Georgia Gwinnett College
School of Science and Technology
ITEC 3300: Information Security
Homework Assignment 4 Solution

Problem 1 [35 Points]

Visit the site www.amazon.com, read its certificate and find the following information.

a) **[5 Points]** Which CA issued and signed the certificate?

Answer: DigiCert Global CA G2.

b) **[5 Points]** What is the subject's identity? That is, to which company and website is the certificate issued?

Answer: The certificate is issued to Amazon.com, Inc. whose website's URL is www.amazon.com.

c) **[5 Points]** Which digital signature scheme and hash function is used to sign the certificate?

Answer: The digital signature scheme is RSA. The hash function is SHA-256.

d) **[5 Points]** Which *public-key* encryption *scheme* is used to secure the communication between your browser and the site www.amazon.com, and what is the length of the public key?

Answer: The public-key encryption scheme is RSA. The public key length is 2048 bits.

e) **[5 Points]** Which *private-key* encryption *scheme* is used to secure the communication between your browser and the site www.amazon.com, what is the length of the key and what is the mode of operation?

Answer: The private-key encryption scheme is AES. The key length is 256 bits. The mode of operation is GCM.

f) **[5 Points]** Which key exchange protocol is used to establish a shared private key between your browser and the site www.amazon.com?

Answer: The key exchange protocol is ECDHE_RSA with P-256.

g) **[5 Points]** What is the certification path for www.amazon.com?

Answer: The certification path is

DigiCert Global Root G2 → DigiCert Global CA G2 → www.amazon.com

Problem 2 [25 Points]

During the discussions on TLS, we emphasized the importance of the integrity of the certificate authority (CA). What damages can an attacker cause if he is able to compromise a trusted CA? Be as comprehensive as you can in your answer and use a good concrete example to illustrate your answer.

Answer:

If an attacker is able to compromise a trusted CA, then he can create for himself a *fake yet valid* certificate for any entity he desires. For example, suppose that the attacker has compromised DigiCert. The attacker can construct a phishing site www.amazan.com that mimics www.amazon.com, and create a certificate that lists DigiCert as the issuer and Amazon as the subject certified, but contains the *phishing site's URL* www.amazan.com as the subject's URL and *the attacker's public key* as the subject's public key. The attacker then signs the fake certificate using DigiCert's private signing key. The attacker would then try to trick users to visit the phishing site www.amazan.com by social engineering. When a user visits www.amazan.com, the browser will *not* detect the attack even with the help of TLS, because the issuer of the certificate is DigiCert, a trusted CA, the URL www.amazan.com appears as the subject's URL on the fake certificate, and the digital signature on fake certificate is a valid signature of (the compromised) DigiCert. Therefore, as a user visits www.amazan.com, its fake certificate will be verified as valid, and thus a TLS session will be successfully established between the user's browser and www.amazan.com. If the user trusts the site and enters his account credentials (e.g. username and password) at the site, then it would be captured by the attacker. Using this information, the attacker can then access the user's account at Amazon.

Problem 3 [40 Points]

In this question, we revisit the basic key exchange protocol described on Slides 32 – 35 in the PowerPoint presentation titled Public-Key Encryption. (See also the video of the lecture on 6/15)

a) **[5 Points]** As a warm-up, explain why this protocol is secure against *passive* attackers. A passive attacker is one who can only intercept data.

   Answer: A passive attacker can only capture Bob's public encryption key pk and the ciphertext $E_{pk}(K)$. Without Bob's private decryption key, the attacker would not be able to learn the secret *K* from its encryption.

b) **[20 Points]** Describe how an *active* attacker can break this protocol. An active attacker is one who can not only intercept data, but also block and alter the data transmitted over the network and inject his own data into the network. Be as comprehensive as you can in your answer.

   Answer: An active attacker can block the public encryption key pk that Bob sends to Alice. In the meantime, the attacker generates his pair of keys (pk', sk'), and forwards to Alice his own public encryption key pk'. Thinking that pk' comes from Bob, Alice would encrypt the secret K using pk' and send the ciphertext $E_{pk'}(K)$ to Bob. The

attacker again blocks the ciphertext $E_{pk'}(K)$, and then decrypts it to obtain the secret K using his private decryption key sk': $D_{sk'}\left(E_{pk'}(K)\right) = K$. After uncovering the secret K, the attacker re-encrypts K using Bob's public encryption key pk, and forwards the ciphertext $E_{pk}(K)$ to Bob. Bob then obtains the secret K by decrypting the ciphertext $E_{pk}(K)$ using his private decryption key sk. By this time, the protocol is complete. Alice and Bob have established the common secret key K without noticing what happened in between. In the meantime, the active attacker has also obtained the key K.

c) **[15 Points]** Describe how to secure this protocol against active attackers. Be as comprehensive as you can in your answer.

Answer: The problem with the basic protocol is that it had no mechanism for data integrity, that is, it had no mechanism that allows one to verify that the data received is the original data from the claimed sender. To secure the protocol, we use the ideas we learned from TLS.

Bob first obtains from a trusted CA a certificate which contains his public encryption key pk. The certificate is signed by the CA using a secure digital signature scheme. In the first step of the modified protocol, Bob sends his certificate to Alice. Upon receiving Bob's certificate, Alice first verifies the CA's signature of the certificate, using the CA's public verification key. If the CA's signature is invalid, then Alice aborts. Only if the CA's signature is valid will Alice trust Bob's pk and proceed as in the original protocol.

We now argue that this modification secures the protocol against active attacks, as long as the trusted CA is not compromised. If the attacker modifies the public key pk on Bob's certificate (e.g. if the attacker attempts to replace Bob's pk with his own pk' on the certificate as in part b), then he would need to forge a valid signature of the CA for the modified certificate. This would be hard without the CA's private signing key, and the attacker's attempt for integrity violation would be detected by Alice when she verifies the CA's signature. If the attacker does not modify the public key on Bob's certificate, then Alice will use Bob's original public key pk to encrypt the secret K and the attacker will not be able to learn the secret K from its ciphertext without Bob's private key. Therefore, the resulting protocol is secure as long as the CA is not compromised by the attacker.