CSE 543/Fall 2007 - Homework

Due: Thursday, December 6, 2007 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness. Write legibly and check your answers before handing it in. **Do your own work!**

1. (*10pts*) Answer the following questions IPsec:

   (a) (3pts) What are three differences between the ESP and AH protocols of IPsec?

   (b) (2pts) What is the main difference between tunnel and transport modes of IPsec?

   (c) (3pts) What are three differences the IPsec protocol and SSL protocol?

   (d) (2pts) Describe how IPsec prevents TCP connection hijacking?

   answer: (a) Only ESP does encryption for confidentiality. Only AH protects the IP header in transport mode. Only ESP does both confidentiality and integrity protection via HMAC. Only AH has to deal with transient data in AH headers. Only ESP hides TCP info from firewalls.

   (b) Transport mode defines end-to-end security protection for a packet, whereas tunnel mode defines protection for intermediate legs of the route.

   (c) IPsec is implemented in-kernel, whereas SSL is integrated with the application. IPsec can be negotiated with shared symmetric keys of certificates, whereas SSL uses certificates built into application. SSL typically only authenticates the server, but IPsec authenticates both.

   (d) When a connection is initiated, an IPsec SA is negotiated. The IPsec negotiation protocol prevents replay. The subsequent TCP connections will be protected from replay by IPsec sequence numbers. The attacker will not be able to generate a legitimate IPsec packet.

2. (*8pts*) Answer the following questions about web cookies:

(a) (2pts) What is a web cookie?

(b) (2pts) Design a web cookie to store a secret value X on a client's system, given that the server has K_s and the client has K_c.

(c) (2pts) List two security problems with the use of web cookies.

(d) (2pts) What is a problem with using the same passport key to encrypt all passport cookies? What's a solution?

answer:

(a) A blob of information stored on a client computer by the server to store state of a web session with the server.

(b) $E(K_s, X) + HMAC(K_s, X)$

(c) They can be stolen and may be reused on another computer if poorly designed. They may contain private information in the clear. They may be replayed from the same computer after the user has gone (library attack).

(d) Unnecessary exposure of encrypted information generated via a single key. Should use a master key to generate per-client keys for encrypting information.

3. (*10pts*) Consider the following intrusion detection system that is monitoring a shipping website. On average, there are 500 malicious login a day, and the website receives 25,000 legitimate logins a day. Moreover, assume you have an 90% accurate intrusion detection algorithm. Fill in the following probabilities and **show your work**. *Hint* - Bayes rule states:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

(a) *attacks per day* = **500**

(b) (1 pt) $logins\ per\ day = 25,000$

(c) (1 pt) $P(attack) = attacks\ per\ day / logins\ per\ day = 500/(25,000) = 0.02$

(d) (1 pt) $P(!attack) = 1 - P(attack) = 0.98$

(e) (1 pt) $P(flag|attack) = 0.90$

(f) (1 pt) $P(flag|!attack) = 1 - P(flag|attack) = 0.10$

(g) (1 pt) $P(flag) = P(flag|attack) * P(attack) + P(flag|!attack) * P(!attack) = 0.116$

(h) (2 pts) true positives $= P(attack|flag) = \frac{P(flag|attack)P(attack)}{P(flag)} = 0.155$

(i) (2 pts) false positives $= 1 - true\ positives = 0.845$

4. (*10pts*) Suppose you have a network as defined above. Create stateless firewall policies for the following network firewalls FW1 and FW2. Create only as as many rules as you need (use the minimum) in the order they should be evaluated.

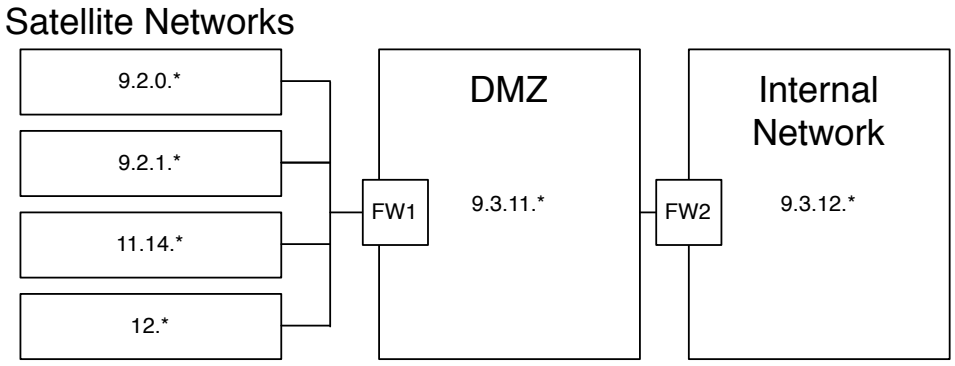
   (a) Unless otherwise specified, all traffic should be denied.

   (b) The satellite networks, except 12.0.0.0, should be able to communicate with any DMZ host over http (port 80).

   (c) Satellite network 9.2.1.0 should be able to speak with 9.3.11.4 over ssh (port 22).

   (d) Nobody outside the DMZ should be able to contact the internal network.

   (e) Any host in the internal network should be allowed to talk to the DMZ to vsftp (port 21).



FW1				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny

FW2				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny

answer:

FW1				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny
9.2.0.*	*	9.3.11.*	80	A
9.2.1.*	*	9.3.11.*	80	A
11.14.*	*	9.3.11.*	80	A
9.3.11.*	80	9.2.0.*	*	A
9.3.11.*	80	9.2.1.*	*	A
9.3.11.*	80	11.14.*	*	A
9.2.1.*	*	9.3.11.4	22	A
9.3.11.4	22	9.2.1.*	*	A
*	*	*	*	D

FW2				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny
9.3.12.*	*	9.3.11.*	21	A
9.3.11.*	21	9.3.12.*	*	A
*	*	*	*	D