Final Exam
CSE 5339/7339 - Computer System Security
Fall 2023
Mark D. Hoffman

Name: Bingying Liang
ID: 48999397

Dec 5 2023

Instructions: Please keep all answers as short as possible while still conveying all necessary concepts. Please show all necessary work. **Copying information (i.e. – Copy and Paste) from any source that you did not author yourself will result in zero (0) points for that problem.** Copying on more than 2 problems will result in a zero for the exam. Please note the points distribution given with each question. **NO hand-written responses, answers converted to images, or other techniques used to avoid plagiarism detection will be accepted.**

1) In a standard Challenge-Response type authentication request, Trudy establishes a successful Man-In-The-Middle (MITM) interception between Alice and Bob and captures the following traffic:

Alice: ”I am Alice”
Bob: ”Prove it”
Alice: ”My password is RedShoes”
Bob: ”Access Granted”

(a) What is the simplest type of attack that Trudy could then employ to establish a successful authentication as Alice in a subsequent session? (3pts):
A. Brute Force
B. Denial of Service
C. Replay
D. Backdoor
E. Cross Site Scripting

Solution: C

(b) Why would hashing or encryption of the message not prevent the type of attack described above. (5pts)

Solution: Hashing or encrypting messages does not protect against the above types of attacks, since an attacker does not attempt to decrypt or hash the password during a replay attack. They simply retransmit the entire message or response previously captured. Since the replayed authentication sequence is the same as the original transmission, the system considers the message valid regardless of whether it is hashed or encrypted. Thus, hashing or encrypting messages does not protect against the types of attacks described above.

2) Which of the following protocols are transmitted in clear text (not encrypted) in their original implementation (Circle ALL appropriate answers): (5pts)

Solution:

[✓ 1. FTP] 2. HTTPS 3. SFTP 4. SSH

[✓ 5. TELNET] [✓ 6. RTP] [✓ 7. HTTP] [✓ 8. SMTP]

3) What is the term used to describe the one time use of a ‘secret’ number (number used once)? Briefly describe how it could be used to prevent the type of authentication attack described above? (3+5= 8pts)

Solution:

(a) Term: Nonce

(b) Description of use: A unique number used once. Random or pseudorandom numbers are commonly used in authentication protocols to ensure that old communications cannot be reused in replay attacks. In the case of preventing authentication attacks, the nonce is used as follows:

i. Unique request: When Alice wishes to authenticate Bob, Bob issues a challenge containing a nonce value.

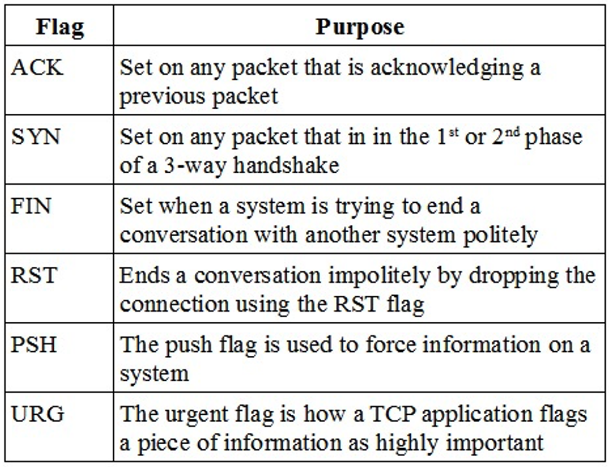
ii. Response using Nonce :Alice must include this Nonce in the response, which usually requires using this Nonce in some cryptographic computation, such as hashing it with the password.

iii. validation: Bob validates Alice’s response by performing the same computation on his terminal and comparing the results. If it matches, he knows that Alice received the nonce and that her response is not a replay of a previous authentication attempt, since the nonce is never reused.

iv. One-time validity: If the attacker Trudy tries to replay Alice's old message, the attempt will fail because the nonce from the previous session is no longer valid. Bob will issue a new nonce for each authentication session, making all replayed responses invalid.

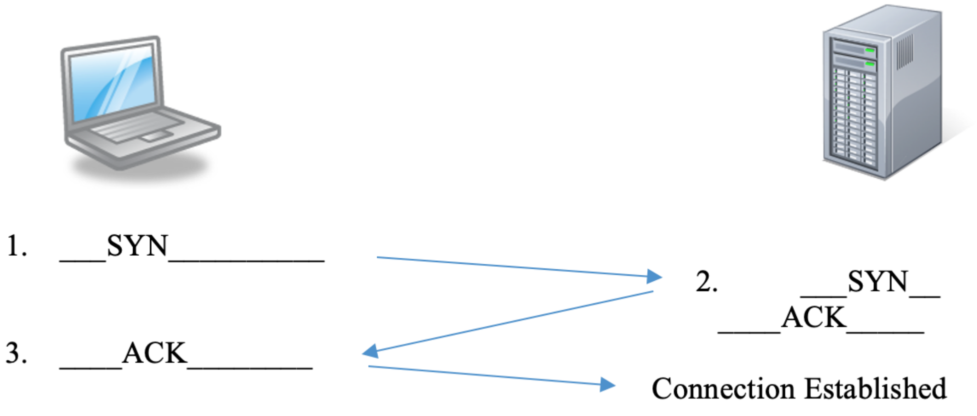
The use of nonce ensures that each authentication session is unique and that the captured authentication data cannot be reused by an attacker.

4) TCP uses the following flags to establish communications: Fill in the flags used to establish a proper TCP 3-way handshake to establish communications between a client and server in the diagram below: (8pts)



Flag	Purpose
ACK	Set on any packet that is acknowledging a previous packet
SYN	Set on any packet that in in the 1st or 2nd phase of a 3-way handshake
FIN	Set when a system is trying to end a conversation with another system politely
RST	Ends a conversation impolitely by dropping the connection using the RST flag
PSH	The push flag is used to force information on a system
URG	The urgent flag is how a TCP application flags a piece of information as highly important

Solution:



1. ___SYN__________

2. ___SYN__
____ACK_____

3. ____ACK________

Connection Established

5) In addition to these flags, a Sequence Number is also transmitted with each packet. Why is it important that these Sequence Numbers be generated at random instead of in a set pattern? (8pts)

Solution: The reasons are in the following:

(a) Security, where an attacker can exploit predictable sequence numbers to hijack sessions. This is known as a TCP sequence prediction attack. By guessing the sequence number of subsequent packets, an attacker can inject malicious packets into the communication stream and thus interrupt or take over the connection.

(b) Session uniqueness, random sequence numbers help ensure that each TCP session is unique. This reduces the risk of confusion between segments from different connections, which can occur if connections use the same sequence number for a short period of time (also known as sequence number collisions).

(c) The prevention of replay attacks, where random sequence numbers help prevent replay attacks, where an attacker captures a packet from the network and sends it again to have an unauthorized effect.

(d) The robustness of connection initialization, during the TCP 3-way handshake, the use of random sequence numbers contributes to the robustness of the SYN-ACK process. It helps to ensure that old duplicate segments from a previous connection are not misinterpreted as valid for the current connection.

6) Fill in the blanks using the terms listed below: (1pt each - 9 pts total)

SSH Transport Mode WEP SSL Tunnel Mode
IPSec Encapsulating Security Payload(ESP) Authentication Header
(AH)Address space layout randomization (ASLR)

SSL This is the ‘s’ in HTTPs. Used for the majority of secure transactions on the internet. Built into applications (such as browsers) so therefore it resides in the Application Layer of the OSI model.

(AH)Address space layout randomization (ASLR) is a memory-protection process for operating systems (OSes) that guards against buffer-overflow attacks by randomizing the location where system executables are loaded into memory.
Encapsulating Security Payload (ESP) When used in Transport Mode of IPSec, provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload. Does not sign the entire packet. Only the IP payload (not the IP header) is protected.

IPSec Network Layer - Very (overly) complex. Built into the operating system. Often used for VPNs (Virtual Private Networks)

Tunnel Mode in IPSec, is useful for protecting traffic between different networks, when traffic must pass through an intermediate, untrusted network. This is primarily handled from Firewall to Firewall and thus leaves the data unprotected within the internal network.

WEP Supposed to be as secure as wired LAN connections, but lacks the physical security of controlling the ports.

Transport Mode is the default mode for IPSec, and it is used for end-to-end (Host-to-Host) communications. In this mode, IPSec encrypts only the IP payload.

SSH Encrypted replacement for Telnet. Can use Public Keys, Digital Certs, or passwords for Authentication

Authentication Header (AH) provides authentication, integrity, and anti-replay protection for the entire packet (both the IP header and the data payload carried in the packet) in IPSec. It does not provide confidentiality (by itself).

7) Describe at least one flaw in the design of WEP making it so that WEP should never be used as a means to secure Wireless Access Points? ("intended to be as secure as wired LANs" is not a valid response) (10pts)

   Solution: First, WEP uses static encryption keys, which is one of its flawed design flaws that can make it insecure when protecting wireless access points. And in WEP, the same encryption key is used for every packet transmitted over the network. This design flaw leads to several vulnerabilities that make it WEP should never be used as a means to secure wireless access points for the following reasons:

   (a) Key reuse, because WEP uses a static key, this key is reused to encrypt the packet. However, this repetition allows the attacker to collect enough packets to analyze and eventually break the key with a relatively simple cryptographic attack.

   (b) WEP uses a 24-bit IV, which is very small. WEP uses an IV combined with a key to encrypt data. However, the IV is only 24 bits, which is quite short. The limited range of IV means that it repeats frequently, especially in high-traffic networks. The repetition of the IV, in combination with the static key, makes it easier for an attacker to infer the key using statistical methods.

   (c) Flawed integrity check, WEP uses the CRC-32(Cyclic Redundancy Check) algorithm to ensure data integrity, but the algorithm does not prevent deliberate tampering. An attacker can modify packets and easily recalculation valid CRC values, thus tampering with traffic without detection.

   Tools and techniques that can break WEP encryption in minutes are widely available, making any network that uses WEP vulnerable to unauthorized access and eavesdropping. Therefore, WEP should not be used to secure wireless networks.

8) Briefly describe a "Buffer Overflow" and name at least two mitigation methods. (9pts).

   Solution: A "buffer overflow" is a common software coding error that occurs when a program writes more data into a buffer than it can hold. Because the buffer size is fixed, then excess data could overwrite adjacent memory, which could lead to unpredictable behavior as well as crashes or security breaches, including potentially malicious code execution.

   To mitigate buffer overflow, there are two methods in the following:

   (a) Bounds Checking: This involves implementing checks in the program to ensure that no more data is written to the buffer than its capacity. This is a fundamental approach that can be done at different levels of software, including in the programming language itself or in the runtime environment.

(b) Use safe programming languages: Some modern programming languages such as Python, Java, and Rust are designed to automatically manage memory and prevent buffer overflows. Choosing such a language for software development inherently reduces the risk of buffer overflow.

These approaches, when used together, can significantly reduce the risk and impact of buffer overflow vulnerabilities.

9) (Based on the information presented in the last lecture and current events) Though not considered a form of classic of cyber threat, manipulation of information presented via social media and other online sources can exploit users into making decisions that they likely would not have made otherwise. Targeted advertising is a prime example of how this can be used, but other examples have occurred that have a much larger impact. This can affect not only individual opinion, but also wide-spread public opinion. Briefly explain at least one way such tactics could be used for harm and describe how you can reasonably help keep yourself and others better protected from such. (20pts)

Solution:
This issue relates to the manipulation of information on social media and online platforms and its impact on individual and public opinion. One type of manipulation is the spread of ”fake news.” Fake news refers to information that is deliberately fabricated or distorted, often to influence public opinion or advance some agenda. Such messages can spread quickly on social media because they are often designed to be attention-grabbing or to provoke emotional responses, such as anger or fear. Just as the teacher mentioned VPN in class, in some countries, due to policy problems, the government has conducted network protection and does not allow native people to use other networks. If you want to use other networks, you need to use a VPN for access. It is impossible to use Google and YouTube, which allows the government to manipulate the news to some extent for certain purposes. The spread of fake news can not only mislead individuals but also lead to social polarization and misunderstanding of important issues. For example, they may mislead voters during elections or spread false health information during public health crises such as during the COVID-19 pandemic. To protect yourself and others from this kind of information manipulation, I believe the following steps can be taken: First is critical thinking and being skeptical of the information you receive, especially those that elicit strong emotional reactions. The reliability of the information source is then checked to see if other trusted channels are reporting the same news. Secondly, we need to verify the truth of the news by using fact-checking websites or other trusted media. These websites usually analyze and refute the rumors of popular fake news. Most important is education and awareness raising, spreading knowledge about fake news and information manipulation to family and friends. Because they may be more easily misled, it’s also about using reliable news sources and following and subscribing to reputable news organizations, which often adhere to stricter fact-checking and editorial standards. I think that through these methods, I can help myself and the people around me better identify and prevent the harm of information manipulation and fake news.

10) Are there any topics in System Security that you feel we failed to cover or topics that we

covered that you wish we would have gone more in detail on? What did you like most about the class? The least? (15pts)

Solution:

In terms of system security, I think the broad categories that cover almost all the topics in the class like Ciphers and Symmetric Encryption, Symmetric Encryption (continued) and Public Key Encryption, Access Controls, and Software Security. I am personally interested in Software Security and hope we can discuss this topic in more detail. I liked the practical part of the course and the teacher's demonstration the most. Once heard on the Internet, hackers crack passwords and other technologies, the principle behind this is this. These seemingly cool things under the teacher's patient guidance, I also gained a lot. This is a very good process of enlightenment. The difficulty of the coursework is within my ability. I need to study hard but it will not scare me away, which is very good. It also ignited my interest in system security, and I still hope to learn knowledge in this field bit by bit in the future. In addition, the teacher combined the knowledge on the campus with the actual work and shared some work experience and interesting facts when meeting relevant knowledge points. All in all, I like this course very much and I am very grateful for the teacher's guidance and the well-designed course arrangement.