ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

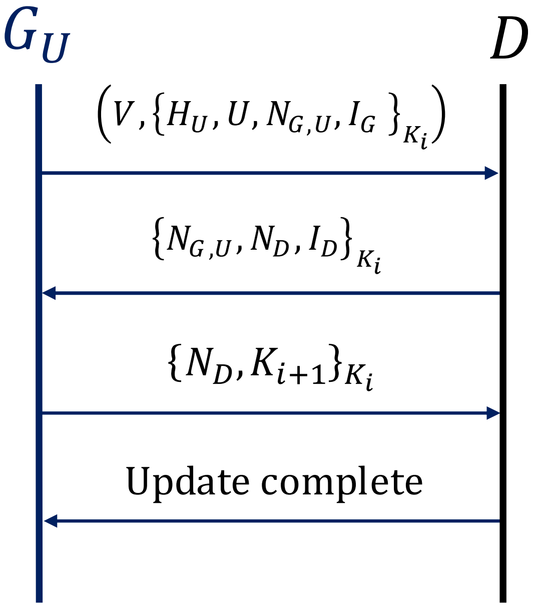
Homework 5, 85 pts.

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).

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).

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).

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.

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

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

2) (20 pts.) In class on Thursday Sept. 11, 2024, 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.

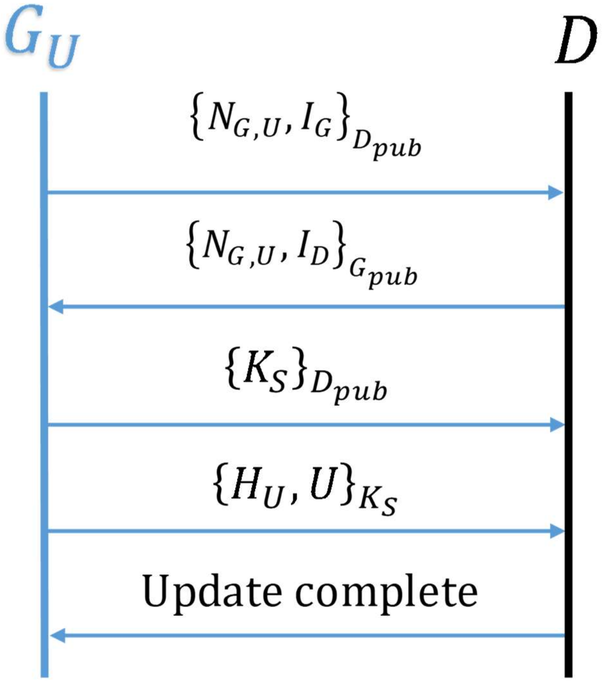
3) (20 pts.) In Chapter 3.3 on page 60 in the course textbook, Schneier says the following about Kerberos: "The protocol works, but it assumes that everyone's clocks are synchronized with Trent's clock. In practice, the effect is obtained by synchronizing clocks to within a few minutes of a secure time 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?

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

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 reply 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.

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!).