Homework #4

Oregon State University

ECE 478 Network Security

Spring 2016

Student:
Sam Quinn
Quinnsa@Oregonstate.edu

Professor:
Dr. Attila A Yavuz
Attila.Yavuz@oregonstate.edu

June 6, 2016

Oregon State
UNIVERSITY

College of Engineering

Contents

1 [20] Group Diffie-Hellman

Group Diffe-Hellman (GDH): We use the GDH3 protocol, and there are ve participants in the system. Let α be a generator and q is the order of the algebraic group. M_i denotes the i-th member of the group, N_i is the random exponent generated by the group member M_i . K denotes the group key.
(10 points) Write the up-ow and down-ow messages, and then show how each member derives the group key K.
Upflow:

1. P_1: $\alpha^{N_1} \rightarrow P_2$
2. P_2: $\alpha^{N_1 N_2} \rightarrow P_3$
3. P_3: $\alpha^{N_1 N_2 N_3} \rightarrow P_4$
4. P_4: $\alpha^{N_1 N_2 N_3 N_4} \rightarrow P_5$
5. P_5: $\alpha^{N_1 N_2 N_3 N_4 N_5} \rightarrow K$

$P_5 \rightarrow P_1 P_2 P_3 P_4$ via broadcast.
Down-flow:

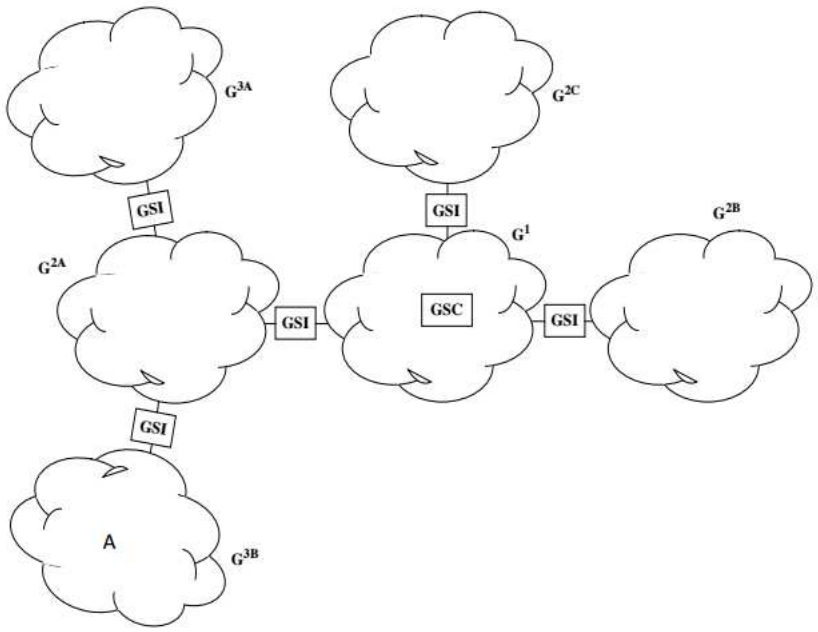
1. P_1 extracts their own key from the group key and sends to P_5
   P_1: $\alpha^{N_2 N_3 N_4 N_5} \rightarrow P_5$
2. P_2 extracts their own key from the group key and sends to P_5
   P_2: $\alpha^{N_1 N_3 N_4 N_5} \rightarrow P_5$
3. P_3 extracts their own key from the group key and sends to P_5
   P_3: $\alpha^{N_1 N_2 N_4 N_5} \rightarrow P_5$
4. P_4 extracts their own key from the group key and sends to P_5
   P_4: $\alpha^{N_1 N_2 N_3 N_5} \rightarrow P_5$

$P_5 \rightarrow \{\alpha^{N_2 N_3 N_4 N_5}, \alpha^{N_1 N_3 N_4 N_5}, \alpha^{N_1 N_2 N_4 N_5}, \alpha^{N_1 N_2 N_3 N_5}\}$ Via broadcast.

(10 points) Write the number of rounds, total message size, exponentiations per M_i , and total number of exponentiations.
Rounds: 6
Message Size: 9
Exponentiations: 19

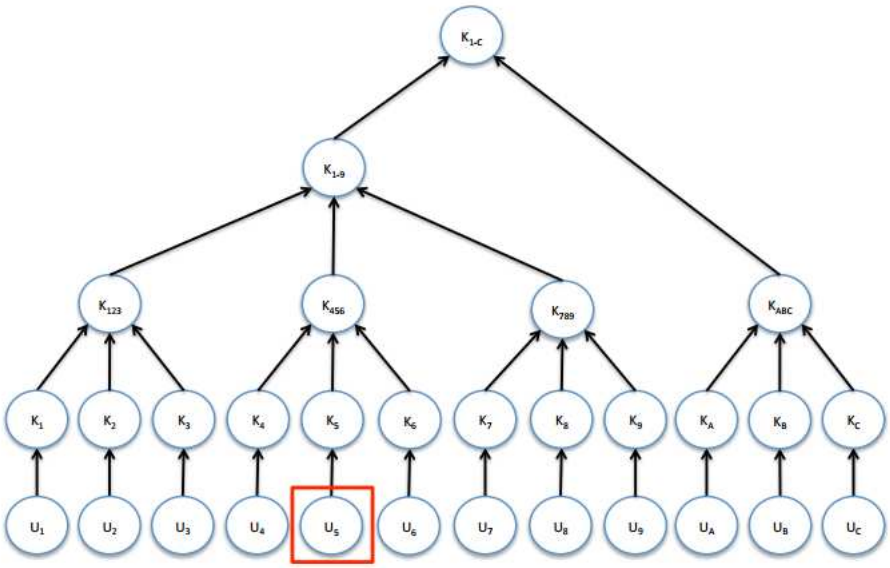
2 [20] Iolus

Consider the following network conguration in which Iolus is used.



Assume the GSC is distributing a new group key to the to the group members using Iolus. How many times will this new key be encrypted and decrypted before A learns the value of the new key? Also describe what entity performs each of the encryptions and decryptions.
The new key will be first encrypted by the GSC and sent to the GSI of the G^{2A}. The GSI of G^{2A} will decrypt the new key, then re-encrypt the key for the GSI of subgroup G^{3B}. Once the GSI of G^{3B} recives the encrypted key the GSI will decrypt it and once again encrypt for the user A. The last step will be user A reciving
Encryptions: 3
Decryptions: 3

3 [12] Key Trees



(6 points) If u5 is removed from the group, what keys should be changed? Write down how keys are distributed with each required step. Assume user oriented re-keying.
If the u_5 is removed from the key tree, then k_{1-c}, k_{1-9}, and k_{456} should change.

$$\begin{array}{lcl} s \rightarrow \{u_1, \ldots, u_c\} & : & \{k_{1-9}\}_{k_{1-c}} \\ s \rightarrow \{u_4, u_6\} & : & \{k_{1-9}, k_{4-6}\}_{4,6} \\ s \rightarrow u_5 & : & \{k_{1-9}, k_{4-6}\}_{k5} \end{array}$$

(6 points) Assume a new member is added (at now vacant location u5). Write down how keys are distributed with each required step. Assume key-oriented re-keying.

$$\begin{array}{lcl} s \rightarrow \{u_1, \ldots, u_c\} & : & \{k_{1-9}\}_{k_{1-c}} \\ s \rightarrow \{u_4, u_6\} & : & \{k_{1-9}, k_{4-6}\}_{4,6} \\ s \rightarrow u_5 & : & \{k_{1-9}, k_{4-6}\}_{k5} \end{array}$$

4 [20] SSL/TSL

(10 points) What is "The Heartbleed Bug", describe in detail how it works against SSL, and how it can be present.
The "Heartbleed Bug" was a serious weakness in the OpenSSL library. The bug allows specially

crafted packet that triggers a use after free attack. In the vulnerable version of OpenSSL the size of the message is sent with the message itself and is never verified. An adversary can exploit this bug by sending a very small message but say it is much larger. This will make the server allocate more memory than is needed for the message. The memory that is allocated "could" contain sensitive data including X.509 certificate secret keys, usernames, passwords, or other data. The sensitive data would be returned to the adversary upon request for their message.

(10 points) The proper key exchange and cipher suite choices for SSL/TLS continually change. We have discussed a potential key exchange mode and cipher suite selection that would be a reasonable choice at this moment during the class (also with an email). Write down some of the algorithms (discussed on the board), and also state what should be an ultimate care while you congure SSL/TLS (especially while doing international business).

5 [14] Needham-Schroeder, Otway-Rees

(12 points) In the Needham-Schroeder protocol (extended version in slides)

i **(2 points) How is Alice authenticated by the KDC?**
The KDC will send an encrypted message with Alice's public key. Alice should be the only one to decrypt this message as she is the only one with her secret key.

ii **(2 points) How is Bob authenticated by the KDC?**
Bob will send an encrypted nonce to Alice encrypted by Bob's secret key. Alice will send this encrypted nonce to the KDC in message #3 which if Bob is authentic the KDC will be able to decrypt the nonce.

iii **(2 points) How is the KDC authenticated to Alice?**
Alice is authenticated to the KDC through the trust of Bob. After the KDC sends Alice the "Ticket to Bob" and Alice forwards that to Bob, if Bob responds then then Alice can authenticate the KDC.

iv **(2 points) How is the KDC authenticated to Bob?**
The KDC is authenticated to Bob through the nonce that was sent to Alice and put in the "Ticket to Bob".

v **(2 points) How Alice is authenticated to Bob?**

vi **(2 points) How Bob is authenticated to Alice?** Because both Alice and Bob trust the KDC the generated shared key K_{ab} will be authenticate mutually between Alice and Bob.

(2 points) In the Needham-Schroeder protocol, Alice is the party that is in contact with the KDC, but in the Otway-Rees protocol, Bob is the party that is in contact with the KDC. Explain why this is the case.

This reduces the work load that the KDC will need to process. Bob will be able to determine if Alice is not legitimate quicker since he is the one talking to the KDC.

6 [14] Kerberos

(3 points) When Bob receives a ticket from Alice, how does he know it is genuine?
Bob will directly send the encrypted token to the KDC in the second message. If the KDC verifies that Alice is authentic then comunication will continue, if not then Bob knows that Alice is a fraud.

(3 points) When Bob receives a ticket from Alice, how does he know it came from Alice?
In the second message when Bob is authenticating Alice in message 2, the message to the KDC contains both of their Names and tokens encrypted under their private keys. If the name of Alice and her encrypted message do not pass verification from the KDC then Bob will know it did not come from Alice.

(3 points) When Alice receives a replay, how does he know it came from Bob (that it is not a replay of an earlier message from Bob)?

** I am assuming "replay" in this question is a typo and should have been *reply*. **

Alice will know that the message is from Bob since the message contains the nonce set in the first message directly to Bob, that was encrypted under her private key.

(5 points) What does the Ticket contain that allows Alice and Bob to communicate securely?
The ticket contains a shared key that is unique to only Alice and Bob. Because the KDC, Bob, and Alice have all been authenticated, further comunication between Alice and Bob are secure. However, if the KDC is compramized then all security is void.

References