

a. (5 pts.) Does the protocol protect against the replay attack? Make sure to explain your answer with details regarding how the replay attack succeeds or in what way it will always fail. You must give at least one valid reason to receive any credit for your answer (a correct "yes" or "no" alone without any valid reason for the answer will receive zero points).

A straightforward replay attack after completion of the above protocol will not work because the symmetric key is changed at the end. So, let us suppose that the attacker can interrupt and restart the protocol.

If the attacker interrupts the protocol after $\{N_D, K_{i+1}\}_{K_i}$ is sent to D, the attacker can pretend to be G_u and resend $(V, \{H_U, U, N_{G,U}, I_G\}_{K_i})$. After D responds with $\{N_{G,U}, N_{Dnew}, I_D\}_{K_i}$, the attacker is stuck because the value of nonce N_{Dnew} is new this time (by the definition of what is a nonce). The previous reply $\{N_D, K_{i+1}\}_{K_i}$ cannot be replayed since $N_D \neq N_{Dnew}$.

In conclusion, there does not appear to be any way to successfully carry out a replay attack against the newly proposed protocol.

b. (5 pts.) Does the protocol protect against the Man-in-the-Middle (MitM) attack? Make sure to explain your answer with details regarding how the MitM attack succeeds or in what way it will always fail. You must give at least one valid reason to receive any credit for your answer (a correct "yes" or "no" alone without any valid reason for the answer will receive zero points).

The MitM attack cannot start because the proposed protocol assumes that G_U and D both have K_i which the attacker does not have. Without K_i, there is no way for the attacker to ever begin to pretend to be either G_U or D.

c. (5 pts.) Does the protocol protect against Organization Spoofing attack? Make sure to explain your answer with details regarding how the Organization Spoofing attack succeeds or in what way it will always fail. You must give at least one valid reason to receive any credit for your answer (a correct "yes" or "no" alone without any valid reason for the answer will receive zero points).

As with the MitM attack analysis, the attacker cannot pretend to be G_U because the attacker does not have K_i. Without K_i, there is no way for the attacker to fake the first message from G_U in the proposed protocol, so there is no way to begin an Organization Spoofing attack.

d. (5 pts.) Please state any assumptions you found necessary for your answers to the above, including how we ensure that the initial key, call it *K_0*, is not revealed to the attacker. It is OK if the assumption for *K_0* suffices for your answers to the above questions, but if more assumptions were needed, please explain them here.

Clearly, if we assume (which we should) that the attacker has full and complete access to all messages sent over the communications channel, it is necessary for the initial key K_o to be communicated some other way, e.g., through providing K_o to device D directly (e.g., through a connection with a physical wire) in the factory or other central facility prior to being distributed in the field.

e. (5 pts.) Name one important advantage (benefit) with this new protocol.

One advantage is that only one symmetric key cryptographic protocol is required. This will reduce processing and memory needs as compared to any alternative using a public key cryptographic protocol together with a symmetric key cryptographic protocol. For the device in particular, these reduced processing and memory requirements can improve battery life as well as reduce both device cost and size.

f. (5 pts.) Name one important disadvantage (possible problem) with this new protocol.

One big problem is that if any K_i is discovered, then K_{i+1} is also revealed to the attacker, which in turn reveals K_{i+2}, etc. This is a very big problem with the proposed protocol, especially if the adversary keeps a record of messages going back for years.

Another disadvantage occurs if the device for any reason loses its copy of the current K_i, e.g., if the memory storing K_i becomes corrupted. There does not appear to be any way to start over with the protocol if the most recently used symmetric key is lost.

Many students incorrectly stated that a disadvantage would be increased processing requirements. In general, the processing requirements to update the symmetric key are far outweighed by not requiring the processing of asymmetric cryptographic primitives.

2) (20 pts.) In class on Thursday Sept. 11, 2025, it was explained how in a single session the MitM attack will not work against the interlock protocol. However, what happens if Mallory is allowed multiple sessions where Mallory can pretend to "lose the connection" and require either Alice or Bob (or both) to start the Interlock protocol over again. Does the interlock protocol protect against the MitM attack where the attacker (Mallory) is allowed to cause any session to "lose connection" and thus start over again? Make sure to explain your answer with all attack steps regarding how the MitM attack succeeds when augmented with the capability of causing lost sessions; alternatively, explain in what way it will always fail. You must clearly and unambiguously explain all steps (to success or failure) to receive full credit. Please state any assumptions you believe are important and/or necessary.

If Mallory is allowed to cause Alice and Bob to "lose" their connection and thus be forced to restart, Mallory can break the Interlock protocol, assuming that the same initial messages are sent by Alice and Bob to each other upon each session restart.

Mallory first allows the following steps to occur:

1) Alice sends Mallory her public key, and Mallory sends Bob a fake Alice key "Public$_{\text{AliceFake}}$"
2) Bob sends Mallory his public key, and Mallory sends Alice a fake Bob key "Public$_{\text{BobFake}}$"
3) Alice encrypts a message for Bob using Public$_{\text{BobFake}}$ but only sends half of the message
4) Bob encrypts a message for Alice using Public$_{\text{AliceFake}}$ but only sends half of the message
5) Alice sends the rest of her message to Bob encrypted with Public$_{\text{BobFake}}$

Then, Mallory causes Alice and Bob to "lose" their connection and thus be forced to restart. However, since Mallory has possession of Private$_{\text{BobFake}}$, Mallory can now decrypt Alice's message! So, Mallory obtains the message Alice will initially send to Bob.

Next, the following steps occur:

1) Alice sends Mallory her public key, and Mallory sends Bob a fake Alice key "Public$_{\text{AliceFake}}$"
2) Bob sends Mallory his public key, and Mallory sends Alice a fake Bob key "Public$_{\text{BobFake}}$"
3) Alice encrypts a message for Bob using Public$_{\text{BobFake}}$ but only sends half of the message which Mallory intercepts; since Mallory has the full message already, Mallory sends Bob half of the message encrypted with Bob's public key
4) Bob encrypts a message for Alice using Public$_{\text{AliceFake}}$ but only sends half of the message
5) Alice sends the rest of her message for Bob using Public$_{\text{BobFake}}$ which Mallory intercepts; since Mallory has the full message already, Mallory sends Bob the rest of the message encrypted with Bob's public key
6) Bob puts together both halves of Alice's message and decrypts it; then he sends the rest of his message to Alice using Public$_{\text{AliceFake}}$.

Then, Mallory causes Alice and Bob to "lose" their connection and thus be forced to restart. However, since Mallory has possession of Private$_{\text{AliceFake}}$, Mallory can now decrypt Bob's message! So Mallory obtains the message Bob will initially send to Alice.

Now in possession of both Alice's initial message and Bob's initial message, Mallory can successfully carry out an MitM attack since Mallory can encrypt either half of each message as needed in the protocol steps.

3) (20 pts.) In Chapter 3.3 on page 60 in the course textbook, Schneier says the following about Kerberos: "The protocol works, but it assumes that everyone's clocks are synchronized with Trent's clock. In practice, the effect is obtained by synchronizing clocks to within a few minutes of a secure time server and detecting replays within the time interval." Suppose that due to the clocks becoming dramatically unsynchronized due to some error, a decision is made to proceed with the Kerberos protocol but without checking the accuracy of the timestamps (but the timestamps are still sent). For this question, you are asked to come up with the most efficient attack you can with the assumption that timestamp checking has been turned off for some reason.

a. (5 pts.) Describe the intuition behind your attack without necessarily describing all of the details. In other words, suppose you were to be required to summarize the key one or two (or at most three) ideas behind your attack, how would you proceed?

The key idea is to replay Alice's communications and perhaps modify some aspects to learn new information.

b. (15 pts.) Now describe your attack in detail using Alice, Bob, Trent and Mallory. Please clearly state any necessary assumptions.

Note: In the following answer, it is important to explain all steps and variables used when providing instructions.

First, Mallory makes recordings of an earlier session:

1) Alice sends Trent her identity and Bob's: A,B
2) Trent generates key K and adds a timestamp T plus a lifetime L ; he then encrypts two messages as follows and sends them to Alice
   $E_A(T,L,K,B)$; $E_B(T,L,K,A)$
   Mallory copies this and saves it for future use
3) Alice then uses K to send Bob her identity and timestamp, plus Trent's message
   $E_K(A,T)$; $E_B(T,L,K,A)$
   Mallory also copies this and saves it for future use
4) Bob responds with the timestamp plus one
   $E_K(T+1)$
5) Alice sends some messages which Mallory copies and saves it for future use

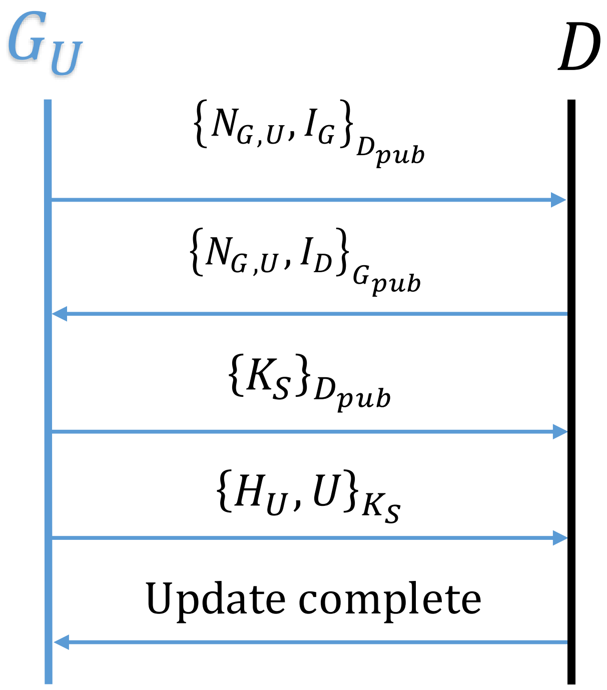
(continued on the next page!)

Next, later Mallory decides to attack:

6) Mallory pretends to be Alice and sends Bob the identity of Alice and a timestamp, plus Trent's message
$E_K(A,T)$; $E_B(T,L,K,A)$
7) Bob responds with the timestamp plus one
$E_K(T+1)$
8) Mallory resends some of Alice's earlier messages which Mallory can modify and observe Bob's response to try to learn new information

HINT: you may want to find an answer to part b first! After working out all of the details, it will be easier to summarize part b in your answer to part a.

4) (15 pts.) Let us reconsider the update protocol with a public key cryptography but with only the device authenticated to the server (the device may lack sufficient processing power or memory to properly carry out authentication, e.g., perhaps the device lacks the ability to generate random numbers). Furthermore, (i) assume that no version checking is done and (ii) suppose that an older version of the software (e.g., an old version of the operating system) has a known bug which an adversary would like to exploit. Can an adversary carry out a replay attack in order to downgrade device D to the previous version with the known bug?



Make sure to explain your answer with all attack steps regarding how the replay attack succeeds in downgrading; alternatively, explain in what way it will always fail. You must clearly and unambiguously explain all steps (to success or failure) to receive full credit. Please state any assumptions you believe are important and/or necessary.

Note: It is important to explain all steps and variables used when providing instructions.

First, Mallory makes recordings of an earlier session:

1) G_U sends D a nonce and G_U's identifier encrypted with D's public key:

$$\{N_{G,U}, I_G\}_{D_{pub}}$$

Mallory makes a copy of this.

2) G_U sends D a symmetric key encrypted with D's public key:

$$\{K_S\}_{D_{pub}}$$

Mallory makes a copy of this as well.

3) G_U sends D a hash of an update and the update itself in a message encrypted with the symmetric key:

$$\{H_U, U\}_{K_S}$$

Mallory makes a copy of this too. Let us call this version V.

At some later date, Mallory decides to replay the recorded messages to return the software on D to version V:

4) Mallory sends D the first recorded message containing the same nonce and G_U 's identifier encrypted with D's public key

$$\{N_{G,U}, I_G\}_{D_{pub}}$$

5) D responds to Mallory according to the protocol:

$$\{N_{G,U}, I_D\}_{G_{pub}}$$

Mallory does nothing with this response.

6) Mallory replays the earlier message (the second one recorded, see above) containing a symmetric key encrypted with D's public key:

$$\{K_S\}_{D_{pub}}$$

7) Mallory sends D a hash of the version V update and the update itself in a message encrypted with the symmetric key:

$$\{H_U, U\}_{K_S}$$

Mallory has succeeded in causing D to revert to version V!

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES. ALL LABORATORY SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SHEETS MUST BE STAPLED TOGETHER. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE ONLY ON ONE SIDE OF EACH SHEET OF PAPER THAT YOU SUBMIT AND MAY NOT BE ABLE TO USE RECYCLED PAPER). FAILURE TO FOLLOW INSTRUCTIONS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).