CS 4476(5413) FINAL EXAMINATION

April 11th, 2007

Duration: Three hours

Name:

Student Number:

Note. Each student is asked to solve 10 problems. All the students should solve 3 problems in Set A. For students of CS 4476, choose 4 problems in Set B, 3 problems in Set C. For students of CS 5413, choose 3 problem from Set B, 4 problems from Set C. If you have chosen more than 10 problems, please indicate which of the problems you want to be marked. This examination set has total 17 pages. Check the pages before you start to solve problems.

Set A

Problem 1.

Suppose $q = 11, p = 67, \alpha = 3$ and $\beta = \alpha^2 \pmod{67}$. For $x = 4$, select a random number k and compute (γ, δ) as follows.

$$\begin{aligned} \gamma &\equiv (\alpha^k \pmod{67}) \pmod{11}, \\ \delta &\equiv (x + 2\gamma)k^{-1} \pmod{11}. \end{aligned}$$

Problem 2.

Answer the following questions.

1. Use examples to explain that sometimes we need a hash function to have collision free property, but sometimes we just need it to be a one-way function.

2. In SET, what certificates should the merchant possess and what certificates should the merchant check?

3. What is the main difference between a macro virus and a logic bomb.

4. Why a tunnel mode of IPSec can be used to prevent IP spoofing attacks?

Problem 3.

The packet filtering rules for a firewall are as in the following diagram.

rule	action	src	port	dest	port	flag
1	block	hecker.com	*	*	*	
2	allow	{ our hosts}	*	*	*	
3	allow	*	*	*	*	ACK
4	allow	*	*	{ our GW}	*	
5	allow	*	*	*	> 1024	
6	block	*	*	*	*	

Answer the following questions.

1. Is this a stateful or stateless filtering?.

2. Suppose the mail server port is 25. Can we receive and send emails?

3. If the rule 1 and rule 4 are exchanged, then what kind of traffic control rules will be changed?

Set B

Problem 4.

Signature schemes and HMAC are used for message authentications. In PGP, a signature scheme is used. Can we use the HMAC instead of the signature scheme in secure email systems? If yes, then explain how to do that. If no, then explain why.

Problem 5.

(1) Why Radix-64 can change a binary file to a printable file?

(2) What are the advantages and disadvantages to use Radix-64 in a secure email system?

Problem 6.

The structure of a public-key ring is as follows.

Time-stamp	Key ID	Public key	Owner trust	User ID	Key legitimacy	Signa-tures	Signature trusts
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Explain the contents and purposes of following fields: Time-stamp, Key ID, Signatures, Signature trusts.

Problem 7.

In SSL, a pre_master_secret is used. To establish a pre_master_secret, two methods can be used. One uses the RSA system, the other used Diffie-Hellman key exchange. Explain a clint and a server how to establish the pre_master_secret using two methods. Explain why the pre_master_secret is not decided by one party even an RSA system is used.

Problem 8.

What are the differences between a transport mode and a tunnel mode when AH or ESP is used in IPSec? Use examples to explain when we need to use a transport mode and when we need to use a tunnel mode.

Problem 9.

What is a signature based Intrusion Detection? What is the advantages and disadvantages of this method comparing to the statistical anomaly detection?

Problem 10.

Resident virus can be divided into fast infection and slow infection types. Explain what are the differences between these types and what different damages they will make.

Set C

Problem 11.

In a secure email system, A sends a message M to B. Consider the following two methods:

1. $e_K(zip(Sig_A(H(M))||M)$
2. $zip(e_k(Sig_A(H(M))||M)$

where Sig_A is A's signature, H is a secure hash function, zip is a compression function and $e_K()$ is a block cipher. Which method is better to send the email? Explain why.

Problem 12.

Suppose we use the following key exchange in IPSec:

(1) $I \longrightarrow R : KE; NONCE; IDi$

(2) $I \longleftarrow R : KE; NONCE; IDr$

(3)* $I \longrightarrow R : AUTH$

where I is initiator, R is responder, KE is key exchange payload, $NONCE$ is nonce payload, IDi and IDr are identification payload, $AUTH$ is generic authentication payload (CERT, HASH, SIG etc). * means the payload is encrypted. Are there any problems for this exchange? How to fix it?

Problem 13.

Suppose both Alice and Bob have RSA public key systems. If Alice and Bob use the following method to establish a session key:

- $A \rightarrow B : Sig_A(E_B(K_1))$
- $A \leftarrow B : Sig_B(E_A(K_2))$
- The session key is $K = K_1 \oplus K_2$

Here Sig_A is Alice's RSA signature, E_B is Bob's public key encryption, etc., K_1, K_2 are random numbers. Is this method secure? If not secure, then indicate how to improve.

Problem 14.

A dual signature DS in SET is defined as follows.

$$DS = Sig_K(h(h(\texttt{PI})||h(\texttt{OI}))),$$

where h is a hash function, Sig_K is customer's signature, PI is customer's payment information, OI is customer's order information. If we change the signature to be

$$Sig_K(h(\texttt{PI}))||Sig_K(h(\texttt{OI})),$$

then does it work? Explain why.

Problem 15.

A company FSI needs to design a firewall for its computer system. The system has the following requirements:

- There is a database SDA and a print server which only can accessed by users inside the company.
- There is a web pages WP (TCP port 80) which should allow public access.
- There are an SSH server (TCP port 22), an e-mail server (TCP port 25) in the system.

Design a firewall system for FSI. Explain why you design in that way.

Problem 16.

Suppose a local area network (for example, the LU's network) needs to establish an anti-virus system. Give the main ideas about how to design such a system.