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

Sirindhorn International Institute of Technology
Thammasat University

Final Examination Answers: 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 16 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.

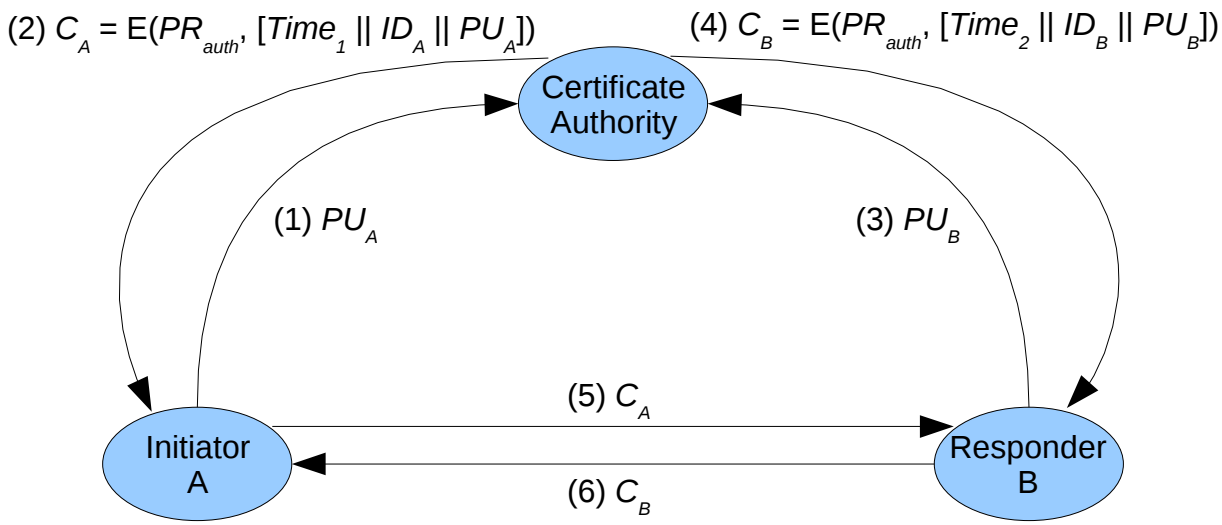


Figure 1: Certificate Authority Key Distribution Scheme

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]

Answer

PR_{auth}, PU_{auth}

ii. User A [1 mark]

Answer

PR_A, PU_A, PU_{auth}

iii. User B [1 mark]

Answer

PR_B, PU_B, PU_{auth}

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

i. Certificate Authority (Auth) [1 mark]

Answer

PR_{auth},PU_{auth}, PU_A, PU_B

ii. User A [1 mark]

Answer

PR_A, PU_A, PU_{auth}, PU_B

iii. User B [1 mark]

Answer

PR_B, PU_B, PU_{auth}, PU_A

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]

Answer

These messages are for A to obtain a certificate (C_A). A informs the CA of its public key, and the CA issues a certificate including that public key, the identity of A, all signed with the CA's private key (PR_{auth}). These steps must be performed in a secure medium, for example A physically visiting CA, because the CA must be certain that PU_A actually belongs to A.

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

Answer

No. A and B may obtain their certificate from the CA at any time, so long as they are obtained before A initiates communications with B.

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]

Answer

The certificate C_A received by B is signed with CA's private key. As B has CA's public key (and we assume B trusts/knows it is in fact CA's public key), then B can validate that the public key included in the certificate belongs to A.

Question 2 [16 marks]

The encryption algorithm of RSA is defined as:

$$C = M^e \bmod n$$

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

Answer

$$M = C^d \bmod n$$

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

Answer

$$PU = \{e, n\}$$

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

Answer

$$PR = \{d, n\}$$

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]

Answer

Select two large prime integers, p and q.

Calculate $n = p * q$ and $\Phi(n) = (p-1)*(q-1)$.

Select e such that it is relatively prime with $\Phi(n)$ or $gcd(e, \Phi(n)) = 1$

Calculate d, the multiplicative inverse of e in mod $\Phi(n)$.

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]

Answer

Attacker knows: e, n, C

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

Answer

Approach 1. Determine *p* and *q* by factoring *n* into its prime factors, so that $\Phi(n)$ can be easily calculated, and subsequently *d*.

Approach 2. Given *C*, *e* and *n*, calculate the inverse of $C = M^e \bmod n$. That is, find an *M* such that: $e = discretelog_{M,n}(C)$.

Approach 3. From *n*, calculate $\Phi(n)$ without knowing *p* and *q*.

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

Answer

Approach 1. Determining the prime factors of a large number is computationally hard.

Approach 2. Calculating the discrete logarithm (inverse exponential) for large numbers is computationally hard.

Approach 3. Calculating $\Phi(n)$ for large *n* is computationally hard.

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.

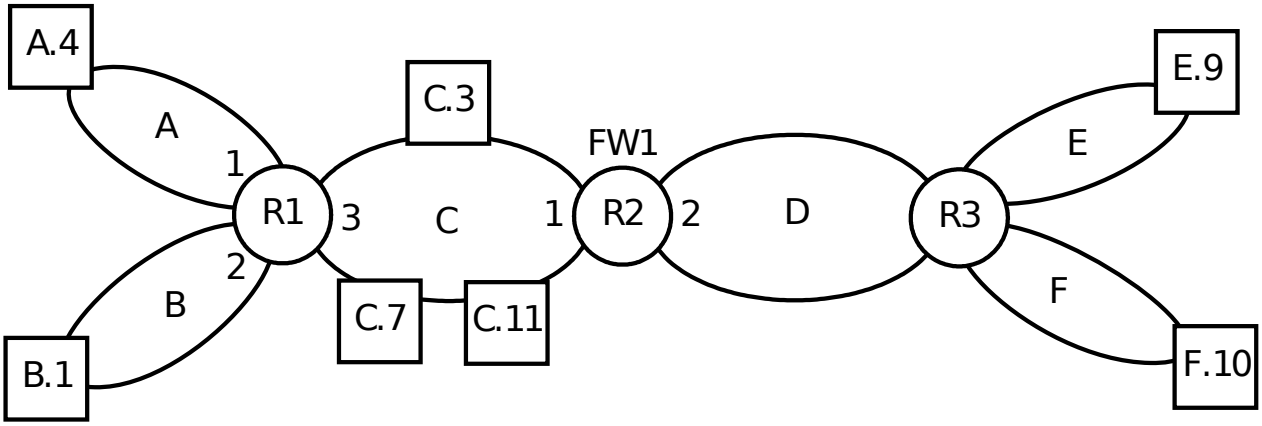


Figure 2: Firewall Network

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

Answer

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
2	*	*	C.7	80	TCP	Allow
2	*	*	A.4	80	TCP	Allow

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

Answer

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	A.*	*	*	80	TCP	Allow
1	B.*	*	*	80	TCP	Allow

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

Answer

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	C.3	*	*	22	TCP	Drop
1	C.7	*	*	22	TCP	Drop
1	C.*	*	*	22	TCP	Allow

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

Answer

Initiator IP	Initiator Port	Responder IP	Responder Port
E.9	52123	C.7	80

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

Answer

Firewall FW1:

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	C.3	*	*	80	TCP	Allow
2	*	80	C.3	*	TCP	Allow

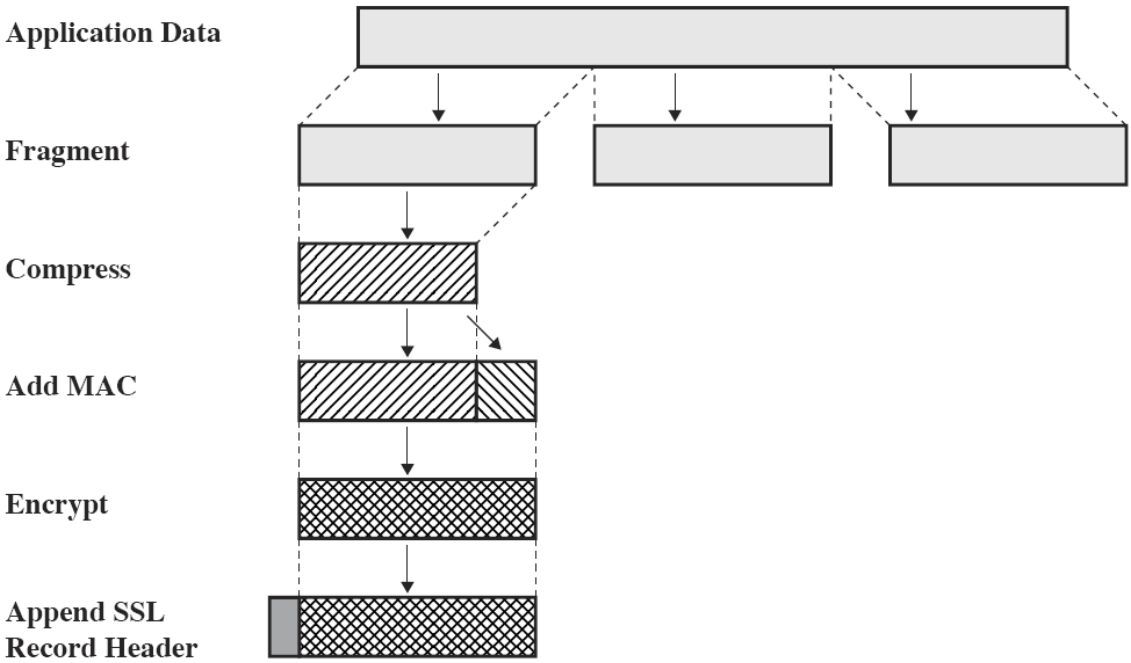
Firewall FW2:

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	*	*	C.3	80	TCP	Allow
2	*	*	C.3	80	TCP	Allow
3	C.3	80	*	*	TCP	Allow

Alternatively, you could rely on SPI to create the last two rows of each table.

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]

Answer

Confidentiality, authentication and integrity

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

Answer

Advantage of SSL: Implemented more widely; Often implemented in applications, and therefore can be easily distributed in applications (as opposed to operating systems)

Disadvantage of SSL: Only applicable for TCP applications (not UDP).

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]

Answer

HTTP

SSL

TCP

IP

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]

Answer

Attacker must infect (or gain control) of slaves. The attacker then triggers the slaves to start an attack on a specific target. The slaves send many, frequent TCP SYN segments to the target, but with fake random (usually incorrect) source IP addresses. The target responds to the SYNs, saving in memory the source address and connection status. The attack uses up network bandwidth, however the main impact is that the target's resources are consumed, i.e. CPU and memory. For each SYN received, the target stores an entry in memory until it receives a TCP ACK from the source. Since the source doesn't exist, the memory will be consumed up until a timeout expires. All the CPU must be used to maintain the timers.

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

Answer

Slave nodes are infected by (under control of) attacker – need to have vulnerabilities to be infected. Reflector nodes are (almost) any random node on the Internet – do not need to be infected.

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

Answer

As reflector nodes don't have to be infected (that is, they can be any random host on the Internet), you can use many more in an attack – the more you use the more traffic you can generate towards the target.

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

Answer

No. Reflectors require a request response type protocol where the response is sent by the reflector. If slaves sent a TCP SYN to the reflector with fake source address set to the target, then the reflectors would send a TCP SYN+ACK to the target. The target will immediately notice that it did not send the original TCP SYN, and ignore the SYN+ACK. Although reflectors could be used to consume network bandwidth, they would not consume memory/CPU of target.

Question 6 [10 marks]

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

$$S = a^{X_S} \bmod n$$

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]

Answer

$F = a^{X_F} \bmod n$

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

Answer

F

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

Answer

$K_S = F^{X_S} \bmod n$

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

Answer

a, n, F, S

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

Answer

X_F

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]

Answer

$$K_F = S^{X_F} \bmod n$$
$$= (a^{X_S} \bmod n)^{X_F} \bmod n$$
$$= (a^{X_S})^{X_F} \bmod n$$
$$= a^{X_S X_F} \bmod n$$

$$
\begin{aligned}
K_S &= F^{X_S} \bmod n \\
&= (a^{X_F} \bmod n)^{X_S} \bmod n \\
&= (a^{X_F})^{X_S} \bmod n \\
&= a^{X_F X_S} \bmod n
\end{aligned}
$$

Therefore $K_F = K_S$.

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]

Answer

Encrypting a message with a private key means it can only be successfully decrypted using the corresponding public key. That means the message is linked to only a single user – the user with the private key. With symmetric key cryptography, because a key is shared between two users, a message cannot be linked to a single user.

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]

Answer

S = E(H(M),PrivateKey)

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

Answer

Weak-collision resistance means it is computationally hard for an attacker to find a message Y, such that H(Y)=H(M), where M is given.

Strong-collision resistance means it is computationally hard for an attacker to find two messages, X and Y, such that H(X) = H(Y).

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]

Answer

If the hash function is not weak-collision resistant, then it is easy for the attacker to find another message Y that has the same hash value as message M. Therefore, if previously B had sent message M, signed to C, then later, A can take an exact copy of the signature (E(H(M),PrivateKey) and attach it to message Y. Since H(M) = H(Y), C would assume the message is signed by B.

Question 8 [8 marks]

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

Answer

A virus involves user interaction (e.g. opening a file) whereas a worm does not. A worm will automatically distribute itself.

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

Answer

A parasitic virus simply copies itself, as is, to other files. When a polymorphic virus copies the original virus to create a new virus, the new virus appears different than the original, but functions the same. For a metamorphic virus, the new virus both appears different and functions differently.

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

Answer

Introduce instructions that do nothing, e.g. NOP in assembly. Re-arrange lines of code, assuming the lines are independent of each other.

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

Answer

Metamorphic, because anti-virus software detects based upon known code or signatures of virus. If the anti-virus knows the code for a virus to be V, then it looks for that code in files. However if the virus changes its code to X, then anti-virus would also need to know X and compare files to both V and X. Metamorphic is harder to detect than polymorphic because with poloymorphic there are only a limited number of combinations of instructions that still result in the same behaviour. Metamorphic allows many more combinations.

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]

Answer

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

Answer

PC2

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

Answer

TCP Header, App Header, App Data, ESP Trailer

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]

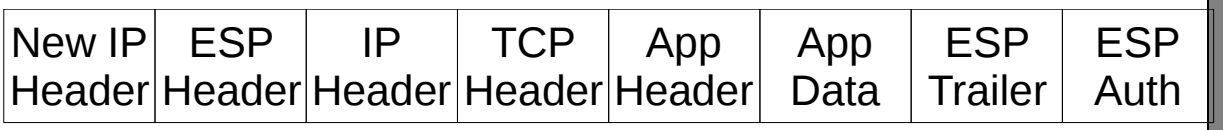
Answer

No. In ESP authentication is not applied on the IP header.

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]

Answer



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

Answer

R4

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

Answer

IP header (inner), TCP header, App Header and App Data, ESP trailer

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]

Answer

One advantage is that the configuration and maintenance of the security parameters is performed at only two devices (the routers), as opposed to at all hosts on the LAN. This makes the management of the network simpler.

Another advantage is that hosts do not need to support IPsec (nor specific encryption algorithms).