ECE568: Assignment3

Name: Chuanrui Li; Student Number: 1000010846

SSL

Part1:

If there is an error in the message or attacker changes the message content, the entire message will be resent again. However, if we send 4KB fragments one by one, we only need to resend the fragment with error not entire message. Also, some network protocols may not be able to transfer a large file in one package, resulting in a failure.

Part2:

There will be more bytes that need to be transferred, which costs more time to transmit a file. As a result, it becomes less efficiency when messages are longer.

Part3:

Attacker can do the reordering and replay attacks, or even delete the message in the middle of transmission.

Part4:

Attacker can do spoofing attack and break the integrity rule. For example, he can change the data in the package during the transmission. Also, receiver does not know the sender without MAC, breaking the authenticity rule, too.

Part5 (not required in assignment):

Attacker can break confidentiality rule. For example, he can know the content of message and MAC value for the message

Hash Function

Part1:

Attacker is trying to commit an existential forgery. Attacker tries random input without any control of the input message.

Part2:

The probability that attacker can succeed on its first attempt is $1/2^n$ because the total possibility for the n bits encrypted text is 2^n, so the probability for one attempt to succeed is $1/2^n$.

Part3:

The probability that attacker can succeed on its kth attempt is $(1-\frac{1}{2^n})^{k-1} * \frac{1}{2^n} = \frac{(2^n-1)^{k-1}}{2^{kn}}$, because the total possibility for the n bits encrypted text is 2^n and the probability for k-1 attempt to fail is $(1-\frac{1}{2^n})^{k-1}$.

Part4:

The expected number of attempts before success is 2^n. Based on the Expected Value (i.e., Mean) of a Discrete Random Variable rule ($E(X) = \sum x_i p_i$), the expected number of attempts should be $E(X) = \sum_{k=1}^{\propto}(1 - \frac{1}{2^n})^{k-1} * \frac{1}{2^n} * k = 2^n$.

Web Security

Part1:

- What is amplification attack?

Amplification attacks using other device as amplifiers to increase transmission traffic to the target machine. The victim, target, will waste a lot of recourse, causing itself denial of service.

- How it increases the impact of DDos?

The request and reply model is the key principle in amplification attack. Whenever attacker sends a request to the amplifiers, those devices send back a replay. If attacker is sending packets with spoofed IP address of the victim, amplifier will increase the amount of packages and then send back to the victim, which will significantly increase the traffic to the target and cause denial of service.

Part2:

- Load balancing mitigation approach

This method uses several extra devices performed in parallel to achieve the maximum available connections. For example, if one device is overloaded, the other devices will take it role to support the connection. In short, the methods spend more money buying the computation resource to handle the huge traffic.

- Bottom neck resource management mitigation approach

Because the denial of service targets at the bottom neck of the service, this method allocates more resource for the bottom neck and protects itself being overflowed. However, it is hard for system to differentiate legal and attack traffic. The TCP SYN Flood attack will still be able to overflow the protected bottom neck in the system.

- Attack resource identification mitigation approach

Victim server active identifies the resource of attacks and shuts it down. By investigating the received packages, victim can detect the path of the packages and then determine the source of an attack.

Part3:

- Novel TFTP amplification attack

Since there is no authentication method built into the TFTP, any user can connect to TFTP and download data. In this case, attacker sends the smallest possible RRQ TFTP packets with spoofed source IP address in order to generate large amount of response to the target machine, which results in denial of service. Furthermore, the maximum data block number is not defined in TFTP, so one signal request of a filename may trigger a response of unlimited data to the target in theory.