Introduction to Computer Security, exercise 5, February 23-25, 2011

1. Examine what the standard
   NIST SP-800-88 (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)
   says about cleaning hard disks and other memories. What kind of techniques are in use? Is it always necessary to overwrite many times in order to quarantee that the memory has been cleaned?

2. Examine the certificate lists of Internet Explorer and Mozilla Firefox. How many certificate authorities do they contain? Are there differences? How many of the authorities do you know?

3. Examine some certification revocation lists of Verisign. How large are they? (Google verisign crl, save some of the crl files. You can watch them, for example, with command openssl crl -inform Der -text -noout -in tiedosto.crl)

4. One approach to defeating the tiny fragment attack against firewalls is to enforce a minimum length of the transport header that must be contained in the first fragment of an IP packet. If the first fragment is rejected, all susequent fragments can be rejected. However, the nature of IP is such that fragments may arrive out of order. Thus, an intermediate fragment may pass through the filter before the initial fragment is rejected. How can this situation be handled?

5. SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following ruleset:

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

   a) Describe the effect of each rule.

   b) Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown:

Packet	Dir	Src Addr	Dest Addr	Prot	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

Indicate which packets are permitted or denied and which rule is used in each case.

c) Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.1.1	TCP	8080	?
6	Out	172.16.1.1	10.1.2.3	TCP	5150	?

Will the attack succeed? Give details.

6. Consider the following simple protocol, where A sends an encrypted message M to B using public key cryptography.

   (a) $A \longrightarrow B$: $(A,\ E(PU_B, [M, A]),\ B)$

   (b) $B \longrightarrow A$: $(B,\ E(PU_A, [M, B]),\ A)$

   Thus A sends a message to B and the message contains sender and receiver in plaintext plus message M and sender A encrypted by B's public key. B acknowledges in the same way. Simplify the protocol as folow an attackerlows:

   (a) $A \longrightarrow B$: $(A,\ E(PU_B, M),\ B)$

   (b) $B \longrightarrow A$: $(B,\ E(PU_A, M),\ A)$

   Thus a sender is no more in the encrypted part. Now an attacker can decrypt M, if he can listen to the data traffic and he also has a public key. How?