Operating System **Hsu PO-CHUN**
10610 CS342302 Student ID: s105062803
Prof. Pai H. Chou Submitted: Dec. 28, 2017
TA: Due Date: Dec. 31, 2017

Assignment 14

1 Problem 1

[20 points] 15.1 Buffer-overflow attacks can be avoided by adopting a better programming methodology or by using special hardware support. Discuss these solutions.

1.1 Answer

Programming Methodology
Most of the approaches use various methodologies of programming that are built typically around the use of validation of bounds that guard it against the overflow of buffer. The condition of buffer overflows does not occur in the language such as java where each of array access is confidential and guaranteed with the software bound-checking.
Hardware Support
A hardware support is one that places a guarantee regarding the buffer overflow attack that it does not take place and prevents the code execution that is located within the segment of stack of the address space of the process. Recalling the attack of the buffer-overflow which is performed by the overflow of the buffer that is present on the frame of the stack. Next, it jumps on to the another frame of the stack where the malicious executable code is present and returns the address of the function thus result in the buffer overflow. Thus, by code execution prevention from the stacks segment, this problem could be eliminated.

2 Problem 2

[20 points] 15.2 A password may become known to other users in a variety of ways. Is there a simple method for detecting that such an event has occurred? Explain your answer.

2.1 Answer

Password is one of the secure means to provide security to the unauthorized access of the highly confidential and secure documents. Thus, its security is a high mean to its author ,but, sometimes this security measure could become known to some unauthorized user in various ways. But such type accessing can be detected by authentication tools and etc.
Alternative way to detect the unauthorized users:
The best method to detect the user who is login-ed to the system is record of time and date when such events have occurred. When a user logs into the system, it record some events like log-in time, date, login name, IP address etc. Then the computer gives the last login details including the date and time to the authorized user. Therefore, authorized user can detect somebody logged into my system at this time.

3 Problem 3

[20 points] 15.4 The list of all passwords is kept within the operating system. Thus, if a user manages to read this list, password protection is no longer provided. Suggest a scheme that will avoid this problem. (Hint: Use different internal and external representations.)

3.1 Answer

To keep the password secure and protected from an unauthorized access just internally encrypt all the passwords so that the password can be accessed only in their encrypted and coded form. Next, only the authorized person or system operator who have knowledge and is a master of decrypting the password.

4 Problem 4

[20 points] 15.11 What commonly used computer programs are prone to man-in-the- middle attacks? Discuss solutions for preventing this form of attack.

4.1 Answer

Man-in-the-middle attacks:
Any protocol that requires a sender and a receiver to agree on a session key before they start communicating are prone to the man-in-the-middle attacks. For instance, if the two communicating systems are communicating with a common session key. The protocol messages for exchanging the session key are not protected by the appropriate authentication mechanism. Then, it is possible for an attacker to manufacture a session key and get access to the data being communicated between the two parties. And it is also possible by using fake session keys with the client and server interaction. When the attacker receives the data from the client, it can decrypt the data, re-encrypting it with the original key from the server, and transmit the encrypted data to the server without alerting either the client or the server about the attacker's presence.

The methods to remove attacks are:

- Port Scanning
- Denial of Service attacks

For example, the person who wants to send out the public key but attackers send the 'bad' public key as well. The person who wants to send the encrypted message knows nothing and using the 'bad' key to encrypt the message. Thus, the message is breach of the confidential.

The method to solve MITM: Digital Signature
Digital signature is used to authenticate messages from the server. If the server could communicate the session key and its identity in a message that is guarded by a digital signature granted by a certifying authority. So, the attacker would not able to forge the session key. Therefore, the man-in-the-middle attacks could be avoided by using digital signatures.

5 Problem 5

[20 points] 15.12 Compare symmetric and asymmetric encryption schemes, and discuss the circumstances under which a distributed system would use one or the other.

5.1 Answer

Table 1: Compare symmetric and asymmetric encryption schemes

	Symmetric	Asymmetric
1	Only single and same key is used for both encryption and decryption purposes	Different keys are used for both encryption and decryption
2	A commonly used encryption standard algorithm called DES and includes an advanced encryption standards(AES)	An asymmetric algorithm named as RSA or Rivest, Shamir, and Adleman algorithm
3	Base on transformation	Based on the foundation of mathematics that providing theoretical guarantee.
4	Cheap and efficient	Much more expensive and compute-intensive
5	Monotonic scheme	Be used for various other purpose of providing the security such as confidentiality, key distribution and authentication.

Asymmetric schemes of key cryptography are based basically on the foundation of mathematics that helps in providing the guarantee for the reverse engineering intractability of the encryption schemes. As these schemes is expensive as compared to the symmetric encryption scheme.
Due to the vast superiority usage of asymmetric schemes that is used for various other purposes of providing the security such as confidentiality, key distribution and authentication. Thus, a distributed system will use asymmetric encryption scheme while the cost is endurable and the contexts are more valuable.