Thursday, February 4, 2010 M2-NT, Spring 2010

Time: 6:00 PM – 9:00 PM Open textbooks and notes

Midterm Exam

**G50 - Network Security**

1. **Kerberos Authentication System (2.5 points)**
   1. *(1 point)*

We investigate the possibility of usurping a Kerberos 5 client's ticket. Consider a pirate who sniffs the network and sees the ticket that the ticket granting server (TGS) sends to the client (C). The pirate also knows the identity of the client to whom the ticket is destined. What prevents the pirate from using the ticket to obtain the service in place of the legitimate client?

* 1. *(1.5 points)*

In the Kerberos 5 authentication system, the symmetric key used by the client (C) and the authentication server (AS) is the hash of the client's password. The server thus has a list of the hashes of all the passwords. If a pirate manages to steal this list, can he authenticate himself as if he were a client? If not, why? If not, what could be done to eliminate this problem?

1. **Distribution of Public Keys (3 points)**

Security for public-key distribution can be achieved by maintaining a directory of public keys. Maintenance and distribution of the directory have to be the responsibility of a central authority. In such a scheme, the authority maintains a directory with a {identifier, public key} entry for each participant. Each participant registers a public key with the authority. Registration has to be in person or by some form of secure authenticated communication. Each participant reliably knows a public key for the authority, with only the authority knowing the corresponding private key.

* 1. *(1 point)*

Consider the following public-key distribution scheme.

A → Public-key authority : *IDB*

Public-key authority → A : auth{*KUB*}

A sends a message to the public-key authority containing an identifier of B to request for B's public key. The authority responds with B's public key *KUB* signed with the authority's private key.

If an adversary succeeds in obtaining or computing the private key of the public-key authority, then how can he compromise the security of participants' public keys?

* 1. *(2 points)*

Stronger security for public-key distribution can be achieved by providing tighter control over the distribution of public keys from the authority with the following scheme.

A → Public-key authority : *IDB*

Public-key authority → A : auth{*KUB*}

A → B : E*KUB*[*IDA* ║ *NA*]

B → Public-key authority : *IDA*

Public-key authority → B : auth{*KUA*}

B → A : E*KUA*[*NA*]

where, *IDA* and *IDB* are identifiers of A and B respectively, *KUA* and *KUB* are public keys of A and B respectively, *NA* is a nonce generated by A to identify the transaction uniquely.

In this scheme, if an adversary succeeds in obtaining or computing the private key of the public-key authority, can he compromise the security of B's public key? Why?

1. **PGP Deployment (3 points)**

Alice, division manager of the company Tareek, must regularly provide an activity report to Tareek's CEO. For this, the latter recommends to all of the managers of the company to use PGP in order to encrypt and sign all transmitted data. After having installed PGP on her computer, Alice generates a pair of asymmetric keys (public key/private key) for data encryption and signature. She keeps a pair of keys only on her computer's hard disk.

* 1. *(1 point)*

Suppose that Alice and the CEO have exchanged their public keys in a secure manner. Alice wishes to send her activity report to the CEO. She encrypts the file but forgets to sign it. Amazingly, PGP does not ask her for any password. Why?

* 1. *(1 point)*

Given that asymmetric encryption systems are much slower than symmetric encryption systems, PGP does not directly use the recipient's public key to encrypt data. Explain the procedure used by PGP.

* 1. *(1 point)*

Satisfied with PGP's services, Alice also wants to use it to encrypt her hard disk backups: she encrypts her directory with PGP and saves the file obtained on a magnetic tape. What risk does she faces if her hard disk crashes?

1. **S/MIME Functionality (1.5 point)**

Why does S/MIME include a public-key certificate in *signedData* messsages, whereas this isn’t the case in *envelopedData* messages?

1. **IPSec Security Association (3 points)**

Draw the format of the IPv4 IPSec packets as transmitted by a remote host to a workstation behind the firewall of an organization. IPSec is implemented on all theses three devices (remote host, workstation, and firewall). The remote host establishes a tunnel mode security association to the firewall to provide limited traffic flow confidentiality. Data origin authentication and data confidentiality are supported by means of a transport mode security association between the remote host and the workstation. Are the given packets protected against data modification and replay attacks? Explain.

1. **Oakley Key Determination Protocol and ISAKMP (3 points)**

Rewrite the X.509 three-way authentication procedure so that it corresponds to the ISAKMP authentication only exchange. Indicate which parameters in each message go in which ISAKMP payload types.

1. **SSL/TLS (4 points)**

Consider the SSL Handshake Protocol. Suppose that the Ephemeral Diffie-Hellman key exchange method is used. The client needn’t send a *CertificateVerify* message to the server to prove its identity.

* 1. *(1 point)*

Draw the message exchange expected for this scenario.

* 1. *(3 points)*

Draw the format of the TCP segments exchanged between the client and the server during phases two and three.