CS 333: Network Security and Defense

Role-Playing Game - Public Key Infrastructure

Author: Jidong Xiao

1 Introduction

This in-class game is mainly used to engage students in class, and help students to understand how the Public Key Infrastructure works. Note: when the narrator says something, the performers need to act accordingly.

1.1 Sketch One

This sketch describes two parties exchange information when there is no man-in-the-middle attackers, or even if there is an attacker who can eavesdrop the communication but can't intercept or manipulate the communication.

Characters: Narrator, Alice, Bob, Jason.

The script goes like this:

- Narrator: Alice, Bob, and Jason meet at a college party, they are chatting together. At the end of the party, Alice wants Bob to contact her in the future.
- Alice to Bob: Bob, it's really nice talking to you tonight, my campus mailbox is #20, feel free to drop me a letter.
- Bob to Alice: Sure, I will.
- Narrator: Two days later, Bob drops a letter in mailbox #20.
- Narrator: Five minutes later, Alice comes to her campus mailbox #20, opens the mailbox with her key - a private key, and only she has the key. After openning the mailbox, Alice gets the letter.
- Narrator: Jason is disappointed because there is nothing he can do: he can't get the letter because he doesn't have that private key.

End.

1.2 Sketch Two

This sketch describes two parties exchange information when there is a man-in-the-middle attacker, who not only can eavesdrop the communication but also can intercept or manipulate the communication. (This happens when you use a proxy, or when you use a public wifi - in which the owner of the wifi is like a proxy.)

Characters: Narrator, Alice, Bob, Jason.

The script goes like this:

- Narrator: Alice wants Bob to contact her, but she is too shy to talk to Bob directly, so she wants Jason to do her a favor.
- Alice to Jason: Hey, Jason, can you tell Bob that my campus mailbox is #20 so that he can drop me a letter if he wants to.
- Jason to Alice: No problem, I will let him know.
- Jason to Bob: Hey, Bob, Alice wants me to tell you, her campus mailbox is #21, and if you want, you can drop her a letter.
- Bob to Jason: Oh, great, I definitely will. Thanks!
- Narrator: Two days later, Bob drops a letter in mailbox #21.
- Narrator: Five minutes later, Jason comes to his campus mailbox #21, opens the mailbox with his key - a private key, and only he has the key. After openning the mailbox, Jason gets the letter.
- Narrator: Jason reads the letter and then puts it in mailbox #20.
- Narrator: Five minutes later, Alice comes to her campus mailbox #20, opens the mailbox with her key - a private key, and only she has the key. After openning the mailbox, Alice gets the letter.

End.

1.3 Sketch Three

This sketch describes two parties exchange information when there is a man-in-the-middle attacker, who not only can eavesdrop the communication but also can intercept or manipulate the communication. (This happens when you use a proxy, or when you use a public wifi - in which the owner of the wifi is like a proxy.)

However, this time, public key infrastructure is used.

Characters: Narrator, Alice, Bob, Jason, DMV Officer.

The script goes like this:

- Preparation: The instructor needs to prepare one certificate, with Alice's name on it, which also says her campus mailbox is #20, and the expiration date is Jan 01, 2020.
- Narrator: Alice goes to DMV, and tells the DMV officer that she wants a certificate.
- Alice to DMV Officer: Hello, officer, can I get a public key certificate?
- DMV officer to Alice: Sure, let me make one for you.
- Narrator: The DMV officer puts his signature on the certificate and then gives the certificate to Alice.
- Narrator: Alice gets the certificate. Alice wants Bob to contact her, but she is still too shy to talk to Bob directly, so she wants Jason to do her a favor.
- Alice to Jason: Jason, can you do me a favor and give this certificate to Bob?
- Jason to Alice: Absolutely. I will do it.
- Narrator: Jason passes the certificate to Bob. (Note: This is the attacker's option 1)
- Jason to Bob: Hi, Bob, Alice wants me to pass this certificate to you.
- Bob to Jason: Oh, great! Thanks!
- Narrator: Bob learns from the certificate that Alice's campus mailbox is #20. Two days later, Bob drops a letter in mailbox #20.
- Narrator: Five minutes later, Alice comes to her campus mailbox #20, opens the mailbox with her key - a private key, and only she has the key. After openning the mailbox, Alice gets the letter.
- Narrator: Jason doesn't have a chance to read the letter as he doesn't have the key of mailbox #20.

End. Attack fails.

1.4 Sketch Four

This sketch describes two parties exchange information when there is a man-in-the-middle attacker, who not only can eavesdrop the communication but also can intercept or manipulate the communication. (This happens when you use a proxy, or when you use a public wifi - in which the owner of the wifi is like a proxy.)

However, this time, public key infrastructure is used.

Characters: Narrator, Alice, Bob, Jason, DMV Officer, Bob's friend Firefox.

The script goes like this:

- Preparation: The instructor needs to prepare two certificates. The first certificate has Alice's name on it, which also says her campus mailbox is #20, and the expiration date is Jan 01, 2020. Another certificate has Alice's name on it, which says her campus mailbox is #21, and the expiration date is Jan 01, 2020.
- Narrator: Alice goes to DMV, and tells the DMV officer that she wants a certificate.
- Alice to DMV Officer: Hello, officer, can I get a public key certificate?
- DMV officer to Alice: Sure, let me make one for you.
- Narrator: The DMV officer puts his signature on the certificate, place it in an envelope and then gives the certificate to Alice.
- Narrator: Alice gets the certificate. Alice wants Bob to contact her, but she is still too shy to talk to Bob directly, so she wants Jason to do her a favor, therefore she passes the certificate (in the envelope) to Jason.
- Alice to Jason: Jason, can you do me a favor and give this certificate to Bob?
- Jason to Alice: Absolutely. I will do it.
- Narrator: Instead of passing the certificate to Bob, Jason creates a fake certificate, which has Alice's name on it, but it says Alice's campus mailbox is #21, instead of #20, and the expiration date is Jan 01, 2020. Jason puts his signature on this fake certificate and place the fake certificate in another envelope.
- Narrator: Jason then passes this fake certificate (in the envelope) to Bob. (Note: This is the attacker's option 2)
- Jason to Bob: Hi, Bob, Alice wants me to pass this certificate to you.
- Bob to Jason: Oh, great! Thanks!
- Narrator: Bob opens the envelope and learns from the certificate that Alice's campus mailbox is #21.
- Narrator: Before Bob drops a letter in mailbox #21, Bob's cautious friend Firefox reminds Bob.

- Firefox to Bob: Wait, Bob, these days certificates can be fake, you can't just trust a random certificate. How about this, I have a friend who works at the DMV, and he is responsible for issuing certificates. At least I can call him and verify if this certificate is legitimate or not.
- Bob to Firefox: Okay, sounds good, please call your friend.
- Narrator: Firefox takes a picture of the certificate and sends the picture over text to his friend at DMV.
- Firefox to DMV officer in a phone call: Hey, man, I just sent you a certificate, and I am wondering that did you sign this certificate?
- Narrator: The DMV officer reads that text message and looks at the picture.
- DMV officer to Firefox: Haha, that's not my signature, and I don't think it's my colleague's signature. I am pretty sure this is a fake signature, looks like someone is impersonating me or my colleague. Don't trust it.
- Firefox to DMV officer: Okay, got it, thanks man!
- Firefox to Bob: My friend said it's fake, the signature is fake, the certificate is therefore fake as well.
- Narrator: After learning the certificate is fake, Bob is disappointed and decides not to drop the letter.

End. Attack fails.

1.5 Sketch Five

This sketch describes two parties exchange information when there is a man-in-the-middle attacker, who not only can eavesdrop the communication but also can intercept or manipulate the communication. (This happens when you use a proxy, or when you use a public wifi - in which the owner of the wifi is like a proxy.)

However, this time, public key infrastructure is used.

Characters: Narrator, Alice, Bob, Jason, DMV Officer, Bob's friend Firefox.

The script goes like this:

- Preparation: The instructor needs to prepare two certificates. The first certificate has Alice's name on it, which also says her campus mailbox is #20, and the expiration date is Jan 01, 2020. Another certificate has Jason's name on it, which also says his campus mailbox is #21, and the expiration date is May 01, 2021.
- Narrator: Alice goes to DMV, and tells the DMV officer that she wants a certificate.
- Alice to DMV Officer: Hello, officer, can I get a public key certificate?
- DMV officer to Alice: Sure, let me make one for you.
- Narrator: The DMV officer puts his signature on the certificate, place the certificate in an envelope, and then gives the certificate to Alice.
- Narrator: Alice gets the certificate. Alice wants Bob to contact her, but she is still too shy to talk to Bob directly, so she wants Jason to do her a favor, therefore she passes the certificate (in the envelope) to Jason.
- Alice to Jason: Jason, can you do me a favor and give this certificate to Bob?
- Jason to Alice: Absolutely. I will do it.
- Narrator: Jason goes to DMV, and tells the DMV officer that he also wants a certificate.
- Jason to DMV Officer: Good afternoon, officer, can I get a public key certificate?
- DMV officer to Jason: Sure, let me make one for you.
- Narrator: The DMV officer puts his signature on the certificate, place the certificate in an envelope, and then gives the certificate to Jason.
- Narrator: Jason then passes his certificate to Bob. (Note: This is the attacker's option 3)
- Jason to Bob: Hi, Bob, Alice wants me to pass this certificate to you.
- Bob to Jason: Oh, great! Thanks!
- Narrator: Bob receives the envelope and he is excited, but Bob's cautious friend Firefox warns Bob.

- Firefox to Bob: Wait, Bob, these days certificates can be fake, you can't just trust a random certificate. How about this, I have a friend who works at the DMV, and he is responsible for issuing certificates. At least I can call him and verify if this certificate is legitimate or not.
- Bob to Firefox: Okay, sounds good, please call your friend.
- Narrator: Firefox, opens the envelope, takes a picture of the certificate, sends the picture over text to his friend at DMV.
- Firefox to DMV officer in a phone call: Hey, man, I just sent you a certificate, I am wondering that did you sign this certificate?
- Narrator: The DMV officer reads that text message and looks at the picture.
- DMV officer to Firefox: Oh, yeah, this is my signature, I signed this certificate the other day.
- Firefox to DMV officer: Okay, got it, thanks man!
- Firefox to Bob: My friend said it's his signature, so I think it's a legitimate certificate.
- Bob to Firefox: Oh, nice, so I guess that certificate tells me Alice's mailbox, and I will drop a letter into her mailbox.
- Firefox: Wait, what did you say? Alice? That's not Alice's certificate, that's Jason's certificate.
- Bob to Firefox: Seriously? I can't believe Alice didn't give me her real certificate.
- Narrator: After learning that is not Alice's certificate, Bob is disappointed and decides not to dropbox the letter.

End. Attack fails.