Tecnológico de Costa Rica

Escuela de Ingeniería en Computación
Principios de Sistemas Operativos

31 de octubre de 2017

Samantha Arburola León
2013101697

Operating System Concepts

Chapter 15

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

. Una forma de soporte de hardware que garantiza que no se produzca un ataque de bufferoverflow es evitar la ejecución del código que está ubicado en el segmento de pila del espacio de direcciones de un proceso.

Recuerde que los ataques de desbordamiento de búfer se realizan desbordando el búfer en un marco de pila y sobrescribiendo la dirección de retorno de la función, saltando de ese modo a otra parte del marco de pila que contiene código ejecutable malicioso, que se colocó allí como resultado del desbordamiento de búfer

Los enfoques que utilizan una mejor metodología de programación generalmente se basan en el uso de la comprobación de límites para evitar desbordamientos de búfer. Los desbordamientos de búfer no ocurren en lenguajes como Java, donde se garantiza que todos los accesos de matriz están dentro de los límites a través de una comprobación de software.

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.

Cada vez que un usuario inicia sesión, el sistema imprime la última vez que el usuario inició sesión en el sistema.

15.3 What is the purpose of using a “salt” along with the user-provided password? Where should the “salt” be stored, and how should it be used?

Cuando un usuario crea una contraseña, el sistema genera un número aleatorio (salt)

y lo agrega a la contraseña proporcionada por el usuario, encripta la cadena resultante y almacena el resultado cifrado y la sal en el archivo de contraseña. Cuando se va a realizar una verificación de contraseña, primero se concatena la contraseña presentada por el usuario con la sal y luego se cifra antes de verificar la igualdad con la contraseña almacenada.

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.)

Encripta las contraseñas internamente para que solo puedan accederse en forma codificada. La única persona con acceso o conocimiento de descodificación debe ser el operador del sistema

15.5 An experimental addition to UNIX allows a user to connect a watchdog program to a file. The watchdog is invoked whenever a program requests access to the file. The watchdog then either grants or denies access to the file. Discuss two pros and two cons of using watchdogs for security.

El programa de vigilancia se convierte en el mecanismo de seguridad principal para el acceso a archivos. Debido a esto, encontramos sus principales beneficios y detracciones. Un beneficio de este enfoque es que tiene un mecanismo centralizado para controlar el acceso a un archivo, el programa de vigilancia. Al garantizar que el programa de vigilancia tenga suficientes técnicas de seguridad, tiene la seguridad de tener acceso seguro al archivo. Sin embargo, este es también el principal aspecto negativo de este enfoque: el programa de vigilancia se convierte en el cuello de botella. Si el programa de vigilancia no se implementa correctamente (es decir, tiene un agujero de seguridad), no hay otros mecanismos de copia de seguridad para la protección de archivos

15.6 The UNIX program COPS scans a given system for possible security holes and alerts the user to possible problems. What are two potential hazards of using such a system for security? How can these problems be limited or eliminated?

El programa COPS mismo podría ser modificado por un intruso para desactivar algunas de sus características o incluso para aprovechar sus características para crear nuevos fallos de seguridad. Incluso si COPS no está resquebrajado, es posible que un intruso obtenga una copia de COPS, la estudie y detecte infracciones de seguridad que COPS no detecta. Entonces, ese intruso podría aprovecharse de los sistemas en los que la administración depende de COPS para la seguridad (pensando que está proporcionando seguridad), cuando todo lo que proporciona COPS es la complacencia de la administración. COPS podría almacenarse en un medio de solo lectura o sistema de archivos para evitar su modificación. Se podría proporcionar solo a los administradores de sistemas de buena fe para evitar que caiga en las manos equivocadas. Sin embargo, ninguno de estos es una solución infalible.

15.7 Discuss a means by which managers of systems connected to the Internet could have designed their systems to limit or eliminate the damage done by a worm. What are the drawbacks of making the change that you suggest?

Se pueden instalar "Firewalls" entre los sistemas e Internet. Estos sistemas filtran los paquetes que se mueven de un lado a otro, asegurando que solo los paquetes válidos propiedad de usuarios autorizados puedan acceder a los sistemas de protección. Dichos cortafuegos usualmente hacen que los sistemas sean menos convenientes (y las conexiones de red menos eficientes).

15.8 Argue for or against the judicial sentence handed down against Robert Morris, Jr., for his creation and execution of the Internet worm discussed in this chapter.

Un argumento en contra de la sentencia es que fue simplemente excesivo. Además, muchos han comentado que este gusano realmente hizo que la gente fuera más consciente de las posibles vulnerabilidades en la Internet pública. Un argumento para la oración es que este gusano les costó mucho tiempo y dinero a los usuarios de Internet y, considerando su aparente intención, la frase fue apropiada. Alentamos a los profesores a utilizar un caso como este, y los muchos casos contemporáneos similares, como un tema para un debate de clase.

15.9 Make a list of six security concerns for a bank's computer system. For each item on your list, state whether this concern relates to physical, human, or operating-system security.

En un lugar protegido, bien protegido: físico, humano. Red a prueba de manipulaciones: física, humana, sistema operativo. Acceso a módem eliminado o limitado: físico, humano. Transferencias de datos no autorizadas prevenidas o registradas: humano, sistema operativo. Medios de copia de seguridad protegidos y protegidos: físicos, humanos. Programadores, personal de entrada de datos, confiable: humano.

15.10 What are two advantages of encrypting data stored in the computer system?

Los datos cifrados están protegidos por las instalaciones de protección del sistema operativo, así como una contraseña que se necesita para descifrarlos. Dos claves son mejores que una cuando se trata de seguridad.

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

Cualquier protocolo que requiera que un emisor y un receptor acuerden una clave de sesión antes de que comiencen a comunicarse es propenso al ataque man-inthe-middle.

En particular, si se supone que el servidor debe fabricar la clave de sesión, el atacante podría obtener la clave de sesión del servidor, comunicar su clave de sesión fabricada localmente al cliente y convencer al cliente para que use la clave de sesión falsa. Cuando el atacante recibe los datos del cliente, puede descifrar los datos, volver a cifrarlos con la clave original del servidor y transmitir los datos cifrados al servidor sin alertar al cliente o al servidor sobre la presencia del atacante.

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

Un esquema de cifrado simétrico permite utilizar la misma clave para cifrar y descifrar mensajes. Un esquema asimétrico requiere el uso de dos claves diferentes para realizar el cifrado y el descifrado correspondiente. Los esquemas criptográficos de clave asimétrica se basan en fundamentos matemáticos que brindan garantías sobre la intratabilidad de la ingeniería inversa del esquema de cifrado, pero suelen ser mucho más costosos que los esquemas simétricos, que no proporcionan ninguna de estas garantías teóricas. Los esquemas asimétricos también son superiores a los esquemas simétricos, ya que podrían usarse para otros fines, como autenticación, confidencialidad y distribución de claves.

15.13 Why doesn't D(kd , N)(E(ke, N)(m)) provide authentication of the sender? To what uses can such an encryption be put?

D (kd, N) (E (ke, N) (m)) significa que el mensaje se cifra con la clave pública y luego se descifra usando la clave privada. Este esquema no es suficiente para garantizar la autenticación ya que cualquier entidad puede obtener las claves públicas y, por lo tanto, podría haber fabricado el mensaje. Sin embargo, la única entidad que puede descifrar el mensaje es la entidad propietaria de la clave privada, que garantiza que el mensaje es un mensaje secreto del remitente a la entidad propietaria de la clave privada; ninguna otra entidad puede descifrar el contenido del mensaje.

15.14 Discuss how the asymmetric encryption algorithm can be used to achieve the following goals.

a. Authentication: receiver knows that only the sender could have generated the message.

b. Secrecy: only the receiver can decrypt the message.

c. Authentication and secrecy: only the receiver can decrypt the message, and the receiver knows that only the sender could have generated the message.

Deje que k s e sea la clave pública del emisor, que sea la clave pública del receptor, k s d sea la clave privada del emisor yk sea la clave privada Ejercicios 107 del receptor. La autenticación se realiza haciendo que el remitente envíe un mensaje codificado utilizando k s d. El secreto se garantiza haciendo que el emisor codifique el mensaje usando k r e. Tanto la autenticación como el secretismo están garantizados al realizar una doble encriptación utilizando k s d y k r e.

15.15 Consider a system that generates 10 million audit records per day. Also assume that there are on average 10 attacks per day on this system and that each such attack is reflected in 20 records. If the intrusiondetection system has a true-alarm rate of 0.6 and a false-alarm rate of 0.0005, what percentage of alarms generated by the system correspond to real intrusions?

La probabilidad de ocurrencia de registros intrusivos es 10 * 20/106 = 0.0002. Usando el teorema de Bayes, la probabilidad de que una alarma corresponda a una intrusión real es simplemente 0.0002 * 0.6 / (0.0002 * 0.6 + 0.9998 * 0.0005) = 0.193.