EP2500/EP3200 Networked System Security

Midterm Exam

Panagiotis (Panos) Papadimitratos

The total is **100** points.

Pass for MSc students: 55 points

Pass for PhD students: 60 points

Closed books. Closed notes. No computers, smart-phones, calculators, cameras, etc.

Please write your name on all the answer sheets, number them too.

Please add your name on the exam questions handout and return it intact with your answers.

Maximum duration, 1.5 hours; all answers must be handed back in well before the allocated time.

December 9, 2015

Contents

1 Basic security protocols

Code	Description
$i : a$	Entity i executes the action a
$x \leftarrow y$	Assign value y to x
RNG	Generate a random number
$x == y$	Check if x is equal to y
Pub_i	Public Key of i (known to all other hosts)
$Priv_i$	Private Key of i
Gen_{K_s}	Generate Session key
$E_k(m)$	Encrypt m with the key k
$D_k(m)$	Decrypt m with the key k
$h = H(m)$	Hash for m with the common hash function H
$(a, b, \ldots) \rightarrow i$	Send a message to i containing a, b, $\ldots$

Table 1: Primitives for the cryptographic tools.

Exercise 1 Authentication, Integrity, Confidentiality (15 pts)

Based on Table 1, suppose you want to connect two hosts A and B over a WLAN system. Assume the following two scenarios:

a) Host B wants to authenticate host A based on a **challenge-response** protocol. Someone designed the following protocol:

   (a) $B : challenge \leftarrow RNG$

   (b) $B : (challenge) \rightarrow A$

   (c) $A : response \leftarrow E_{Priv_A}(challenge)$

   (d) $A : (response) \rightarrow B$

   (e) $B : E_{Pub_A}(response) == challenge$

   Does it offer mutual authentication? If not, how would you change/redesign the protocol to achieve that?

b) The nodes want to exchange **large volumes of data** ensuring *Integrity*, *Sender Authenticity* and *Confidentiality*. Design the communication scheme using notation from the Table 1 to achieve the desirable security in an efficient manner.

Answer of exercise 1

a) Does it offer mutual authentication? If no how would you change the protocol?
   No! Both parties should challenge each-other to achieve mutual authentication.

b) The nodes want to exchange large volumes of data ensuring integrity, sender authenticity and confidentiality. Design the communication scheme using notation from the Table 1 to achieve the desirable security.

(a) $A : K_s \leftarrow Gen_{K_s}$

(b) $A : k \leftarrow E_{Pub_B}(K_s)$

(c) $A : c \leftarrow E_{K_s}(m)$

(d) $A : h \leftarrow H(m)$

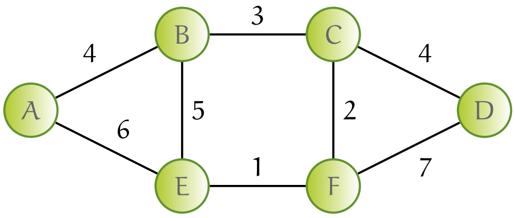
(e) $A : s \leftarrow E_{Priv_A}(h)$

(f) $A : (k, c, s) \rightarrow B$

2 Secure Routing

Exercise 2 Secure Link State Routing (30 pts)

Consider the autonomous system shown in the following figure where nodes A . . . F, are routers running Open Shortest Path First (OSPF).



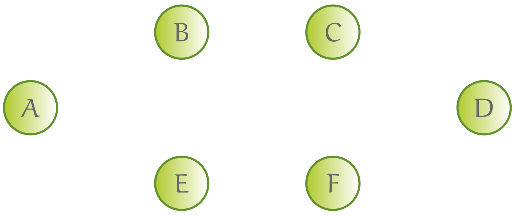
Answer the following questions:

1. Compute the shortest path from D to every other router in the network. Demonstrate the execution of the algorithm that the routers use.
2. Assume that router E gets compromised by an attacker. The attacker wants to attract all traffic originating from A through E. What could he do with the existing topology and links to achieve this.
3. Assume that the attacker succeeds in attracting all traffic through B. How would you ensure the confidentiality and integrity of the data exchanged between A and D? Routers cannot share secret keys a priori.
4. Describe a scheme that would allow routers to securely send updates, and would eliminate the possibility of a random adversary to inject false updates. Describe how and why the scheme would work. (Recall: as in (3) routers cannot share secret keys)

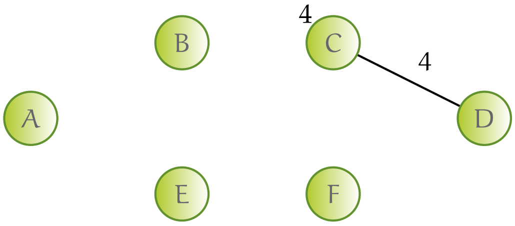
Answer of exercise 2

1. OSPF uses the Dijkstra algorithm to compute the shortest path to every other node in the network.

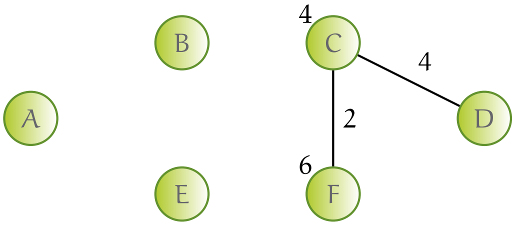
   In the beginning we have a network graph without edges.



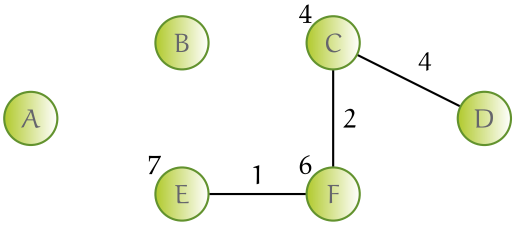
   The algorithm then initializes a set of nodes $N = \{D\}$, containing the source node that we want to evaluate. At each step the algorithm evaluates the minimum distance from D to of every other node $V \notin N$ and connected to at least one element in the set. The value for $D \rightarrow V$ is then the sum of the minimum distance between D and the predecessor of V and the edge that connects to V.



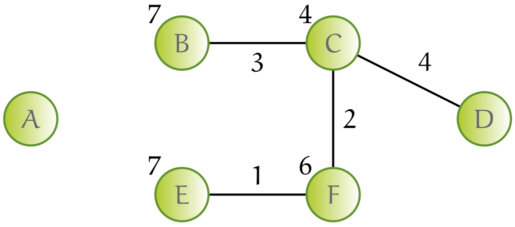
Therefore, the minimum distance between D and C is by the direct edge CD and has a value of 4. C is added to the set and $N = \{D, C\}$.



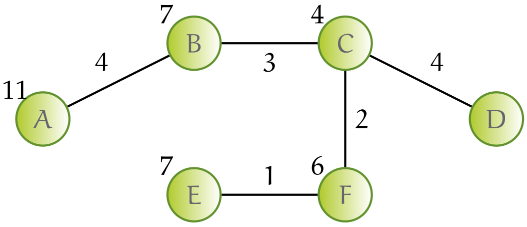
Now the algorithm selects the edge $C \to F$ since the direct edge $DF = 7 > 6 = CD + DF = 4 + 2$. Now the set is $N = \{D, C, E\}$.



The algorithm then selects the edge EF and update the set adding E.



Again, for the minimum edge CB.



And finally for the node A.

2. The attacker can advertise a *"cheap"* link to A and attract its traffic. By advertising 1 instead of 6 all the traffic will go through E. You can use Dijkstra as in 1 to verify this.

3. If routers cannot share a key a priori, it means that public key cryptography has to be implemented. Every router, would have to create a public-private key pair. When A wants to communicate with D, it will encrypt the packets that it wishes to send, using D's public key. To ensure data integrity, it can hash the packet payload too. (lets leave this a bit broad, because hashing can occur at different layers as we have seen)

   As we have seen in the lectures though, this scheme would not be secure at all. How would A be sure that the public key it uses is D's indeed? Even if the router hashed the IP block it advertises and then encrypted the packet and the hash with D's public key, the scheme would still not be secure. How would D be sure that A is indeed contacting it and not an adversary, that uses a wrong IP address block?

4. As we have seen in the lectures, this problem is solved by using a trusted third party, the Certificate Authority (CA). In other words a Public Key Infrastructure (PKI).

   The CA has its own private - public key pair. Using the private key that it keeps secret, it can sign the public keys of the routers. The signed public key is trusted by everyone, because only the CA can produce that signature. Moreover, everyone can read the signature, because the public key of the CA is available to everyone.

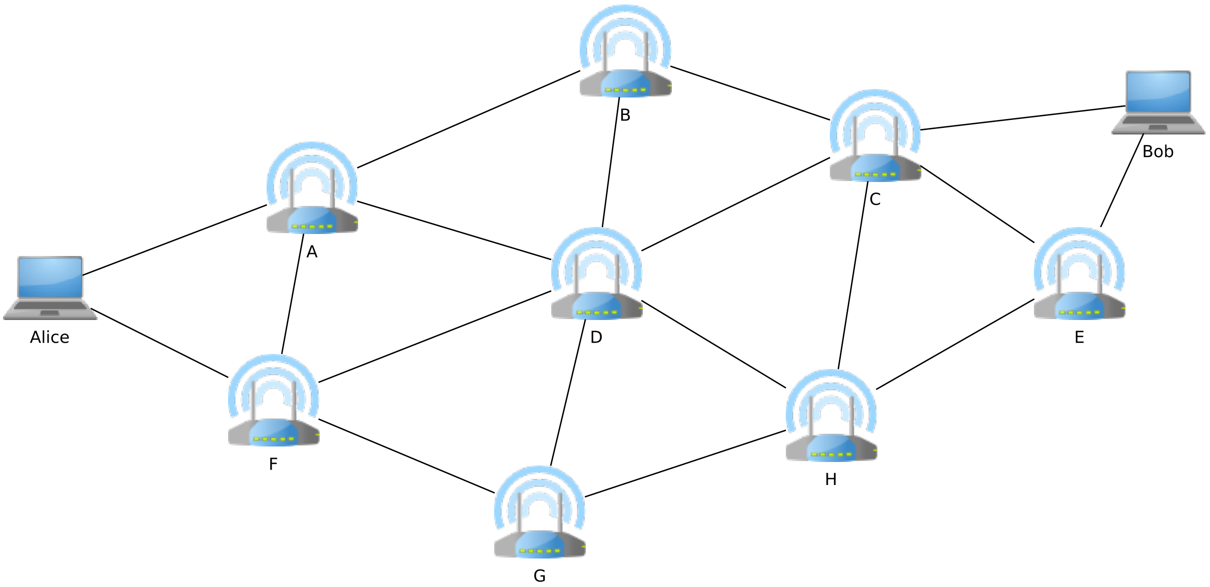


Figure 1: Wireless multi-hop network Topology.

Exercise 3 Secure Routing Protocol (SRP) (40 pts)

Consider a wireless multi-hop network as shown in Fig. 1. Each line represents a wireless link across which the incident nodes communicate directly with each other (i.e., they are neighbors). Based on the operation of such a *neighbor discovery protocol*, each one of the network nodes knows its neighborhood; the IDs of neighboring nodes that are in its vicinity. If no link exists, then there is no direct connection. For example, F and H are out of range. Communication is locally a broadcast, i.e., a packet sent by A goes simultaneously over (A,Alice), (A, F), (A, B), and (A, D).

Each one of the nodes has a unique (and only one) pair of public-private keys certified by a central Certification Authority (CA), where Pub_i and Priv_i denote the public and private keys of node i, respectively.

Consider a route discovery initiated by Alice, using SRP: it sends a RREQ, looking for a route to Bob. Recall that each intermediate node, A,...,H, rebroadcasts each fresh RREQ once. Otherwise it ignores a previously heard RREQ. Each route discovery is identified by a sequence number, Q_{SEQ}, and a random Q_{ID}.

a) Recall that in SRP, the two entities that want to establish a route must share a symmetric key that they can use to calculate a Message Authentication Code (MAC). However, this is not the case here; on the contrary, Alice and Bob have public-private key pairs. Explain how SRP should work. Alice and Bob can easily get each others certificates from the CA.
Recall that intermediate nodes add their identity to the RREQ they re-broadcast. Please give a concrete example through a valid path, e.g., over A, B and C.

b) For simplicity, please consider each such different packet for the same route discovery as a copy of the RREQ. What is the least number of Alice's RREQ packets that will be transmitted across the entire network? Can you approximate the number of RREQ packets for the shown topology? Explain how.

c) Consider a RREP crafted by $\mathtt{Bob}$ with the following fields:

- Q_{SEQ},Q_{ID}
- $\{\mathtt{Bob}, \mathtt{C}, \mathtt{B}, \mathtt{A}, \mathtt{Alice}\}$
- $\mathtt{MAC}_{K_{\mathtt{Alice},\mathtt{Bob}}}(\{\mathtt{Bob}, \mathtt{C}, \mathtt{B}, \mathtt{A}, \mathtt{Alice}\}, Q_{SEQ}, Q_{ID})$

Is it a valid RREP? Please explain how this or any RREP reaches back the source of the corresponding RREQ, that is, $\mathtt{Alice}$ in our network.

d) What would happen if $\mathtt{B}$ modifies the above RREP, by removing itself?

e) What if $\mathtt{B}$ added correctly its identity in the RREQ but it removed $\mathtt{A}$'s identity from the same RREQ? Please repeat (b).

f) As a continuation of the above, provide the RREP that Bob would craft. What would happen to such a RREP?

g) Consider the case where node $\mathtt{D}$ is malfunctioning and cannot participate in the route discovery protocol. Then, two possible routes from $\mathtt{Alice}$ to $\mathtt{Bob}$ are: (i) $\mathtt{Alice} \rightarrow \mathtt{A} \rightarrow \mathtt{B} \rightarrow \mathtt{C} \rightarrow \mathtt{Bob}$ and (ii) $\mathtt{Alice} \rightarrow \mathtt{F} \rightarrow \mathtt{G} \rightarrow \mathtt{H} \rightarrow \mathtt{E} \rightarrow \mathtt{Bob}$. However, nodes $\mathtt{A}$ and $\mathtt{B}$ do not want take up the burden of forwarding messages between $\mathtt{Alice}$ and $\mathtt{Bob}$ and, therefore, decide to "collude" in an attempt to trick Bob that their route consists of many intermediate paths (e.g., 8). This way, $\mathtt{Bob}$ will choose route (ii). Explain what they will have to do through a concrete example (i.e., run of the protocol). (Be careful, stating that they will simply not forward the messages is not sufficient.)

h) As a continuation of the above, what would be a possible countermeasure? Again, give a concrete example.
(Hint: Is it sufficient for $\mathtt{Bob}$ to authenticate (somehow) intermediate nodes comprising the route?)

Answer of exercise 3

a)
- Alice generates a RREQ packet including her ID, Bob as the destination, the query identifer Q_{ID}, an authenticator Auth of the route query fields and an empty NodeList. Auth will be calculated and signed with Alice's private key so that Bob can verify it upon reception; $\mathtt{Auth} = \mathtt{Alice}_{\mathtt{Privkey}}(\mathtt{Alice}, \mathtt{Bob}, Q_{ID})$. Alice then transmits the route request, i.e., $\mathtt{BcastL}(\mathtt{RREQ})$. She also initialize the ForwardList.
- A upon reception will check that this RREQ has not been previously processed. If this is the case, it will verify the address of its precursor, it will check that no loop is detected and, then, will append its own identity to the RREQ updating the NodeList.
- B and C will follow the same steps as A.
- Bob upon reception will make the necessary checks on the ID of its precursor, the Q_{ID}, possible duplicate entries in the NodeList and, then, will verify the validity of Auth using Alice's public key. If successful, he will generate a RREP including his ID, destination Alice, Q_{ID} and the RouteList containing the discovers route. Also, he calculates and signs with his private key an authenticator $\mathtt{Auth}' = \mathtt{Bob}_{\mathtt{PrivKey}}(\mathtt{Alice}, \mathtt{Bob}, U_{ID}, \mathtt{Route})$. If necessary, Bob can also generate

a private session key to be used for any later communication with Alice, encrypt it with Alice's public key and sign it with his own private key.

For more details on how the lists are generated and calculated check the notes on secure routing.

b) 8, one per intermediate node, not counting the initial by Alice. In that case 9.

c) A RREP crafted by Bob with the following fields:

- Q_{SEQ},Q_{ID}
- $\{Bob, C, B, A, Alice\}$
- $MAC_{K_{Alice,Bob}}(\{Bob, C, B, A, Alice\}, Q_{SEQ}, Q_{ID})$

is valid and it reaches back the source of the corresponding RREQ, that is, $Alice$ across the included route.

d) If B modifies the above RREP, by removing itself, the MAC checking will fail.

e) If B added correctly its identity in the RREQ but it removed A's identity from the same RREQ, the route that Bob would extract is Bob, c-b-Alice.

f) The RREP that Bob would craft would reach back at B but Alice - A would ignore it.

g) They would have to introduce "fake" node IDs in the REEQ packet. However, only A can inject new IDs because if B follows the same process it will be discovered by Bob when validating the ID of its precursor. Thus, A upon reception of the RREQ will add in the NodeList its ID and the IDs of 4 ghost nodes (i.e., $K, L, M, andN$). This is also possible because D is out of operation in order to perform the check of precursor nodes. Then, B will continue to follow the steps of SRP as normal. As a result, Bob when calculating the Route back to Alice will think that it consists of 8 intermediate paths and will not choose it.

h) Bob must be able to authenticate the IDs of all intermediate nodes that exist in the NodeList. Since each network node has public-private key pairs, it can sign its ID with its private key. In this way, Bob upon reception can request their public keys from the CA in order to verify their signatures.

3 Data Plane Attacks

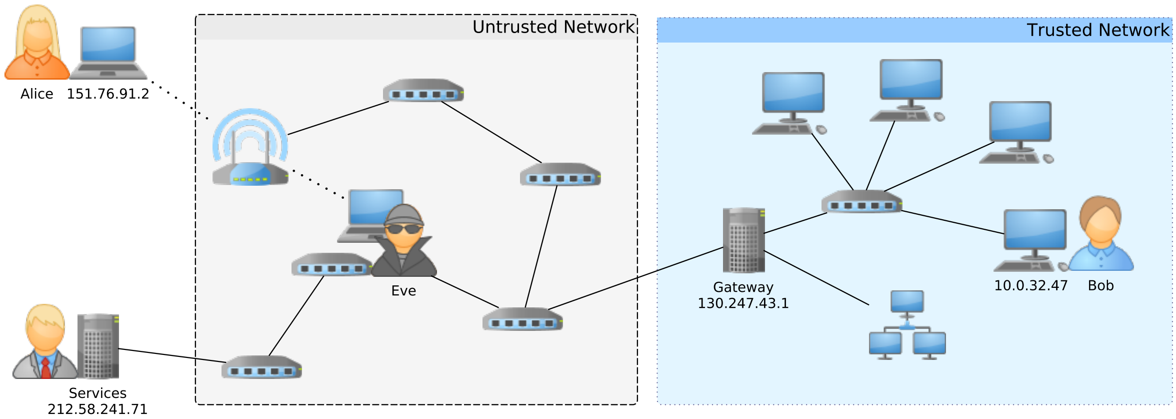


Figure 2: Networking Scenario

Exercise 4 IPSec (15 pts)

In Figure 2 a typical networking scenario is shown: a company user Alice is traveling abroad and connects her laptop to an untrusted (and maybe insecure) network, but she would like to:

i. Access her confidential information from the company trusted network, i.e. exchanging secret document with Bob, and

ii. Use various public services provided by a trusted host, i.e. look at the stock market trends through the "Services" server.

For security reasons, the Gateway will drop every outside packet going to (and coming from) the network where Bob is, e.g. all 10.0.0.0/8, but it will allow security associations to itself.

Eve is eavesdropping the wireless channel where Alice is connected, trying to acquire the exchanged information. At the same time he took control of a router in the Alice ↔ “Services” path and his objective is to deceive Alice on the trends and let her communicate false information to Bob, by tampering the forwarded information.

1. Describe the high level IPSec packet format(s) (mode and headers), and ways that can be used for securing the communication between Alice and the “Services”, with and without encryption.

2. Which one would you prefer? Justify the answer.

3. Describe the high level IPSec packet format(s) (mode and headers), and ways that can be used for securing the communication between Alice and Bob.

Answer of exercise 4

1 For encryption we will use the transport mode with Encapsulating Security Payload (ESP): Original Internet Protocol (IP) Header, ESP Header, Data, ESP Trailer, ESP Authentication. For plaintext format we will use the transport mode with Authentication Header (AH): Original IP, AH, Data.

2 Usually it's a good idea to use only the bare essentials techniques, not increase complexity and/or make design flaws. Thus, it's enough to use just the AH in Transport Mode.

3 Since the Gateway will drop every packet, more likely we need to establish a security association with it and then let forward the packets to the network. This means Alice will create an IPSec tunnel with the Gateway, using the Tunnel Mode with ESP. Therefor the packet will be: New IP Header, ESP, Original Packet, ESP Trailer, ESP Authentication.