2 PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

Manual de clases

Objetivo

- Describir varios de los principios que subyacen a las comunicaciones seguras.

Última modificación:
20 de junio de 2022

Tema 2 de:
SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.

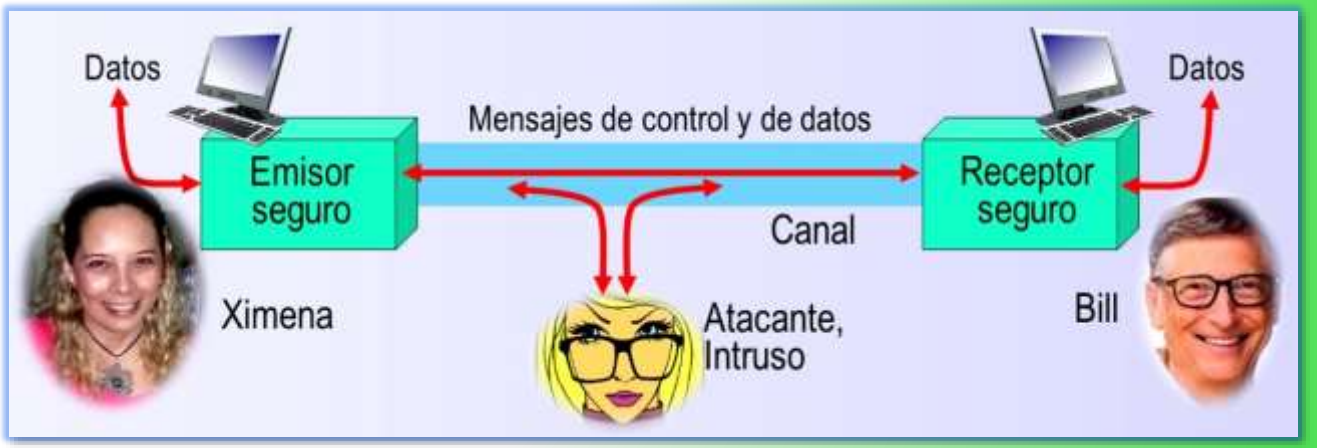
1.- ESCENARIO DE UNA COMUNICACIÓN SEGURA

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

¿Qué quiere decir comunicación segura?

(Kurose, 2017)

- **Se han descrito** algunos de los ataques más dañinos y predominantes en Internet, entre ellos los ataques de software malicioso, de denegación de servicio, de husmeadores, de enmascaramiento de orígenes y borrado y modificación de mensajes.
- **Ahora**, con los conocimientos de redes de computadoras y de los protocolos de Internet, se identificarán y definirán las propiedades deseables en una comunicación segura para, posteriormente, analizar cómo las redes pueden defenderse de los malos y garantizar una comunicación segura.
- **Para tener un visión panorámica** del escenario de la seguridad, se presenta a Ximena y a Bill que desean comunicarse y desean hacerlo "de manera segura", resaltando que estas dos personas podrían ser:
  - ▶Dos routers que desean intercambiar sus tablas de routing en forma segura.
  - ▶Un cliente y un servidor que desean establecer una conexión de transporte segura.
  - ▶Dos aplicaciones de correo electrónico que quieren intercambiar mensajes de correo seguros.



- **Los asuntos** amorosos, las comunicaciones en tiempo de guerra y las transacciones de negocios son las necesidades humanas de comunicaciones seguras habituales.

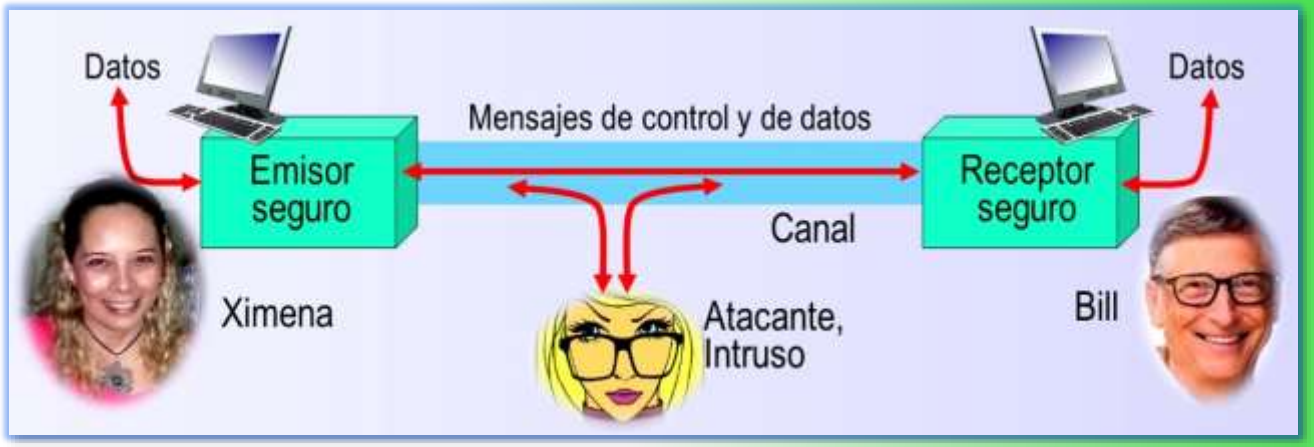
Escenario de una comunicación segura

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

¿Qué es la seguridad de red?

(Kurose, 2017)

- **Ximena y Bill** desean comunicarse de "forma segura", pero, ¿qué quiere decir esto exactamente? La seguridad es algo que tiene muchos matices. En realidad:
- ▶**Ximena** quiere que solo Bill sea capaz de comprender los mensajes que ella envía, incluso aunque estén comunicándose a través de un medio no seguro en el que un intruso pueda interceptar lo que Ximena transmite.



- ▶**Bill** también quiere estar seguro de que el mensaje que él recibe de Ximena fue realmente enviado por Ximena.
- ▶**Ximena** quiere estar segura de que la persona que se está comunicando con ella es realmente Bill.
- ▶**Ambos** también quieren estar seguros que el contenido de sus mensajes no ha sido alterado en el camino.
- ▶**Además**, quieren estar seguros de que siempre podrán comunicarse, es decir, que nadie les puede denegar el acceso a los recursos necesarios para comunicarse.

2.- PROPIEDADES DE UNA COMUNICACIÓN SEGURA

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

Propiedades de una comunicación segura

(Kurose, 2017)

- **Teniendo en cuenta** estas consideraciones, se pueden identificar las siguientes cuatro propiedades deseables en una comunicación segura.

Propiedades de una comunicación segura			
1. Confidencialidad	2. Integridad de los mensajes	3. Autenticación del punto terminal	4. Seguridad operacional

- ▶**1. Confidencialidad**. Solo el emisor y el receptor deberán comprender el contenido de los mensajes transmitidos. Puesto que los curiosos pueden interceptar los mensajes, es absolutamente necesario que los mensajes sean cifrados de alguna manera, de modo que un mensaje interceptado no pueda ser comprendido por el que lo ha interceptado.
  - Este aspecto de la confidencialidad es probablemente el concepto más comúnmente percibido del término comunicación segura.
- ▶**2. Integridad de los mensajes**. Las personas que se comunican quieren estar seguras de que el contenido de sus comunicaciones no se vea alterado durante la transmisión, ni maliciosamente ni por accidente.
  - En los protocolos TCP/IP, se pueden emplear extensiones a las técnicas de detección de errores CRC en los protocolos de enlace de datos y de suma de comprobación en los protocolos de transporte fiable, para proporcionar integridad a los mensajes.

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

Propiedades de una comunicación segura (cont.)

(Kurose, 2017)

- **▶3. Autenticación del punto terminal**. Tanto el emisor como el receptor deberán poder confirmar la identidad del otro en el proceso de comunicación (confirmar que el otro es de hecho quien dice ser). La comunicación humana frente a frente resuelve este problema fácilmente gracias al reconocimiento visual. Cuando las entidades se comunican a través de un medio en el que no es posible ver al otro, la autenticación no es tan sencilla.
  - Por ejemplo, cuando un usuario accede a su bandeja de entrada ¿cómo verifica el servidor de correo que el usuario es la persona que dice ser?

Propiedades de una comunicación segura			
1. Confidencialidad	2. Integridad de los mensajes	3. Autenticación del punto terminal	4. Seguridad operacional

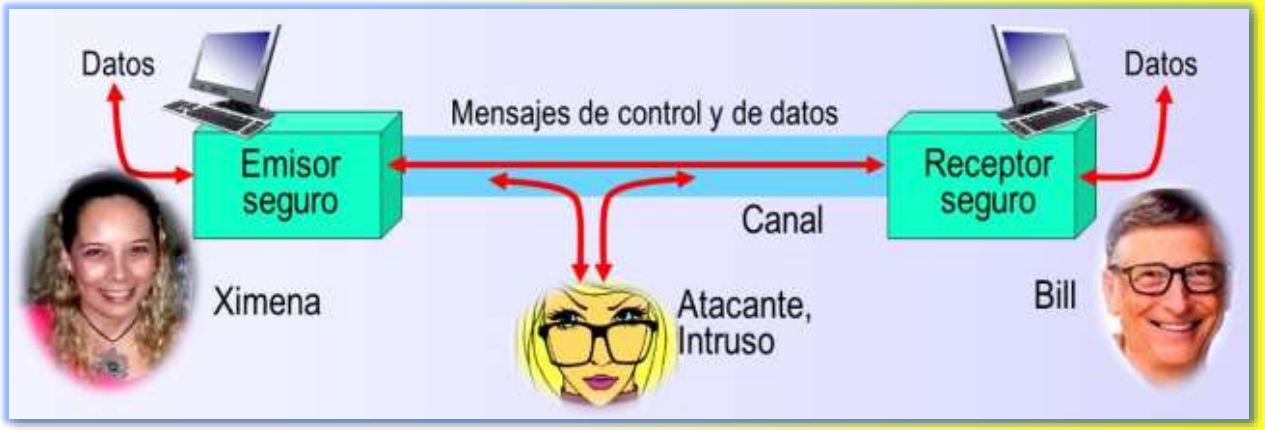
- **▶4. Seguridad operacional**. Casi todas las organizaciones (empresas, universidades, etc.) disponen de redes que están conectadas a Internet. Estas redes pueden, potencialmente, verse comprometidas. Los atacantes pueden intentar depositar gusanos en los hosts de la red, conseguir secretos corporativos, realizar un mapa de las configuraciones internas de la red y ejecutar ataques DoS.
  - Para responder a estos ataques, se emplean dispositivos operacionales como los firewalls y los sistemas de detección de intrusiones. Un firewall se coloca entre la red de la organización y la red pública, controlando el acceso de paquetes procedentes de Internet. Un sistema de detección de intrusiones realiza una “inspección profunda de los paquetes”, alertando a los administradores de la red cuando detecta cualquier actividad sospechosa.

Propiedades de una comunicación segura

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

¿A qué información puede acceder un atacante? (Kurose, 2017)

- **Una vez establecido** el concepto de la seguridad de la red, se analizará exactamente a qué información puede tener acceso un atacante y qué acciones puede llevar a cabo.
- **Ximena es el emisor** y desea enviar datos a Bill que es el receptor. Para intercambiar datos de forma segura y poder cumplir los requisitos de confidencialidad, integridad de los mensajes y autenticación del punto terminal, Ximena y Bill intercambiarán mensajes de control y mensajes de datos (de forma similar a cómo los emisores y receptores TCP intercambian segmentos de control y segmentos de datos).



- **Normalmente**, todos o algunos de estos mensajes serán cifrados. Potencialmente un atacante o intruso puede:
  - ▶Curiosear, es decir husmear y registrar los mensajes de control y de datos que se transmiten por el canal.
  - ▶Modificar, insertar o borrar mensajes o el contenido de los mismos.
- **A menos** que se tomen las contramedidas adecuadas, estas capacidades permitirán a un atacante o intruso montar una amplia variedad de ataques contra la seguridad de la red: escuchando las comunicaciones (posiblemente robando las contraseñas y los datos), suplantando a otra entidad, pirateando una sesión activa, denegando el servicio a los usuarios legítimos de la red, por sobrecarga, de los recursos del sistema, etc.

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

Resumen y preguntas de repaso

(Kurose, 2017)

Resumen. En esta presentación, se han examinado los diversos mecanismos que los actores, Ximena y Bill, pueden utilizar para comunicarse de forma segura. Se ha visto que Ximena y Bill están interesados en la confidencialidad (en el sentido de que solo ellos sean capaces de entender el contenido de los mensajes transmitidos), en la integridad de los mensajes (quieren estar seguros de que sus mensajes no son alterados en el camino) y en la autenticación del punto terminal (con el fin de estar seguros de que están hablando entre ellos).

- ▶**P1.** ¿Cuáles son las diferencias entre la confidencialidad de los mensajes y la integridad de los mismos? ¿Puede existir confidencialidad sin integridad? ¿Puede existir integridad sin confidencialidad? Justifique su respuesta.
- ▶**P2**. Las entidades de Internet (routers, switches, servidores DNS, servidores web, sistemas terminales de usuario, etc.) a menudo necesitan comunicarse de forma segura. Proporcione tres parejas específicas de ejemplo de entidades de Internet que puedan desear comunicarse de forma segura.

MAPA DE LOS SIGUIENTES TEMAS DE SEGURIDAD EN REDES

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

¿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 cifrados de alguna manera, por lo tanto, en el **siguiente tema** se analizará cómo pueden utilizarse los **principios de criptografía** de clave simétrica y de clave pública para dotar de confiabilidad a las comunicaciones en la red y se continuará con otras técnicas.

Principales ataques a las redes modernas			
1. Introducción de software malicioso	**2. Ataque a los servidores y a la infraestructura de red**	**3. Examen y análisis de paquetes**	**4. Suplantación IP**
Virus	Ataque de vulnerabilidad	Programas sniffers	Inyección de paquetes
Gusano	Inundación del ancho de banda		
Troyano	Inundación de conexiones		

Propiedades de una comunicación segura			
1. Confidencialidad	**2. Integridad de los mensajes**	**3. Autenticación del punto terminal**	**4. Seguridad operacional**

- **Luego**, se analizarán y seleccionarán los protocolos seguros en cada una de las cuatro capas superiores, comenzando por la capa de aplicación.
- **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.

PROPIEDADES DESEABLES DE UNA COMUNICACIÓN SEGURA

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 2 de:

SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.