Security Applications in Networking and Distributed Systems

Examination - Answers

June 2016

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.

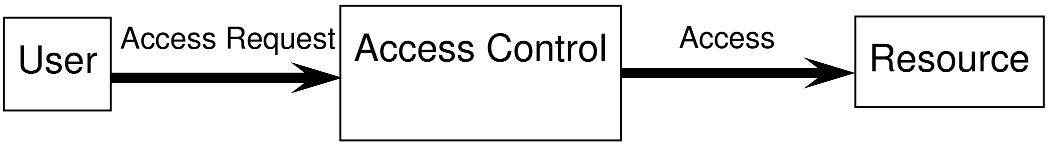
Write your name on every sheet you return. Answer in English or in French.

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

The total number of points is 33.

Q1 (2 Points)

A typical access control scenario can be depicted as follows:



a) The Access Control function shown above usually is subdivided into two basic functional components. Briefly describe them.

b) What is the XML-based standard that encompasses these functional components and their interactions in processing an access request?

c) Which feature of that standard is dedicated to represent the access control matrix?

Answer:

a) These are the access control decision function and the access control enforcement function, cf. course about the description.

b) XACML

c) The Policy.

Q2 (6 Points)

In a sample access control scenario, the access control policy is summarized by the following table:

ROLES	PERMISSIONS
Financial Advisor	P1 (buy, stock); P2 (sell, stock)

Account Rep	P3 (read, deposit), P4 (write, deposit); P5(read, stock)
Teller	P6 (read, deposit)

where

- each row shows the permissions granted to the corresponding role;

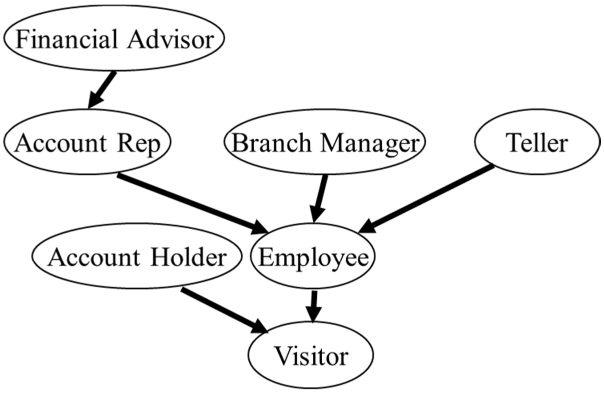
- (buy, stock) (resp. (sell, stock)) represents the authorization to buy (resp. sell) shares on the stock market on behalf of customers,

- (read, deposit) (resp. (write, deposit)) represents the authorization to read (resp. write to) a customer's deposit account

- (read, stock) represents the right to lookup a customer's stock market account without the capability to write (issue transactions).

Employee and Visitor roles that are not shown on the policy table are not granted with any permission on stock and deposit accounts.

In addition to the policy, each user is assigned with one or several roles that he/she is authorized to take and the roles are organized in a role hierarchy as shown in the following diagram:



Let U1 and U2 be two users with the following role assignments:

(U1, Financial Advisor) , (U2, Account Rep).

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

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

c) Is U1 allowed to buy or sell shares on the stock market on behalf of customers?

d) Is U2 allowed to buy or sell shares on the stock market on behalf of customers?

e) Is U1 allowed to read a deposit account?

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) Yes, because U1 bears the Financial Advisor role that has permissions P1 and P2 which allow U1 to buy and sell stock.

d) No, because U2's role assignment as an Account Rep does not grant him with sufficient permission to buy or sell stock and inherited permissions are not sufficient either.

e) Yes, because U1 bears the Financial Advisor role that inherits P3 from the Account Rep role and P3 allows U1 to read the deposit account.

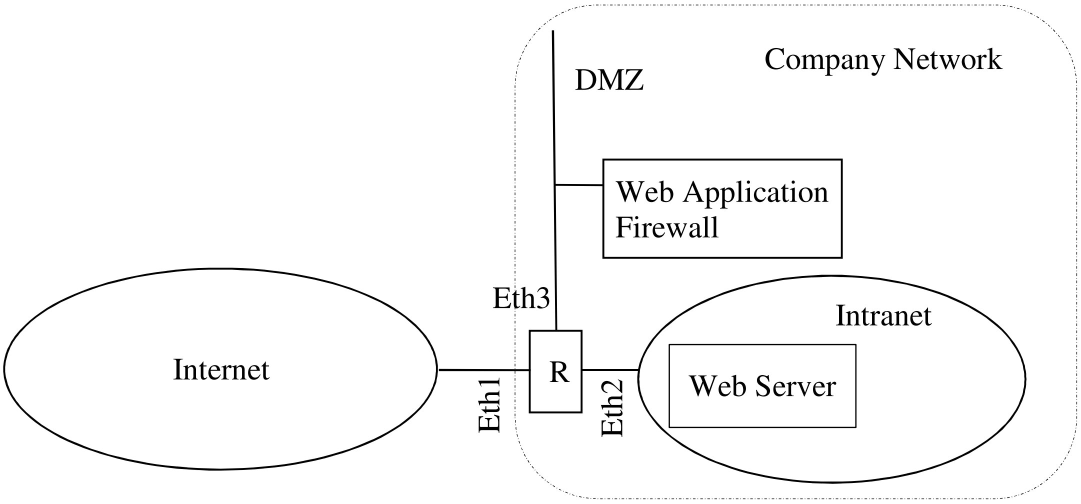
Q3 (1 Point)

Among the two alternative approaches (capability list and access control list) for implementing the basic access control matrix, which one is used by Windows Server Security Architecture? Where is the access control information stored?

Answer:

Access control lists are used as part of Object Security Descriptor s to store the access control information.

Q4 (7 points)



The figure above depicts a simple network interconnection scenario whereby

- address block 192.125.1.0/24 is 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 host 192.125.1.10 located in the DMZ

- 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 Web Application Firewall.

- 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 assigned to the Intranet and select one of this 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 the traffic from the Internet reach the Web Server using this IP address?

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 192.125.1.10. 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.

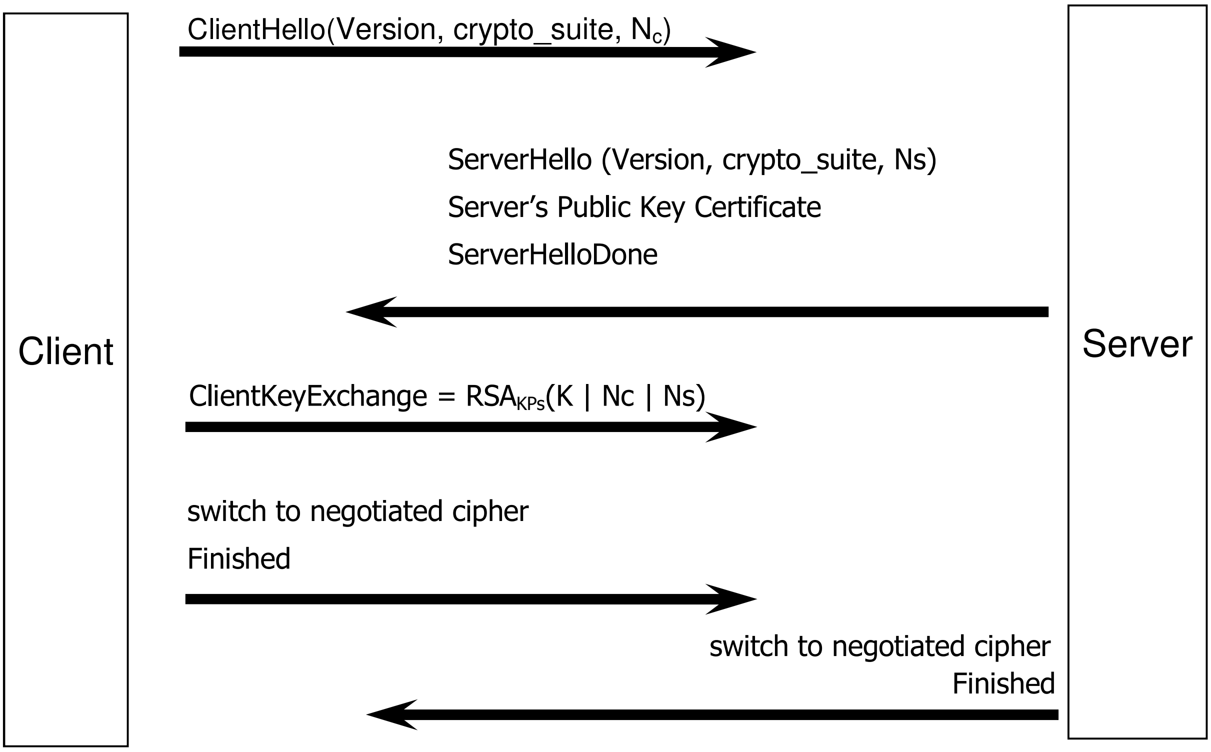
c)

```
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 192.125.1.10 --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 192.125.1.10 -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 192.125.1.10 --dport 80 -m state
--state NEW,ESTABLISHED –j ACCEPT
iptables –A FORWARD -i Eth3 -o Eth1 -p tcp -s 192.125.1.10  -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 192.125.1.20
```

Q5 (4 Points)

The figure below depicts the session negotiation phase of TLS/SSL.


Client
Server
ClientHello(Version, crypto_suite, N_c)
ServerHello (Version, crypto_suite, Ns)
Server's Public Key Certificate
ServerHelloDone
ClientKeyExchange = RSA_{KPs}(K | Nc | Ns)
switch to negotiated cipher
Finished
switch to negotiated cipher
Finished

a) What are the main security exposures with TLS/SSL that exploited this phase of the protocol in early versions? Briefly sketch the attacks that take advantage of these exposures.

b) Which features of TLS/SSL were implemented in further versions in order to prevent these attacks?

Answer:

a) Version rollback attacks, cf. course material.

b) The Finished messages included the signature on the entire negotiation trace to prevent such attacks.

Q6 (4 Points)

Let’s suppose a centralized chat service whereby each message transmitted by a user first flows between the user’s terminal and one of the servers of the chat service which then forwards the message to its destination. We also assume that the users trust the servers but not the third party attackers that might eavesdrop, intercept, and tamper with chat traffic. There is a strong requirement for the chat application software to be clientless in that the users must be able to run the chat client on standard terminals, with no prior installation of software, by using widespread standard tools like web browsers.

a) Briefly state the security services required by this application .

b) Discuss the feasibility of a solution that would meet the security requirements for each of the following scenarios:

1) Each chat server is protected by a packet filtering firewall equipped with some application gateways;

2) The solution is based on TLS/SSL;

3) The solution uses IPSec.

Answer:

a) end-to-end data confidentiality and integrity for chat messages between the users and the servers.

b) 1) Firewalls do not meet the end-to-end requirement.

2) TLS/SSL is the most appropriate solution especially because of the clientless requirement.

3) IPSec would meet the security requirements in principle but the need to integrate resident IPSec endpoint functions on the client side would conflict with the clientless requirement.

Q7 (6 Points)

a) Suggest a secure remote access solution based on IPSec that should allow each remote host to access the company network using Internet as the main connection mechanism. Sketch your solution by describing details such as the protocol type, active components (security gateway, host), modes of operation, security associations, cryptographic keys, key establishment method.

b) What type (private, public) of IP addresses should be assigned to nodes located within the company network and to the remote host?

c) Let’s assume that an IP packet carrying transport layer data is transmitted by the remote host to a host in the company network using the suggested IPSec solution. What is the structure of such a packet captured at the link between the remote host and Internet. Describe the packet structure using a simple figure whereby the following fields are positioned (don’t mention the internal details of each field):

- IP Headers
- Source and Destination IP Addresses in each IP header - indicate the type (public/private) of each address

- ESP or AH headers
- Upper Layer Header (ULH)

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

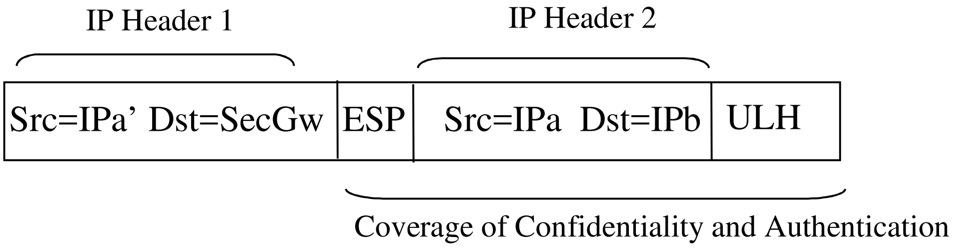
d) Let’s assume that the IP packet in c) is captured further within the company network on the way from the security gateway to the destination local host. Describe the structure of this packet using a simple figure like in c).

Answer:

a) IPSec ESP in tunnel mode. There should be a Security Gateway (SG) between the corporate network and Internet. There should be at least one SA between the SG and the remote host in ESP tunnel mode. IPSec session keys can be derived either from a manually distributed pairwise secret key for each remote host or using the hybrid key distribution method with a pair of private and public keys for each host and the SG.

b) private IP addressing within the company network. The remote host should have a public address and a private address.

c) IPa’, IPa, IPb, and SecGw are the public address of the remote host, the private address of the remote host, the private address of the destination host, and the public address of the security gateway, respectively. The packet is structured as follows:



d)

Src=IPa	Dst=IPb	ULH

Q8 (3 points)

Let’s suppose that wireless terminals can get access to a campus network through various Access Points located inside the campus buildings using the 802.11 protocol. Let’s assume that the network access control on the wireless links is assured based on the 802.1x protocol using a RADIUS Server and the EAP protocol. It is also assumed that only authorized people can get access to the building.

a) What are the security exposures that would not be covered despite the abovementioned security measures?

b) Suggest two alternative security solutions that would protect the communications between hosts connected to the LAN and the wireless terminals against these exposures. State the name and main features of the protocols that are part of the solution and additional components required by the security solution, if any.

Answer:

a) Data exchanged over the wireless link is still exposed to eavesdropping and tampering. So there is no data confidentiality nor data integrity.

b) First solution: IPsec in tunnel mode between the Wireless Terminal and a Security Gateway that would be put in place as a new component. Second solution: WPA or WPA2 on the wireless link.