Name …...ID …............................... Section …........Seat No..........

Sirindhorn International Institute of Technology
Thammasat University

Final Examination: Semester 2/2009

Course Title : CSS322 Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Monday 8 March 2010, 13:30 to 16:30

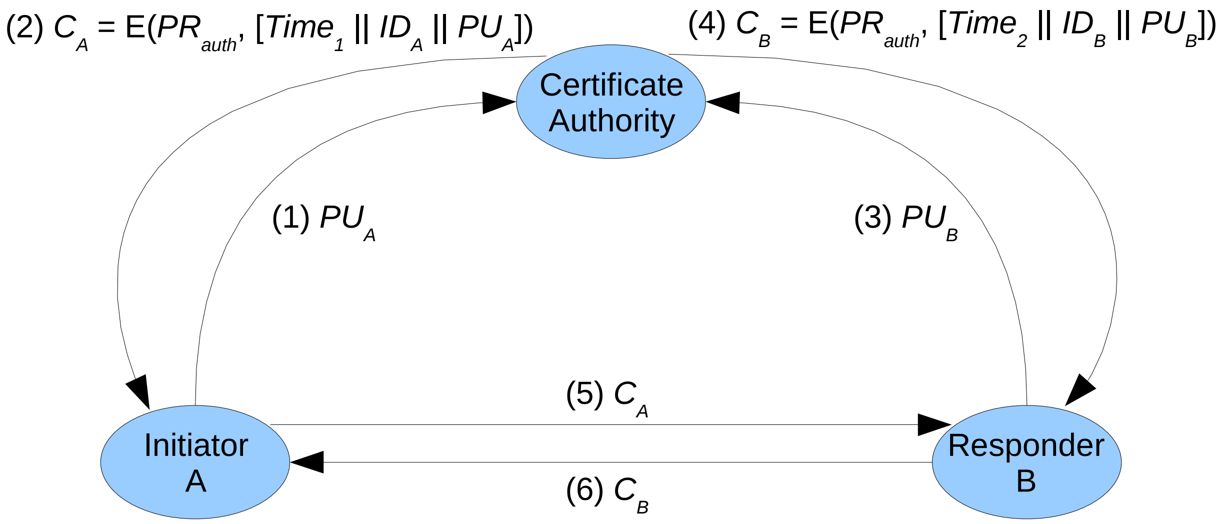
Instructions:

- This examination paper has 12 pages (including this page).
- Condition of Examination
  Closed book
  No dictionary
  Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student ID, section, and seat number clearly on the answer sheet.

Questions [100 marks]

Question 1 [13 marks]

Figure 1 shows an example key distribution method for public key systems.



(2) $C_A = E(PR_{auth}, [Time_1 \| ID_A \| PU_A])$
(4) $C_B = E(PR_{auth}, [Time_2 \| ID_B \| PU_B])$
Certificate Authority
(1) PU_A
(3) PU_B
(5) C_A
Initiator A
Responder B
(6) C_B

Figure 1: Certificate Authority Key Distribution Scheme

a) The procedure in Figure 1 assumes each node already has (or knows) some keys. List those keys for each node:

   i. Certificate Authority (Auth) [1 mark]

   ii. User A [1 mark]

   iii. User B [1 mark]

b) After the procedure is complete, list the keys that each node has/knows:

   i. Certificate Authority (Auth) [1 mark]

   ii. User A [1 mark]

   iii. User B [1 mark]

c) Explain the purpose of messages 1 and 2, including what is the purpose of a C_A. Also indicate whether these messages are transferred in a secure medium or not and why. [3 marks]

d) Must message 1 (and 2) be sent before message 3 (and 4)? Explain why or why not. [2 marks]

e) After all steps are complete, explain why B knows it has the public key that belongs to A (and not a forged public key). Also state any assumptions for this to be true. [2 marks]

Question 2 [16 marks]

The encryption algorithm of RSA is defined as:

$$C = M^e \, mod \, n$$

a) What is the decryption algorithm of RSA? [1 mark]

b) What is the public key in RSA? [1 mark]

c) What is the private key in RSA? [1 mark]

d) Describe the steps for generating the public/private key pair. You must state the conditions/properties of any values to be selected or calculated. (You do not need to explain why those conditions are necessary) [5 marks]

Based on the definition of RSA, there are three theoretical approaches for an attacker, knowing only public information, to discover the private information and/or a plaintext message.

e) What public information is it assumed that an attacker knows in RSA? (Refer to the variables defined in parts (a) to (d)). [1 mark]

f) Describe one of the three theoretical approaches that an attacker can use. [5 marks]

g) What makes the above approach practically impossible for an attacker to use? [2 marks]

Question 3 [14 marks]

Consider the diagram below where a packet filtering firewall (FW1) is running on router R2. The “internal” networks are on the left of the firewall (that is, connected to interface 1 of router R2). Each IP network is identified by a letter (e.g. “Network A”), and each host on a particular network is identified by a number (e.g. “Host A.4”). You can refer to “any” value using * (e.g. “A.*” meaning all hosts on network A). Note that although only several hosts are shown in the figure, you must assume there may be more hosts than shown in each network.

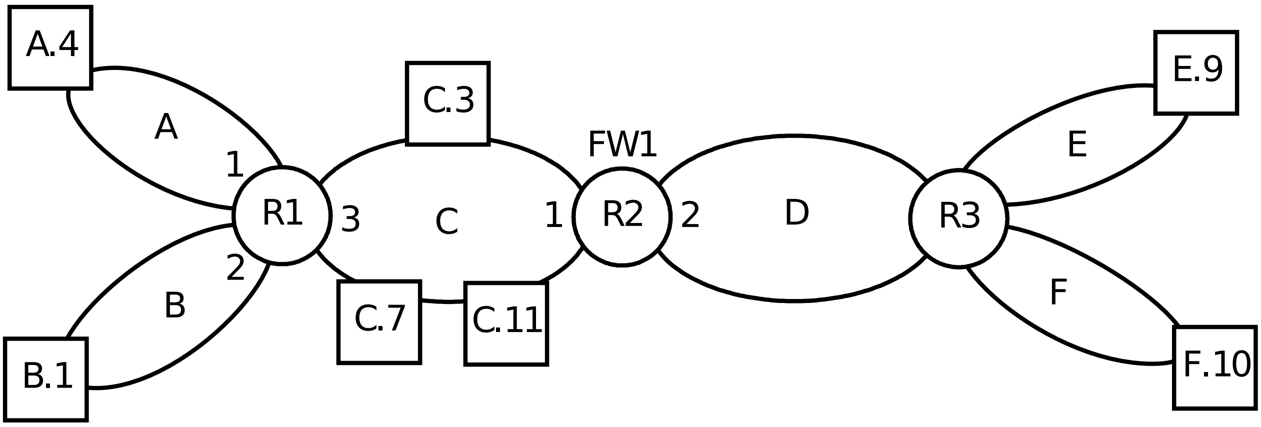


Figure 2: Firewall Network

For the following scenarios, complete the necessary firewall rules in the table provided. You do not have to use all table rows, and you can add more rows if necessary. You must use the correct values in the table (e.g. “*” or “A.4” or “A.*” are valid addresses; a written description is not valid). The default policy in all cases is DROP. Treat each part independent of other parts. All application protocols in this question use TCP. The interface numbers are written next to the router in the above figure. Assume Stateful Packet Inspection (SPI) is used.

a) Allow all external hosts to connect to the web servers on C.7 and A.4. [2 marks]

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

b) Allow all hosts on network A and B to connect to any external web server. [2 marks]

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

c) Allow all hosts on network C, except the two servers (C.3 and C.7), to connect to all external secure shell (SSH) servers. [3 marks]

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Assume the firewall table contains all rules as you created in part (a) and the SPI table is initially empty. (The firewall table does not contain the rules you created in parts (b) and (c)).

d) Complete the SPI table after the following connections have been established or blocked. [2 marks]

- Web browser with port 52123 on Host E.9 has initiated a connection to the web server on C.7.
- Web browser with port 49876 on Host F.10 has initiated a connection to the web server on C.11.

Initiator IP	Initiator Port	Responder IP	Responder Port

Assume a second packet filtering firewall (FW2) is installed on router R1 to create a Demilitiarised Zone (DMZ) in network C. An application-level firewall that acts as a proxy for web traffic is installed on C.3. Other traffic (that is not web) is not allowed. Assume the firewall entries from the previous parts are deleted (that is, the firewall and SPI tables are empty).

e) Complete the firewall tables for both firewalls so that the traffic cannot bypass the application-level firewall. [5 marks]

Firewall FW1:

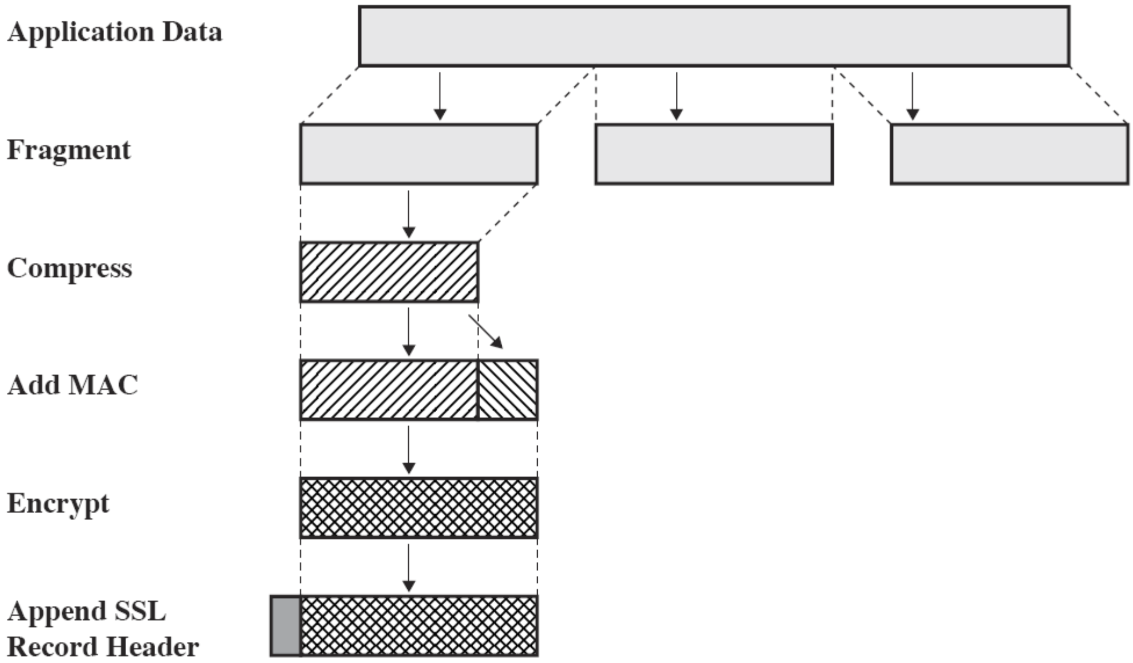
Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Firewall FW2:

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Question 4 [7 marks]

The figure below shows the steps applied to application data by the SSL Record Protocol.



a) List all security services provided by SSL/TLS. [2 marks]

b) List and explain an advantage and disadvantage of using SSL compared to using IPsec. [3 marks]

c) For normal (unsecure) web browsing, HTTP and TCP/IP are used. For secure web browsing, HTTPS is often used. Draw a protocol stack illustrating the protocols used when secure web browsing from application layer down to network layer, clearly showing the role of SSL. [2 marks]

Question 5 [11 marks]

a) Describe the TCP SYN flooding attack. Make sure you explain how the attack is started, and how the attack affects the target. [4 marks]

b) What is the difference between slave nodes and reflector nodes in a distributed denial of service (DDoS) attack? [2 marks]

c) Describe an advantage of using reflector nodes in a DDoS attack. [2 marks]

d) Could the TCP SYN flooding attack make use of reflector nodes? If yes, explain how. If no, explain why not. [3 marks]

Question 6 [10 marks]

In Diffie-Hellman key exchange, user Supat can calculate his public value S as:

$$S = a^{X_S} mod\, n$$

where $X_S < n$, n is a prime number, a is a primitive root of n and $a < n$. Assume Supat wants to exchange a secret, K, with user Funtida.

a) What is the equation for Funtida to calculate her public value, F? [1 mark]

b) What value does Funtida send to Supat in the Diffie-Hellman exchange? [1 mark]

c) What is the equation for Supat to calculate the secret, K_S? [2 marks]

d) What value(s) are public in this Diffie-Hellman exchange (that is, assumed that a malicious user knows them)? [2 marks]

e) What value(s) should only be known by Funtida (that is, no other users should know them)? [1 mark]

f) Prove that the secret calculated by Funtida, K_F, is the same as the secret calculated by Supat, K_S. Show the detailed steps of your proof. [3 marks]

Question 7 [11 marks]

a) Explain how public key cryptography can be used to provide a digital signature. Also explain why symmetric key cryptography cannot be used to provide a digital signature. [2 marks]

b) A common way to provide a digital signature, S, using public key cryptography is to also use a hash function. Write an equation that shows the calculation of the signature S at the source. Assume confidentiality is not needed, and the operators you have available are: E, D, H, meaning encrypt, decrypt and hash, respectively. Use common/meaningful names for the variables. [2 marks]

c) The hash function should have the properties of *weak*- and *strong-collision resistance*. Explain what these properties mean. [4 marks]

d) Explain how an attacker, A, could be successful in making the receiver (C) of a message thinking it is signed by another user (B) if the hash function is not weak-collision resistant [3 marks]

Question 8 [8 marks]

a) Explain the difference between a worm and virus. [2 marks]

b) Explain the difference between a normal (parasitic) virus, a metamorphic virus and a polymorphic virus. [3 marks]

c) Give an example of what a virus could do to be polymorphic. [1 mark]

d) Which of the three types of virus (parasitic, metamorphic, polymorphic) is hardest to detect by anti-virus software? Explain why. [2 marks]

Question 9 [10 marks]

An application on PC1 is sending data to an application on PC2. The route from PC1 to PC2 is via R1, R2, R3 and R4, in that order. You can identify the IP address of a node by its name, e.g. the IP address of R1 is "R1". Assume IPsec Encapsulating Security Payload (with Authentication) is used, and the application uses TCP.

Assume IPsec is used in transport mode between the PC's.

a) Draw the structure of a packet received by router R1. [2 marks]

b) For the packet in part (a), what is the destination address in the outer IP header? [1 mark]

c) Which parts of the packet are encrypted? [1 mark]

d) If the source address field in the original IP header is modified by a malicious user, will PC2 detect that modification? Explain your answer. [1 mark]

Assume IPsec is used in tunnelling mode, from router R1 to R4.

e) Draw the structure of a packet received by router R3. [2 marks]

f) For the packet in part (e), what is the destination address in the outer IP header? [1 mark]

g) Which parts of the packet are encrypted? [1 mark]

h) Explain an advantage of using IPsec in tunnelling mode between two LAN routers to provide a Virtual Private Network (as opposed to using end-to-end encryption between hosts). [1 mark]