6 AUTENTICACIÓN DEL PUNTO TERMINAL

Objetivo

- Describir cómo autenticar un punto terminal y cómo pueden emplearse los números distintivos para frustrar los ataques por reproducción.

Manual de clases

Última modificación:
1 de julio de 2022

Tema 6 de:
SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.

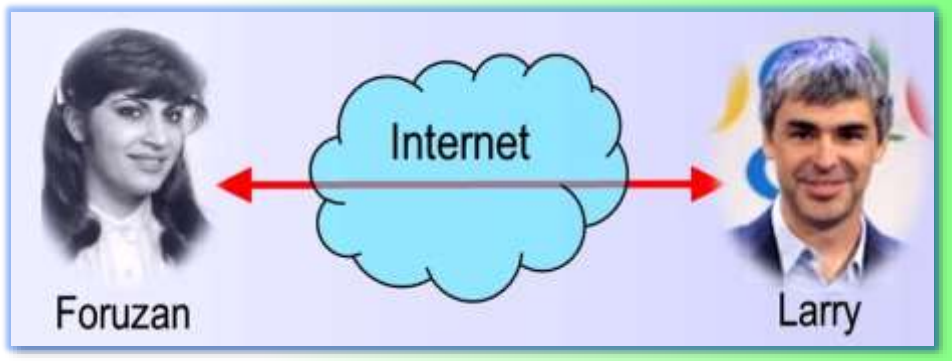
1. LA AUTENTICACIÓN DEL PUNTO TERMINAL

AUTENTICACIÓN DEL PUNTO TERMINAL

¿Qué es la autenticación del punto terminal?

(Kurose, 2017)

- **Es el proceso** de demostrar a alguien la propia identidad a través de una red. Por ejemplo, un usuario demostrando su identidad a un servidor de correo electrónico.
- **En la vida cotidiana** las personas se autentican mutuamente de muchas formas: reconocen sus caras cuando se encuentran, reconocen sus voces a través del teléfono, los autentica el oficial de aduanas que comprueba si se parecen a la fotografía del pasaporte, etc.
- **A la hora** de realizar la autenticación a través de la red, los interlocutores no pueden utilizar información biométrica, como la apariencia visual o el patrón de voz. De hecho, a menudo, son elementos de la red, como routers y procesos elientes/servidor, los que debe autenticarse mutuamente.



- **En esos casos,** la autenticación debe realizarse basándose exclusivamente en los mensajes y datos intercambiados como parte de un protocolo de autenticación.
- **Normalmente**, el protocolo de autenticación se ejecutará antes de que los dos interlocutores ejecuten algún otro protocolo (por ejemplo, un protocolo de transferencia fiable de datos TCP, de intercambio de información de routing OSPF o de correo electrónico). Primero, el protocolo de autenticación establece las identidades de los interlocutores a satisfacción de ambos, y solo después los interlocutores acometerán la tarea que tengan entre manos.

2. DESARROLLO DE UN PROTOCOLO DE AUTENTICACIÓN

AUTENTICACIÓN DEL PUNTO TERMINAL

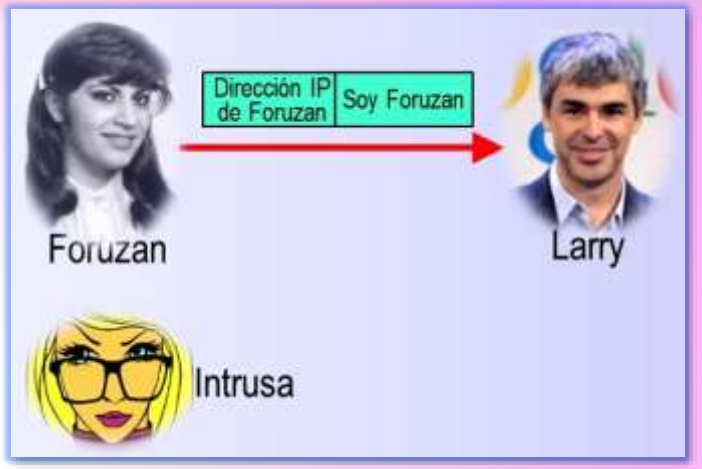
Versión 1.0 del protocolo (Kurose, 2017)

- **Resultará instructivo** desarrollar varias versiones de un protocolo de autenticación y ver los defectos de cada versión a medida que se va avanzando. Se va a suponer que Foruzan necesita autenticarse ante Larry.
- **Quizá el protocolo** de autenticación más simple que se pueda imaginar es uno en el que Foruzan simplemente envíe un mensaje a Larry diciéndole que es Foruzan. Este protocolo se ilustra en la figura.
- ▶**Escenario de falla**. La falla aquí resulta obvia: no hay forma de que Larry compruebe que la persona que está enviando el mensaje "Soy Foruzan" es, efectivamente, Foruzan. Una **intrusa** podría también enviar ese mensaje.

Desarrollo de un protocolo de autenticación

AUTENTICACIÓN DEL PUNTO TERMINAL

Versión 2.0 del protocolo (Kurose, 2017)



- **Si Foruzan dispone** de una direccion de red IP bien conocida desde la que siempre se comunica, Larry podrá tratar de autenticar a Foruzan verificando que la direccion de origen del datagrama IP que transporta el mensaje de autenticación se corresponde con la dirección IP de Foruzan. Si es así, Foruzan seria autenticada.
  - ✉ Esto podría impedir que algún intruso sin demasiado conocimiento de redes se hiciera pasar con Foruzan.
- ▶**Escenario de falla**. Si uno tiene acceso al código del sistema operativo y puede construir su propio kernel del sistema operativo, como es el caso con Linux y otros sistemas operativos disponibles de forma gratuita, no es difícil crear un datagrama IP, incluir en él cualquier dirección IP de origen que se desee (por ejemplo la dirección IP de Foruzan) y enviar el datagrama a través del protocolo de la capa de enlace hacia el router del primer salto.

- **A partir de ahí**, el datagrama con la dirección de origen incorrecta será reenviado hacia Larry. Esta es una forma de suplantación IP.
  - ✉ La suplantación IP puede evitarse si el router de primer salto de la Intrusa está configurado para reenviar solo aquellos datagramas que contengan la verdadera dirección IP de origen de la Intrusa (RFC 2827). Sin embargo, esta capacidad no está universalmente implantada, ni tampoco se la impone de manera universal. Por ello, Larry sería muy ingenuo si asumiera que el administrador de la red de la Intrusa ha configurado el router del primer salto para que solo reenvíe los datagramas que contengan direcciones auténticas.

Desarrollo de un protocolo de autenticación

AUTENTICACIÓN DEL PUNTO TERMINAL

Versión 3.0 del protocolo

(Kurose, 2017)

- **Una solución clásica** al problema de la autenticación consiste en usar una contraseña secreta, es decir un secreto compartido por el autenticador y la persona que está siendo autenticada. Gmail, Facebook, Telnet, FTP y muchos otros servicios necesitan autenticación de contraseñas. En esta versión del Protocolo, Foruzan envía su contraseña secreta a Larry, vea la figura.
- ▶**Escenario de falla**. Dado lo mucho que se utilizan las contraseñas, se podría pensar que esta versión 3.0 del protocolo no es suficientemente seguro. La falla de seguridad aquí está bastante clara: si la Intrusa espía las comunicaciones de Foruzan, entonces puede averiguar cuál es su contraseña.
  - ✉ Si piensa que esto es poco probable, considere el hecho de que, cuando se conecta con Telnet a otra máquina e inicia su sesión, la contraseña de inicio de sesión se envía sin cifrar al servidor de Telnet.
- **Cualquiera que esté conectado** a la red LAN del cliente o del servidor Telnet podría interceptar (leer y almacenar) todos los paquetes trasmitidos a través de LAN y robar así la contraseña de inicio de sesión.
- **De hecho**, esta es una técnica bien conocida de robo de contraseñas. Dicha amenaza es, obviamente, bastante real, por lo que está claro que esta Versión 3.0 del protocolo no sirve.

Desarrollo de un protocolo de autenticación

AUTENTICACIÓN DEL PUNTO TERMINAL

Versión 3.1 del protocolo

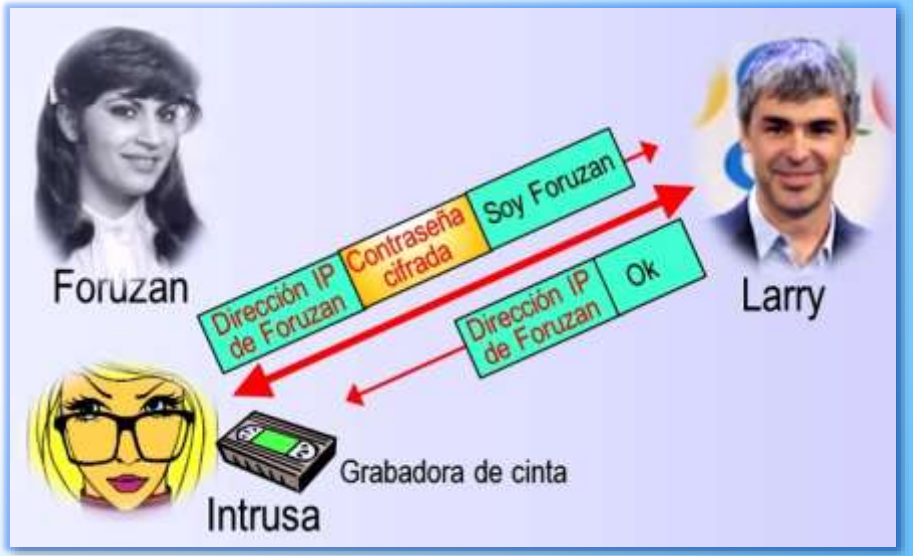
(Kurose, 2017)

- **La idea** para corregir la Versión 3.0 consiste en cifrar la contraseña, con ello se impide que la Intrusa averigüe la contraseña de Foruzan. Si se asume que Foruzan y Larry comparten una clave secreta simétrica K_{F-L} entonces Foruzan puede cifrar la contraseña y enviar a Larry su mensaje de identificación "Soy Foruzan" junto con la contraseña cifrada. K_{F-L} es una secuencia de números o caracteres secretos como entrada para el algoritmo de cifrado.

- **Larry descifra** la contraseña recibida y, suponiendo que sea correcta, autentica a Foruzan. Larry no tiene problemas de autenticarla, ya que Foruzan no solo conoce la contraseña, sino que también conoce el valor de la clave secreta compartida necesaria para cifrar la contraseña.

- ▶**Escenario de falla**. Aunque es cierto que esta Versión 3.1 impide a la Intrusa averiguar la contraseña de Foruzan, el uso de la criptografía en este caso no resuelve el problema de la autenticación.

  - ✉ Larry esta sujeto a un posible ataque por reproducción. Para hacerse pasar por Foruzan, la Intrusa solo necesita interceptar las comunicaciones de Foruzan, anotar la versión cifrada de la contraseña y mandar a Larry una copia de esa versión cifrada de la contraseña.



AUTENTICACIÓN DEL PUNTO TERMINAL

Versión 4.0 del Protocolo (Kurose, 2017)

- **El escenario de la falla** que presenta la Versión 3.1 surge del hecho de que Larry no podía distinguir entre la autenticación original de Foruzan a y la posterior reproducción. Es decir Larry no podía determinar si Foruzan se estaba comunicando "en vivo" (es decir si estaba realmente al otro extremo de la comunicación en ese momento) o si los mensajes que estaba recibiendo eran la reproducción de una autenticación previa de Foruzan, que hubiera sido grabada.

- **En el protocolo de negociación** en tres fases de TCP se enfrentaba a este mismo problema: el lado del servidor de una conexión TCP no quería aceptar una conexión si el segmento SYN recibido era una copia antigua (retransmisión) de un segmento SYN de una conexión anterior.

- **¿Cómo resolvía** el lado del servidor TCP el problema de determinar si el cliente estaba realmente comunicándose en vivo? Lo que hacía era elegir un número inicial de secuencia que no se hubiera utilizado durante muchísimo tiempo, enviar ese número al cliente y luego esperar a que el cliente respondiera con un segmento ACK que contuviera dicho número. Se puede adoptar aquí la misma idea de cara a la autenticación.

- **Un número distintivo** (***nonce***) es un número que un protocolo solo utilizará una vez en la vida. Es decir, una vez que un protocolo emplea un número distintivo, nunca volverá a usar ese número.

Desarrollo de un protocolo de autenticación

AUTENTICACIÓN DEL PUNTO TERMINAL

Versión 4.0 del Protocolo (cont.)

(Kurose, 2017)

- **Este versión del protocolo** usa los números distintivos de la forma siguiente:
  - ▶**1.** Foruzan envía a Harry el mensaje "Soy Foruzan"
  - ▶**2.** Harry selecciona un número distintivo *R*, y se lo envía a Foruzan.
  - ▶**3.** Foruzan cifra el número distintivo mediante la clave secreta simétrica que comparten Foruzan y Harry, K_{F-L}, y devuelve el número distintivo cifrado $K_{F-L}(R)$ a Harry.
  - ▶**4.** El hecho de que Foruzan conozca K_{F-L} y la use para cifrar un valor, permite a Harry saber que el mensaje recibido ha sido generado por Foruzan. El número distintivo se utiliza para cerciorarse que Foruzan se está comunicando en vivo.
  - ▶**5.** Harry descifra el mensaje recibido. Si el número distintivo descifrado coincide con el que envió a Foruzan. Foruzan quedará autenticada.
- **Esta versión** del protocolo se ilustra en la figura. Utilizando el valor distintivo, *R*, y comprobando el valor devuelto, $K_{F-L}(R)$, Harry puede asegurarse de que Foruzan es quien dice ser (ya que conoce el valor de la clave secreta necesaria para cifrar *R)* y está comunicándose en vivo (ya que ha cifrado el número distintivo, *R*, que Harry acaba de generar).
- **El uso de un número distintivo** y de la criptografía de clave simétrica forma la base de un protocolo de autenticación. Una pregunta natural es si se puede usar un número distintivo y criptografía de clave pública (en lugar de criptografía de clave simétrica) para resolver el problema de la autenticación.

AUTENTICACIÓN DEL PUNTO TERMINAL

¿Qué es el número distitivo *nonce*?

- **El *nonce*** o "número de un solo uso", es simplemente un número. Un número aleatorio y de características únicas que tiene como finalidad ser usado en sistemas criptográficos. Es un sencillo concepto, pero lo realmente difícil se encuentra en su implementación, hacerlo una realidad.
- **Pero**, ¿por qué es tan difícil implementarlo o ponerlo en práctica? La respuesta a esto viene implícita en la frase "número de un solo uso". Un *nonce* es un número aleatorio. Puede ser el número 1 o el número 1.000.0000.000 (mil millones), no importa, lo realmente importante es que su generación es ciertamente aleatoria**.**
- **La generación** de estos números es tarea de un generador de números aleatorios. Estos generadores pueden ser software o hardware, pero la tarea de ambos es la misma: crear números aleatorios únicos en todo momento. Cada número aleatorio o *nonce* generado, luego es tomado para ser usado en una función criptográfica específica.
- **Una vez allí**, la función lo usa dentro de su programación. Con ello genera una clave y al mismo tiempo se genera un ciclo de uso para ese *nonce* específico. Luego de este punto, dicho número jamás deberá ser usado nuevamente. Es en esto último donde se puede ver lo difícil en esta implementación. Y es que, garantizar que dicho número jamás se repita durante la existencia del sistema criptográfico es complejo.

AUTENTICACIÓN DEL PUNTO TERMINAL

Resumen y preguntas de repaso

(Kurose, 2017)

- **Resumen**. En esta presentación, se ha examinado la autenticación del punto terminal y se ha visto cómo pueden emplearse los números distintivos para frustrar los ataques por reproducción.
- ▶**P1.** ¿Cuál es el propósito de un número distintivo en un protocolo de autenticación de punto terminal?
- ▶**P2.** ¿Qué quiere decir que un número distintivo es un valor que solo se usa una vez en la vida? ¿En la vida de quién?
- ▶**P3**. El esquema de integridad de los mensajes basado en HMAC, ¿es susceptible a los ataques por reproducción? En caso afirmativo, ¿cómo se puede incorporar al esquema un número distintivo con el fin de eliminar dicha susceptibilidad?

MAPA DE LOS SIGUIENTES TEMAS DE SEGURIDAD EN REDES

AUTENTICACIÓN DEL PUNTO TERMINAL

¿Cómo se abordará la seguridad en redes?

- **Hasta aquí**, ya se han identificado las amenazas de seguridad en las redes modernas y se han identificado y definido las propiedades deseables en una comunicación segura.
- **Para una comunicación segura** es absolutamente necesario que los mensajes sean encriptados de alguna manera, para ello, se han analizado los principios de criptografía, las funciones hash criptográfica y las firmas digitales, para dotar de confiabilidad e integridad de los mensajes en las comunicaciones en la red. También se ha analizado cómo pueden emplearse los números distintivos para mejorar la seguridad implementando la autenticación del punto terminal.
- **En el siguiente tema** se analizará cómo se utilizan hoy en día las herramientas mencionadas para proporcionar servicios de seguridad en cualquiera de las cuatro capas superiores de la pila de protocolo de Internet.
- **Por último**, se considerará la seguridad operacional, la cual se ocupa de la protección de las redes institucionales frente a los ataques. En particular, firewalls y los sistemas de detección de intrusos.

Referencias bibliográficas

- CISCO (2015). *CCNA Routing and Switching. Introduction to Networks*. CISCO.
- CISCO (2016). *Introducción a las redes.* Madrid: Pearson Education, S.A.
- Forouzan, B. A. (2020). *Transmisión de datos y redes de comunicaciones.* Madrid: McGraw-Hill.
- Huawei Technologies (2020). *Basics of data communication networks*. Huawei.
- Kurose, J. Keith, R. (2017). *Redes de computadoras: un enfoque descendente*. Madrid: Pearson Education, S.A.

FIN

Tema 6 de:

SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.