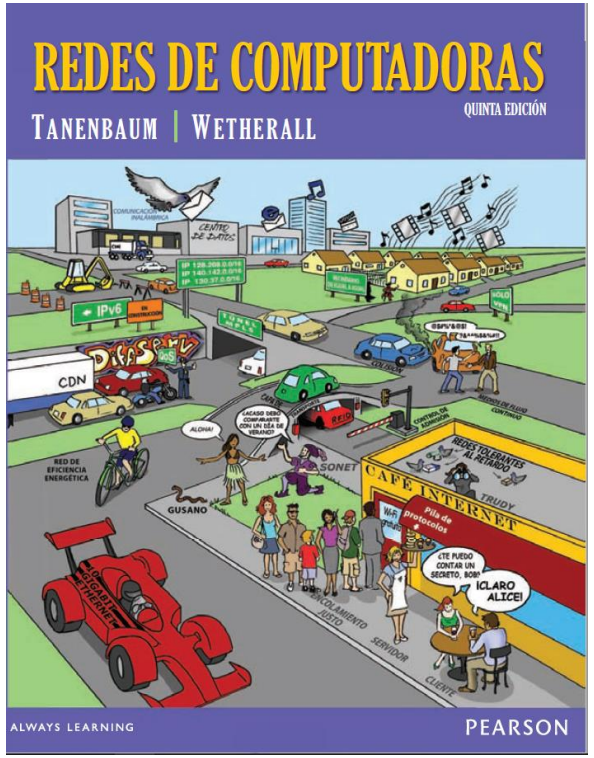
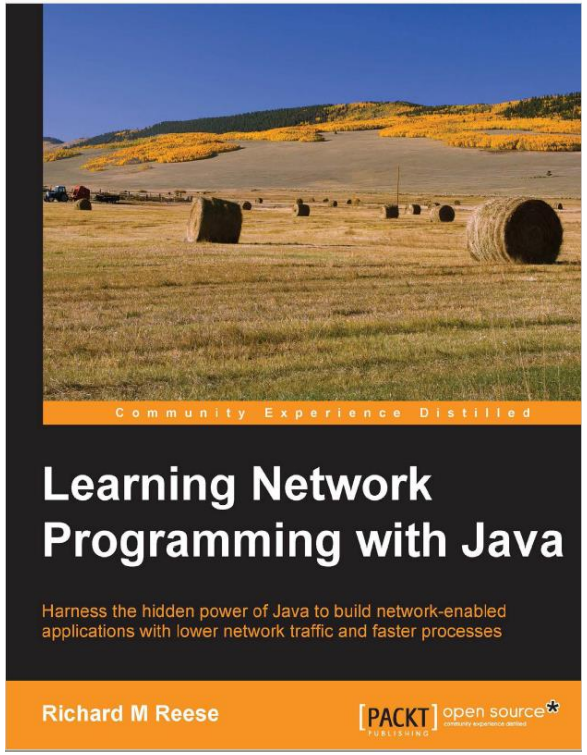
REDES DE COMPUTADORES Y LABORATORIO

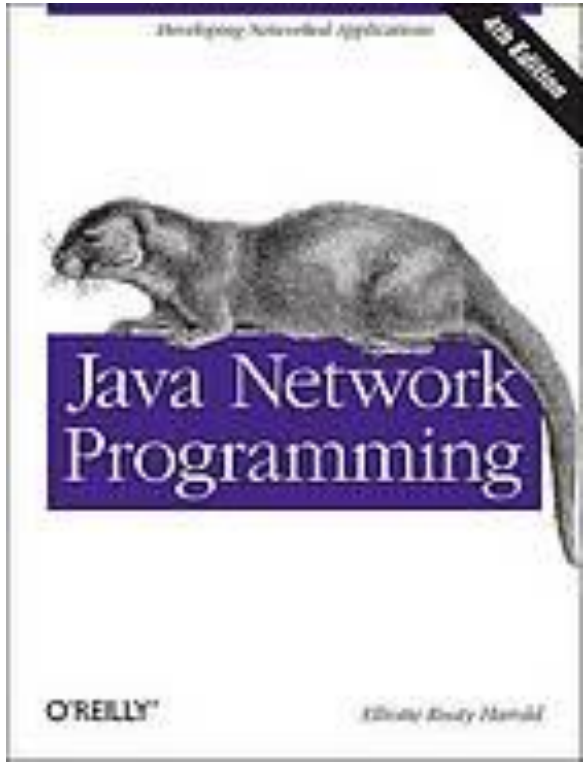
Christian Camilo Urcuqui López, MSc

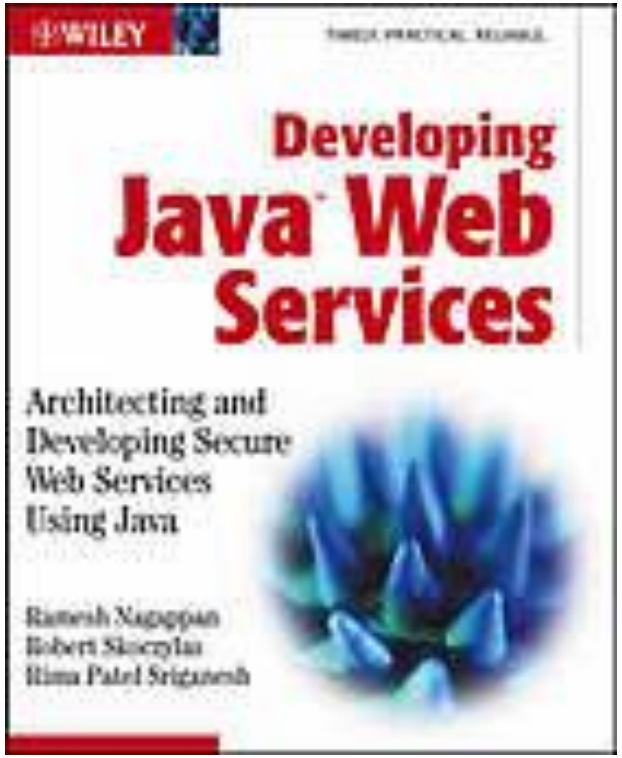
UNIVERSIDAD ICESI | A OTRO NIVEL

BIBLIOGRAFÍA









RECORDEMOS...

SESIÓN 1

- ¿Qué es una red?
- ¿Cuáles son los elementos de una red de comunicaciones?
- ¿Cómo se clasifica una red y que tipos existen?
- ¿Cuáles son los componentes de una estructura de una red y que topologías existen?
- Explique el funcionamiento de una red
- Interredes
- Explique los modelos de referencia, protocolos y redes basadas en niveles
- Explique las capas de una red
- ¿Qué es una dirección IP, un nombre de dominio y un puerto?

SESIÓN 2

- ¿Qué es una dirección IP, un nombre de dominio y un puerto? (de la sesión 2)
- Explique el modelo de referencia OSI (capa 1-3)
- Explique el modelo de referencia OSI (capa 4-7)
- Explique Internet, firewall y proxy server

SESIÓN 3

- Explicar la definición y el uso de las direcciones IP
- Explicar el direccionamiento en Internet y las clases de direcciones IP
- Describir DNS
- Aplicar los Factory methods de la API de Java **(Desarrollo)**

SESIÓN 4

- Aplicar los Factory methods de la API de Java **(Desarrollo)**
- Comparé los modelos de referencia OSI y TCP/IP.
- Explicar las unidades métricas de cantidad de información.
- Explicar la aplicación del análisis de red para la investigación de amenazas cibernéticas. **(Investigación)**

SESIÓN 5

- Explicar cliente/servidor
  - ¿Qué es?
  - ¿Cuáles son los componentes básicos?
  - Tipos de arquitectura Cliente/Servidor
  - ¿Cuáles son los mecanismos involucrados en una comunicación entre cliente/servidor?
- Explicar el uso de puertos y sockets.
  - Defina puerto y explique la asignación universal y dinámica.
  - Defina socket, ¿Qué elementos debe especificar una aplicación para crear un socket?
- Aplicar los métodos de Java para la comunicación entre un cliente (jueves y viernes)
  - Socket (cliente/servidor), Streams (flujos), Buffer

SESIÓN 6

- Defina que debe hacer un componte servidor y uno de cliente
- Aplicar los métodos de Java para la comunicación entre un cliente (**Desarrollo**)
  - Socket (cliente/servidor), Streams (flujos), Buffer
- Identificar los componentes de acceso al medio alambrado
  - Describa los medios de transmisión guiados. Enuncia los tipos de enlaces.

SESIÓN 7

- Identificar los componentes de acceso al medio alambrado.
  - Describa los medios de transmisión guiados. Describa los tipos de enlaces: medios magnéticos, par trenzado, cable coaxial, líneas eléctricas, fibra óptica (cables de fibras y comparación entre fibra óptica y alambre de cobre).
- Explicar los medios de transmisión no guiados.
  - Describa el espectro electromagnético y la radiotransmisión.
  - Describa la transmisión por microondas y las políticas del espectro electromagnético.
  - Describa la transmisión infrarroja y la transmisión por ondas de luz.
- Enuncie los tipos de Redes (complemento)

SESIÓN 8

- Describe la ciberseguridad y los pilares fundamentales de la seguridad de la información.
- Explique la administración de recursos de un sistema operativo
  - Tipos de recursos
  - Gestión de procesos
  - Gestión de memoria
  - Comunicación y sincronización entre procesos
  - Construcción y ejecución de programas
- Explique multihilos (**desarrollo**)
  - ¿Qué son hilos?¿cuales son las razones para utilizarlos?
  - Miltihilos en Java
  - Propiedades de los hilos
- Enuncie algunos elementos de la API de Java para la aplicación de multihilos (**desarrollo**)

SESIÓN 9

- Identifica las bases de datos de la Universidad para la búsqueda de literatura
- Enuncie algunos elementos de la API de Java para la aplicación de multihilos (**desarrollo**)
  - Aplique la API de Java para el desarrollo de hilos con prioridades.
  - Aplique la API de Java para la gestión de grupos de hilos.
  - Aplique la API de Java para la sincronización de hilos

SESIÓN 10

- Identifique el hardware de las 2 últimas capas del modelo OSI.
  - Explique la capa de enlace de datos
  - Explique redes Ethernet LAN
  - Explique IEEE 802.3 y 802.11
- Explique la capa de enlace de datos
  - Defina el uso de los puentes
  - Explique la operación de los dispositivos por capas
  - Defina una red VLAN

PARCIAL NÚMERO 1

CONTENIDO TEORÍA 40% - 20 preguntas	CONTENIDO APLICATIVO 40% - 4 requerimientos
INVESTIGATIVO 20%	

NO ENTRA EN LA PARTE TEÓRICA...

SESIÓN 11

- Describa la seguridad en redes y la criptografía
  - Clave simétrica, criptoanálisis, criptología (criptografía)
  - El principio de *Kerckhoof*
- Describa IPSec
  - Modo de transporte
  - Modo de túnel
- Describa VPN
- Describa firewall

ALGORITMOS DE CLAVE SIMÉTRICA

- **Algoritmos de clave simétrica** utilizan la misma clave para encriptar y desencriptar.
- DES, triple DES, AES

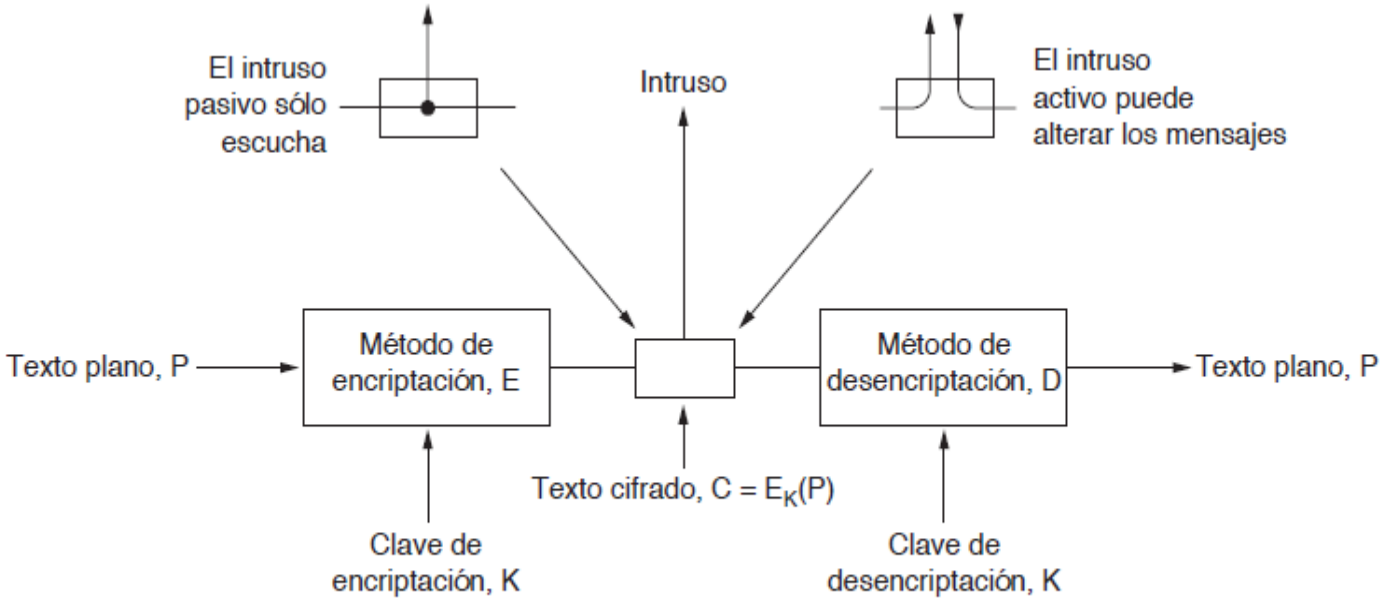
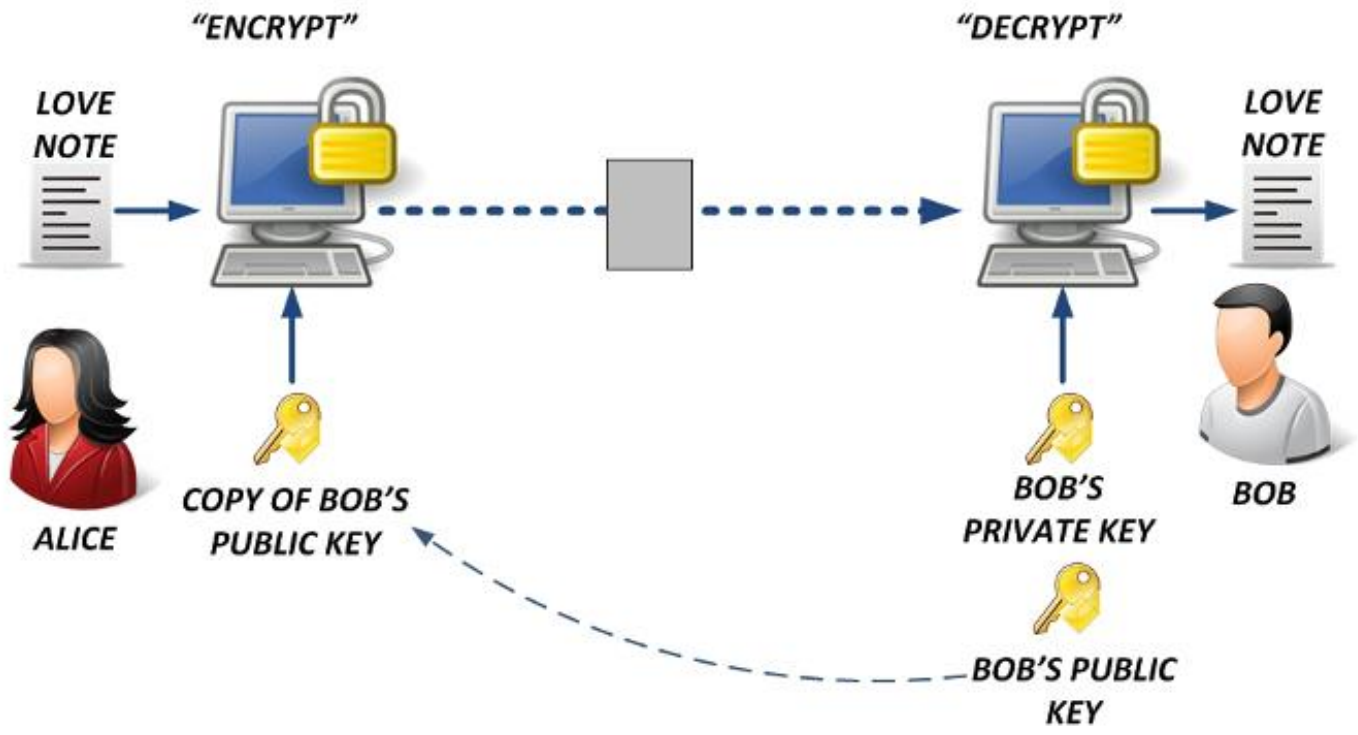


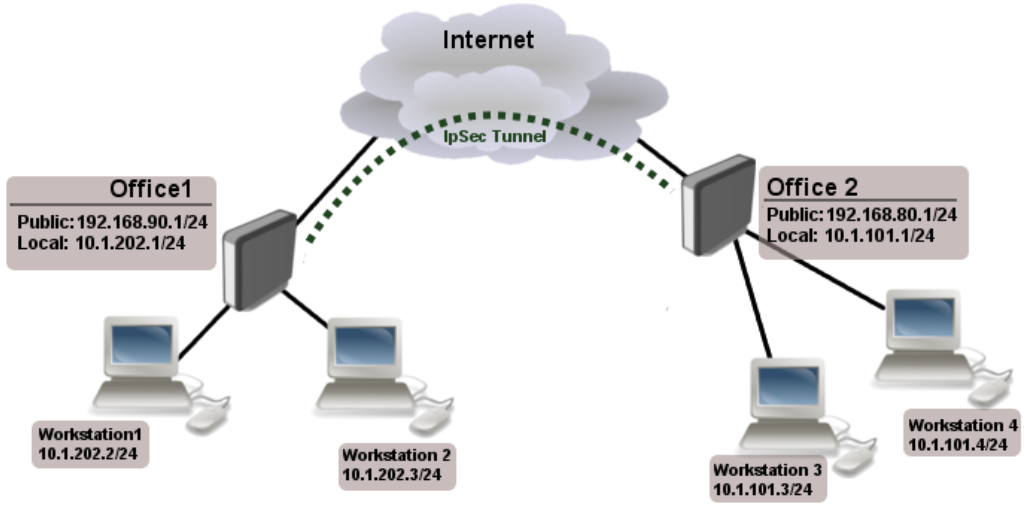
Figura 8-2. Modelo de encriptación (para un sistema de cifrado de clave simétrica).

ALGORITMOS DE CLAVE PÚBLICA



IPSEC – IP SECURITY

- Es un estándar de seguridad de la capa de red, específicamente, un marco de trabajo que integra **múltiples servicios, algoritmos y niveles de granularidad**.
- Un encriptado de extremo a extremo a través de clave simétrica.
- https://www.ietf.org/about/who/
- https://www.rfc-editor.org/info/rfc2401

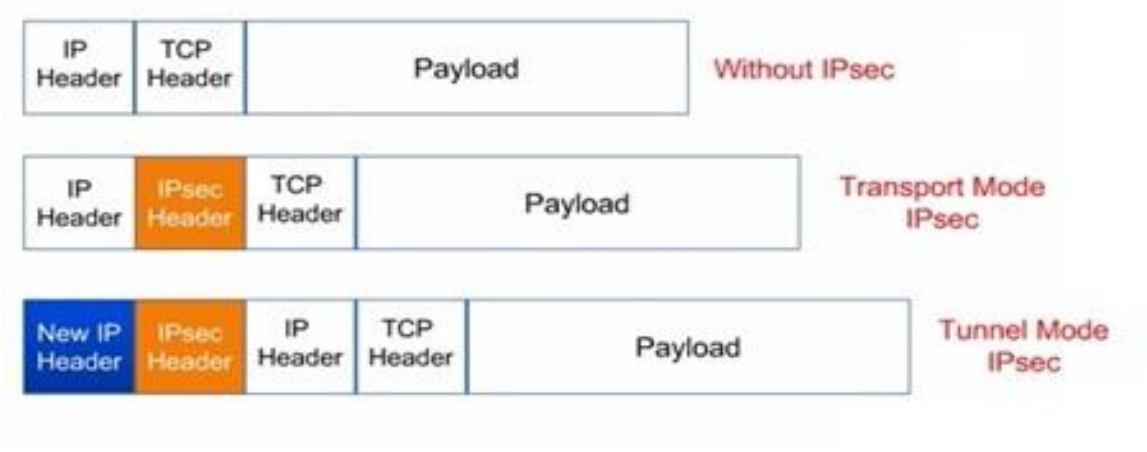


IPSEC – IP SECURITY

- Orientado a conexión.
- Los servicios principales son confidencialidad, integridad y protección contra ataques de repetición.
- Una SA (Asociación de seguridad) es una conexión simple entre dos nodos que tiene asociado un identificador de seguridad.
- Puede ser utilizado de dos modos:
  - **Modo de transporte**.
  - **Modo túnel.**

IPSEC – IP SECURITY

- **Modo de transporte**
  - El encabezado IPSec contiene información de seguridad, principalmente el identificador de SA, un nuevo número de secuencia y tal ves una verificación de integridad del campo de carga.
- **En el modo de túnel**
  - Todo el paquete IP, con encabezado y demás información es encapsulado en el cuerpo de un paquete IP nuevo. Es muy útil cuando los datos no terminan en el destino final, por ejemplo un firewall. Es muy utilizado en redes privadas virtuales (VPN).



IPSEC – IP SECURITY

- **AH** (**Encabezado de Autentificación**) proporciona la verificación de integridad y la seguridad anti repetición, pero no la confidencialidad (es decir, no hay encriptación de datos).
- El *Índice de parámetros de seguridad* es el identificador de la conexión. El emisor lo inserta para indicar un registro específico en la base de datos del receptor.

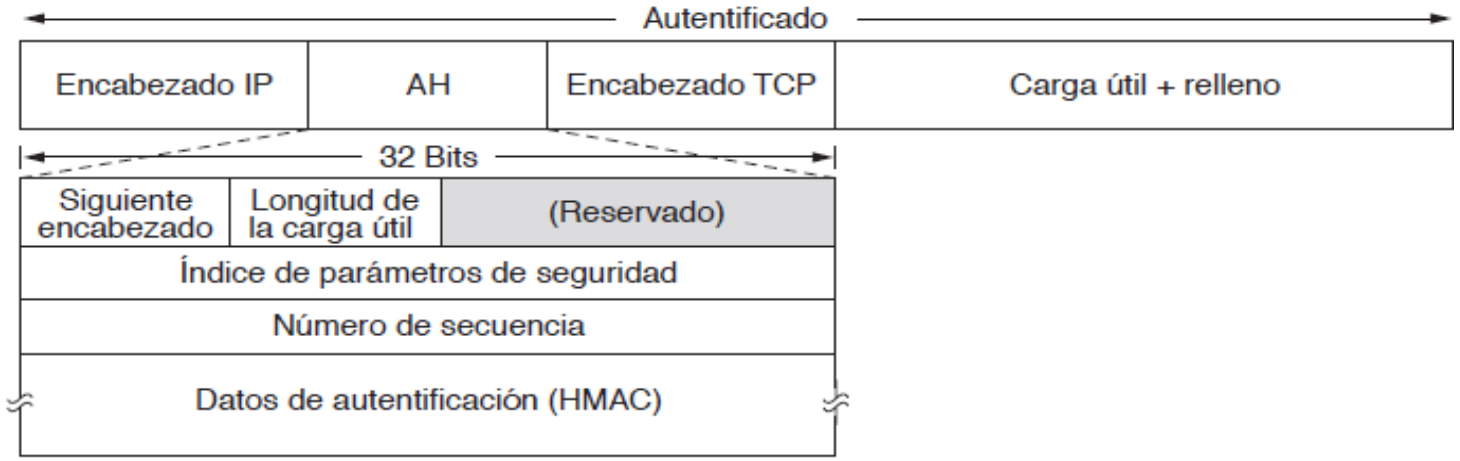


Figura 8-27. El encabezado de autentificación de IPsec en el modo de transporte para IPv4.

IPSEC – IP SECURITY

- El campo *Número de secuencia* se utiliza para numerar todos los paquetes enviados en una SA. Permite detectar ataques de repetición. No es el mismo número de secuencia.
- *Datos de autentificación*, contiene la firma digital de la carga útil, es decir, el cálculo del hash del paquete más la clave compartida. El algoritmo de firmas.

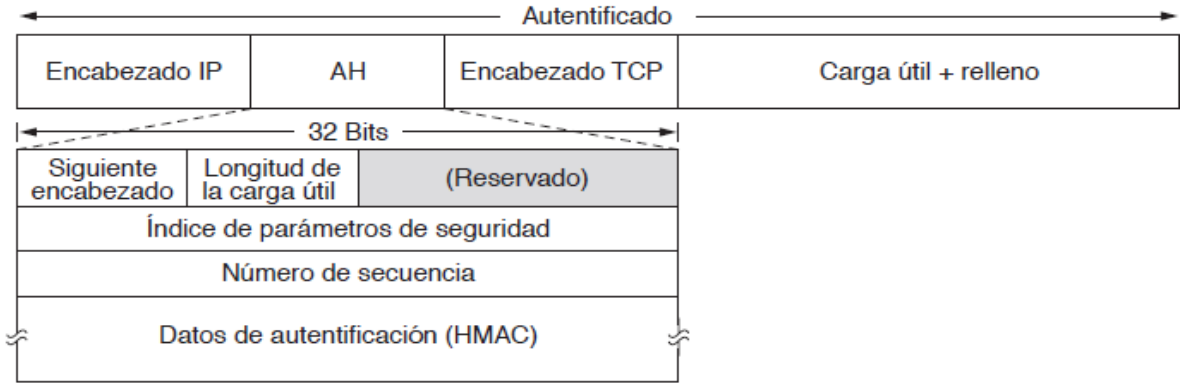


Figura 8-27. El encabezado de autentificación de IPsec en el modo de transporte para IPv4.

FIREWALL

- Los firewall (servidores de seguridad) actúan como un filtro de paquetes a través de una inspección y un conjunto de reglas formuladas por el administrador de la red.
- El conjunto de reglas se encuentra compuesto por origines y destinos aceptables.

VPN

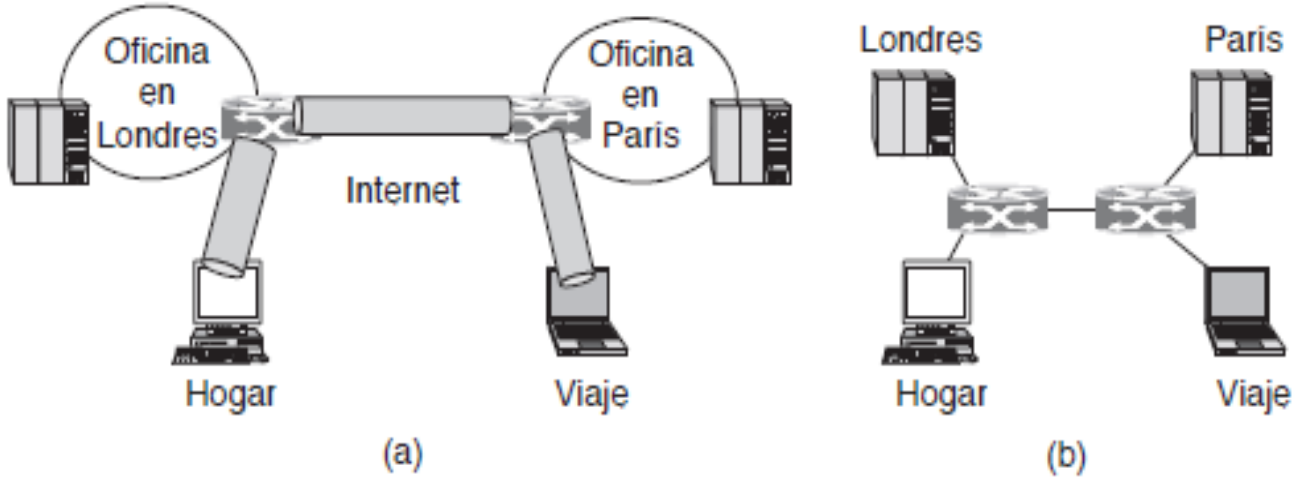


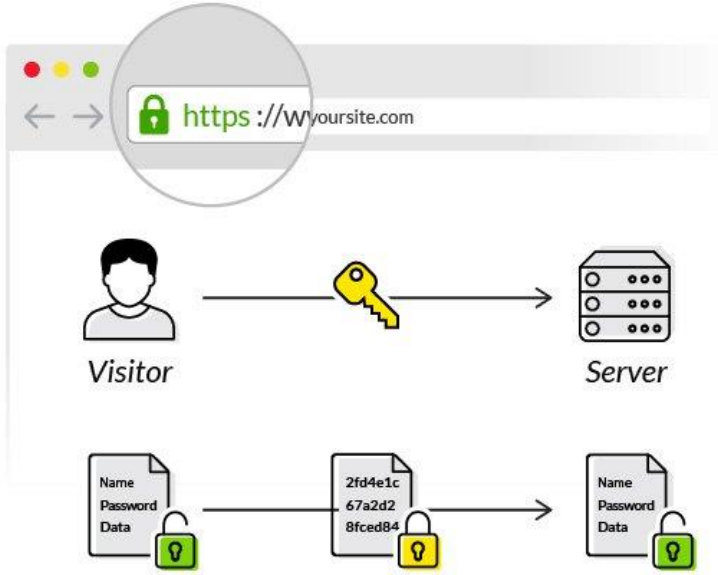
Figura 8-30. (a) Una red privada virtual. (b) La topología vista desde el interior.

SEGURIDAD INALÁMBRICA

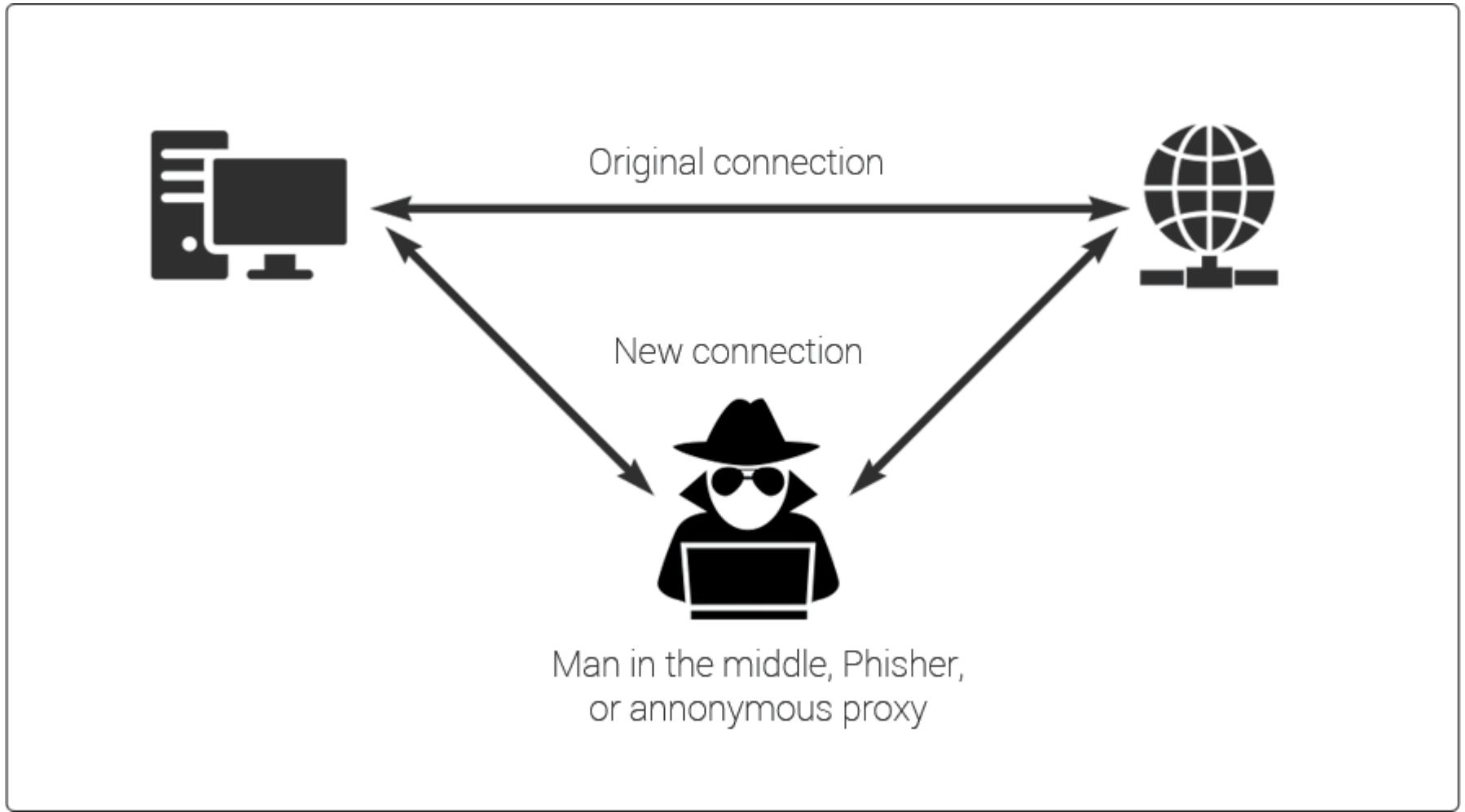
- La tecnología inalámbrica es el sueño de todo espías, datos gratuitos sin tener que hacer nada. Por lo tanto, sobra decir que la seguridad es mucho más importante para los sistemas inalámbricos que para los cableados.
- WPA2 y WPA3

SECURE SOCKETS LAYER

"SSL permite asegurar una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal."

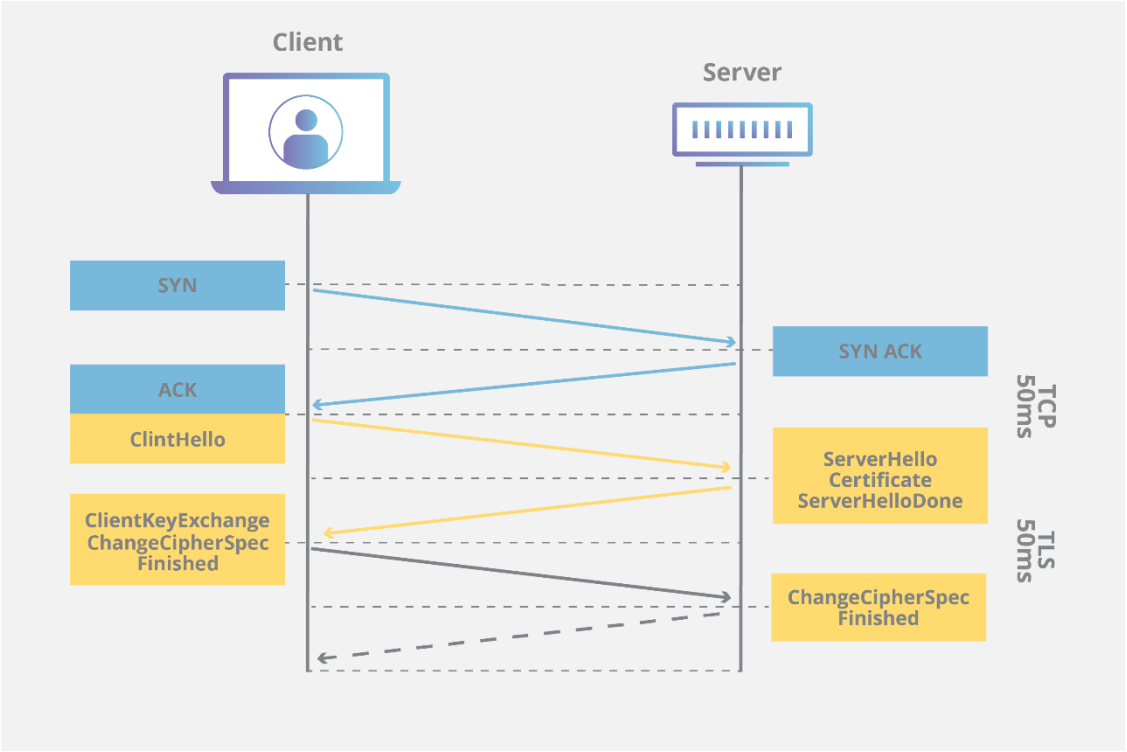


MAN IN THE MIDDLE



TRANSPORT LAYER SECURITY

"Es solo una versión actualizada y más segura de SSL, es decir, son certificados que implementan cifrados ECC, RSA o DSA. Funciona en la capa de transporte."



HYPER TEXT TRANSFER PROTOCOL SECURE

"HTTPS aparece en la dirección URL cuando un sitio web está protegido por un certificado SSL. Un certificado incluye información sobre la entidad emisora y el nombre corporativo del propietario del sitio web, se pueden ver haciendo clic en el símbolo de candado de la barra del navegador."

SEGURIDAD DE LA INFORMACIÓN

- Seguridad de la información – ISO 27001, define activo de información los datos que tienen valor para una empresa

Ley 1273 de 2009

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

https://youtu.be/ewsnP85vSTc?list=PLGsF4QfCJgJnSOG4X9QOJYe15Zdeymr_9

LECTURAS

Material utilizado	1. Arboleda, L. (2012). Programación en Red con Java. 2. Harold, E. (2004). Java network programming. " O'Reilly Media, Inc.". 3. Tanenbaum, A. S. (2003). Redes de computadoras. Pearson educación. 4. Reese, R. M. (2015). Learning Network Programming with Java. Packt Publishing Ltd.
Actividades DESPUÉS de clase	A2. Leer la sección 8 del libro 1

PRÓXIMAS CLASES

- Aplicar las clases de Java para exponer servicios no orientados a la conexión - UDP

REFERENCIAS

1. https://3.bp.blogspot.com/-RPoJvwyN3Ic/WtQVBltajaI/AAAAAAAAALWY/tzutcLAvXlwvHM0TSOyho2GxduDG14HIwCLcBGAs/s640/Site-to-site-ipsec-example.png
2. http://www.rfwireless-world.com/images/IPSec-Transport-mode-vs-IPSec-Tunnel-mode.jpg
3. http://richardgoyette.com/Infosec/Alice/images/encrypt3.jpg
4. https://www.websecurity.symantec.com/es/es/security-topics/what-is-ssl-tls-https
5. https://www.cloudflare.com/img/learning/cdn/tls-ssl/tls-ssl-false-start-handshake.png