Security Applications in Networking and Distributed Systems

Examination - Answers

June 2017

Remarks:

The exam is closed books and notes. You are allowed to keep a single sheet of paper with handwritten notes. The duration is 2 hours.

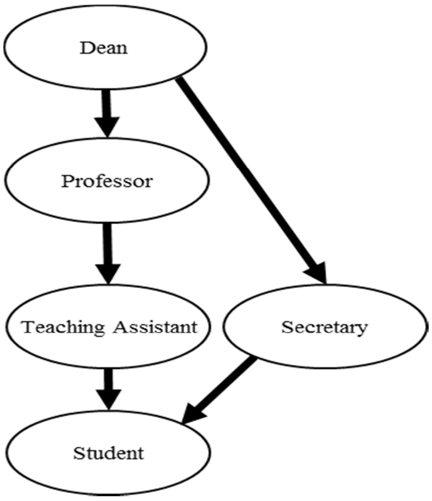
Write your name on every sheet you return. Answer in English or in French.

The answers should be concise but supported by a brief explanation.

The total number of points is 32.

Q1 (4 Points)

Let's imagine a simple access control scenario based on a role hierarchy as shown in the following diagram:



Let's suppose that each user can be granted some permissions according to the role he/she is assigned as summarized by the following table:

ROLES	PERMISSIONS
Student	(read, course); (read, schedule); (read, grade); (read, registration)
Teaching Assistant	(write, course)
Secretary	(write, schedule); (write, registration)
Professor	(write, grade)

In addition to the permissions shown in this table, each role also inherits permissions of the lower ranked roles as shown in the hierarchy.

a) Which access control model would be the most suitable one to represent this policy?

b) Which XML-based standard would be suitable for implementing the user-role relation?

Let Bob, Alice, and Joe be three users with the following role assignments:

(Bob, Professor) , (Alice, Secretary), (Joe, Teaching Assistant).

c) Among these three users which ones are authorized to perform the following operations?

- update courses

- update the schedule

- set grades

- update registration files

d) Can a user assigned with the role "Dean" read the grades, update the schedule, or read and update registration files?

Give a brief explanation for each answer.

Answer:

a) RBAC because of the natural mapping of roles in real life to the ones in the access control model.

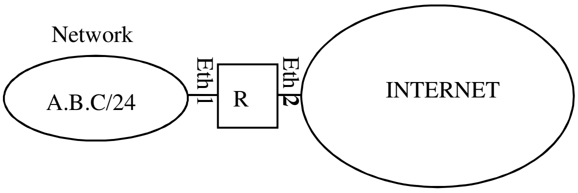
b) SAML and its attribute statement.

c) Bob and Joe can update the courses, Bob inherits the right from Teaching Assistant role. Only Alice can update the schedule and registration files, based on her role as a secretary that is granted the permissions (write, schedule) and (write, registration). Only Bob can set grades, based on his role as a professor that is granted the permission (write, grade).

d) Yes, because this role inherits all the permissions.

Q2 (3 points)

The figure below depicts a private network connected to the Internet through an edge router R.



IP spoofing denotes an attack feature that consist of sending packets bearing randomly chosen source IP addresses for various malicious purposes such as denial of service at the destination.

a) Which filtering rules should be implemented in R in order to prevent some of the IP spoofing attacks? Answer using the *iptables* notation as in the following sample ruleset and comment the rules by stating their purpose:

# The following ruleset assures that . . .

```
iptables –F FORWARD
iptables –N FORWARD
iptables –P FORWARD DROP
iptables –A FORWARD –I Ethy –d y.y.y.y/ DD –s x.x.x.x/DD –j ACCEPT
. . . . . . . .
. . . . . . . .
```

b) What are the limitations of this approach? (which IP spoofing attacks cannot be detected using it?)

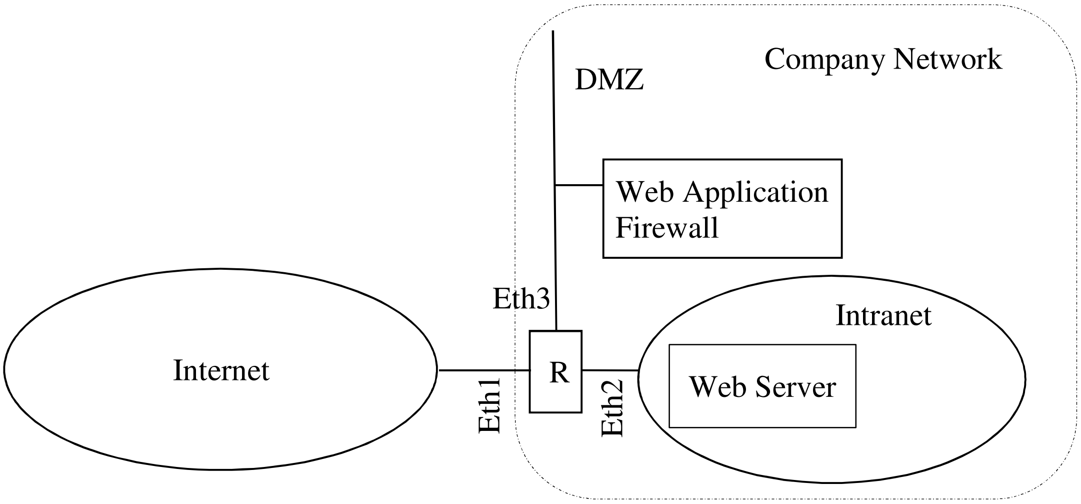
Answer:

a) Some IP spoofing attacks originating from Network can be detected using the following ruleset:

```
iptables –F FORWARD
iptables –N FORWARD
iptables –P FORWARD DROP
iptables –A FORWARD –I Eth1 –s A.B.C/24 –j ACCEPT
iptables –A FORWARD –I Eth2 –s !A.B.C/24 –j ACCEPT
```

b) Limitations of this technique are: 1) a node in Network that impersonates another node from the same network cannot be detected. 2) majority of IP spoofing attacks originating from the Internet without using the addresses of Network cannot be detected.

Q3 (7 points)



The figure above depicts a simple network interconnection scenario whereby

- three IP addresses (192.125.1.100, 192.125.1.200, 192.125.1.250) are allocated to the Company Network

- R is a router and a packet filter based on iptables equipped with the (stateful) netfilter package and the network address translation (NAT) package

- interface Eth3 of R is connected to a Demilitarized zone (DMZ)

- a Web Application Firewall (WAF) runs on a host located in the DMZ and identified by the IP address 192.125.1.100

- the port number for HTTP is 80

- a Web Server runs on a host located inside the Intranet.

The security policy governing this network is summarized by the following statements:

- Hosts located within the Intranet are authorized to initiate connections and to communicate through those connections with hosts located in the Internet using the application protocol identified by TCP port number Q.

- Hosts from the Internet are authorized to initiate connections and to communicate through those connections with the Web Server using HTTP.

- HTTP traffic between the Internet and the Web Server must be screened by the WAF.

- All traffic across router R that is not explicitly authorized by the statements of this policy must be blocked.

Answer the following questions by keeping in mind the goal of enforcing this security policy:

a) What kind of IP addresses should be assigned to the hosts located in the Intranet? Specify the address range that would be assigned and select one of these addresses as the IP address of the Web Server.

b) If Web Server is to be used as the public web server of the company, under which IP address should the company's public web server be announced in the Internet through DNS? How does an HTTP request from Internet reach the Web Server? What would be the destination IP address of a request packet transmitted by a web client located in the Internet and the one of the packet that is received by the Web Server?

c) Suggest a set of filtering rules required to implement the abovementioned policy.

Answer:

a) hosts in the Intranet should be assigned private addresses, let 192.168.1.0/24 be the address block used for this purpose and 192.168.1.10 the address of the Web Server

b) WAF's public IP address 192.125.1.100. The traffic from the Internet first reaches the WAF then after screening the traffic, WAF redirects it to 192.168.1.10 on the Intranet. The destination IP addresses in the request packet and in the one received by the Web Server are 192.125.1.100 and 192.168.1.10, respectively.

c)

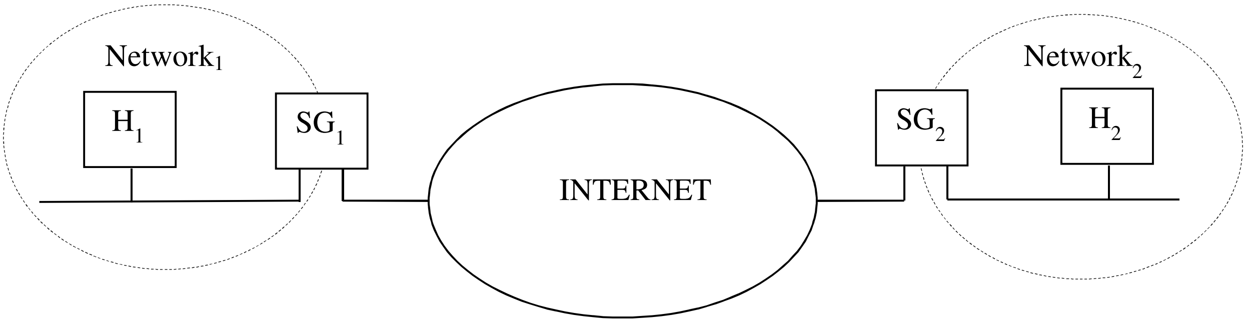
```
iptables –F FORWARD
iptables –N FORWARD
iptables –P FORWARD DROP
```

```
# Hosts from Intranet are authorized to initiate the application protocol identified by TCP port
number Q with hosts located in the Internet
iptables –A FORWARD -i Eth2 -o Eth1 -p tcp -s 192.168.1.0/24 --dport Q -m state
--state NEW,ESTABLISHED –j ACCEPT
iptables –A FORWARD -o Eth2 –p tcp -m state --state  ESTABLISHED –j ACCEPT
# WAF is authorized to establish web connections with Web Server.
iptables –A FORWARD -i Eth3 -o Eth2 -p tcp -s 192.125.1.100 --d 192.168.1.10 --dport 80 -m
state --state NEW,ESTABLISHED –j ACCEPT
iptables –A FORWARD -o Eth3 -i Eth2 -p tcp -s 192.168.1.10 -d 192.125.1.100 -m state
--state  ESTABLISHED –j ACCEPT
# Internet hosts are authorized to establish web connections with WAF.
iptables –A FORWARD -i Eth1 -o Eth3 -p tcp -d 192.125.1.100 --dport 80 -m state
--state NEW,ESTABLISHED –j ACCEPT
iptables –A FORWARD -i Eth3 -o Eth1 -p tcp -s 192.125.1.100  -m state
--state  ESTABLISHED –j ACCEPT
# NAT with port translation for internal hosts identified with a private address.
iptables -nat  -A POSTROUTING -i Eth2 -o Eth1  -j SNAT --to 192.125.1.200
```

Q4 (4 Points)

Network$_1$ and Network$_2$ in the figure below belong to the same organization. The goal is to interconnect the two local networks through the Internet using IPSec protocols in order to achieve a Virtual Private Network as if the nodes in both networks were part of a single private network.

We assume that H$_1$ and H$_2$ are local hosts connected to Network$_1$ and Network$_2$, respectively, and SG1 and SG2 are security gateways equipped with the IPSec protocol suite and connected to both the Internet and the local networks as depicted in the figure.



a) Suggest an addressing scheme by assigning IP addresses to H$_1$, SG$_1$, H$_2$, and SG$_2$ for each of their interfaces as shown in the figure, by taking into account usual network security criteria.

b) State the security associations (SA), protocol type and mode of operation for each SA of the IPSec protocol configuration required to implement the Virtual Private Network scenario.

c) Let's assume that an IP packet carrying transport layer data is transmitted by H$_1$ to H$_2$ using the suggested IPSec solution. What is the structure of such a packet captured at the link between SG$_1$ and SG$_2$? Describe the packet structure using a simple figure whereby the following fields are positioned *without* specifying the details of the fields except where indicated otherwise:

- IP Headers
- IP Addresses in each IP header (specify using the values assigned in a))
- IPSec protocol headers
- Upper Layer Header

and indicate the fields that are protected by authentication and/or confidentiality.

Answer:

a) H$_1$: 192.168.1.1 (private Address)

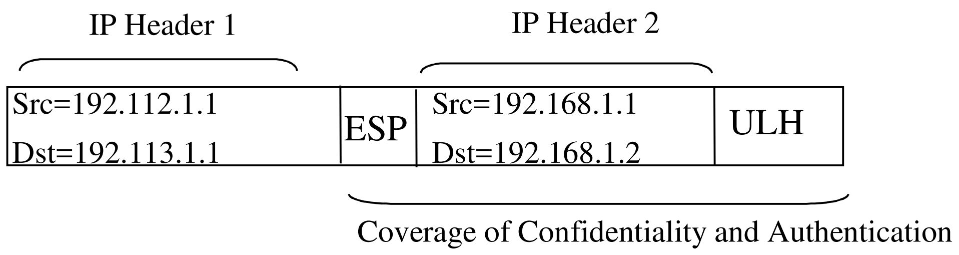
SG$_1$: 192.168.1.10 (private address) and 192.112.1.1 (public address)

H$_2$: 192.168.1.2 (private Address)

SG$_2$: 192.168.1.20 (private address) and 192.113.1.1 (public address)

b) At least one SA with IPSec ESP in tunnel mode between SG1 and SG2.

c)



Q5 (3 Points)

a) Briefly describe the version rollback attack that was feasible with early versions of TLS/SSL.

b) What is the countermeasure adopted in recent versions in order to prevent version rollback attacks?

c) Let's suppose a TLS session uses a ciphersuite including ephemeral Diffie-Hellman key exchange with RSA signatures, how is the pairwise Master Secret (MS) computed by each party? Briefly describe using simple expressions with function types (pseudo-random function,hash function, encryption, etc.) and input parameters (keys, nonces, etc.).

Answer:

a) Using the version rollback attack, the attacker fools one of the parties to switch to a version of TLS/SSL that is known to be weak, then it actively exploits some of those weaknesses.

b) The Finished message including the keyed hash of all the handshake messages exchanged for the establishment of the current session.

c) MS = pseudorandom_function($g^{\text{client's exponent x server's exponent}}$, Ns, Nc)

Q6 (2 Points)

Let's suppose a web-based secure electronic banking application through which each customer can access the bank's web site using commonly available web browsers and perform the following operations:

- look up his/her account to read the balance and the details of operations,
- place orders for transferring money to other accounts.

For each of the following security mechanisms, briefly discuss the feasibility of a security solution that would be based on the mechanism and that would meet the requirements raised by this application.

- packet filtering stateful firewall
- TLS/SSL
- IPSec protocols

Answer:

TLS/SSL is the only suitable solution because this is the only one that would be both end-to-end and supported by commonly available web browsers. The packet filter cannot provide end-to-end security and IPSec is not supported by commonly available web browsers.

Q7 (2 Points)

a) Briefly describe the DNS Cache Poisoning Attack and how DNS Security Extensions would prevent it.

b) Do DNS Security Extensions assure Client Authentication for DNS queries?

Answer:

a) Cache poisoning consists in tampering with the information stored as part of a DNS Cache in a malicious way. It is prevented by DNSSEC thanks to the fact that each DNS record is signed when generated and stored in the DNS servers and caches.

b) DNSSEC does not provide client authentication.

Q8 (3 Points)

A common feature of security mechanisms in mobile systems like GSM, UMTS (3G), and further generations of these systems is a proxy scheme whereby the Mobile Terminal (MT) runs a security protocol with a Visiting Location Registry (VLR) that is located in the area that is being visited by the MT. Each MT in turn is permanently registered with a Home Location Registry (HLR) that is located at the home network of the MT and, as part of the registration, the MT and the HLR share a secret key K (usually stored in the SIM card) that is used to perform further security operations like authentication and key distribution.

a) When the MT roams through remote areas, does the MT share its key K with the VLR of each area? What is the rationale behind the option taken by the mobile system standards with respect to this question?

b) Briefly describe the authentication protocol used in this context by simply mentioning the basic parameters like keys and nonces exchanged between parties, the ones known by each party as well as operations performed by each party using these parameters.

Answer:

a) VLR's never get to know the key K. This would be a critical exposure reckoning from the number of areas that can be visited by a single MT.

b) cf. course material.

Q9 (4 points)

a) Explain the main weaknesses of Wireless Equivalent Privacy (WEP) with respect to data confidentiality and data integrity.

b) What are the mechanisms implemented in 802.11i (WPA2) in order to cope with these weaknesses? Briefly mention the name and type of algorithms and operational modes.

c) How is the Pairwise Master Key (PMK) of 802.11i obtained in the enterprise WPA mode and in the personal WPA mode?

Answer:

a) data confidentiality. the set of keystreams will be the same for each different execution of the protocol. Attacker can get parts of k(i) from one execution based on known parts of data by simply x-oring ciphertext with the bits of those known parts of data. Using the parts of k(i) that are thus retrieved, he can then decrypt any further i'th data packet because the same keystream k(i) will be used in further executions. Solution: use a different initial value for the key generation based on some external random source like time and transmit this value in cleartext. data integrity. new (valid) ciphertext can be computed from existing ciphertext without the knowledge of the keystream:

Existing ciphertext $C = k \oplus (M \mid h(M))$

New ciphertext resulting from the targeted modification on M (=x-or with D) :

$$C' = C \oplus (D \mid h(D)) = k \oplus (M \mid h(M)) \oplus (D \mid h(D))$$

$$= k \oplus (M \oplus D \mid h(M) \oplus h(D))$$

$$= k \oplus (M \oplus D \mid h(M \oplus D))$$

b) CCMP with AES algorithm uses counter mode for confidentiality and CBC-MAC for integrity.

c) In enterprise mode, the PMK is the AAA key resulting from the EAP authentication. In personal mode, the PMK takes on the value of the Pre-Shared Key.