CSS 322 – QUIZ 7 ANSWERS

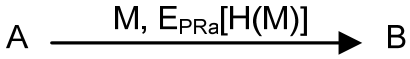
First name: _____ Last name: _____

ID: _____ Total Marks: _____

out of 10

Question 1 [3 marks]

User A sends a message to user B, and a digital signature is attached, as shown below.



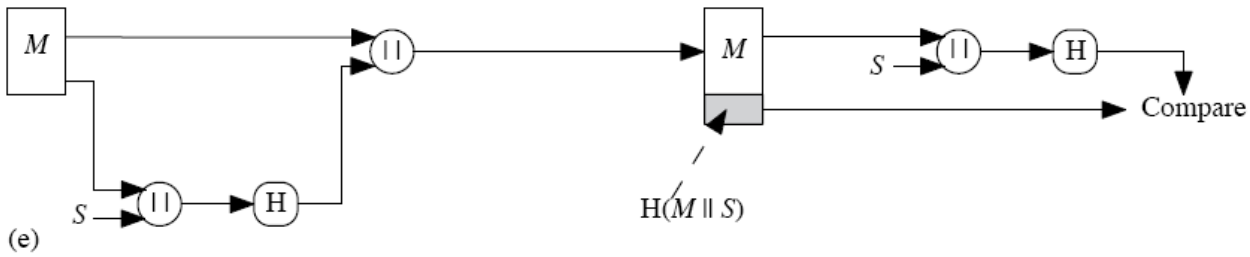
Explain how a malicious user C can attack this system if the hash function H() is not weak collision resistant. Your explanation should say what C needs to do, and what C gains (or achieves) from the attack, and what happens at B for the attack to be successful.

Answer:

C intercepts the packet, and since H() is not weak collision resistant, C can find another message X, such that the H(M) = H(X). C exchanges M for X, but sends the original EPRa[H(M)] (since C cannot change this as they don't have PRa). B receives the message, and decrypts using PUa and compares H(X) with H(M) – as they are the same, B believes the message X is signed by A.

Question 2 [3 marks]

The figure below shows a method of combining symmetric key encryption and hash functions.



a) List the security service(s) that the method provides. [1 mark]

b) Explain the attack that a malicious user can perform if the hash function, H(), does not have the one-way property. Your explanation should say what the malicious user can gain, at how the perform the attack. [2 marks]

Answers:

a. Authentication, data integrity.

b. The malicious user intercepts M || H (M || S). Since the one way property does not hold for H(), the malicious user can calculate M || S, and since they know M, can find S. That is, the malicious user determines the secret S.

Question 3 [2 marks]

a) What is the difference between a Hash function and a Message Authentication Code (MAC) function? [1 mark]

Answer:

Hash function takes only a message as input, whereas MAC takes message and key, and generates output dependant on key.

b) What can be used to convert most hash functions to MAC functions? [1 mark]

Answer:

HMAC

Question 4 [2 marks]

a) How can you make a system more secure against online password guessing? [1 mark]

b) A Unix password file often contains a username and hash of the password for each user. The file is often readable by all users (that is, public). Explain how does adding a "salt" value improve security (including what type of attack it can prevent)? [1 mark]

Answers:

a. Several ways: force users to use strong passwords, limit the number of guesses a user can make, limit the speed at which guesses can be made, track and report unsuccessful attempts.

b. Without a salt value, an existing user can immediately learn the password of another user, *if they have the same password.* Adding a random salt value, means a user cannot identify the hash values even if the passwords are identical.