Network Security

Professor Gaurav S. Kasbekar

Department of Electrical Engineering

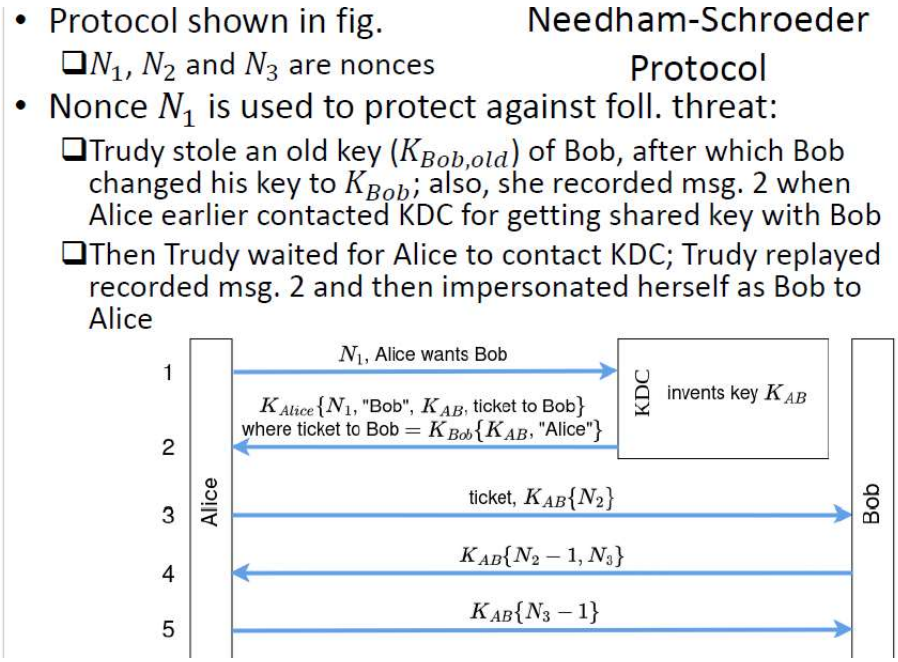
Indian Institute of Technology, Bombay

Week - 04

Lecture - 25

Authentication: Part 6

Hello, recall that in the previous lecture, we discussed a protocol for KDC-mediated authentication, which had some vulnerabilities. We will now discuss improved protocols for KDC-mediated authentication. So, the secure protocol is the Needham-Schroeder protocol. It improves upon the protocol that we discussed in the previous lecture. This protocol is shown in this figure.



Here, N_1, N_2, and N_3 are nonces. So, this is a scenario where there is a KDC in a network, and a user, Alice, wants to communicate with a user, Bob. So, this protocol operates as follows. First, Alice sends a message to the KDC saying that she wants to communicate with Bob, and Alice includes a nonce in this message, N_1. So, as we will see, this nonce is included so that some intruder, Trudy, who has stolen an old key of Alice cannot use an old message sent from the KDC to Alice to communicate with Bob.

So, this nonce is included to check the freshness of this communication from Alice to Bob. So, to start with, Alice sends this message, which includes a nonce N_1 to the KDC. Then, the KDC invents a key K_{AB}, which can be used for secure communication between Alice and Bob, and the KDC sends this message. K_{Alice}, along with the nonce N_1, the same nonce N_1 is included in this message, along with 'Bob', this is Bob's identifier. And this is K_{AB}, that is, the secret key that the KDC has invented, which Alice and Bob can use for secure communication.

And the KDC includes a ticket to Bob in the message. So, the ticket to Bob is $K_{Bob}\{K_{AB}$, "Alice"}, where this is Alice's identifier. This is the same shared secret key, K_{AB}, which can be used for communication between Alice and Bob. So, notice that, as before, the KDC does not have to initiate communication with Bob to share the key K_{AB} with Bob. Instead, the KDC just provides a ticket in the message sent to Alice.

Subsequently, Alice can contact Bob and share the ticket obtained from the KDC. In the third message, Alice sends the ticket obtained from the KDC to Bob. And $K_{AB}\{N_2\}$, where N_2 is another nonce. This $K_{AB}\{N_2\}$ is a challenge to Bob to check whether Bob indeed knows the secret K_{AB} or not. So, assuming that this message reaches Bob, that is the legitimate Bob, in that case, Bob can use this ticket and decrypt it because Bob has the key K_{Bob} shared with the KDC.

So, Bob can decrypt this ticket and obtain K_{AB} and Alice. So, by checking this message $\{K_{AB}$, 'Alice'}, Bob can verify that the person who has contacted Bob is indeed Alice. Now, Bob has obtained the key K_{AB}. Bob can decrypt this message K_{AB} $\{N_2\}$ to obtain the nonce N_2, and then Bob decrements the nonce N_2 to get N_2-1 and generates another nonce, N_3, which is a challenge to Alice, and appends N_2-1 and N_3, and the result is encrypted using K_{AB} and sent to Alice. Now, Bob has sent a challenge N_3 to Alice to check whether Alice knows the key K_{AB}.

Now, Alice decrypts this message and checks whether the first part of the message N_2-1 equals the nonce that she sent minus 1. If yes, then she is convinced that Bob knows the secret K_{AB}. Now, the second part of the message is a nonce, N_3, which is a challenge to Alice. Alice decrements that by 1 to get N_3-1, and then encrypts the result using K_{AB} to get K_{AB} $\{N_3\text{-}1\}$ and sends it to Bob. Bob decrypts it and finds out N_3-1 and checks whether that equals the nonce that he sent to Alice minus 1.

If so, then Bob knows that Alice knows the secret K_{AB}. So, at this point, KDC-mediated authentication has been done. So, in particular, Alice and Bob have agreed upon the secret key K_{AB}, which they can use for communication, as well as they have mutually authenticated. So, the Needham-Schroeder protocol not only allows Alice and Bob to agree on a secret shared key, K_{AB}, but it also allows them to subsequently mutually authenticate. So, let us now analyze this protocol.

Why is the nonce N_1 used? So, it is used to protect against the following threat. Suppose Trudy stole an old key of Bob. Let us call it (K_{Bob}, old). Then, Bob changed his key to K_{Bob}.

Bob may have suspected that his old key was stolen. So, Bob changed his key from (K_{Bob}, old) to K_{Bob}. Also, Trudy recorded message 2 when Alice earlier contacted the KDC for getting the shared key with Bob. Now, Trudy waits for Alice to contact the KDC and then Trudy replaces the recorded message 2. So, Trudy impersonates the KDC's network address and waits for Alice to contact the KDC.

So, the connection of Alice to the KDC actually goes to Trudy, and then Trudy replaces the recorded message 2, and then impersonates herself as Bob to Alice. This is done as follows. When Trudy sends this old recorded message to Alice, Alice then extracts the ticket from it. So, notice that this ticket is encrypted with Alice's key. So, Trudy cannot directly obtain the ticket.

But when this message reaches Alice, Alice decrypts this message and obtains the ticket. And then Alice initiates a communication with Bob. Now, Trudy intercepts that communication as well. Trudy impersonates Bob's network address. So, this message reaches Trudy.

Now, Trudy has obtained the ticket. Notice that this old message 2 was sent when Bob's key was (K_{Bob}, old). So, the ticket is (K_{Bob}, old)$\{K_{AB}$, 'Alice'$\}$. So, Trudy is able to decrypt this message using the old key of Bob, that is (K_{Bob}, old), and obtain the secret K_{AB} from this ticket. So, from this ticket, Trudy is able to obtain the secret key K_{AB}, and then Trudy has impersonated herself as Bob to Alice.

Subsequently, Trudy can start a communication with Bob, pretending to be Alice. So, Trudy can also communicate with Alice, pretending to be Bob. So, this is a vulnerability against which the nonce N_1 defends. So, it defends against this attack that is possible in the absence of this nonce. So, since this nonce N_1 is sent, this nonce is included in this message 2 by the KDC.

So, this attack fails because in this attack Trudy replayed the old message 2. But looking at the nonce in the message, Alice will come to know that it's a recorded old message. So, this nonce must be the same as the nonce that Alice sent to the KDC for this message to be accepted by Alice. So hence, this nonce N_1 defends against vulnerabilities such as these. Now, why is this string 'Bob' included in this message 2?

That is done to protect against the following threat. Suppose Trudy intercepts this first message: 'N_1, Alice wants Bob', and modifies the identifier 'Bob' to 'Trudy' in this message 1. So, the message reads 'N_1, Alice wants Trudy'. So, the KDC generates a key that is to be used for communication between Alice and Trudy. So, Trudy obtains that message and is able to obtain the key, say K_{AT}, which is a shared key between Alice and Trudy.

And then Trudy passes on the message to Alice, and Alice is tricked into talking to Trudy, thinking that she's talking to Bob. So, this is one attack that is possible because this identifier is not included in this message 2. So, for defending against such an attack, this string 'Bob' is included in this message 2. So, when Alice receives this message 2, after decrypting this message, Alice can check that this key K_{AB}, which is passed on by the KDC, is indeed meant for communication with Bob and not with someone else. So, this string 'Bob' assures Alice that this key K_{AB} is meant for communication with Bob.

So, that's the reason for including this string 'Bob' in this message 2. Note that the Needham-Schroeder protocol has been criticized for unnecessarily doubly encrypting the ticket to Bob. So, this ticket to Bob is encrypted using K_{Alice}, but the ticket itself is already encrypted using K_{Bob}. So, it is encrypted first using Bob's secret key, K_{Bob}, and then using Alice's secret K_{Alice}. There is no loss in security if the ticket to Bob is sent from the KDC to Alice without encrypting with K_{Alice}.

Notice that, anyway, the ticket is going to be sent after Alice has decrypted it. So, in this message 3, the ticket is anyway sent after Alice decrypts the message. So, hence, there is no need for encryption using K_{Alice} in this message 2. That adds some overhead, and there is no loss in security if this ticket were to be sent without any encryption with K_{Alice}. Now, in message 3, Alice sends a challenge K_{AB} (N_2) to Bob.

Then Bob decrypts this message K_{AB} (N_2) to get N_2, decrements it to get N_2-1, and then re-encrypts it to get K_{AB} {N_2-1, N_3}. So, this response K_{AB} (N_2-1) proves that Bob knows the secret K_{AB}. In message 4, Bob also sends his own challenge K_{AB} (N_3) to Alice. Alice

decrypts this message to get N_2-1 as well as N_3, decrements N_3 to get N_3-1, and then encrypts it using the key K_{AB} and sends it to Bob. This proves that Alice knows K_{AB}.

- In msg. 3, Alice sends a challenge ($K_{AB}(N_2)$) to Bob
  - Bob responds to challenge by sending $K_{AB}(N_2 - 1)$ in msg. 4, which proves that he knows K_{AB}
- In msg. 4, Bob also sends a challenge ($K_{AB}(N_3)$) to Alice
  - Alice responds to challenge by sending $K_{AB}(N_3 - 1)$ in msg. 5 ,which proves that she knows K_{AB}
- Note: in above protocols, response to challenge $K_{AB}(N)$ is $K_{AB}(N - 1)$; alternatively, response could have been N

So, in these protocols, notice that the response to the challenge K_{AB} (N) is K_{AB} (N-1). An alternative is the response could have been just N. So, suppose Alice were to send K_{AB} (N_2) to Bob, and then Bob just sent N_2-1 along with K_{AB} (N_3), then that would have served the purpose as well. So, that demonstrates that Bob knows the secret K_{AB}. So, because Bob is able to decrypt K_{AB} (N_2) to get N_2, so the response to K_{AB} (N) could have been N itself. So, this is a variant in which a different kind of response is used to this challenge.

Now, there is one attack possible on this protocol. If this K_{AB} (N_2-1), N_3 is of a certain form, specifically, suppose a block cipher with electronic codebook is used to send message 4 such that it is of this form: K_{AB} (N_2-1), K_{AB} (N_3). So, this message can be separated out into these components: K_{AB} (N_2-1), K_{AB} (N_3). So, this would be the case, for example, when a block cipher is used to encrypt these messages: N_2-1 and N_3. We discussed electronic codebook in an earlier class.

- Suppose a block cipher with Electronic Code Book (ECB) is used to send msg. 4 such that it is of the following form: $K_{AB}(N_2 - 1), K_{AB}(N_3)$
- An intruder, Trudy, can launch following attack:
  - First, she eavesdrops on authentication exchange between Alice and Bob shown in fig., and records msg. 3
  - Later, she sends the recorded msg. 3 to Bob
  - Bob responds with $K_{AB}(N_2 - 1), K_{AB}(N_4)$, where $N_4 \neq N_3$
  - Trudy cannot compute $K_{AB}(N_4 - 1)$; instead, she opens a new connection to Bob and sends $K_{AB}(N_4)$
  - Bob responds with $K_{AB}(N_4 - 1), K_{AB}(N_5)$
  - Trudy then uses $K_{AB}(N_4 - 1)$ to complete the first authentication exchange
  - Note that the above attack is an instance of the *"reflection attack"*

So, suppose the electronic codebook is used and the block cipher has K bits, N_2-1 has K bits, and N_3 also has K bits. So, the electronic codebook separately encrypts the different blocks. So, it would encrypt N_2-1 separately and N_3 separately using the key K_{AB}. So, the message would be of this form. It would be separable into K_{AB} (N_2-1) and K_{AB} (N_3).

Then, an intruder Trudy can launch the following attack. This attack is an instance of the reflection attack that we discussed earlier. When Bob sends a challenge to Alice, Alice opens a new connection and obtains a response to the challenge from Bob himself. So, specifically, first Trudy eavesdrops on the authentication exchange between Alice and Bob and then records this message 3. Later on, she sends the recorded message 3 to Bob.

So, the message sent is ticket, K_{AB} $\{N_2\}$. Now, Bob responds with K_{AB} $(N_2\text{-}1)$, K_{AB} (N_4), where N_4 is a nonce different from N_3. Now, Trudy needs to send K_{AB} $(N_4\text{-}1)$. So, Trudy needs to find K_{AB} $(N_4\text{-}1)$. But Trudy cannot compute K_{AB} $(N_4\text{-}1)$ because she does not know the secret key K_{AB}.

To obtain this K_{AB} $(N_4\text{-}1)$, she opens a new connection to Bob and sends K_{AB} (N_4). So, Trudy opens another connection with Bob and sends ticket, K_{AB} (N_4) to Bob, and then Bob includes the response K_{AB} $(N_4\text{-}1)$ in this message sent to Trudy. And then, when Bob responds with K_{AB} $(N_4\text{-}1)$, K_{AB} (N_5), Trudy has got the necessary information to respond to the first connection. So, Bob responds with K_{AB} $(N_4\text{-}1)$, K_{AB} (N_5), and Trudy uses K_{AB} $(N_4\text{-}1)$ to complete the first authentication exchange. So, this is an instance of the reflection attack as we mentioned earlier.

So, for this reason, this message K_{AB} $\{N_2\text{-}1, N_3\}$ should not be separable into its components. So, it should not be of the form K_{AB} $(N_2\text{-}1)$, K_{AB} (N_3). So, to defend against this attack, this message 4 should be encrypted in such a manner that K_{AB} $(N_2\text{-}1)$ cannot be reduced from K_{AB} $(N_2\text{-}1, N_3)$, if K_{AB} is unknown. One simple example in which this can be done is as follows. Suppose $N_2\text{-}1, N_3$ is of K bits, where the block cipher encrypts blocks of K bits each. So, in that case, the entire message $N_2\text{-}1, N_3$ is encrypted in one go by the block cipher.

So, K_{AB} $(N_2\text{-}1)$ cannot be extracted from K_{AB} $(N_2\text{-}1, N_3)$. So, this defends against this attack. Now, there is a vulnerability in the Needham-Schroeder protocol that is shown in this figure. Suppose initially, Alice's key is J_{Alice}. When Alice contacts the KDC for a ticket to talk to Bob, an intruder, say Trudy, records messages 1 and 2 of the exchange.

And also assume that in message 2, J_{AB} was the shared key generated by the KDC. So, Alice sent "N_1, Alice wants Bob," and then the KDC sent J_{Alice} $\{N_1$, "Bob", J_{AB}, ticket to Bob$\}$, where ticket to Bob is $K_{Bob}\{J_{AB}$, 'Alice'$\}$. Later, Trudy finds out the old key of Alice, that is, J_{Alice}, and uses it to find J_{AB}. Notice that Trudy has recorded this message 2, which was encrypted using J_{Alice}. So, since Trudy has found out J_{Alice}, she's able to decrypt this message and obtain the old key J_{AB}.

Now, Alice suspects that her key has been stolen and hence changes her key to K_{Alice}. So, K_{Alice} is the new key of Alice. But even after Alice changes her key, the protocol is still not secure because Trudy can still use the old key J_{AB}, and the old ticket K_{Bob} (J_{AB}, 'Alice') to impersonate herself as Alice to Bob. So, since Trudy has recorded the old messages that were sent using the key J_{Alice} and J_{AB}, Trudy can just initiate a connection sending message 3 to Bob. It contains the message: "ticket, J_{AB} $\{N_2\}$" since Trudy knows J_{AB}.

- Suppose initially, Alice's key is J_{Alice}; also, when Alice contacts KDC for a ticket to talk to Bob, an intruder, Trudy, records msgs. 1 and 2 of the exchange; also, in msg. 2, J_{AB} was the shared key generated by KDC
- Later, Trudy finds out J_{Alice} and uses it to find J_{AB}; Alice suspects that her key has been stolen and changes her key to K_{Alice}
- However, even after Alice changes her key, Trudy can still use J_{AB} and the old ticket $K_{Bob}(J_{AB}, \text{"Alice"})$ to impersonate herself as Alice to Bob

So, Trudy can send "ticket, J_{AB} $\{N_2\}$", where the ticket is K_{Bob}(J_{AB}, 'Alice'), and then subsequently, Trudy can start communicating with Bob, pretending to be Alice. So, to defend against this vulnerability, there must be some way for Bob to check whether this is a fresh connection by Alice or it is based on a replay from a previous exchange with the KDC. So, to defend against this vulnerability, there are two additional messages used at the beginning of the protocol in which Alice asks for a nonce from Bob, and Bob sends a nonce to Alice. So, at the beginning of this protocol, we add some messages; we add two messages in which Alice will ask for a nonce from Bob, and Bob sends a nonce to Alice, and this nonce is used to defend against this attack. That is, it is used by Bob to check whether this is a new connection from Alice or it is based on some old messages, which use some old insecure key.

The resulting protocol with these two messages added is called the Expanded Needham-Schroeder protocol. So, this Expanded Needham-Schroeder protocol is shown in this figure. So, it's very similar to the previous protocol except that two messages are added at the beginning. So, now there are seven messages in this protocol. First Alice sends a message to Bob initiating the communication saying that I want to talk to you.

So, Alice wants to talk to Bob. Then, Bob sends a nonce to Alice encrypted with his secret key K_{Bob}. So, Bob sends a message K_{Bob} $\{N_B\}$ to Alice. And this nonce has to be included in the message sent from Alice to the KDC, and then the KDC includes this nonce, N_B, in the message that the KDC sends to Alice. So, the KDC includes this nonce, N_B, in the ticket to Bob.

So, now the ticket to Bob contains a nonce N_B. So, when the ticket is sent subsequently from Alice to Bob, Bob is able to decrypt the ticket using his secret key K_{Bob} shared with the KDC and is able to check whether this nonce, N_B is the same as the nonce that he had sent to Alice. If yes, then Bob knows that this message corresponds to this initiation of communication from Alice to Bob. So, Bob knows that if this nonce N_B is the same as the one in this ticket, then this connection is legitimate. If this nonce does not match the nonce that was sent from Bob, then Bob knows that something is wrong.

- In msg. 2, Bob sends $K_{Bob}(N_B)$, where N_B is nonce generated by Bob
- KDC includes N_B in the ticket to Bob

It may have been an old message that is replayed. So, in this message 2, Bob sends K_{Bob} (N_B), where N_B is a nonce generated by Bob. Then the KDC includes N_B in the ticket to Bob. So, as we have seen here, N_B is included in the ticket to Bob. So, the vulnerability that we discussed on the previous slide is fixed because old recorded exchanges of Alice with the KDC will not enable Trudy to authenticate as Alice to Bob because the nonce in the old ticket will not match the new nonce that is sent by Bob.

So, after Alice changes her key to K_{Alice}, the KDC knows that her key is now K_{Alice}, so Trudy will also not be able to talk to the KDC using the old key J_{Alice}. So, for these reasons, the vulnerability that we discussed on the previous slide is fixed, and this is a secure protocol which overcomes the vulnerability in the original Needham-Schroeder protocol. So, using a nonce N_B, this expanded Needham-Schroeder protocol overcomes the previous vulnerability. So, in summary, we discussed protocols for KDC-mediated authentication. We discussed the Needham-Schroeder protocol, and then there was a vulnerability in it which was overcome by the expanded Needham-Schroeder protocol.

This concludes our discussion on authentication. Thank you.