Security Midterm

1) Reflection attacks will not work. If a second session is used Bob will have a different a (nonce).

-Replay attacks will not work. Bob will have a different nonce every time.

-Dictionary attacks can work against this protocol. Mallory has access to a nonce, g^a mod p, and K{N}. -If impersonating Alice, Mallory can choose words from a dictionary and calculate K. If Mallory finds a K{N} that is equal to the K{N} sent by Bob, a successful attack can be made. This can only work if Alice is impersonated with a dictionary attack, not Bob.

3) A CRL is a log of digital certificates that have been revoked by the issuing certificate authority. A signature is required for a revocation list because it maintains and protects records. If there is not a certified authority signature, attacks could be made resulting in an altered list.

4) In addition to maintaining the CRL, it acts as a type of dictionary for requests. When a browser makes a connection with a site, the accessed site needs to validate the request and check the CRL. During the validation process, the certificate provided needs to be matched against the log. Having the certificate number and hash of the key values are then needed to verify it exists or doesn’t exist on the CRL. It is also important to have both values because it prevents an attacker from spoofing the certificate number or implementing a Denial of Service attack.

5) a) The extra IP-Header is needed to store the location of the source and destination of the packets. This is because the data transmitted will be encrypted and eventually needed to be decrypted. Having the extra header information will then correspond to the key needed for decryption.

b) Furthermore, if the packets were only encrypted and then left with the original source and destination information, the packets would not be able to be decrypted. This is due to each firewall having a different key. In addition, this type of protocol would make this type of transmission vulnerable against IP spoofing.

6) SSL does not protect against the MitB. This type of malware is a type of Trojan horse that infects web browsers by taking advantage of vulnerabilities. If security has been breached, and the trojan is successfully installed, then an SSL will not protect against the attack. The Trojan will still modify, insert, or remain covert on a system. For example, if the infected user is requesting to transfer money from their bank account to another user, the trojan could alter the routing information to a dummy account. This alteration can be made at any time. The money can then be transferred securely using SSL but this will not matter to the user because their system has already been compromised.

7) Hashing a message twice will provide extra security because it takes longer for an attacker to decrypt the message. For example, the 40 bits that will be hashed twice will take a total of 2\*2^40 cycles to generate a key. Conversely, the 40 bits concatenated to a constant 88-bits will only take 2\*40 cycles to generate a key for decryption. If an attacker is reliant on a time sensitive session, a double hash system could provide more security. For example, if the average shopper on Amazon takes 5 – 60 minutes to order merchandise using a SSL connection and it takes 2 hours to decrypt a multi-hashed transmission, then a hashed message may have an advantage. However, it’s important to know how long it takes to generate a hashed message, because a less secure protocol could be used for other scenarios. Overall, double hashing and concatenation have advantages and disadvantages due to the scenario its being used. Two important attributes to consider when maximizing their use is: encryption speed and decryption speed (if intercepted).