Tutorial 5 - Solutions

Computer Security
School of Informatics
University of Edinburgh

In the fifth tutorial for the Introduction to Computer Security course we cover Cryptographic Protocols. The tutorial consists of questions from past years exams.

You are free to discuss these questions and their solutions with fellow students also taking the course, and also to discuss in the course forum. Bear in mind that if other people simply tell you the answers directly, you may not learn as much as you would by solving the problems for yourself; also, it may be harder for you to assess your progress with the course material.

1 Encryption

One-time pads Inspired by the one-time pad, Alice decides to design her own protocol to confidentially send messages to Bob. Alice's protocols works as follows:

- When Alice is ready to send her message $M \in \{0,1\}^\ell$, she randomly selects $K_A \in \{0,1\}^\ell$, and sends to Bob the message $M_1 = M \oplus K_A$.
- Bob then randomly selects $K_B \in \{0,1\}^\ell$ and sends to Alice the message $M_2 = M_1 \oplus K_B$.
- Next, Alice computes $M_3 = M_2 \oplus K_A$ and sends it to Bob.
- Bob may now retrieve the message M.

1. Show that $M = M_3 \oplus K_B$.

   Solution

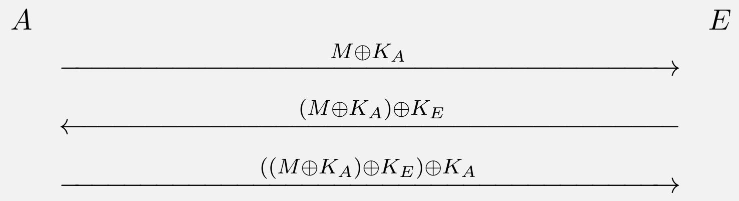
   The relies only on commutativity and associativity of $\oplus$:

   $$\begin{aligned} & M_3 \oplus K_B \\ = \; & (M_2 \oplus K_A) \oplus K_B \\ = \; & ((M_1 \oplus K_B) \oplus K_A) \oplus K_B \\ = \; & (((M \oplus K_A) \oplus K_B) \oplus K_A) \oplus K_B \\ \overset{a \oplus a = 0}{=} \; & M \end{aligned}$$

2. This protocol is insecure. Show that Eve can retrieve any message intended for Bob.

Solution

We say that Eve is an active adversary if she can eavesdrop on the messages of the legitimate parties and additionaly can send malicious messages to others and otherwise disrupt the communication (e.g. replay messages sent earlier, prevent a legitimate message from being delivered and so on). On the other hand, Eve is said to be passive if she can only eavesdrop on the messages of others.
If Eve is considered to be active, she can mount a MITM attack pretending to be Bob since messages coming from either Alice or Bob are not authenticated.


A
E
$M \oplus K_A$
$(M \oplus K_A) \oplus K_E$
$((M \oplus K_A) \oplus K_E) \oplus K_A$

As we just saw, the last message received by Eve is nothing more than $M \oplus K_E$ which Eve can decrypt since she knows K_E.
Eve is able to retrieve M even if she is passive. Eve knows only the information that was communicated. More precisely, she knows M_1, M_2 and M_3. It is

$$\begin{aligned} & M_1 \oplus M_2 \oplus M_3 \\ = & (M \oplus K_A) \oplus M_2 \oplus (M_2 \oplus K_A) \\ = & M \oplus K_A \oplus K_A \\ = & M \end{aligned}$$

Thus $M_1 \oplus M_2 \oplus M_3 = M$ and Eve can retrieve the original message.

ElGamal

3. Recall the details of the ElGamal encryption scheme seen in class.

Solution

- Fix prime p, and generator $g \in (\mathbb{Z}_p)^*$
- $\mathcal{M} = \{0, \ldots, p\text{-}1\}$ and $\mathcal{C} = \mathcal{M} \times \mathcal{M}$
- $G_{EG}() = (pk, sk)$ where $pk = g^d \ (\mathsf{mod}\ p)$ and $sk = d$ and $d \overset{r}{\leftarrow} \{1, \ldots, p\text{-}2\}$
- $E_{EG}(pk, x) = (g^r \ (\mathsf{mod}\ p),\ m \cdot (g^d)^r \ (\mathsf{mod}\ p))$ where $pk = g^d \ (\mathsf{mod}\ p)$ and $r \overset{r}{\leftarrow} \mathbb{Z}$
- $D_{EG}(sk, x) = e^{\text{-}d} \cdot c \ (\mathsf{mod}\ p)$ where $x = (e, c)$
- Consistency: $\forall (pk, sk) = G_{EG}()$, $\forall x$, $D_{EG}(sk, E_{EG}(pk, x)) = x$

  Proof: Let $pk = g^d \ (\mathsf{mod}\ p)$ and $sk = d$

$$\begin{aligned} D_{EG}(sk, E_{EG}(pk, x)) &= (g^r)^{\text{-}d} \cdot m \cdot (g^d)^r \ (\mathsf{mod}\ p) \\ &= m \ (\mathsf{mod}\ p) \end{aligned}$$

4. Assume you are given an ElGamal public key pk, but not the corresponding private key. Assume you are also given the ciphertexts $(e_a, c_a) = E\,(pk, m_a)$ and $(e_b, c_b) = E\,(pk, m_b)$ corresponding to the encryption using ElGamal of messages m_a and m_b under pk respectively. You are not given m_a nor m_b though. Show that you can construct a ciphertext which is a valid ElGamal encryption under the key pk of the message $m_a \cdot m_b$ (mod p).

Solution

By the definition of ElGamal, there exists r_a and r_b such that

$$\begin{aligned} (e_a, c_a) &= (g^{r_a} \ (\mathsf{mod}\ p),\ m_a \cdot (g^d)^{r_a} \ (\mathsf{mod}\ p)) \\ (e_b, c_b) &= (g^{r_b} \ (\mathsf{mod}\ p),\ m_b \cdot (g^d)^{r_b} \ (\mathsf{mod}\ p)) \end{aligned}$$

But then by the properties of modular arithmetic we can compute

$$\begin{aligned} e_a \cdot e_b &= g^{r_a + r_b} \ (\mathsf{mod}\ p) \\ c_a \cdot c_b &= m_a \cdot m_b \cdot \left(g^d\right)^{r_a + r_b} \ (\mathsf{mod}\ p) \end{aligned}$$

And thus the ciphertext $(e, c) = (e_a \cdot e_b, c_a \cdot c_b)$ which corresponds to the ElGamal encryption of $m_a \cdot m_b$ (mod p) under pk.

5. Assume you are given an ElGamal public key pk (but not the corresponding private key) and a ciphertext $(e, c) = E\,(pk, m)$ which is the ElGamal encryption of some unknown message m under pk. You are also given access to an oracle that will decrypt any ciphertext other than c. ElGamal is said to be vulnerable to a chosen ciphertext attack if you can retrieve m. Show that ElGamal is indeed vulnerable to a chosen ciphertext attack.

Solution

Since we know the public key pk, we can compute the ElGamal encryption of 2 under pk. Let (e', c') be the encryption of 2 under pk. We just saw in the previous question that we can compute $(e \cdot e', c \cdot c')$, which is the encryption of $m \cdot 2 \pmod{\mathrm{p}}$. Now using the decryption oracle we can obtain $m \cdot 2 \pmod{\mathrm{p}}$. Finally since 2 and p are coprime, 2 admits an inverse mod p which we can compute and divide $m \cdot 2 \pmod{\mathrm{p}}$ by 2 to retrieve m.

2 The Diffie-Hellman protocol

In class, we saw the Diffie-Hellman protocol, which is a two-party key establishment protocol, secure against passive attackers. However, as we saw, the Diffie-Hellman protocol is insecure against active attackers. Indeed, a malicious agent can mount a man-in-the-middle attack to learn a key not intended for her. This attack is possible because their is no mechanism to authenticate the two parties to one another. We consider the following extension of the Diffie-Hellman protocol to thwart this attack. We assume that the parties A and B have a private signing key sk_A and sk_B respectively, and a certificate on the corresponding public key CERT_A and CERT_B respectively signed by a common Trusted Third Party.

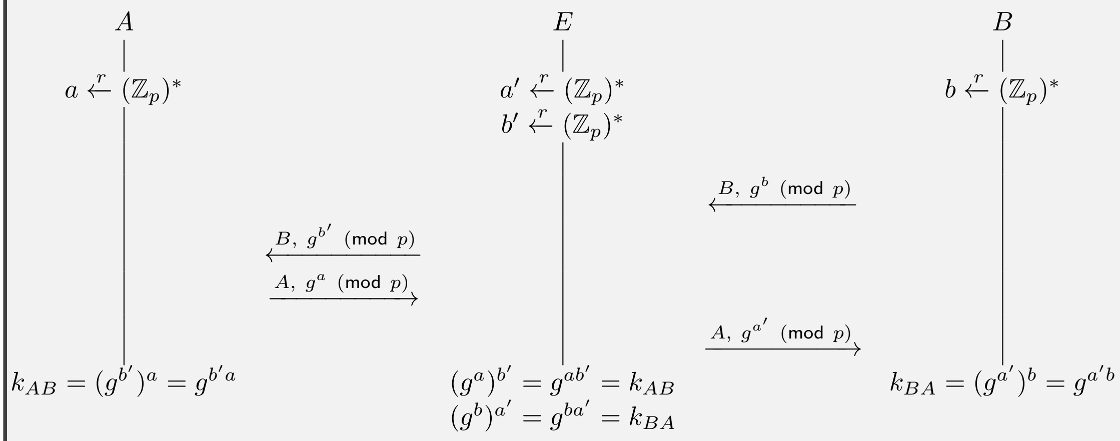
$$
\begin{array}{ccc}
A & & B \\
 & \xrightarrow{\qquad\qquad g^x \qquad\qquad} & \\
 & \xleftarrow{g^y,\ B,\ \mathsf{CERT}_B,\mathsf{sig}(\mathsf{sk}_B,(g^x,g^y))} & \\
 & \xrightarrow{A,\ \mathsf{CERT}_A,\mathsf{sig}(\mathsf{sk}_A,(g^x,g^y))} &
\end{array}
$$

The result is a shared secret $K_{AB} = g^{xy}$ from which the parties derive a session-key.

1. Briefly explain the purpose of the signatures in the protocol above. How does it defend against the attack discussed in class?

Solution

The original Diffie-Hellman has no authentication mechanism to ensure the two parties that they are indeed talking to each other. In class, we saw that the DH protocol is subject to the following man in the middle attack


A
E
B
$a \xleftarrow{r} (\mathbb{Z}_p)^*$
$a' \xleftarrow{r} (\mathbb{Z}_p)^*$
$b' \xleftarrow{r} (\mathbb{Z}_p)^*$
$b \xleftarrow{r} (\mathbb{Z}_p)^*$
$B,\ g^b \pmod p$
$B,\ g^{b'} \pmod p$
$A,\ g^a \pmod p$
$A,\ g^{a'} \pmod p$
$k_{AB} = (g^{b'})^a = g^{b'a}$
$(g^a)^{b'} = g^{ab'} = k_{AB}$
$(g^b)^{a'} = g^{ba'} = k_{BA}$
$k_{BA} = (g^{a'})^b = g^{a'b}$

where Eve has caused

- A to think that she is communicating securely with B and that they have both agreed to the key k_{AB};
- B to think that she is communicating securely with A and that they have both agreed to the key k_{BA};
- Eve has learned the keys k_{AB} and k_{BA} which were intended to remain secret from her.

In the variant proposed in the statement of Problem 2, A and B sign their view on k_{AB} and k_{BA}. Now, because Eve cannot forge A or B's signature she cannot mount the attack on the original DH protocol on this variant of the protocol. In particular, she cannot sign with the secret signing key of A the message $(g^{a'}, g^b)$. In other words she cannot build message $\mathsf{sign}(\mathsf{sk}_A, (g^{a'}, g^b))$. Similarly, she cannot sign with the secret signing key of B the message $(g^a, g^{b'})$. In other words she cannot build message $\mathsf{sign}(\mathsf{sk}_A, (g^a, g^{b'}))$.

2. Show that an active man-in-the-middle, Eve, can cause:

   - A to think that she is communicating securely with B (as required),
   - but B to think he is communicating securely with Eve.

   In other words, B is fooled into thinking that the subsequent encrypted messages he is receiving (from A) are coming from Eve. Note that Eve cannot eavesdrop on the resulting encrypted channel.

Solution

If Eve intercepts the third message in an honest execution of the protocol, and replaces it with the following message:

$$E,\ \mathsf{CERT}_E,\ \mathsf{sig}(\mathsf{sk}_E, (g^x, g^y))$$

which she can because she can obtain g^x and g^y from the first to messages of the session, then

- A will think that she is communicating securely with B (as required),
- but B will think he is communicating securely with Eve.

This is possible because in the first two messages g^x and g^y are not linked to A and B in a secure way.

3. Describe how Eve can use this attack to steal money from A. For example, suppose A gives expert advice in a private chat room run by B, and that she gets paid for that.

Solution

Eve could also register as an expert on Bob's private chat to sell her advice. Then she could just relay to A the messages sent from B to her. A will accept these messages as coming from B for her and will reply with her advice. Now Eve, will intercept A's responses and relay them to B as if coming from herself and will get paid for the advice in place of A.

4. Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents the attack from Question 2.

Solution

To fix this problem, A and B need to link g^x and g^y to the two parties of this protocol. This could be achieved as follows

$$A \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad B$$

$$\xrightarrow{\qquad\qquad\qquad g^x \qquad\qquad\qquad}$$

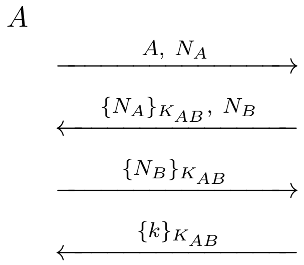
$$\xleftarrow{\ g^y,\ B,\ \mathsf{CERT}_B,\ \mathsf{senc}(g^x \cdot g^y, \mathsf{sig}(\mathsf{sk}_B, (g^x, g^y)))\ }$$

$$\xrightarrow{\ A,\ \mathsf{CERT}_A,\ \mathsf{senc}(g^x \cdot g^y, \mathsf{sig}(\mathsf{sk}_A, (g^x, g^y)))\ }$$

Note that the resulting protocol is the Station-to-Station protocol seen in class.

3 Authentication and key-agreement protocol

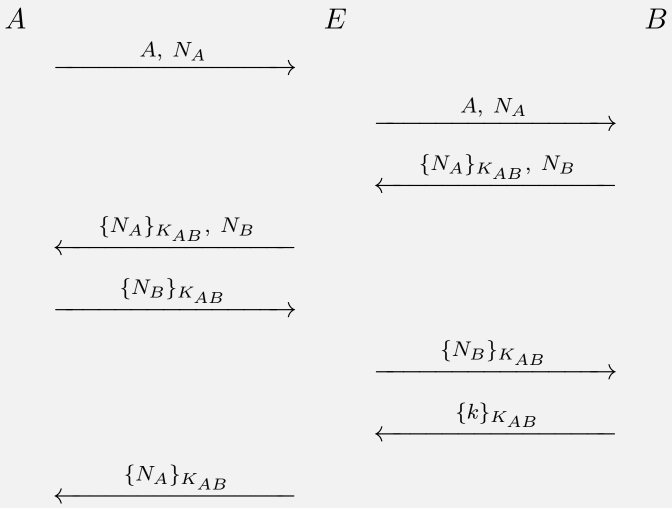
Consider the following two-party authentication and key agreement protocol. Alice and Bob want to establish a session key using a long-term symmetric key K_{AB}. First Alice generates a nonce N_A and sends it along with her identity to Bob. Bob generates his own nonce N_B and sends it together with the encryption of Alice's nonce under the long-term key K_{AB}. Alice acknowledges receipt of this message by sending the encryption of Bob's nonce under the long-term key. Finally Bob generates the session key k and sends it to Alice encrypted under K_{AB}.



1. This protocol is flawed. Show how Eve could learn a session key that Alice thinks she has securely established with Bob. (Assume that nonces and keys have the same length.)

Solution

The following diagram depicts such an attack.

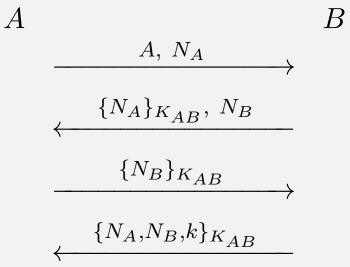


Note that in her last message Eve replayed $\{N_A\}_{K_{AB}}$, which was part of the first message from Bob. At this point A thinks she has securely established the key N_A with B.

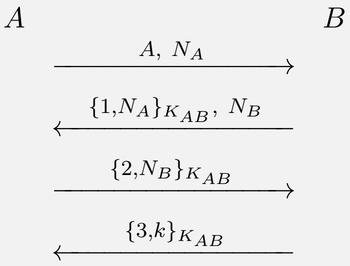
2. Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents this attack.

Solution

Of course having nonces and keys be of different size would thwart this attack. But there are several other possibilities to fix this protocol, for example to include N_A and/or N_B in the message that contains the key:

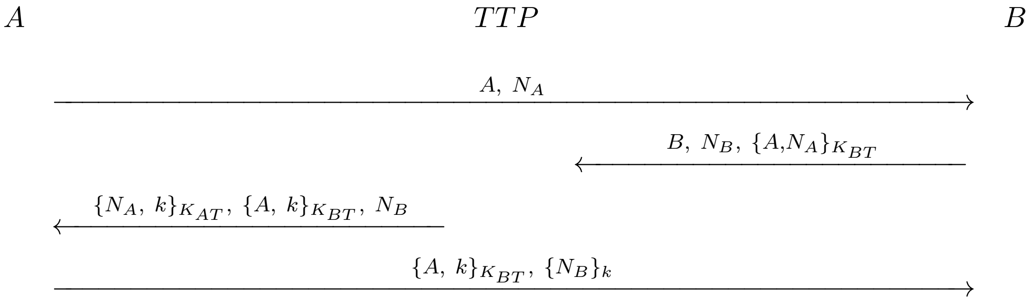


Or include static tags to distinguish the different messages:



Eve does not know K_{AB}, thus in both cases she cannot create the encryption necessary for the last step, nor can she replay a message received earlier.

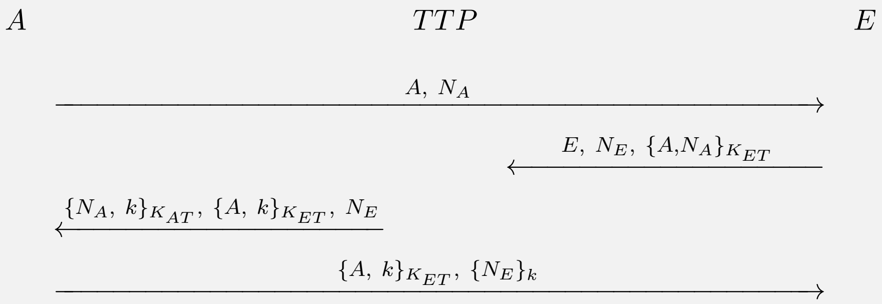
If Alice and Bob do not share a long-term symmetric key they could use the following three-party authentication and key agreement protocol that relies on a trusted third party (TTP). Alice and Bob both share a long-term symmetric key K_{AT} and K_{BT} respectively with the TTP.


A
TTP
B
$A,\ N_A$
$B,\ N_B,\ \{A, N_A\}_{K_{BT}}$
$\{N_A,\ k\}_{K_{AT}},\ \{A,\ k\}_{K_{BT}},\ N_B$
$\{A,\ k\}_{K_{BT}},\ \{N_B\}_k$

3. This protocol is flawed. Show how Eve could learn a session key that Alice thinks she has securely established with Bob. (Assume that nonces and keys have the same length.)

Solution

The following diagram depicts such an attack.

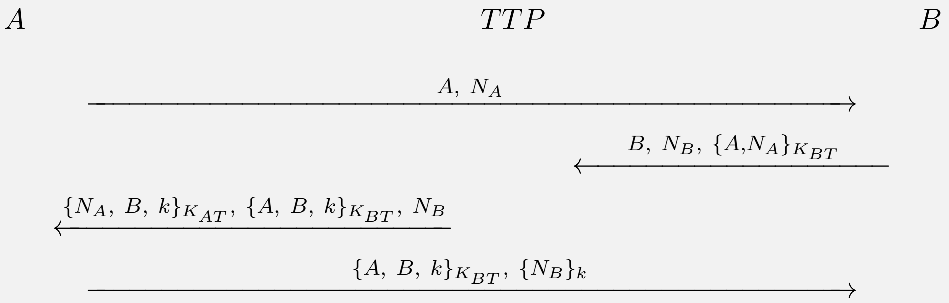

A
TTP
E
$A,\ N_A$
$E,\ N_E,\ \{A{,}N_A\}_{K_{ET}}$
$\{N_A,\ k\}_{K_{AT}},\ \{A,\ k\}_{K_{ET}},\ N_E$
$\{A,\ k\}_{K_{ET}},\ \{N_E\}_k$

At this point A thinks she has securely established the key k with B.

4. Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents this attack.

Solution

The identity of B should be included in the ciphertext from the TTP to A


A
TTP
B
$A,\ N_A$
$B,\ N_B,\ \{A{,}N_A\}_{K_{BT}}$
$\{N_A,\ B,\ k\}_{K_{AT}},\ \{A,\ B,\ k\}_{K_{BT}},\ N_B$
$\{A,\ B,\ k\}_{K_{BT}},\ \{N_B\}_k$

Similarily, to avoid an attack on Bob's perspective the identity of A and B should be included in the ciphertext from the TTP to B.