Ayush Jain (UNI : aj2672)

COMS W4180 Network Security
Written Assignment 2

1 Problem 1

With the above protocol, it is not possible to establish the identity of the servers. This is because the Reflection attack is still possible in the above protocol. Lets say any person Trudy sends the nonce $\{r_A\}$ to Bob. Bob in turn sends the message $\{E\_K_{AB}(r_A, timestamp), r_B\}$ and expects the message $\{E_K AB(r_B, timestamp)\}$ in turn.

Trudy on a separate connection could then send r_B to Bob. As a reply, Bob would then send $\{E\_K_{AB}(r_B, timestamp), r_C\}$. Trudy can now easily remove r_C and send the rest of the message to Bob from the first connection. The only requirement is that the round trip message transfer of the message $\{E\_K_{AB}(r_B, timestamp)$ from Bob to Trudy and then back to Bob should take less than 0.5 seconds, which is possible and cannot be ensured against. Hence, the Reflection attack works in this case and does not ensure the identity of Alice and Bob.

The protocol can be fixed in the following way:

1. Alice sends $\{r_A\}$ to Bob
2. Bob sends $\{E\_K_{AB}(r_A, timestamp), r_B\}$ to Alice
3. Alice sends $\{E\_K_{AB}(r_B, timestamp + 1)\}$ Bob

So we change the last step so that Alice sends the same value of timestamp as sent by Bob incremented by 1. This ensures that Alice decrypted the message and prevents the working of Reflection attack.

2 Problem 2

a. Alice knows that the she is really connected to Bob and the real KDC was involved because of the keys K_A, K_B and K_{AB}. The TGT is encrypted using the key K_A, which is known only to KDC and Alice herself. Since KDC is able to encrypt the TGT with the correct K_A means that the real KDC must be involved.
In the second stage, as part of the ticket response the KDC encrypts the key K_{AB} with the key K_B (known only to KDC and Bob). Bob is supposed to decrypt this message and then use K_{AB} to encrypt the value (timestamp+1), where timestamp is the value sent by Alice. This makes sure that actual Bob is involved.

b. KDC can impersonate both Alice to Bob and Bob to Alice. This is because he knows all the keys K_A, K_B and K_{AB} used between Alice and Bob for communications.

3 Problem 3

a. Finger prints are not constant. They may degrade in quality due to ageing, injury and any activities an individual may involve in. This is the major usability issue regarding using finger prints for authorization. They may work for a limited period of time but are not entirely dependable over longer periods. They are usually supported with password based authorization.

b. The difference between using the biometric method versus the deterministic method is that using deterministic gives you surety that only the intended user is accessing the system. The deterministic methods can be easily impersonated and does not give the surety that the user accessing

the system is the same as the intended one and not an impersonator.

4 Problem 4

a. The signature at the end of the certificate is required to establish the authenticity of the certificate. The server uses the public key of the issuer to verify the same.

b. For all valid domains we have a chain of certificates, one signed by another. These chains end at a root, which is one of a few designated certificate issuing organizations. All browsers are aware of a comprehensive list of such root acting organizations. For example, ssol.columbia.edu certificate is issued by the InCommon RSA Server, CA which is in turn issued by USERTrust RSA Certification Authority. The root organization AddTrust External CA Root signs the USERTrust RSA Certification Authority and is one of the few certificate signing organizations.

In order to verify the certificates, the browser moves up this tree, verifying the signature of a certificate with the immediate issuing authority's public key. With respect to our example, ssol.columbia.edu's certificate is authorized by verifying its signature using the pubic key of InCommon RSA Server, CA. Similarly InCommon RSA Server, CA is authorized with the public key of USERTrust RSA Certification Authority which is in turn authorized using the public key of AddTrust External CA Root. The AddTrust External CA Root, being the root certificate signature is verified using its own public key which is present with the browser itself.

c. In addition to the signature the browser is also supposed to check the expiration date of the certificate and make sure that the certificate is still valid.

5 Problem 5

a. 15

b. TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)

c. Three certificates were observed:
- Subject: ssol.columbia.edu, **Signature Algorithm:** sha256WithRSAEncryption
- Subject: InCommon RSA Server CA, **Signature Algorithm:** iso.2.840.113549.1.1.12
- Subject: USERTrust RSA Certification Authority, **Signature Algorithm:** iso.2.840.113549.1.1.12

d. AddTrust External CA Root

e. Following Diffie-Helman parameters were present:
- p : ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd1...
- g : 02
- pubkey: 2a693cc4a6107c790f4f9c2d9afcc9e624b6136caff647f9...
- signature: 0aeb048641596fdd14b6c71cc4d53479e7a649867e035974...

f. 14

g. In Client Hello, TLS v1.2 is used where as in Server Hello, TLS v1.0 is used.