Security Applications in Networking and Distributed Systems

Examination - Answers

June 2014

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 27.

Q1 (4 Points)

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

USER CATEGORY [maximum population]	AUTHORIZED RESOURCES (rights)
Student [1500]	course (read), schedule (read)
Professor [75]	course (read, write), schedule (read), exam (read, write)
Admin [50]	accounting (read, write), schedule (read, write)

a) Give a list of relations that would be required to represent this policy using Role Based Access Control (RBAC). Relations can be defined by means of tuples such as (subject$_i$, object$_j$, …..), (role$_i$, …..), (subject, role, ….), etc.

b) In this scenario, what is the advantage of RBAC over the classical access control model that is based on a simple (subject, object, right) relation?

c) Briefly suggest a set of security mechanisms (authentication, encryption, ACL, capabilities, attribute certificates, etc.) required to implement this access control policy using RBAC.

d) Among the XML-based security standards discussed during the course, which one would be suitable for implementing the (user, role) relation? Briefly mention the feature of the standard that would be required to implement this relation.

Answer:

a) We get two sets of relations in RBAC :

1- (role, resource, right) relations :

{(Student, course, (read)), (Student, schedule, (read)),

(Professor, course, (read, write)), (Professor, schedule, (read)), (Professor, exam, (read, write)),

(Admin, accounting, (read, write)), (Admin, schedule, (read, write))}

2- (user, role) relations :

{ (user$_i$, Student), (user$_j$, Professor), (user$_k$, Admin)}

b) The main advantages of RBAC over the classical model are the ease of representation for the user categories and the saving in terms of relations that need to be represented (there are only three roles instead of 1625 individual users).

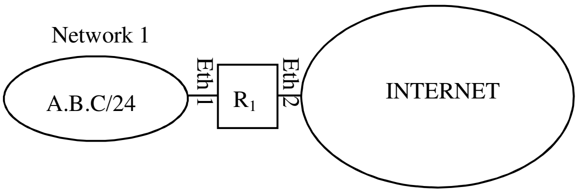
c) the (user, role) relation can be implemented using attribute certificates of the form

(userid, role, validity) signed by the access control authority and the (role, resource, right) relation can either be implemented by attribute certificates in a similar way or in ACLs. In addition to providing the attribute certificates along with each request, the users should authenticate themselves in each request using a digital signature or a MAC using a key shared with the resource owner.

d) SAML and its attribute statement.

Q2 (4 points)

The figure below depicts a private network connected to Internet through an edge router R$_1$.



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$_1$ in order to prevent IP spoofing attacks originating from Network 1?

b) Which filtering rules should be implemented in R$_1$ in order to prevent IP spoofing attacks targeting Network 1? Can all such attacks be prevented using packet filtering?

Answer using the *iptables* notation as in the following sample ruleset:

```
#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
```

Answer:

a) Ruleset for R$_1$

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

b) Ruleset for R$_1$

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

IP spoofing packets that do not carry a source address in Network 1 cannot be detected.

Q3 (1 Point)

What is the built-in chain in iptables that provides Network Address Translation (NAT) in simple port translation mode?

Answer:

POSTROUTING chain.

Q4 (1 Point)

Briefly explain how network isolation can be assured using application gateways such as the Web Application Firewall (WAF)?

Answer:

Cf. course material.

Q5 (3 Points)

a) What is the goal of identity protection in key exchange protocols?

b) Briefly describe a key exchange protocol that achieves identity protection.

c) Cite a key exchange solution among Internet security protocols that implements identity protection during key exchange.

Answer:

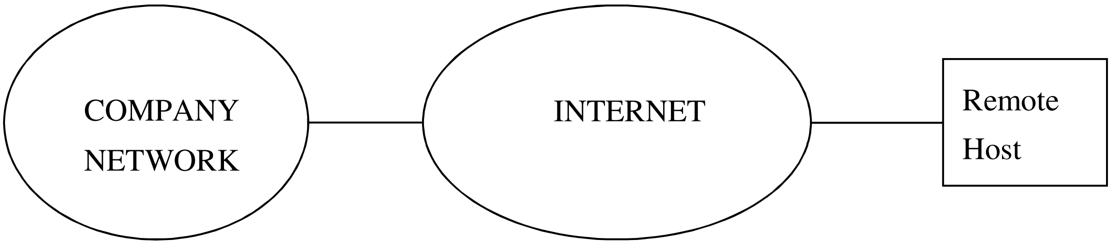
a) A third party that monitors the key exchange between two peers cannot find out about their identities.

b) The parties first run an unauthenticated Diffie-Hellman to establish a session key K, then using K they send each other a signature of the Diffie-Hellman exponents exchanged in the first round. The signature reveals and proves the identity to one another but the third parties cannot retrieve it since it is encrypted under K.

c) Internet Key Exchange (IKE).

Q6 (5 Points)

A company needs to provide a secure remote access solution to its traveling users in the following setup:



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 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.

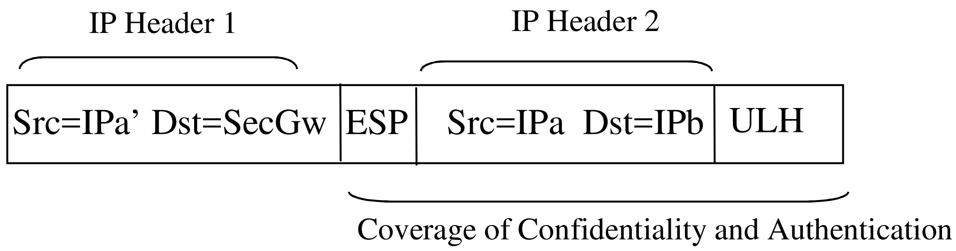
d) Let's assume that the IP packet in c) is captured further within the company network on the way from the security gateway to the destination local host. Describe the structure of this packet using a simple figure like in c).

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

Q7 (2 points)

a) Briefly explain the “version rollback attack” that was feasible on some old version of the TLS/SSL protocol.

b) What was the solution that prevented the attack in further versions of TLS/SSL?

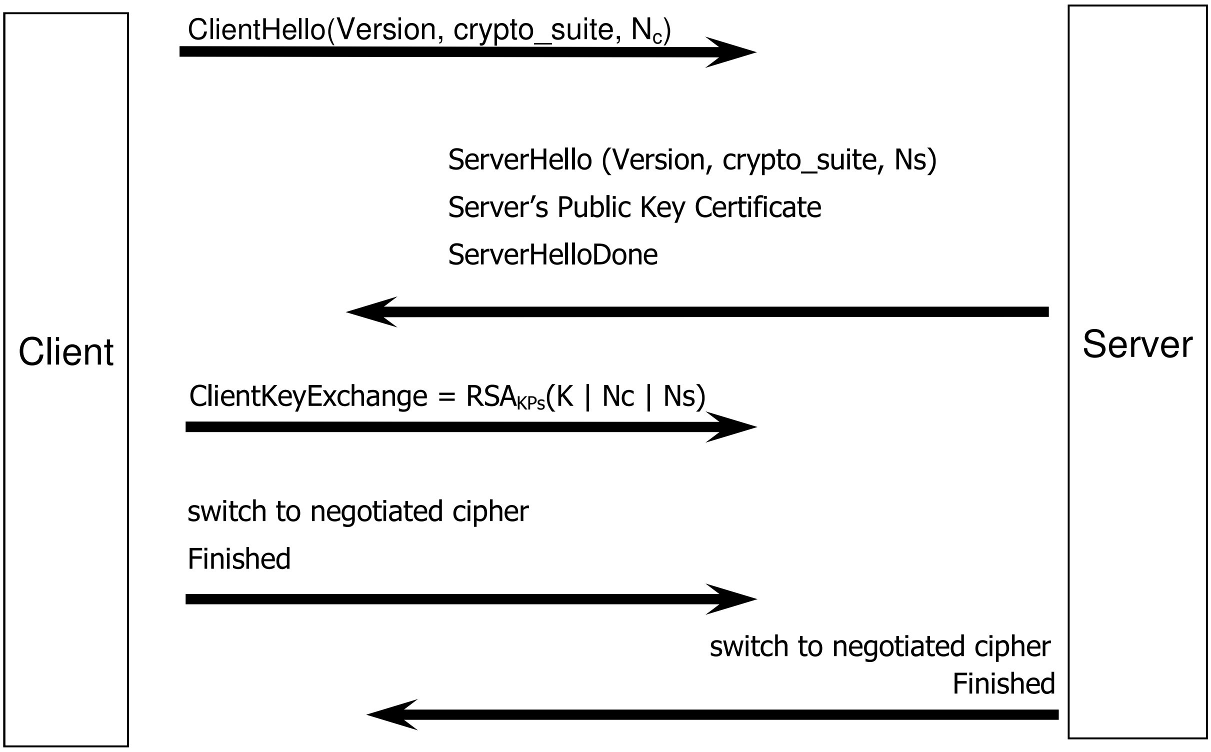
Answer:

a) This attack allowed the attacker to send a modified ClientHello message in which a weak version of the TLS/SSL protocol is offered in the version field. Based on this message the server switched to the weak version and the data exchanges between client and server was then vulnerable.

b) The solution that was suggested in further versions is to exchange the signed trace of all past handshake messages during the closing exchange of Finished messages.

Q8 (4 Points)

The message flows below depict a sample of the handshake protocol using the TLS (SSL) protocol, where Nc and Ns are the nonces generated by the client and the server, respectively, KPs is the public RSA key of the server, and K is a secret generated by the Client.


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) How does the client authenticate the server using this protocol? Briefly state the steps of the verification performed by the client.

b) How can the server authenticate the client using this protocol?

c) How are the data encryption keys and data authentication keys generated?

Answer:

a) The flows allow the client to authenticate the server since if the server is able to further decrypt with the session key, the server must have the private RSA key matching KPs. The private key and KPs are linked to server's id in the public key certificate of the server transmitted in the previous flow. The client must also verify that the server's id in the certificate matches the one used in the protocol flows.

b) The server cannot authenticate the client only based on these protocol flows. The client can authenticate by sending a secret password using the encrypted channel established thanks to these flows.

a) This protocol allows the client and the server to exchange a session key K. Using K, further session keys are derived as follows:

session key = pseudorandom_function(K, Ns, Nc, randomizer)

Q9 (3 Points)

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

- look up his/her account to read the balance and the details of operations,
- place orders in the stock market (sell or buy shares).

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

b) Amid a packet filtering stateful firewall, a solution with security gateways using IPSec, and client-server applications using TLS/SSL which one is the most suitable solution to provide the security services required by this application? Briefly state the rationale for the choice.

Answer:

a) authentication of the customer, confidentiality and integrity of all messages, optionally non-repudiation of the origin for messages sent by the customer.

b) TLS/SSL because this is the only one that would be both end-to-end and supported by clientless terminals on the user side.