104062203 陳涵宇

1. Problem Set

1. Buffer-overflow attacks can be avoided by adopting a better programming methodology or by using special hardware support. Discuss these solutions.

One form of hardware support that guarantees that a buffer overflow attack does not take place is to prevent the execution of code that is located in the stack segment of a process's address space. By preventing the execution of code from the stack segment, this problem is eliminated. Approaches that use a better programming methodology are typically built around the use of bounds checking to guard against buffer overflows.

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.

Whenever a user logs in, the system prints the last time that user was logged on the system.

3. 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.)

Encrypt the passwords internally so that they can only be accessed in coded form. The only person with access or knowledge of decoding should be the system operator.

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

Any protocol that requires a sender and a receiver to agree on a session key before they start communicating is prone to the man-in-the-middle attack. For instance, if one were to implement on a secure shell protocol by having the two communicating machines to identify a common session key, and if the protocol messages for exchanging the session key is not protected by the appropriate authentication mechanism, then it is possible for an attacker to manufacture a separate session key and get access to the data being communicated between the two parties. Such attacks could be avoided by using digital signatures 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, then the attacker would not be able to forge a session key, and therefore the man-in-the-middle attack could be avoided.

5. Compare symmetric and asymmetric encryption schemes, and discuss the circumstances under which a distributed system would use one or the other.

A symmetric encryption scheme allows the same key to be used for encrypting and decrypting messages. An asymmetric scheme requires the use of two different keys for performing the encryption and the corresponding decryption. Asymmetric key cryptographic schemes are based on mathematical foundations that provide guarantees on the intractability of reverse-engineering the encryption scheme, but they are typically much more expensive than symmetric schemes, which do not provide any such theoretical guarantees. Asymmetric schemes are also superior to symmetric schemes since they could be used for other purposes such as authentication, confidentiality, and key distribution.