Week 11

Lecture 1

User Authentication
Additional Material on Kerberos from the textbook

Lecture 2

Secure Socket Layer
Additional Material on TLS layer from the textbook

Workshop 11: Workshop based on Lectures in Week 9

Quiz 11

Secure Socket Layer

COMP90043

Lecture 2

Udaya Parampalli

Public Key Cryptography: Diffie-Hellman and RSA

Lecture 2

1.1 Secure Socket Layer

- Hybrid Encryption Method
- Transport Level Security
- SSL

Udaya Parampalli

Hybrid Encryption

- Let us look at a scenario for Alice and Bob to exchange a large file (1 G bytes).
- Assume that they use a public key encryption algorithm such as RSA of 128 bytes size public address.
- # of encryptions required = 10^9/ 128= 7,812,500
- Assume now the speed of encryption about 1000 per second.
- So, time required for the file transfer is = 7,812.5 seconds = 130.2 minutes = approx. 2 hours!
- So, using only public key method is not a solution.

Hybrid Encryption

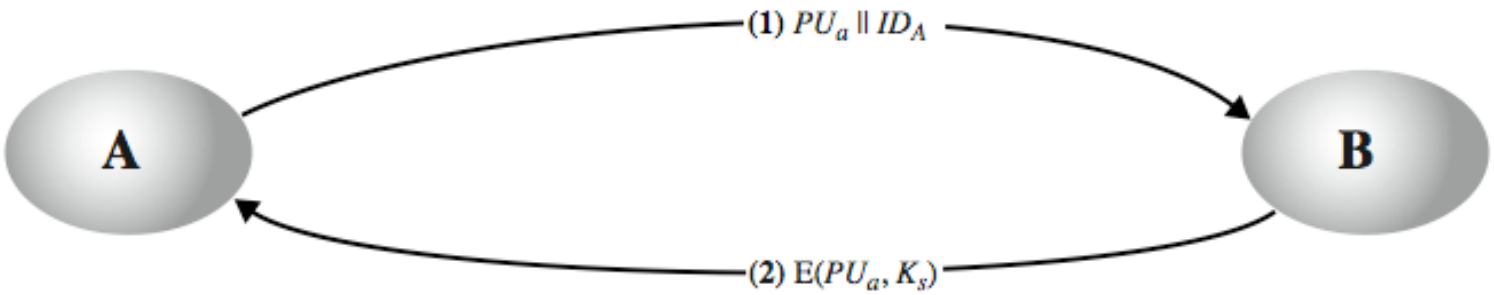
- For the same file using a symmetric key encryption the transfer would be much faster.
- Assuming that AES algorithm can encrypt with 1000 K bytes per second, the time for transfer would be
- 10^9/ 1000 10^3 = 0.00006 seconds.
- So definitely, symmetric key system is a better solution. However, it demands Alice and Bob share a secret key in advance.
- Hybrid encryption is combining Public and Symmetric key algorithms to improve the speed of transfer.

Hybris Method

- Alice and Bob first exchange a random secret key using a public algorithm such as RSA.
- Alice then encrypts the large file using a symmetric key algorithm such as AES using the secret and send the encrypted file to Bob.
- Since Bob has the secret, he decrypts the encrypted file.
- SSL uses a similar strategy, but we need to mindful of network's transport later properties to create the protocol.

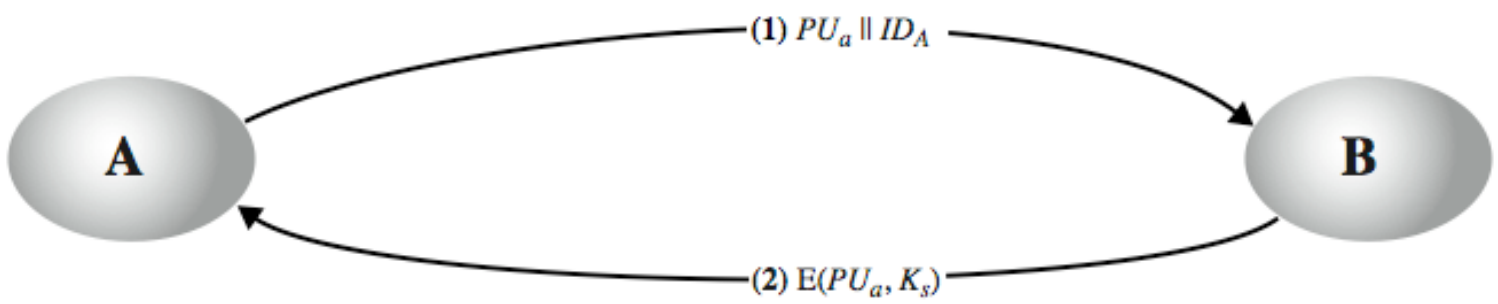
Recap from Week 7: Merkle Key Distribution

1. A generates a public/private key pair [*PUa, Pra]* and transmits a message to B consisting of PUa and an identifier of [A, IDA]
2. B generates a secret key, Ks, and transmits it to A, encrypted with A's public key.
3. A computes D(PRa, E(PUa, Ks)) to recover the secret key. Because only A can decrypt the message, only A and B will know the identity of Ks.
4. A discards PUa and PRa and B discards PUa.



From the textbook a version of Fig 14.7

Hybrid Protocol



A: C= $E(K_s, File)$ → B: File = $E(K_s, C)$

E is a symmetric key encryption function such as AES.

Security Issues

- As the Public key exchange method in the previous slide is vulnerable to Man in the Middle (MITM) attack, so also this Hybrid protocol has similar security properties.
- In practice we need to have some way of ensuring authentication of public addresses.
- One way is to avoid the problem is using certificates based methods. This method requires establishment of Public key infrastructure.

SSL

- Secure Socket layer protocol uses Transport Later features of Modern Internet.
- The main idea is to create a transport session between two nodes and then exchange a session key using a protocol similar to the Hybrid protocol.
- Session key is used in the symmetric key encryption.
- So, a Transport Layer Security (TLS) used two important concepts:
  - Connection between a client and a server
  - Session associated with the connection.
- They use OSI layering model protocols for realizing the above concepts.
- Chapter 17 of the textbook deals with this topic in detail. I have provide some additional material from the textbook for the study.

Week 11

Lecture 1

User Authentication
Additional Material on Kerberos from the textbook

Lecture 2

Secure Socket Layer
Additional Material on TLS layer from the textbook

Workshop 11: Workshop based on Lectures in Week 9

Quiz 11