Homework 2

Reading Assignment

to be completed (preferably) by Tuesday, September 29, 7:20pm

W. Stallings, "Cryptography and Network-Security,"

- Chapter 2.1 Symmetric Cipher Model
- Chapter 9.1 Principles of Public-Key Cryptosystems
- Chapter 1.3 Security Attacks
- Chapter 1.4 Security Services
- Chapter 11.1 Applications of Cryptographic Hash Functions
- Chapter 13.1 Digital Signatures
- Chapter 14 Key Management and Distribution

Written Assignment

due by Saturday, October 3, 11:59pm

Problem 1

Which of the following five security services are implemented by Protocols 1, 2, 3, and 4, respectively?

Please explain why (answers without justification will not be graded).

Services:
C - Confidentiality
AS - Authentication of the Sender
AR - Authentication of the Receiver
NS - Non-repudiation of the Sender
NR - Non-repudiation of the Receiver

Protocol 1

1. A sends to B
   A, \ E(PU_B, M), h(M \ || \ A), \ B
2. B sends to A
   B, h(M \ || \ B), \ A
Protocol 2

1. A sends to B
   A, E(\text{PU}_B, M), E(\text{PR}_A, h(M \parallel A \parallel B)), B
2. B sends to A
   B, E(\text{PR}_B, h(M \parallel B \parallel A)), A

Protocol 3

1. A sends to B
   A, E(\text{PU}_B, K_{AB}), E(K_{AB}, M), E(\text{PR}_A, M \parallel A), B
2. B sends to A
   B, h(K_{AB} \parallel M \parallel B), A

Protocol 4

1. A sends to B
   A, E(K_{AB}, M \parallel h(M)), B
2. B sends to A
   B, h(M), A

Notation:

X represents a unique name of user X, where X=A or B
M means a message
(V \parallel W) means V concatenated with W
E(\text{PU}_Y, Z) means Z encrypted using a public key of Y
E(\text{PR}_Y, Z) means Z encrypted using a private key of Y
E(K_{AB}, Z) means Z encrypted using a secret key shared by A and B
Problem 2

Draw a four-level hierarchy of the certification authorities (U.S.-state-city/county-institution), that includes GMU, UVA (University of Virginia), and UF (University of Florida).

Assuming the use of Public Key Infrastructure with Reverse Certificates, answer the following questions:

1) Which certificates need to be added to a signed message sent
   a. by Betty from UVA to Tom from GMU,
   b. by Shilpa from GMU to Chandu from UF?

2) Which certificates need to be downloaded from the public repository and verified by a sender before sending an encrypted message to the respective receiver in case of the following transmissions:
   a. from Betty at UVA to Tom at GMU,
   b. from Shilpa at GMU to Chandu at UF?

Please use notation introduced in slides for Lecture 3 to denote certificates.

Hint: The correct answers for case 1) are substantially different than correct answers for case 2)

3. How many public key operations (encryptions, decryptions, signature generations, signature verifications) need to be performed by the sender and the receiver in each of the four aforementioned cases: 1a, 1b, 2a, 2b?

Assume that Certificate Revocation Lists (CRLs) are issued separately by each Certification Authority, and cover only certificates issued by the respective CA.

Certificates and CRLs are issued separately by each Certification Authority, but are stored in a single public repository.

4. What are the possible ways of minimizing the number of certificates that need to be
   a. verified by receivers in case 1), and
   b. verified by senders in case 2) ?

Problem 3

Explain why public key of the Certification Authority needs to be given to each user during registration, instead of being distributed through a public network as a part of a self-signed certificate including the name and the public key of the Certification Authority signed by the private key of the Certification Authority.
Problem 4 (bonus)

Demonstrate graphically an active attack against the following protocol:

1. A sends to B
   
   (A, E(\text{PU}_B, M), B)

2. B sends to A
   
   (B, E(\text{PU}_A, M), A)

The attack should break the following security services attempted to be implemented by this protocol:

C - Confidentiality
AR - Authentication of the Receiver.

Hint:
Assume that

- the receiver knows the identity of the sender only based on the contents of the data stream received in the first step of the protocol
- an attacker can be a valid user of a network.