Security Applications in Networking and Distributed Systems
Examination - Answers
June 2013

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 31.

Q1 (1 point)

Briefly explain (in a few sentences) the main role of the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP) in XACML.

Answer:

The PEP is in charge of enforcing the access control decision taken by the PDP whereas the PDP takes the actual decision as to whether to authorize the request or not.

Q2 (4 points)

Let's imagine an on-line professional news service (like www.bloomberg.com business news, stock quotes) based on a distributed authorization scheme. The components of the service infrastructure are: several customers, one or several authorization centers, and one or several news servers.

For each of the scenarios below, suggest the most suitable access control technique. Briefly sketch the access control solution for each scenario by stating the flows and the contents of messages exchanged between the components. State details such as keying material, certificates, etc. if any are required for the access control scheme.

a)The service is provided by a single server and there is a single authorization center. Customers get a monthly subscription to read the news.

b)There are several authorization centers and several servers geographically distributed over Internet. Each customer can request any authorization center to get an access right for anyone of the servers. Customers get a monthly subscription to read the news.

Answer:

a) The ACL technique is the most suitable one since the resource is centralized (single server) and updates are not frequent. AC must update the ACL located at S. Each request form C must be authenticated by S either with shared secret keys provided to each authorized customer or using a PKI system that provides a certificate to each customer.

b) capability list (CL) technique is the most suitable because of the lack of centralization for the servers. When the population of the servers is neither small nor under the control of a single organization, management of ACL's for a dynamic user population is too complex.

Using a PKI that provides each customer with a Public-key certificate we get:

C → AC: authorization request (subscription information(payment))

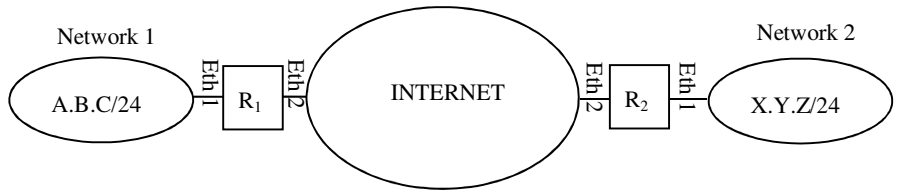
AC → C: CL= (M=(C | expiration_date) E_{KSac}(h(M))

C → S: CL, M=(read request | timestamp), E_{KSc}(h(M))

An alternative solution without a PKI can also be designed by providing C with a secret key as an evidence of its authorization.

Q3 (4 points)

The figure below depicts two private networks interconnected across Internet. R_1 and R_2 represent the edge routers through which each network is connected to Internet.



Edge routers are not part of the private networks and are managed by the Internet Service Providers. Let's suppose that an attacker located in one of the two networks is perpetrating an IP spoofing attack by sending a large number of packets bearing randomly chosen source IP addresses to randomly chosen destinations including the nodes in the other network.

Which filtering rules should be implemented in R_1 in order to block some of the attack packets? 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:

Ruleset for R_1

#iptables –F FORWARD

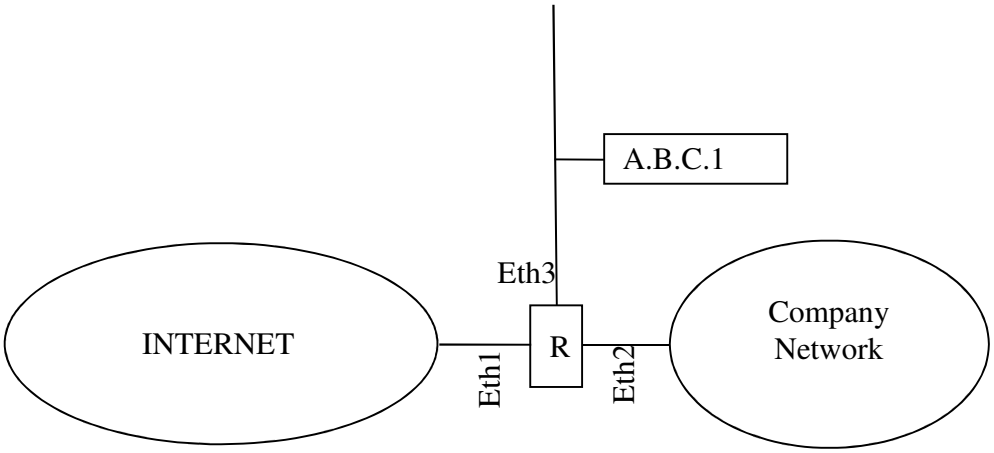
#iptables –N FORWARD

#iptables –P FORWARD DROP

#iptables –A FORWARD –I Eth1 –s A.B.C/24 –j ACCEPT

#iptables –A FORWARD –I Eth2 –s !A.B.C/24 –j ACCEPT

Q4 (5 points)



Let's assume a simple network interconnection scenario as depicted in the figure. Address block A.B.C.0/24 is allocated to the company network. Interface Eth3 of R is connected to a buffer subnet reserved for public servers. A public server for an application identified by protocol (server port number) P runs on host A.B.C.1.

Assuming that R is a stateful packet filter whereby filtering rules can be specified with a notation similar to the one of iptables, suggest a set of filtering rules required to implement each of the following security policy statements:

a) Authorize traffic between Company Network and Internet only for TCP connections initiated by a host located in the Company Network.

b) Authorize traffic between Internet and the public server for the application protocol P.

Answer:

a)

#iptables –F FORWARD

#iptables –N FORWARD

#iptables –P FORWARD DROP

#iptables –A FORWARD –I Eth2 –p tcp –s A.B.C.0/24 –m state

--state NEW,ESTABLISHED –j ACCEPT

#iptables –A FORWARD –I Eth1 –p tcp –d A.B.C.0/24 –m state

--state ESTABLISHED –j ACCEPT

b)

#iptables –F FORWARD

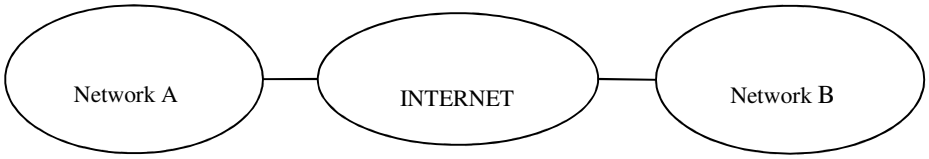
#iptables –N FORWARD

#iptables –P FORWARD DROP

#iptables –A FORWARD –I Eth1 –p tcp –dport P –d A.B.C.1 –j ACCEPT

#iptables –A FORWARD –I Eth3 –p tcp –s A.B.C.1 –d !A.B.C.0/24 –j ACCEPT

Q5 (6 points)



A company's network consists of two parts, namely Network A and Network B, that are geographically distributed as depicted in the figure above. The company network supports several assets such as data and services that are valuable and sensitive. The objective of the company is to come up with a secure interconnection of NETWORK A and NETWORK B through the Internet. The secure interconnection solution should assure that the data and computing assets as well as the company network itself are protected against potential use, disclosure and tampering by unauthorized users from the Internet.

a) Suggest a solution for the secure interconnection of networks A and B that allows a pair of application programs such as a client and a server to transparently communicate with one another, be they located on the same network (A or B) or on two different networks (A and B). 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 Network A and Network B, including the nodes required for the security configuration?

c) Let's assume that an IP packet carrying transport layer data is transmitted by host H1 located in Network A to host H2 located in Network B using the suggested solution. What is the structure of such a packet captured on an Internet link that is part of the interconnection path between the two networks? 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.

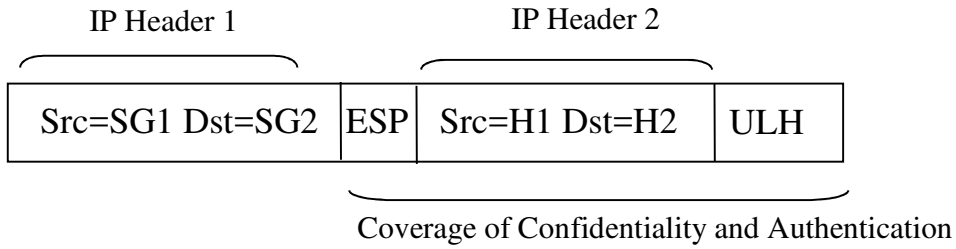
d) Same question as c) but for a packet captured on an internal link that is part of Network A or Network B.

Answer:

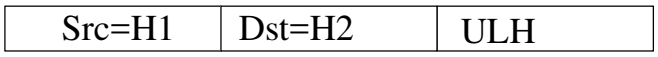
a) Virtual Private Network using IPSec ESP in tunnel mode. There should be a Security Gateway (SG) in each network. There should be at least one SA for each direction between the two SG's in ESP tunnel mode. IPSec session keys can be derived either from a manually distributed pairwise secret key or using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

b) private IP addressing within each network. The SG's should have a public address and a private address.

c) H1, H2 are the private addresses of Hosts H1 and H2, and SG1 and SG2 the public addresses of the security gateways. The packet is structured as follows:



d) On Network A or B:



Q6 (1 point)

Assume that a web server uses Transport Layer Security (TLS) or Secure Socket Layer (SSL) in a configuration where clients **do not have** public key certificates and the web server has a certificate verifiable by all clients.

How can the client be authenticated by the server in this scenario?

Answer:

Since the client does not have a certificate it cannot be authenticated by TLS/SSL. A secret password or PIN is used by the application to authenticate the client using the secret channel established through the key exchange.

Q7 (3 points)

a) State the main reason that may cause errors when IPSec protocols flow across a Network Address Translation (NAT) device.

b) What is the alternative to IPSec using SSL for the secure remote access scenario? What are the main advantages of this alternative over IPSec? Briefly Explain.

c) Between IPSec and the alternative solution referred to in b) which one is more suitable to support native IP traffic during remote access? Briefly explain.

Answer:

a) The problem is due to the fact that NAT modifies IP addresses in the packet header in purpose whereas IPSec assumes that a change in IP addresses of a packet is either an integrity attack or a

protocol error. Thus valid IPSec packets are considered as tampered when they cross a NAT and IPSec simply does not work.

b) VPN/SSL is not affected by NAT or packet filters since original packets traverse NAT and packet filters by being encapsulated by SSL that is universally compatible. Unlike IPSec, VPN/SSL does not require a resident client program.

c) IPSec supports all IP traffic smoothly since it is an IP Layer mechanism whereas all IP support with VPN/SSL would be very cumbersome since the latter performs encapsulation above the transport layer.

Q8 (3 points)

The distributed computing environment of a company that is located in a building consists of several hosts interconnected through a wireline local area network (LAN). Let's suppose that wireless terminals can get access to the LAN through various Access Points located inside the building 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 a password-based version of the EAP protocol. It is also assumed that access to the building is controlled so that only authorized people can get access to the building.

a) What are the vulnerabilities that would not be covered despite the existing security measures, namely, physical access control for the building and the network access control mechanism based on 802.1x?

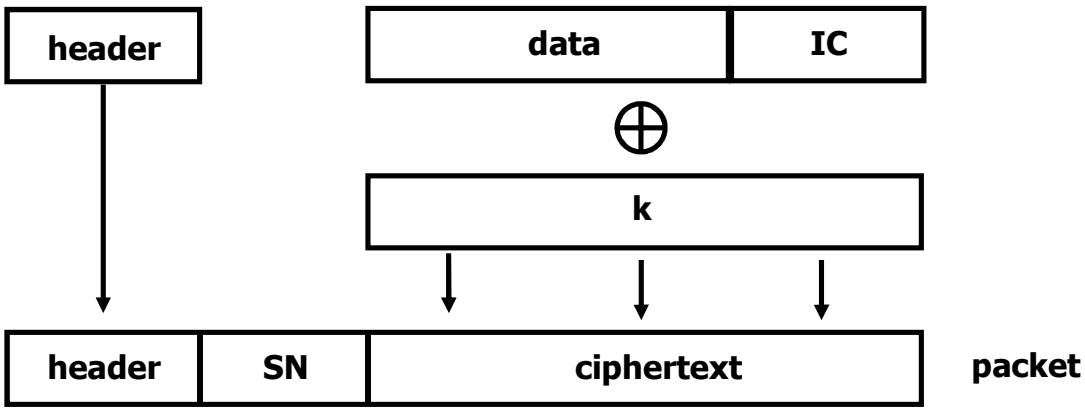
b) Suggest two alternative security solutions that would offer the same security guarantees on the communications between hosts connected to the LAN and the wireless terminals as the ones on the communications between the hosts through the LAN. State the name and main features of the protocols that are part of the solution and additional components required by the 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.

Q9 (4 points)



The figure above depicts the Wireless Equivalent Privacy protocol whereby:

- a keystream **k** is generated for every new data packet using a secure hash function **H** and the long-term secret **K** shared by the sender and the recipient as follows: **k=H(K, SN)**.
- SN is the sequence number of the data packet that is set to zero at the beginning of the connection and incremented by one for each packet.
- ⊕ denotes the bit-wise exclusive-or operation.
- **IC** is the unkeyed hash of the data computed using a hash function h that possesses the following property:
  for all input blocks X and Y of the same size, $h(X) \oplus h(Y) = h(X \oplus Y)$

For each of the following security requirements explain the main weakness(es) of this scheme through an attack scenario and suggest a solution:

a) data confidentiality

b) data integrity.

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.

b) 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) :

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

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

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