Song
Spring 2015

CS 161
Computer Security

Discussion 11

April 7 & April 8, 2015

Question 1 ***RSA*** **(10 min)**

(a) Describe how to find a pair of public key and private key for RSA encryption system.

(b) What is the encryption function?

(c) What is the decryption function?

(d) How to use RSA as a digital signature scheme?

Question 2 ***Public Key Basics*** **(10 min)**

Assume Alice and Bob are trying to communicate over an insecure network with public key encryption. Both Alice and Bob have published their public keys on their website. (You can assume they already know each other's correct public key)

(a) Alice receives a message: *Hey Alice, it's Bob. You owe me 100 bucks. Plz send ASAP.* The message is encrypted with Alice's public key. Can she trust it?

(b) Bob receives a message: *Hey Bob, that last message you sent me was sketchy. I don't think I owe you 100 bucks. You owe me.* The message is digitally signed using Alice's private key. Can he trust it was from Alice? How does he verify this message?

(c) Alice receives a message: *Hey Alice, I know things have been rough these last two messages. But I trust you now. Here is my password: hel1xfoss1l.* The message is encrypted with Alice's public key. Alice decrypted this and tested the password, and it was in fact Bob's! Can an eavesdropper figure out the password?

Question 3 ***Confidentiality and Integrity*** **(10 min)**

Alice and Bob want to communicate with both confidentiality and integrity. They have access to a symmetric key encryption function E and corresponding decryption function D and have already securely shared the key K. They also have a cryptographic hash function H. Recall that H is not keyed, so anyone can compute H(x) given x. However, due to the constraints of their computers they only have enough computing power to compute H once and E or D once per message (whether sent or received). You may assume that H and E do not interfere with each other when used in combination – for example, if you compute H(E(M)), the message M will be confidential because E guarantees it, and the computation of H makes no difference. To send message M to Bob, Alice has the option to use any of the five schemes listed on the next page.[1]

[1] Alice could also send the plaintext, but that is not a good idea.

a) Consider the threat model in which Eve is only able to eavesdrop and Alice and Bob are using the key K for the first time and will use it once and only once. In addition, Eve has no partial information about the message that will be sent. For each scheme, determine whether or not the scheme allows Bob to decrypt messages from Alice. (Don't worry about integrity yet.)

b) Out of the schemes you chose in part a), determine which of the schemes also provide integrity; that is, Bob will be able to detect any tampering with the message that Alice sends. Describe what Bob has to do in order to decrypt the message and make sure that it came from Alice. (Remember, Bob can only use D once and H once.) If you think it will not work, explain why. For any that do not work, what is the vulnerability?

Alice Sends to Bob	Confidentiality	Integrity	Decrypt Steps
1. H(E(M))			
2. E(M), H(E(M))			
3. E(H(M))			
4. E(H(M)), H(M)			
5. E(M), H(M)			

c) If Alice and Bob use these schemes to send many messages, the schemes become vulnerable to a replay attack. In a replay attack, Eve remembers a message that Alice sent to Bob, and some time later sends the exact same message to Bob, and Bob will believe that Alice sent the message. How might Alice and Bob redesign the scheme to prevent or detect replay attacks?

Question 4 ***Diffie-Hellman Basics*** **(10 min)**

Recall that in a Diffie-Hellman key exchange, there are values a, b, g and p. Alice computes $g^a \bmod p$ and Bob computes $g^b \bmod p$.

(a) Which of these values are publicly known and which must be kept private?

(b) Assume Eve has tapped into the network between Alice and Bob. Eve can only view the traffic, she cannot change it. Alice and Bob perform the Diffie-Hellman key exchange and have agreed on a shared symmetric key K. However, Bob accidentally sent his b over the network in plain text. If Eve viewed all traffic since the beginning of the exchange, can she figure out what K is?

(c) Assume Mallory has tapped into the network but has managed to not only view the traffic but also intercept and modify it. Alice and Bob perform Diffie-Hellman to agree on a shared symmetric key K. After the exchange, Bob gets the feeling something went wrong and calls Alice. He compares his value of K to Alice's and realizes that they are different. Explain how Mallory could know Bob's K_b and Alice's K_a and how she could use this secretly rewrite traffic between them.

Question 5 ***TLS*** **(10 min)**

(a) In TLS, what security properties are achieved, and what components of the TLS protocol enable these properties?

(b) Recall that in practice, TLS as used on the web typically only provides one-way authentication – that is, when communicating securely over the web, only the server is required to authenticate themselves, and not the client. Why is TLS usually used this way?

(c) How else might a web server authenticate a user? (if the user is not authenticated by TLS)