ECE 568 Assignment 2

Mingqi Hou

999767676

SSL

1. **Omitting step 1**
   Performing fragmentation before compressing and encrypting the messages enables the fragmented messages to be transmitted and decrypted separately. If the fragmentation is not performed here, the long messages will be fragmented by TCP. Thus the compressed and encrypted messages are split into smaller packets. The packets cannot be decrypted until all the fragments are received, resulting in significantly reduced efficiency.
2. **Omitting step 2**
   If the SSL transport phase protocol does not perform compression on each fragment, each message fragment will be longer. The protocol will be less efficient since there would be more data to transmit.
3. **Omitting step 3**
   If the SSL transport phase protocol does not append sequence number to each fragment, the messages will be vulnerable to reordering and deletion. In addition, the SSL protocol will be vulnerable to replay attack as well, as the fragment sequence acts as a nonce as well. Furthermore, the generation of MAC will be impacted as sequence number is used to produce MAC of the fragment.
4. **Omitting step 4**
   If the SSL transport phase protocol does not compute MAC for each fragment, the SSL protocol will be vulnerable to spoofing attacks as messages cannot be verified for authenticity or integrity.

Hash Functions

1. **Is the attacker trying to commit a selective forgery or an existential forgery?**
   The attacker is trying to commit an existential Forgery as the attacker intends to create a valid text-MAC pair. However, the attacker does not have control over the text. Random input strings are used in the attack attempts.
2. **What is the probability that the attacker will succeed on its first attempt?**
   There are 2^n possible strings for the n-bit string generated by hash function $H(m) = h$. Since the hash function is ideal, the probability of success on the first attempt is $\frac{1}{2^n}$
3. **What is the probability that the attacker will succeed on the k'th random try?**
   After k'th random attempt, the probability of success is $\frac{k}{2^n}$, given the string generated by the hash function is n bits long.
4. **What is the expected number of attempts before success?**
   The expected number of attempts before success is $\sum_i^n i \times \frac{i}{2^n}$, given the string generated by the hash function is n bits long.

Web Security

1. **Briefly describe what an amplification attack is and how it increases the impact of DDoS.**
   Amplification attack is a specific type of DoS and DDos attacks. It uses protocol flaws and other vulnerabilities to amplify the amounts of transmitted data against a target system. Amplification attacks could use legitimate, uninfected machines or intermediate devices, which suffer from protocol or other flaws.
   In amplification attacks, the request– reply relationship is a key principle. When an attacker sends a request with the spoofed IP address of the victim to the amplifiers, the amplifier will send back a reply. Amplifiers are used to increase the amounts of packets and/or packet size. Because of a spoofed IP address, the amplified traffic is directed towards the target, which could result in denial of service.
2. **Briefly describe two mitigation approaches for DDoS attacks.**
   1. Load balancing
      Load balancing is one of the easiest mitigation approaches. It increases the available connection and the performance of the protected machine to the maximum economic availability. It uses intermediate devices connected in parallel to mitigate the impact of DDoS attacks. If one of the connected devices is overloaded, the other devices will take over the role of overloaded device.
   2. Attack source identification
      Attack source identification is one of the commonly proposed mitigation approaches. It stops the attacker from performing DDoS attacks by actively identifying the source of the attack. To achieve this, there are 3 main approaches: Active interaction, Probabilistic packet matching schemes and Hash-based schemes.
      a. Active interaction
         In this approach, network administrator of the victim server actively determines the source of the attack and shut it down. Authorities and ISPs are often used to track and filter packets coming from the attackers.
      b. Probabilistic packet matching schemes
         This approach focuses on calculating the probable path of the packet, utilizing a large variety of techniques.
      c. Hash-based schemes
         Routers store the recent packets they transmitted in a form of cache. This cache could be accessed by the hosts under attack in order to determine the source of an attack

3. **Briefly describe the format of the new amplification attack proposed this article.**

The TFTP attack is the new amplification attack proposed this article. It takes advantage of the newly discovered TFTP protocol flaw, allowing it to be applied to any TFTP implementation. To perform the TFTP attack, the attacker sends a smallest possible request for the file on the TFTP server with a spoofed IP address. This action will result in a larger response message together with retransmissions and error codes sent towards the victim. By creating a special adjusted RRQ TFTP request with spoofed source IP address, the

attacker will be able to generate significantly amplified traffic to the victim. The smallest possible valid RRQ TFTP packet is created in order to achieve maximum amplification and best efficiency of an attack.