University of Haifa Winter Semester – 11/1/12

Computer and Network Security – Exercise no. 4

Submit in Pairs/Single to mailbox 19 by 25/1/12, 2:00 p.m.

1. Following the sensitivity of the information in its network, the Tax Authority has decided to defend its network using a stateless packet filter firewall. The network, whose IP address is 112.98.⋆.⋆, is used by the three departments of the Tax Authority: the IRS, the health tax department, and the IT department. Each of these departments has a different subnet (IRS being 112.98.1.⋆ and 112.98.2.⋆, the health tax department being 112.98.3.⋆, and the IT department controlling all the other IPs).

   The IRS has a web server hosted on a webserver named IRS-WEB at 112.98.5.5, and the tax authority has a webserver named Health-WEB at 112.98.5.6. Additionally, the IT department maintains an information server called WEB at 112.98.5.100.

   The following requirements are given:

   - Everybody can access the WEB server (both internal and external users) using HTTP.
   - Everybody (but the IT department) can access the IRS-WEB server using HTTP and HTTPS.
   - Everybody (but the IRS) can access the Health-WEB server using HTTPS.
   - The IRS people can access IRS-WEB using SSH.
   - The IT department is allowed to surf any website outside the company, besides the head of the IT department whose IP is 192.98.100.100 who is not allowed access to the WEB server.
   - IRS people can surf only to the ministry of finance' servers at 145.12.45.68.
   - The health tax department can access passive FTP with any server in the world.
   - A special application allows people submitting their tax reports online. The application connects the user to the IRS-WEB server in https, and after pressing the "submit" button, the IRS-WEB server connects using a special protocol running over port 9811 to a special server called IRS-DATA (with IP 112.98.1.2) to transfer the information to the IRS people.

   Any communication which is not specified above is strictly prohibited.

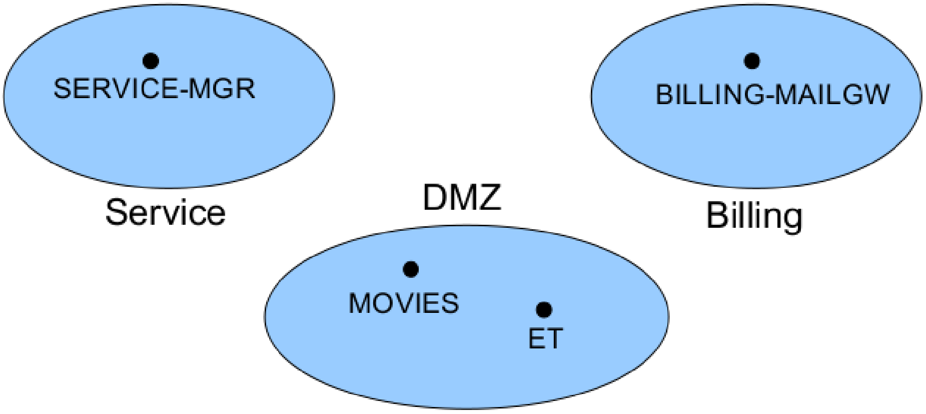
   (a) Devise the structure of the Tax Authority network, taking into consideration that the IRS people do not want the IT department to easily access their computers. Mark exactly the location of the three servers (IRS-WEB, Health-WEB, and WEB), as well as the location of the firewall(s) you use.

   (b) Given the security requirements, fill the firewall rules of the firewall at the entrance to the Tax Authority. You can use the firewall rules file on the course's website.

(c) Given the security requirements, fill the firewall rules of the firewall at the entrance to the IRS' subnet. You can use the firewall rules file on the course's website.

(d) It was claimed that the current configuration is insecure as the Health Tax department people are allowed to connect essentially to any server. Offer a simple solution that improves the security of the network as much as possible.

2. The following question deals with the following network:



The network is composed of two subnets, and a DMZ. In the DMZ, the server MOVIES allows users from all over the world to connect using HTTP and HTTPS to view movies they have paid for. Each movie viewing requires a payment phase that must be protected using HTTPS.

The billing department can connect to the MOVIES server using HTTPS to view the logs of payment, and to issue receipts. The receipts are then sent using email to the users using the mail gateway BILLING-MAILGW, which then sends the receipts out to the users.

The service department can connect to the MOVIES server using SSH. It is also possible to call the service department using a special Voice over IP application, which runs on UDP port 543 on the server ET. The Voice over IP server on the ET server then connects to the relevant employee in the service subnet (connecting to the employee's "server" which runs at UDP port 543).

Besides these communications, no other communication is allowed.

(a) Given the price list of the various security devices:
- Stateless Packet Filter (two subnets) — 2,000$,
- Stateless Packet Filter (three subnets) — 3,500$,
- Stateful Packet Filter (two subnets) — 4,000$,
- Stateful Packet Filter (three subnets) — 7,000$,
- Proxy Server — 6,000$.

Design the company's network to be as secure as possible using a budget of at most 16,000$. Explain your design, and why it offers the best possible security in the allocated budget.

For each security device, you also need to define its functionality.

(b) It was found out that a worker in the billing department was using the BILLING-MAILGW to send spam about his work as a security consultant. What changes to the network are required to prevent the user from doing so? What is the expected price of the new system?

(c) What changes will you need to do in your network design if we want the service department's manager to connect to his desktop SERVICE-MGR from home using SSH in IPsec in transport mode, assuming that there is no additional budget. Will the changes to the network you suggest can risk other computers in the network?

(d) Repeat the previous question, this time, assuming the manager is using IPsec in tunnel mode with an IPsec gateway which is found in the DMZ (which strips the packet, and allows it to continue unencrypted to the SERVICE-MGR computer).

3. (a) When gateways operate IPsec in tunnel mode, they add a new IP header with the IP address of the gateways instead of the original ones.

   i. Why a new header is needed?

   ii. Will an IPsec version where the original IPs are used in the new header (instead of the gateway's ones) would work? If yes, show what are the advantages of this approach, otherwise explain what fails, and why this approach cannot work.

   (b) Due to the fact that packets may get lost, TCP resends packets. Assume that a packet from the designated sender has reached the designated receiver. This packet was sent using transport mode in AH, and was authenticated successfully. Then, the IPsec of the receiver has received yet another packet which may be a re-send of the previous packet or a forged packet being replayed. Note that IPsec must drop the packet if it was sent by an adversary, but forward it to the next layer if the packet is valid.

   Explain how the receiving IPsec layer can distinguish between a re-sent packet by the TCP layer of the legitimate sender or a malicious packet sent by the adversary. Analyze the following cases:

   - A replay by the TCP layer of the legitimate sender,
   - A replay by an adversary who does not change the packet,
   - A replay by an adversary who does change the packet,

In the following questions, various changes to the IPsec protocol are suggested. For each such change, explain whether the new protocol is secure (if yes, explain why, otherwise show an attack that was not applicable to the original IPsec but can be used now) and efficient. All the changes are independent of each other.

(c) In ESP with encryption (using a real cipher) and authentication, only the TCP/UDP headers and the datagram will be encrypted and authenticated. In other words, the encryption will be done the same, but the authentication data will be computed only the encrypted datagram.

(d) In ESP with encryption (using a real cipher) and authentication, the sequence number will be encrypted as well. There is no change to the authentication process.

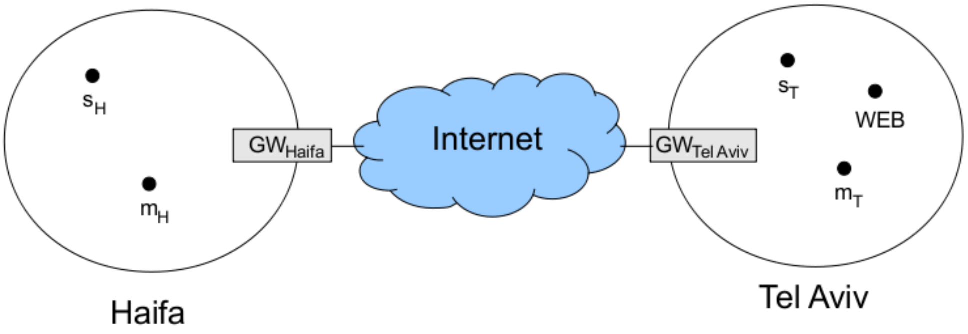
(e) In AH, only the source IP will be authenticated (whereas the destination IP will be assumed to be zero for the computation of the authentication data).

(f) The decapsulation process will be altered as follows: Once a packet is decrypted using the SA pointed to by the SPI, we shall encapsulate the packet again according to the rules of the SPD, and check whether the outcome is the same as the received packet. If so, the packet will be forwarded to the next layer, otherwise the packet will be dropped.

Explicitly, the new decapsulation process will be:

i. Obtain the SA pointed out by the SPI (denoted by SA_1).
ii. Check that the sequence number in the packet matches SA_1.
iii. Check that the authentication data is correct.
iv. If any of the two tests fail, drop the packet.
v. If needed, decrypt the packet using the key in SA_1.
vi. Ask the SPD for the SPI corresponding to the decrypted message, and denote the corresponding SA by SA_2.
vii. Encapsulate the packet according to SA_2 by using the IV and the sequence number from the packet.
viii. Compare the newly formed packet with the original one. If they match, forward the packet to the next layer. Otherwise, drop the packet.

4. The following question deals with the following network:



Note that the Haifa network contains also GW_{Haifa} and the Tel Aviv network contains also $GW_{\text{Tel Aviv}}$.

The security policy with respect to these networks is as follows:

- Any communications between s_H and s_T is allowed in IPsec in transport mode (using ESP with encryption and authentication).
- The above communication does not need to be protected with tunnel mode between GW_{Haifa} and $GW_{\text{Tel Aviv}}$.
- Machines in the Haifa network can connect to any machine in the Tel Aviv network using SSH. This communication is to be encrypted and authenticated by tunnel mode between GW_{Haifa} and $GW_{\text{Tel Aviv}}$.

- Machines in the Tel Aviv network can finger (TCP, port 79) any machine in the Haifa network. This communication is to be authenticated (not encrypted) by tunnel mode between GW_{Haifa} and $GW_{\text{Tel Aviv}}$.
- Machines from the Haifa network are allowed to send emails to any machine in the world. This communication is not protected by IPsec.
- Everyone in the world can access the HTTPS server of the Tel Aviv network WEB. This communication is not protected by IPsec.
- Everyone in the world, except s_H can access the server WEB with DNS queries (UDP, port 53). This communication is to be encrypted (but not authenticated) when the source machine is in the Haifa network, otherwise it is not protected by IPsec.
- Any other communications is not allowed.

(a) Write the Incoming/Outgoing SPDs for GW_{Haifa} that implement the above security policy, taking into consideration the SADs given at the end of the question. You may use the SPD tables found on the course's website.

(b) Given GW_{Haifa}'s SADs, write the SADs of $GW_{\text{Tel Aviv}}$. You may use the SAD tables found on the course's website.

(c) The following packets were sent from the Haifa network to the Tel Aviv network:

i. A finger query from s_H (port 9822) to s_T (port 79).
ii. A DNS query from s_H (port 3922) to s_T (port 53).
iii. An SSH packet from m_H (port 2334) to m_T (port 22).
iv. An HTTPS packet from m_H (port 29011) to WEB (port 80).

For each such packet show how they look when they leave GW_{Haifa} to the internet. If the packet is protected by IPsec, give in the IPsec header the relevant SPI.

GW_{Haifa}'s Incoming SAD

SPI	Source	SA
12	$GW_{\text{Tel Aviv}}$	Enc-Alg: AES-256-CBC, Enc-Key: k_1 Ver-Alg: null, Ver-Key: —
25	$GW_{\text{Tel Aviv}}$	Enc-Alg: AES-128-CBC, Enc-Key: k_2 Ver-Alg: HMAC-MD5, Ver-Key: k_3
32	$GW_{\text{Tel Aviv}}$	Enc-Alg: null-cipher, Enc-Key: — Ver-Alg: HMAC-SHA1, Ver-Key: k_4

GW_{Haifa}'s Outgoing SAD

SPI	Destination	SA
10	$GW_{\text{Tel Aviv}}$	Enc-Alg: AES-128-CBC, Enc-Key: k_1^* Ver-Alg: HMAC-MD5, Ver-Key: k_2^*, SPI 51
15	$GW_{\text{Tel Aviv}}$	Enc-Alg: AES-256-CBC, Enc-Key: k_3^* Ver-Alg: null, Ver-Key: —, SPI 92
58	$GW_{\text{Tel Aviv}}$	Enc-Alg: null-cipher, Enc-Key: — Ver-Alg: HMAC-SHA1, Ver-Key: k_4^*, SPI 37