7 SEGURIDAD EN LAS CAPAS DE PROTOCOLOS

Objetivo

- Describir cómo proporcionar servicios de seguridad en cualquiera de las cuatro capas superiores de la pila de protocolo de Internet.

Manual de clases

Última modificación:
3 de julio de 2022

Tema 7 de:
SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.

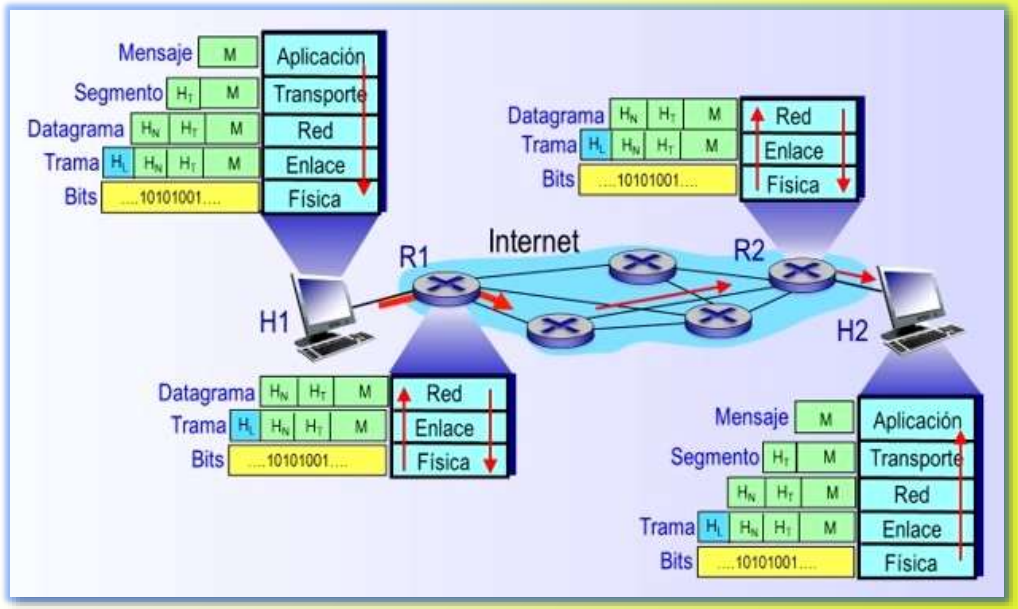
1.- SEGURIDAD EN INTERNET

SEGURIDAD EN LAS CAPAS DE PROTOCOLOS

Seguridad en las capas de protocolos

(Kurose, 2017)

- **En los temas anteriores** se han examinado una serie de problemas fundamentales en el campo de la seguridad de red, incluyendo las técnicas de criptografía de clave simétrica y de clave pública, las de autenticación de punto terminal, los mecanismos de distribución de claves, el problema de la integridad de los mensajes y las técnicas de firma digital. Ahora se va a examinar cómo se utilizan hoy en día dichas herramientas para proporcionar seguridad en Internet.
- **Es interesante observar** que es posible proporcionar servicios de seguridad en cualquiera de las cuatro capas superiores de la pila de protocolo de Internet.
  - ▶En la capa de aplicación. El enfoque consiste en utilizar una aplicación específica como el correo electrónico, como caso de estudio de las técnicas de seguridad de la capa de aplicación. Cuando se proporciona seguridad, como por ejemplo el cifrado PGP, para un protocolo específico de la capa de aplicación, la aplicación que utiliza ese protocolo disfrutará de uno o más servicios de seguridad, como los de confidencialidad, autenticación o integridad.
  - ▶En la capa de transporte. Después se descenderá por la pila de protocolo y se examinará el protocolo SSL, que proporciona seguridad a la capa de transporte. Cuando los mecanismos de seguridad se proporcionan para un protocolo de la capa de transporte, todas las aplicaciones que usan dicho protocolo disfrutarán de los servicios de seguridad del protocolo de transporte.



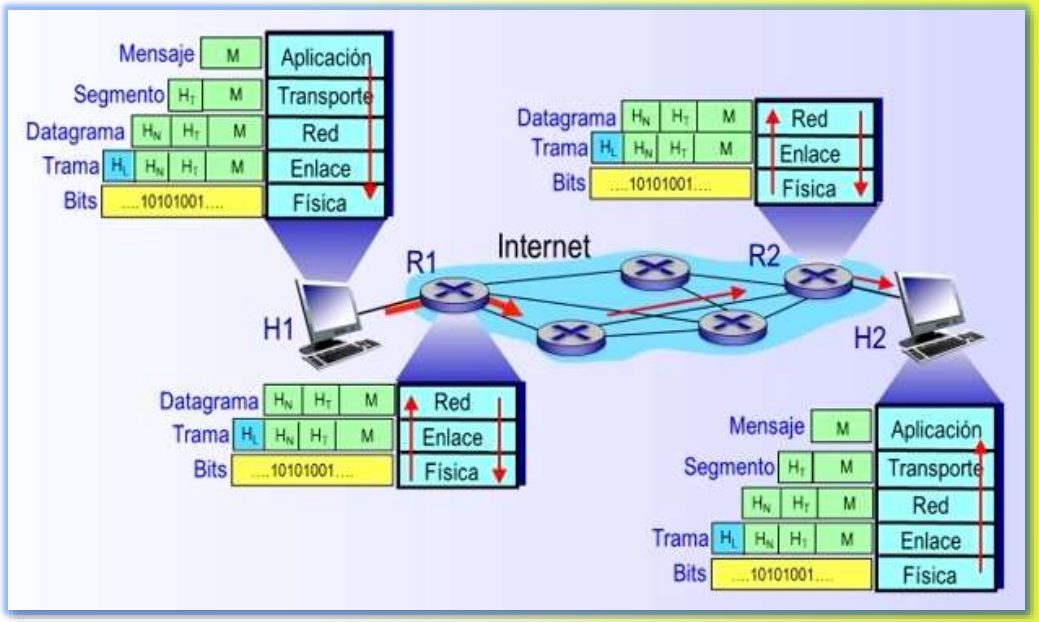
SEGURIDAD EN LAS CAPAS DE PROTOCOLOS

Seguridad en las capas de protocolos (cont.)

(Kurose, 2017)

- ▶En la capa de red. Se examinará el protocolo IPsec, que proporciona seguridad en la capa de red. Cuando la seguridad se proporciona en la capa de red, en un esquema host a host, todos los segmentos de la capa de transporte (y por tanto todos los datos de la capa de aplicación) disfrutarán de los servicios de seguridad de la capa de red.

- ▶En la capa de enlace. Se examinarán los mecanismos de seguridad del protocolo IEEE 802.11 para redes LAN inalámbricas. Cuando se proporciona seguridad a nivel de enlace, entonces los datos de todas las tramas que viajan a través del enlace utilizaran los servicios de seguridad del enlace.



SEGURIDAD EN LAS CAPAS DE PROTOCOLOS

Seguridad en las capas de protocolos (cont.)

(Kurose, 2017)

- **La tabla muestra** un resumen de los protocolos seguros desarrollados para dar seguridad a Internet y los dispositivos que protegen la infraestructura de redes.
- **En los siguientes temas** se examinaran varios protocolos de red seguros que disfrutan de un amplio uso en la práctica. Se verá que:
  - ▶La criptografía de clave simétrica se encuentra en el núcleo de PGP, SSL, IPsec y la seguridad inalámbrica.
  - ▶La criptografía de clave pública es crucial tanto para PGP como para SSL.
  - ▶PGP utiliza firmas digitales para proporcionar la integridad de los mensajes.
  - ▶SSL e IPsec utilizan códigos MAC.

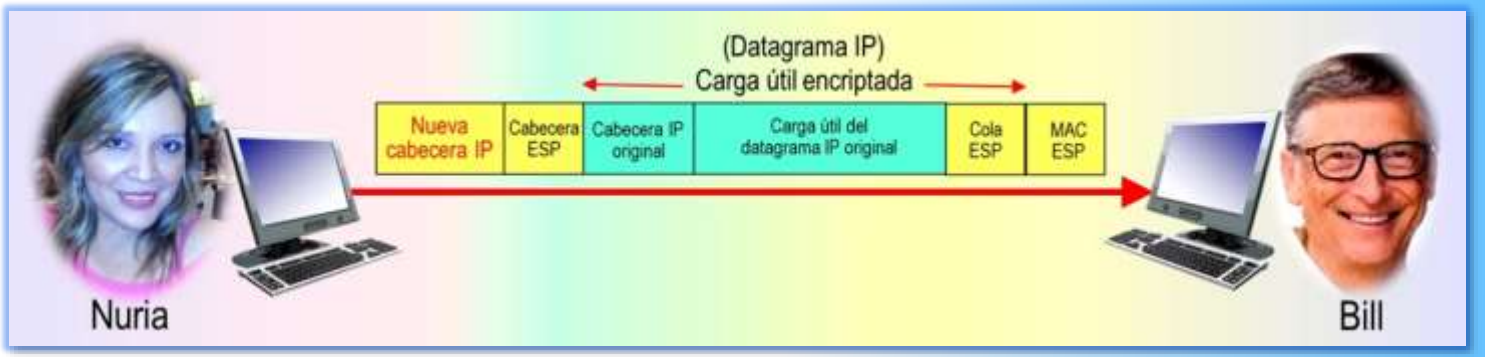
Propiedades de una comunicación segura			
1. Confidencialidad	**2. Integridad de los mensajes**	**3. Autenticación del punto terminal**	**4. Seguridad operacional**
Cifrado PGP para correo	Cifrado PGP para correo	Cifrado PGP para correo	Firewalls (Filtros de paquetes. Filtros con memoria del estado. Gateways de aplicación)
Protocolo TCP-SSL	Protocolo TCP-SSL	Protocolos de autenticación (Contraseñas y números distintivos)	Sistemas de Detección y de Prevención de Intrusiones
Protocolo IPsec (ESP)	Protocolo IPsec (AH, ESP)	Protocolo TCP-SSL Protocolo IPsec (AH, ESP)	Zonas de seguridad y zonas desmilitarizadas

SEGURIDAD EN LAS CAPAS DE PROTOCOLOS

¿Por qué la seguridad en las capas superiores?

(Kurose, 2017)

- **Surge la pregunta**: ¿porqué se proporciona la funcionalidad de seguridad en más de una capa dentro de Internet? ¿No bastaría simplemente con proporcionar la funcionalidad de seguridad en la capa de red?
- **Existen** dos respuestas a estas preguntas:
  - ▶**Respuesta 1.** En primer lugar, aunque la seguridad en la capa de red puede proporcionar la funcionalidad básica de cifrado de todos los datos contenidos en los datagramas (es decir de todos los segmentos de la capa de transporte) y de autenticar todas direcciones IP de origen, lo que no puede es ofrecer seguridad de nivel de usuario.



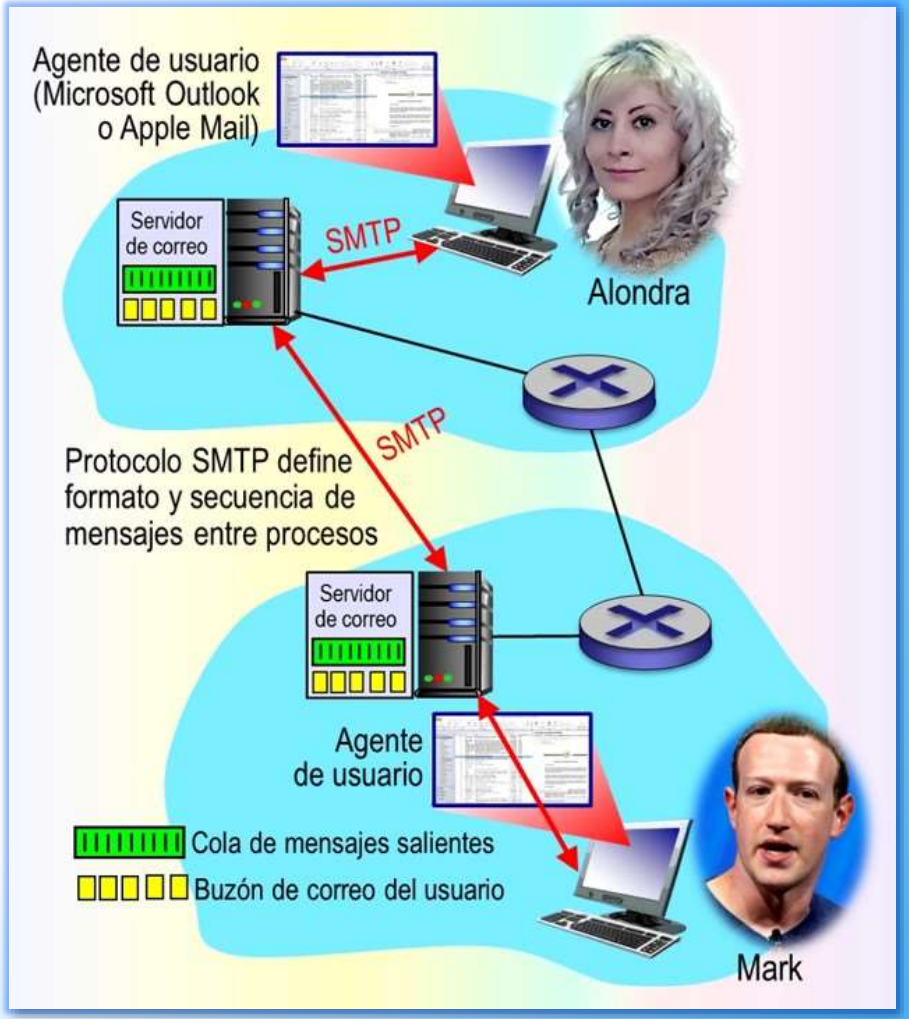
  - ✉ Por ejemplo, un sitio web de correo electrónico (Bill) no puede confiar en la seguridad de la capa IP para autenticar a un cliente (Nuria) que esté comprando bienes o servicios en ese sitio. Por tanto, existe una necesidad de incorporar funcionalidades básicas en la capas superiores.

SEGURIDAD EN LAS CAPAS DE PROTOCOLOS

¿Por qué la seguridad en las capas superiores? (cont.)

(Kurose, 2017)

- ▶**Respuesta 2.** En segundo lugar, es más fácil generalmente implantar servicios Internet nuevos, incluyendo los servicios de seguridad, en las capas superiores de la pila de protocolos. Mientras se espera a que un nuevo mecanismo de seguridad se implante de forma generalizada en la capa de red, lo que puede llegar a tardar años, muchos desarrolladores de aplicaciones simplemente se ponen manos a la obra e introducen la funcionalidad de seguridad en sus aplicaciones favoritas.
  - ✉ Un ejemplo clásico es PGP (*Pretty Good Privacy)*, que proporciona correo electrónico seguro. Requiere únicamente código de aplicación de cliente y de servidor. PGP fue una de las primeras tecnologías de seguridad y se utilizó ampliamente en Internet.
- **El siguiente tema** ofrece una vista panorámica de las aplicaciones de red y del transporte de sus datos, con el objetivo de tener una idea más precisa de cómo funcionan los protocolos y comprender el porqué y cómo se los puede convertir en protocolos seguros, temas que se abordarán posteriormente.



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 7 de:

SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.