

# Módulo 06 Seguridad en Redes (Pt. 3)



Redes de Computadoras  
Depto de Cs. e Ing. de la Comp.  
Universidad Nacional del Sur



---

---

---

---

---

---

---

---

---

---

## Copyright

- Copyright © 2010-2024 A. G. Stankevicius
- Se asegura la libertad para copiar, distribuir y modificar este documento de acuerdo a los términos de la **GNU Free Documentation License**, versión 1.2 o cualquiera posterior publicada por la Free Software Foundation, sin secciones invariantes ni textos de cubierta delantera o trasera
- Una copia de esta licencia está siempre disponible en la página <http://www.gnu.org/copyleft/fdl.html>
- La versión transparente de este documento puede ser obtenida de la siguiente dirección:

<http://cs.uns.edu.ar/~ags/teaching>

---

---

---

---

---

---

---

---

---

---

## Contenidos

- Introducción a la seguridad en redes
- Principios de la criptografía
- Autenticación
- Integridad
- Distribución de claves y de certificados
- Seguridad multinivel

---

---

---

---

---

---

---

---

---

---

## Mails seguros

- Las técnicas criptográficas repasadas permiten el intercambio seguro de correos electrónicos
  - El emisor seguro genera una clave simétrica privada  $K_S$  al azar
  - Posteriormente, encripta el cuerpo  $m$  del mail con  $K_S$  (naturalmente, por razones de eficiencia)
  - A su vez, encripta  $K_S$  con la clave pública  $K^*_R$  del receptor seguro
  - Finalmente, el emisor envía tanto  $K_S(m)$  como  $K^*_R(K_S)$  al receptor

---

---

---

---

---

---

---

---

## Mails seguros

- Continúa:
  - El receptor seguro recibe  $K_S(m)$  como  $K^*_R(K_S)$
  - Usando su clave privada  $K^*_R$  descripta la clave simétrica  $K_S$  creada al azar por el emisor seguro
  - Una vez recuperada la clave simétrica, descripta el cuerpo del mail, accediendo a su contenido  $m$

---

---

---

---

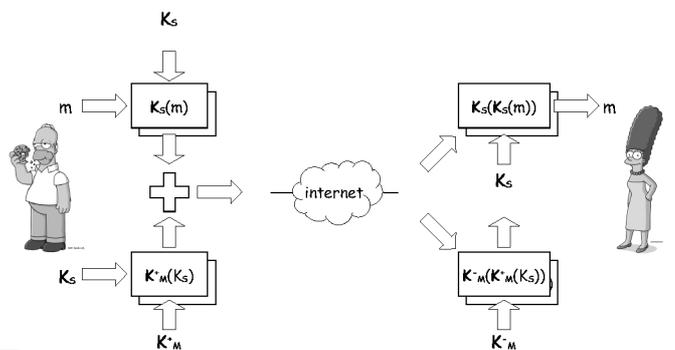
---

---

---

---

## Mails seguros



---

---

---

---

---

---

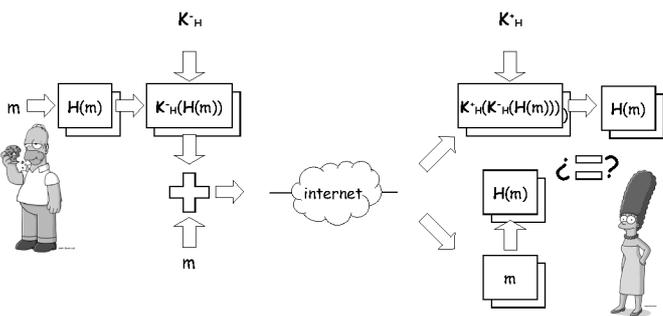
---

---

## Mails autenticados

- El mecanismo de firma digital antes introducido se puede adaptar para posibilitar el intercambio autenticado de correos electrónicos
  - El emisor autenticado simplemente firma digitalmente el cuerpo de todo mensaje enviado
  - Al igual que antes, se adjunta la firma digital (huella digital encriptada) al mensaje original (es decir, sin encriptar)
  - De esta forma se logra autenticar el autor y se asegura la integridad del contenido del mensaje

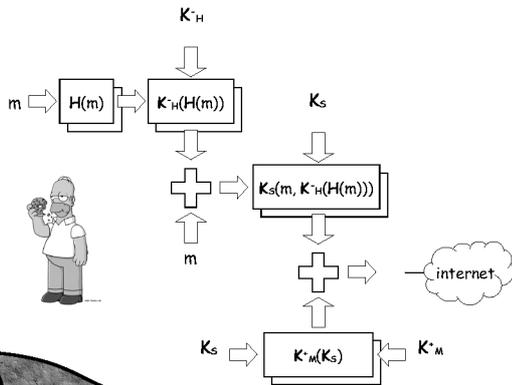
## Mails autenticados



## Mails seguros autenticados

- Ambas técnicas pueden ser combinadas con relativa facilidad, haciendo uso de tres claves:
  - La clave privada del emisor, para firmar digitalmente el mensaje encriptado
  - Una clave simétrica generada al azar para encriptar el cuerpo del mensaje
  - La clave pública del receptor, para encriptar la clave simétrica

## Mails seguros autenticados




---

---

---

---

---

---

---

---

---

---

## OpenPGP

- El estándar abierto OpenPGP reportado en la **RFC 4880** implementa el intercambio seguro y autenticado de correos electrónicos
  - Hace uso de criptografía de clave simétrica, de criptografía de clave pública, una función de hash para calcular digestos y firma digital de la forma antes indicada
  - Permite asegurar la identidad del emisor y tanto la confidencialidad como la integridad del mensaje

---

---

---

---

---

---

---

---

---

---

## Pretty Good Privacy

```
Date: Mon, 28 Jun 2010 01:47:41 -0300
From: "Alejandro G. Stankevicius" <ags@cs.uns.edu.ar>
MIME-Version: 1.0
To: "Alejandro G. Stankevicius" <ags@cs.uns.edu.ar>
Subject: Prueba de mensaje autenticado.
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Probando... 1, 2, 3.

- - -
Saludos,
Alejandro.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.15 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

iEYEARECAAYFAkroKhwACgkQ54MJ5e1PszZomvCFV0+8E0t9qHwv9r8S6aIH6o
fkEAn3xqjFTD04s9doQt1JjxzoL6J5Pa
=4ni4

-----END PGP SIGNATURE-----
```

---

---

---

---

---

---

---

---

---

---

# Pretty Good Privacy

```
Date: Mon, 28 Jun 2010 01:48:32 -0300
From: "Alejandro G. Stankevicius" <ags@cs.ums.edu.ar>
MIME-Version: 1.0
To: "Alejandro G. Stankevicius" <ags@cs.ums.edu.ar>
Subject: Prueba de mensaje autenticado y seguro.
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v2.0.15 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQIOA8pZr5aB6LjFEAT9Fs4q7L1721BcLtoiPnX11bePry0KAn9LmXR99xkd
pju/Kc6qBny9F2uuqVgd4WfEE42p11A0aU0f11/GKEcj iN2KJx5Lcvp06zXf0
Q3rK0T/XL2H5kuqZtho9090wRrS00UcXejv5rj#8LcMGR9vrrhm=03u80hX24R
VcZL0p0S65=7d8XpmncxskfLuv3rAEem9fjBz0u0I1KAfGf0A0K0cyZ071R
A2frSpk0eLNLB3sLz4x0D0u9VTDu9oaL/CHZId3mxHsj60yC0=SwRgRk2Za-R
S9HuhRy2P07y#Uhrf0G1kaXwe3JKE60yG1vawawf9FahNWhKcB0rYrJp*SU3
s7313u871uV0R5s90YSr/2zes74enw0Dp1enReud0a91z1h.Bg3u/GUj1sKq
i4q/pFL/RZL5TzU3msCV417xUu0q3D4LjUkHhLj5wR5A4xksTc3-qkCd6zgc
n76kPnZta0VNG0TfUB3jLsU0H6x3DQRKkpslvqBR/2fWbphqau2bEENLrS0
0z11Pw4GuaE1zG8m0Yc/Anagse0BAPU06UtrP0EDhKp0tppp29uR0u/vj
KcV90ZIK0xUbEnHGuJHVGvLH3Y5BC5ugKXUBwRlq060sU04vWjJbqRfDNByf3
ENLAgHnFw47Fm321s9fvZz=LX0cnk0I1cc2TlFQ05/qqw0Ug5vNhuFsPwLTS
A09Hm020u7M15Vlg-TTcFLb)X2670s5E10E1v0B20719uE120f0K/1KEnyk-
3J05C7dq=zw6Igw1sUrRC7jvU05/7XAEagJK/VscLpUHSXY0GcLN2pdB19K2N8
d/6nMtk7R5ZL5xW/hCIAJNESH/njG0JvsEdUr6buuz10ALbq#853Cm5U7ym0a
A3BLHo/e
=11o
-----END PGP MESSAGE-----
```

# Secure Socket Layer

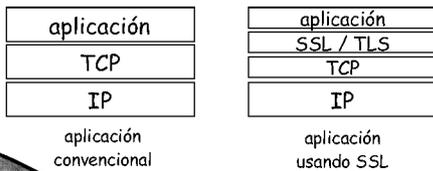
- Secure Socket Layer (SSL) es una solución que extiende a los sockets para brindar:
  - > Confidencialidad
  - > Integridad
  - > Autenticación
- ¡Miles de millones de dólares por año cambian de mano usando esta tecnología!
  - > El famoso “candadito cerrado” de los navegadores quizás sea el ejemplo más conocido de su uso

# Secure Socket Layer

- Objetivos al momento de su concepción:
  - > Facilitar las transacciones comerciales en línea
  - > Brindar encriptado de información sensitiva (especialmente el número de la tarjeta de crédito)
  - > Posibilitar la autenticación del servidor web y, en caso de requerirse, también la del cliente
  - > Minimizar el incordio al negociar con un nuevo comerciante

# Secure Socket Layer

- Inicialmente se trató de un estándar cerrado, implementado en el navegador Netscape
- En la actualidad se trata de un estándar abierto publicado en el **RFC 2246**
  - **SSL** brinda una **API** accesible desde cualquier lenguaje de programación



---

---

---

---

---

---

---

---

---

---

# SSL y TLS

- Autenticación de servidores en **SSL**:
  - Todo navegador seguro viene dotado de las claves públicas de un conjunto de **CAs** en los que se confía
  - El navegador solicita al servidor su certificación, la cual debe haber sido emitida por un **CA** confiable
  - Luego, haciendo uso de la clave pública del **CA** recupera la clave pública del servidor del certificado
  - El menú de seguridad del navegador permite indagar el conjunto de **CAs** considerados confiables

---

---

---

---

---

---

---

---

---

---

# SSL y TLS

- Encriptado de datos en **SSL**:
  - El navegador genera una clave simétrica al azar que será usada sólo durante la interacción, la encripta con la clave pública del servidor y la envía al servidor
  - El servidor haciendo uso de su clave privada puede desencriptar la clave simétrica provista por el cliente
  - En este punto, tanto cliente como servidor tienen acceso a la clave compartida
  - Toda información intercambiada usando el socket **TCP** será encriptada usando esa clave

---

---

---

---

---

---

---

---

---

---

## SSL y TLS

- Autenticación de clientes en **SSL**:
  - La autenticación de clientes en **SSL** se lleva adelante poniendo a disposición del servidor su certificado
- **SSL** evolucionó en el nuevo estándar **TLS**:
  - La nueva versión constituye un estándar abierto de internet, cuya última especificación (la versión **1.3**) está disponible en el **RFC 8446**
  - Los servicios provistos por **SSL** y **TLS** también pueden ser utilizados en otras aplicaciones (por caso, **IMAP**)

## IPsec

- Internet Protocol Security (**IPsec**) introduce un conjunto de protocolos para proveer seguridad y autenticación en capa de red
- Encriptado a nivel de capa de red:
  - El emisor encripta los datos contenidos en los datagramas **IP**
  - Estos datos pueden ser segmentos **TCP** o **UDP**, mensajes **ICMP** o **SNMP**, etc.
- Autenticación a nivel de capa de red:
  - El receptor puede autenticar la dirección **IP** de origen

## Seguridad en capa de red

- Familia de protocolos **IPsec**:
  - Un protocolo para autenticar los datagramas llamado Authentication Header (**AH**), el cual provee integridad y autenticidad del emisor, pero no confidencialidad
  - Otro protocolo para encriptar el contenido de los datagramas llamado Encapsulating Security Payload (**ESP**), el cual provee confidencialidad, integridad y autenticidad del emisor

## Seguridad en capa de red

- Para hacer uso de tanto **AH** como **ESP** emisor y receptor deben llevar adelante un proceso de inicialización
  - Este proceso crea un canal lógico a nivel de capa de red denominado Security Association (**SA**)
  - El **SA** establece un canal unidireccional
  - Cada **SA** se caracteriza a través de la combinación del protocolo de seguridad que se esté usando, la dirección **IP** de origen y un identificador de conexión de 32 bits

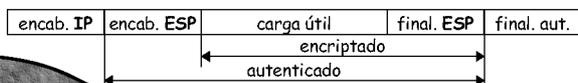
## Protocolo AH

- El encabezado del protocolo **AH** se inserta entre el encabezado **IP** y la carga útil del datagrama
  - Los routers en el núcleo de la red procesan el datagrama de la manera usual
- El encabezado incluye información acerca de:
  - El identificador de conexión
  - Los datos de la autenticación, esto es, el digesto del datagrama original firmado digitalmente
  - El campo próximo encabezado denota el tipo de carga útil (**TCP**, **UDP**, **ICMP**, etc.)



## Protocolo ESP

- El protocolo **ESP** incorpora un encabezado y un finalizador y un segundo finalizador que provee la autenticación
  - Tanto la carga útil como el finalizador **ESP** están encriptados
  - El campo próximo encabezado se encuentra encriptado dentro del finalizador **ESP**
  - La autenticación en **ESP** se maneja de manera análoga a **AH**



## Seguridad en IEEE 802.11

- La naturaleza absolutamente broadcast de los enlaces inalámbricos los hace candidatos a ser atacados por escucha de paquetes
  - Por caso, basta tomar un celular con wifi y salir a dar un paseo para encontrar una multitud de redes inalámbricas desprotegidas
  - Esta actividad se la conoce como war driving (si el paseo lo hacemos en un vehículo)
  - Las redes desprotegidas exponen la privacidad y los datos personales de los usuarios de la misma

## Wired Equivalent Privacy

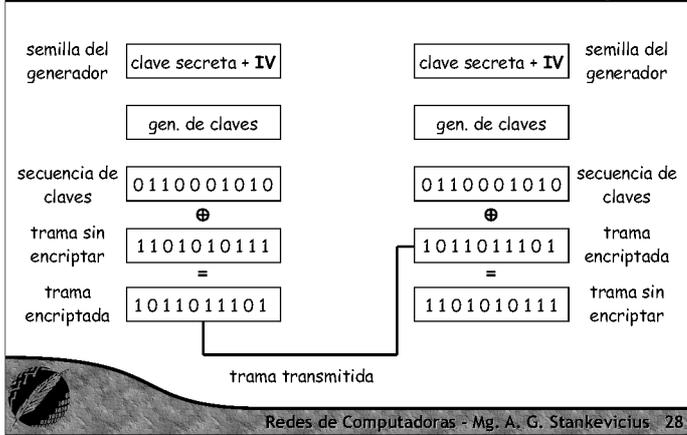
- La primer propuesta para contrarrestar este tipo de ataque la provee el protocolo Wired Equivalent Protocol (**WEP**)
  - **WEP** provee autenticación y encriptado de datos
- Autenticación WEP:
  - El nodo inalámbrico solicita autenticarse con el **AP**
  - El **AP** envía un nonce de 128 bits
  - El nodo encripta el nonce usando una clave simétrica
  - El **AP** al desencriptar el nonce confirma la identidad

## Wired Equivalent Privacy

- Encriptado de datos en WEP:
  - El nodo inalámbrico comparte con el **AP** una clave simétrica de 40 bits
  - El nodo agrega a la clave un vector de inicialización (**IV**) de 24 bits para obtener una clave de 64 bits
  - La clave de 64 bits es utilizada para generar un flujo de claves  $K_i^{IV}$
  - Las claves  $K_i^{IV}$  se usan para encriptar los bytes  $d_i$  de las tramas de la siguiente forma:

$$c_i = d_i \oplus K_i^{IV}$$

# Wired Equivalent Privacy



---

---

---

---

---

---

---

---

---

---

# Vulnerabilidad en WEP

- **WEP** presenta una seria vulnerabilidad:
  - Como se consume un **IV** por trama y el campo **IV** tiene sólo 24 bits, eventualmente se reusarán **IVs**
  - El **IV** se transmite sin encriptar, por lo que la reutilización del **IV** puede ser detectada
- Considerando lo simple y rápido que se puede quebrar el protocolo **WEP**, en la actualidad se lo considera obsoleto
  - El nuevo protocolo **WPA** provee un nivel adecuado de autenticación y seguridad a nivel hogareño

---

---

---

---

---

---

---

---

---

---

# ¿Preguntas?

---

---

---

---

---

---

---

---

---

---