**Answers and grading comments for Assignment 5 – Week 5 & Week 6**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**

**(1) Kerberos was a mythical three headed dog that guarded the gates of hell. What are the 3 "heads" of the Kerberos protocol?**

a) authentication server (which requires a password)  
b) internal firewall  
c) ticket-granting server  
d) client machine  
e) target server (e.g. a print server which requires a ticket to use)

**ANS: a, c, e**

**(2) What is a weakness of the Needham-Schroeder protocol?**

a) the clocks of the sender and receiver machines must be kept synchronized  
b) a predictable random number generator will allow an intruder to guess the session key  
c) a predictable random number generator will allow an intruder to guess the interchange key  
d) the session key doesn't have enough bits  
e) the interchange key doesn't have enough bits.

**ANS: b**

**(3) During key exchange which of the following must be kept secret.**

a) how the key was generated  
b) the key itself  
c) the protocol used to exchange the key  
d) who the sender is  
e) who the receiver is

**ANS: b**

Most students recognized that the key had to be kept secret. Quite a few also selected that how a key was generated must be kept secret. This is a violation of the principle of open design. If you commented that by knowing how the key was generated, you might be able to predict future keys then I gave you credit, but, again, how the key is generated should not be kept a secret. The sender and receiver can't be kept a secret because routers need that information and keeping the protocol a secret is also a violation of the principle of open design.  
  
   
**(4) It is crucial that no attacker is eavesdropping during key exchange.**

a) true  
b) false

**ANS: b**

Many students missed this one. Whenever you are doing anything on the Internet you \*\*\*always\*\*\* assume that somebody is listening (eavesdropping). It is like having a conversation in a restaurant. You have to be aware that there are other people around. The whole reason these protocols were developed was to prevent the eavesdropper from discovering the shared key. Please remember this!!!!  
  
  
**(5) Which, in general, has a longer lifespan: a session key or an interchange key?**

a) session key  
b) interchange key  
c) lifetime of both are the same

**ANS: b**

**(6) Which of the following protocols require clock synchronization between the participants?**

a) Needham-Schroeder  
b) Denning-Sacco  
c) Otway-Rees  
d) Kerberos  
e) None of the above

**ANS: b, d**

Most students selected Denning-Sacco. Quite few did not select Kerberos, but since Kerberos is based on Denning-Sacco, it too uses a timestamp.

**(7) Lets say that I want my bank to wire you $1000. I encipher a message containing this request to the bank as follows:**

  1. First generate a random session key  
  2. Then encipher the session key with the bank's public key  
  3. Then encipher the message with the session key  
  4. Finally send the enciphered message and enciphered session key to the bank

When the bank gets the enciphered message, it does the following:

  1. Deciphers the enciphered session key using its private key  
  2. Uses the session key to decipher the message  
  3. Reads the plaintext of the message telling it to send you $1000  
  4. Sends you the money  
   
This protocol is seriously flawed. It's most serious failing is that it doesn't support which one of the following?

a) confidentiality  
b) origin integrity  
c) data integrity  
d) availability

**ANS: b**

You could capture my request to the bank and replay it until I run out of money. The bank has no idea who sent the message. This is a problem with origin integrity.

**(8) Kerberos uses public key cryptography to exchange the session key between the authenticating server and the ticket granting server.**

a) true  
b) false

**ANS: b**

Kerberos uses interchange keys and session keys that have to be shared by a sender and a receiver. This is not public key cryptography!!

**(9) Which of the following are true statements about a digital signature?**

a) Part of the procedure of creating a digital signature is to hash the message using a cryptographic checksum function.  
b) A message that is digitally signed must be encrypted before it is signed.  
c) Part of the procedure of creating a digital signature is to encrypt the message hash using the private key.  
d) Part of the procedure of creating a digital signature is to encrypt the message hash using the public key.  
e) A digital signature helps assure the integrity of the message.

**ANS: a, c, e**

(b)You can sign an unencrypted message. Digital signing promotes integrity not confidentiality. Since the public key is available to everybody, you don't digitally sign with it. That is like signing a check using a stamp that is freely available to anybody at WalMarts. Curiously several people said that encrypting the message hash with private key was part of digitally signing but did not say that hashing the message in the first place was part of it. You have to hash the message before you sign the hash.

**(10) What is a weakness of the Denning-Sacco key exchange protocol?**

a) the clocks of the sender and receiver machines must be kept synchronized  
b) a predictable random number generator will allow an intruder to guess the session key  
c) a predictable random number generator will allow an intruder to guess the interchange key  
d) the session key doesn't have enough bits  
e) the interchange key doesn't have enough bits.

**ANS: a**

**(11) Which of the following are acceptible ways to get the public key of a CA?**

a) from a list of trusted root certification authorities that ships with a browser  
b) from an unsolicited promotional email sent by the CA  
c) from a certificate chain  
d) from a flash drive mailed to you by the CA after they have validated your identity.  
e) from the home page of the CA

**ANS: a,c,d**

(b)Beware of unsolicited promotional emails. They usually have no origin integrity, i.e., they are not necessarily from the person named in the return address.  
(e)Home page is not secure because Trudy could intercept request (see Lecture09.htm). Several students said that the flash drive might not be secure and I accepted their comment. Otherwise, I feel that expected mail from a CA is an acceptible risk.

**(12) In Kerberos, the print server shares a key with the authenticating server.**

a) true  
b) false

**ANS: b**

The print server shares a key with the ticket granting server not with the authenticating server.

**(13) Which of the following are true about a certificate?**

a) It associates an identity with a public key  
b) It contains the private key to use to decipher messages enciphered with the public key  
c) It is signed by the public key of a certifying authority.  
d) It is signed by the private key of a certifying authority.  
e) The content of a certificate is enciphered using the private key of a certifying authority

**ANS: a, d**

(b)The certificate does NOT contain the private key, it contains the public key.   
(c)Public keys are never used for signing since they are available to everybody; the private key is used for signing.  
(e)The hash of the certificate content is enciphered using the private key of the CA

**(14) A Certifying Authority (CA) always needs to be online to provide certificates to its clients.**

a) true  
b) false

**ANS: b**

The CA doesn't have to be online. It can be in locked room, create a certificate and put it on a floppy disk.

**(15) The SSL protocol uses the private key of the browser to encrypt the session key.**

a) true  
b) false

**ANS: b**

It uses the public key of the server to encrypt the session key.

**(16) Since the domain names https://www.mumde.net and https://mumde.net both are mapped to the same IP address, both are treated identically by a browser.**

a) true  
b) false

**ANS: b**

The domain name is what is compared to the subject name on the certificate. So the browser will issue a warning for at least one of them.

**(17) When you get a certificate from a CA you must provide the CA with both your public and your private key.**

a) true  
b) false

**ANS: b**

Please remember this: you don't give \*\*anybody\*\* your private key. Also, no part of the creation of a certificate requires that the CA use your private key. Giving them the private key would be a violation of the principle of least privilege.

**(18) A PGP certificate can have more than one digital signature**

a) true  
b) false

**ANS: a**

**(19) Let's say that your Student ID was a 20 digit random number instead of in the form of 000-98-xxxx. This was done to increase security by making it more difficult for somebody to guess your SID. This is a violation of which one of the following principles?**

a) principle of least privilege  
b) principle of fail-safe defaults  
c) principle of economy of mechanism  
d) principle of complete mediation  
e) principle of open design  
f) principle of separation of privilege  
g) principle of least common mechanism  
h) principle of psychological acceptibility

**ANS: h**To my mind, this is clearly a violation of the principle of psychological acceptibility. Would you want to have to memorize a 20 digit random SID? I don't think that open design is a good answer because presumably the reason that the SID was made so big was because it is known (open knowledge) that the SID is used to identify a user in a cookie.

**(20) Let eCA be the public key of a CA,  dCA be the private key of that CA and eJack be the public key of Jack.  How would a certificate issued by CA for Jack look like?**

**ANS:**

Jack, Jack's address, eJack, issuer, serial#, expiration date ||  
{Hash(Jack, Jack's address, eJack, issuer, serial#, expiration date)}dCA

**(21) If you use a CA, there is no single point of failure.**

a) true  
b) false

**ANS: a**

The CA does not have to be online when a certificate is used. All you need is the public key of the CA, not the CA itself. In contrast, in Kerberos if the authenticating or ticket granting server is down, no communication is possible.

**(22) Explain any 2 ways by which a Trudy can compromise the verification of a certificate.**

**ANS:**

a. Steal the private key of the CA. She can then use it to sign any certificate. If a CA's private key gets stolen, every certificate that was signed by it should be revoked. This is a major disaster for the CA.  
b. Trudy could work for the CA and issue a certificate without thoroughly checking out the identity of the owner of the certificate. Please remember that many, many security breaches are inside jobs.  
c. Trudy could steal somebody's identity and get a certificate using that identity.  
d. Trudy could take Bob's certificate and modify it in a way that the cryptographic checksum is the same as the checksum of the original certificate. The verification of the certificate will not detect this. A good cryptographic checksum algorithm will make this extremely difficult to do!  
e. Trudy could add the public key of a bogus CA to the list of Trusted Root Certification Authorities in a browser and send a certificate signed by the bogus CA to the browser. This is particularly a problem in a computer lab like we have at M.U.M.

**(23) What is the importance of using Certificate chains?**

**ANS:** A chain is useful if Alice doesn't know the CA that signed the certificate that contains Bob's public key.

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**