Hacker Highschool
SECURITY AWARENESS FOR TEENS

LECCIÓN 9
SEGURIDAD DEL CORREO ELECTRÓNICO (E-MAIL)

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Información sobre la "Licencia de Uso"

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto "Hacker Highschool" son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección "LICENSE" de la página web del proyecto "Hacker Highschool" en www.hackerhighschool.org/license.
El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto. El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a patrocinarlo a través de la compra de una licencia, una donación o un patrocinio.

Todos los Derechos Reservados ISECOM, 2004.

Índice

Contribuciones

Stephen F. Smith, Lockdown Networks

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Rafael Acosta Serrano, T&E Solutions

Jaume Abella - Enginyeria La Salle

9.0 Introducción

Todo el mundo hace uso del correo electrónico. Es la segunda aplicación más utilizada sobre la Internet además del explorador. Lo que no te percatas es del nivel significativo de ataques existentes derivados del uso del correo electrónico. Y en lo concerniente a tu privacidad, el mal uso del e-mail estriba en comprometer y/o divulgar el contenido del mensaje, o proporcionar información spammer acerca de ti. El propósito de éste módulo es proveerte de información sobre cómo funciona el e-mail, la utilización segura de la herramienta, ataques basados en e-mail y las estrategias de seguridad para el e-mail.

9.1 ¿Cómo funciona el correo electrónico?

Al igual que el correo aéreo es enviado por aire, el ´e´-mail es enviado a través del medio "e"-lectrónico en y entre las redes que conforman la Internet. Cuando envías un correo electrónico desde tu computadora, los datos son enviados a un servidor SMTP. El servidor SMTP busca el servidor POP3 correcto y envía tu e-mail a ese servidor, donde espera a que el receptor pueda recuperarlo.

9.1.1 Cuentas de correo electrónico

Las cuentas de correo electrónico están disponibles a través de varias fuentes. Puedes conseguir una a través de tu escuela, trabajo o de un proveedor de servicios de Internet (ISP por sus siglas en inglés). Cuando obtienes una cuenta de e-mail, te darán una cuenta de correo que consta de dos partes usuario@nombre.dominio. La primera parte, el nombre del usuario, te identifica en tu red, diferenciándote de otros usuarios de la misma red. La segunda parte, el nombre de dominio, se utiliza para identificar tu red. El nombre de usuario deberá ser único dentro de tu red, al igual que el nombre del dominio deberá ser único entre todas las redes de la Internet. Sin embargo, los nombres de usuarios no son únicos fuera de sus redes; es posible que dos usuarios en dos redes distintas puedan compartir el mismo nombre. Por ejemplo, un usuario con la dirección bill@bignetwork.net no podrá utilizar el mismo nombre de usuario en la red bignetwork. Sin embargo, bill@bignetwork.net y bill@smallnetwork.net son direcciones válidas de correo electrónico que pueden referir a usuarios distintos. Una de las primeras cosas que harás cuando configures tu cuenta de correo es incorporar tu dirección de correo electrónico en tu cliente de correo. El cliente de correo es el programa que utilizarás para enviar y recibir e-mail. El cliente de correo de Microsoft Outlook Express es el más conocido (puesto que es una distribución gratuita dentro del sistema operativo de Microsoft). Sin embargo existen otros clientes disponibles para la plataforma Windows y Linux, incluyendo a Mozilla, Eudora, Thunderbird y Pine.

9.1.2 POP y SMTP

Después de que tu cliente de correo conoce tu dirección de correo electrónico, necesitará saber dónde buscar el correo entrante y a dónde enviar el saliente.

Tus correos entrantes estarán en una computadora llamada servidor POP. El servidor POP – generalmente con la sintaxis pop.smallnetwork.net o mail.smallnetwork.net – tiene un archivo asociado con tu correo electrónico, el cual contiene correos que te han sido enviados por otros usuarios. POP hace referencia a *post office protocol*.

Tus correos salientes serán enviados a una computadora llamada servidor SMTP. Este servidor –generalmente con la sintaxis smtp.smallnetwork.net – buscará el nombre de domino contenido en la dirección de correo electrónico en cualquiera de los correos que envíes, después realizará una búsqueda por DNS a fin de determinar a qué servidor POP3 deberá enviar el correo. SMTP hace referencia a *simple mail transfer protocol*.

Cuando inicias un cliente de correo electrónico, una serie de acciones se llevan a acabo:

1. el cliente abre una conexión de red hacia el servidor POP
2. el cliente envía tu contraseña secreta al servidor POP
3. el servidor POP envía tu correo entrante a tu computadora
4. el cliente envía tu correo saliente al servidor SMTP.

Algo que debes considerar en primera instancia es que no envías tu contraseña al servidor SMTP. SMTP es un viejo protocolo, diseñado en la temprana edad de la creación del correo electrónico, tiempo en el que casi todos en la Internet se conocían personalmente. El protocolo fue escrito asumiendo que quien lo utilizaba era de confianza, por lo que el SMTP no verifica el usuario para asegurarse de que en realidad tú eres tú. La mayoría de los servidores SMTP utilizan otros métodos para autenticar usuarios, pero –en teoría- cualquier persona puede utilizar cualquier servidor SMTP para enviar correo. (Para mayor información, ver sección 9.2.4 Encabezados Falsos - Forged Headers.)

La segunda consideración es que cuando envías tu contraseña secreta a un servidor POP la envías en formato de texto plano. Podrá estar escondida o enmascarada por pequeños asteriscos en el monitor de tu computadora, sin embargo es transmitida a través de la red en un formato legible. Cualquier persona que esté monitorizando el tráfico en la red –con un analizador de paquetes – será capaz de ver claramente tu contraseña. Puedes sentirte seguro de que tu red es segura, pero la realidad es que tienes poco control sobre lo que está ocurriendo en cualquier otra red por la cual pasan tus datos.

La tercera consideración que debes de saber, y tal vez la más importante, es que –al igual que tu contraseña –tus correos electrónicos son transmitidos y almacenados en formato de texto plano. Es posible que estén monitorizados en cualquier momento en que son transferidos del servidor a tu computadora.

Todo esto apunta hacia una verdad: el correo electrónico no es un método seguro para transferir información. Lo que sí es cierto es que es excelente para reenviar bromas, enviar advertencias de tipo spunkball, etc. Sin embargo, si no te sientes cómodo gritando hacia la ventana de tu vecino, tal vez deberías pensar quizá dos veces antes de ponerlo en un correo electrónico.

¿Te suena paranoico? Bueno, sí es paranoico, pero no necesariamente lo hace no verdadero. Muchas de nuestras comunicaciones de correo tratan acerca de detalles insignificantes.

Nadie excepto tú, Bob y Alice, se preocupan por tus planes para la cena del próximo martes. Y si Carol desea saber desesperadamente dónde cenarán el próximo martes, las probabilidades son pocas de que ella pueda tener un analizador de paquetes corriendo en cualquiera de las redes por donde pasa tu correo electrónico. Pero, si se sabe que una compañía utiliza el correo electrónico para el manejo de transacciones de tarjetas de crédito, no es poco probable que alguien esté intentando o tenga un método para analizar esos números de tarjetas de crédito fuera del tráfico de la red.

9.1.3 Correo Web

Una segunda opción para el correo electrónico es el uso de cuentas de correo basadas en Web. Esto te permitirá utilizar el explorador web para chequear tu correo. Desde que el correo de estas cuentas normalmente es almacenado en el servidor de correo web –no en tu computadora – es más conveniente utilizar estos servicios desde varias computadoras. Es posible que tu proveedor de servicios de internet (ISP) te permita acceder a tu correo electrónico a través de POP o vía Web.
Sin embargo, deberás recordar que las páginas web son almacenadas de manera temporal o local en computadoras locales. Si chequeas tu correo a través de un sistema basado en web en una máquina que no sea la tuya, existe la posibilidad de que tus correos puedan ser consultados por otros que utilicen la misma computadora.

Las cuentas de correo basadas en web puedes obtenerlas de manera fácil y gratuita. Esto significa que te brindan la oportunidad de tener varias identidades en línea. Tú puedes, por ejemplo, tener una dirección de correo electrónico exclusivamente para tus amigos, y otra para tus familiares. Esto es considerado como aceptable, mientras no pretendas defraudar a alguien.

Ejercicios:

1. Puedes aprender bastante acerca de cómo se obtienen los correos POP mediante el uso del programa telnet. Cuando utilizas telnet en lugar de un cliente de correo, tienes que teclear todos los comandos a mano (comandos que un cliente de correo generalmente los utiliza de manera automática). Utilizando un buscador web, encuentra las instrucciones y comandos necesarios para acceder a una cuenta de correo utilizando un programa telnet. ¿Cuáles son las desventajas de utilizar éste método para recuperar correo? ¿Cuáles son algunas de las ventajas potenciales?
2. Encuentra tres organizaciones que ofrecen servicios de correo basados en web. ¿Qué ofrecen, si es que prometen algo, con respecto a la seguridad al enviar o recibir un correo utilizando sus servicios? ¿Hacen algo por autenticar a sus usuarios?
3. (Posiblemente tarea) Determina el servidor SMTP de la cuenta de correo que utilizas frecuentemente.

9.2 Utilización segura del Correo Parte 1: Recibiendo

Todo mundo hace uso del correo electrónico y, para sorpresa de muchos, el correo puede ser utilizado en tu contra. El correo nunca deberá ser manejado como una tarjeta postal, en donde cualquiera puede leer su contenido. Nunca pongas en una cuenta común de correo electrónico algo que no desees que sea leído. Se ha dicho que existen estrategias para asegurar tu correo. En esta sección cubriremos la utilización segura y sana del correo y cómo proteger tu privacidad en línea.

9.2.1 Spam, Phishing y Fraude

A todo mundo le gusta tener un correo. Hace tiempo, en una galaxia no muy lejana, solías tener el correo únicamente de la gente que conocías, existiendo aspectos que cuidabas. Ahora tienes el correo de gente que nunca escuchaste y que preguntarán sobre dónde comprar software, drogas, bienes raíces, por no mencionar aquel en donde te ayudan a obtener 24 millones de dólares desde Nigeria. A este tipo de anuncios no solicitados se les denomina spam. Es sorprendente para mucha gente que este tipo de correos que reciben, puede proporcionar mucha información de quien envía el correo, cuándo fue abierto el

correo y cuántas veces ha sido leído, si ha sido reenviado, etc. Este tipo de tecnología – llamada web bugs – es utilizada tanto por los spammers como por los que realmente envían el correo. También, el contestar un correo o hacer click en un enlace para desuscribirse de una lista puede decirle a quien lo envía que han alcanzado una dirección existente o viva. Otro tipo de preocupación en materia de invasión de privacidad es el creciente ataque conocido como "phishing". ¿Has recibido algún correo donde te piden firmar y verificar tu cuenta de correo bancaria o de E-bay? Cuidado, porque es un truco para robar información de tu cuenta. Para que estés seguro de éste tipo de ataques, existen otras estrategias sencillas para protegerte, descritas más adelante.

9.2.2 Correo HTML

Una de las preocupaciones en material de seguridad con los correos basados en HTML es el uso de los *web bugs*. Los web bugs son imágenes escondidas en tu correo que enlazan hacia el servidor de quien lo envía, y puede proveerles notificación de que han recibido o abierto el correo. Otro defecto con los correos HTML es que quien lo envía puede incluir enlaces en el correo que identifican a la persona que hace click en ellos. Esto puede proporcionar información a quien lo manda acerca del estado del mensaje. Como regla, debes de utilizar un cliente de correo que te permita deshabilitar la descarga automática de imágenes anexadas o embebidas. Otro problema relacionado con los scripts en el correo es que ejecutan una aplicación, si es que tu explorador no ha sido parcheado contra vulnerabilidades de seguridad.

Para los clientes basados en web, tienes la opción de deshabilitar la descarga automática de imágenes, o la visualización del mensaje en modo texto. Cualquiera de ellas es una buena práctica de seguridad. La mejor manera de protegerte contra los ataques de privacidad y seguridad basados en correo HTML es el uso de correos en modo texto.

Si necesitas utilizar correo HTML, ¡ten cuidado!

9.2.3 Seguridad en Archivos Anexados

Otra preocupación real es la relacionada con los archivos anexados a los correos. Los atacantes pueden enviar malware –software malicioso por sus siglas en inglés-, virus, caballos de Troya y todo tipo de programas desagradables. La mejor defensa contra correos con malware es el no abrir un correo si no conoces a quien lo envía. Nunca abras un archivo con extensión .exe o .scr, ya que éstos son extensiones que ejecutan archivos que pueden infectar tu máquina con cualquier virus. Una buena medida de prevención es que cualquier archivo que recibas deberás salvarlo a tu disco duro y posteriormente analizarlo con un programa de antivirus. Ten cuidado con los archivos que parecen ser comunes, como los archivos zip. Algunos atacantes pueden disfrazar un archivo sólo cambiando el icono u ocultando la extensión del archivo, por lo que tal vez no sepas que es un ejecutable.

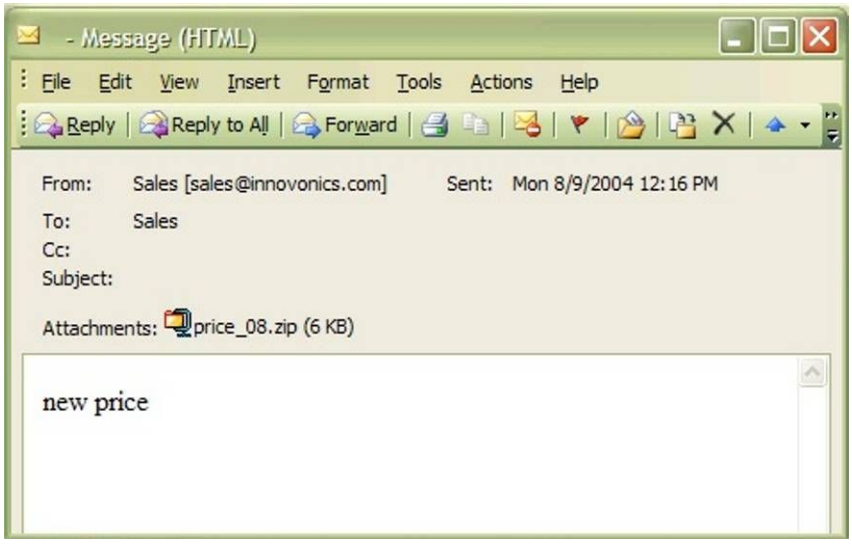
9.2.4 Encabezados Falsos / Forged headers

Ocasionalmente recibirás correos que parecen ser enviados por alguien que conoces, o por el "Administrador", "Postmaster" o "Equipo de Seguridad" de tu escuela o ISP. El tema del correo puede ser "Returned Mail" o "Hacking Activity", o cualquier otro tema interesante. Es muy común que sea un archivo anexado. El problema es que requiere alrededor de 10

segundos de trabajo y poco conocimiento técnico para falsear una dirección de correo electrónico (también, dependiendo de donde vivas, puede ser ilegal.)

Para hacer esto, haces un cambio simple en la configuración de tu cliente de correo y allí donde te pregunta teclear tu dirección de correo (bajo Opciones, Configuración o Preferencias) tecleas cualquier otra cosa. De ahora en adelante todos tus mensajes tendrán una dirección de remitente falsa. ¿Esto significa que ya estás a salvo de ser identificado? No, no realmente. Cualquier persona con la habilidad de leer el encabezado de un correo y que realice una búsqueda podrá imaginarse tu identidad a partir de la información contenida en el encabezado. Lo que significa que un spammer puede ser quien él deseé. Por lo que si Fanni Gyotoku [telecommunicatecreatures@cox.net] te vende una antena mágica para tu celular que resulta ser una caja de cereales cubierta por una hoja de lata, puedes quejarte directamente con cox.net, pero no te sorprendas cuando te digan que no existe tal usuario.

Muchos de los proveedores de internet autentican a los que envían correos, lo que significa que debes ser tú quien dices ser para enviar un correo a través de su servidor SMTP. El problema radica cuando los hackers y spammers corren un servidor SMTP en su propio ordenador y, por lo tanto, no necesitan autenticarse al enviar un correo, y pueden hacer que luzca como ellos deseen. La única manera segura de saber si un correo sospechoso es legítimo o no es conocer a quien envía el correo y llamarle. Nunca contestes un mensaje que sospeches ha sido falseado, ya que le diría a quien lo envía que ha alcanzado una dirección existente. También puedes fijarte en la información que aparece en el encabezado a fin de determinar de dónde viene el correo, tal como aparece en el siguiente ejemplo:



Este es un correo electrónico de alguien que no conozco, con un archivo anexado sospechoso. Normalmente borraría éste correo pero quiero saber de dónde viene realmente. Me fijo en el encabezado. Utilizo Outlook 2003 como cliente de correo, y para ver el encabezado necesito ir a Ver>Opciones y así podré ver la información del encabezado como aparece abajo:

```
Microsoft Mail Internet Headers Version 2.0
Received: from srv1.mycompany.com ([192.168.10.53]) by mx1.mycompany.com
over TLS secured channel with Microsoft SMTPSVC(6.0.3790.0);
Mon, 9 Aug 2004 11:20:18 -0700
Received: from [10.10.205.241] (helo=www.mycompany.com)
```

```
by srv1.mycompany.com with esmtp (Exim 4.30)
id 1BuEgL-0001OU-8a; Mon, 09 Aug 2004 11:15:37 -0700
Received: from kara.org (67.108.219.194.ptr.us.xo.net [67.108.219.194])
by www.mycompany.com (8.12.10/8.12.10) with SMTP id i79IBYUr030082
for <sales@mycompany.com>; Mon, 9 Aug 2004 11:11:34 -0700
Date: Mon, 09 Aug 2004 14:15:35 -0500
To: "Sales" <sales@mycompany.com>
From: "Sales" <sales@innovonics.com>
Subject:
Message-ID: <cdkdabgurdgefupfhnt@mycompany.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="--------cfwriebwwbnnfkkmojga"
X-Scan-Signature: 178bfa9974a422508674b1924a9c2835
Return-Path: sales@innovonics.com
X-OriginalArrivalTime: 09 Aug 2004 18:20:18.0890 (UTC) FILETIME=
[868FEAA0:01C47E3D]
----------cfwriebwwbnnfkkmojga
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
----------cfwriebwwbnnfkkmojga
Content-Type: application/octet-stream; name="price_08.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="price_08.zip"
----------cfwriebwwbnnfkkmojga—
```

Ahora, la parte en la que estoy interesado está subrayada arriba. Fíjate que el campo de "Received" es de kara.org con una IP que parece ser una línea DSL de xo.net, la cual no concuerda con innovonics.com, el supuesto remitente.

Además, si busco el servidor de correo innovonics.com utilizando nslookup, la dirección que me muestra es la siguiente:

```
C:\>nslookup innovonics.com
Server: dc.mycompany.com
Address: 192.168.10.54
Non-authoritative answer:
Name: innovonics.com
Address: 64.143.90.9
```

Entonces, mi sospecha era correcta, éste es un correo que contiene algún malware en un archivo ejecutable a través de un archivo zip. El malware ha infectado la computadora de la persona que tiene la línea DSL, el cual se conoce como un zombie, ya que envía copias del malware a todos aquellos que tiene en su agenda. ¡Qué bueno que verifiqué ésto!

Ejercicios:

1. Citibank y PayPal son dos de los objetivos más comunes de correos phishing. Investiga qué están haciendo Citibank o PayPal para evitar/controlar el phishing.
2. Investiga si tu banco o emisor de tarjeta de crédito ha publicado una declaración acerca del uso de correo e información personal.
3. (posiblemente tarea) Investiga un correo spam que hayas recibido y mira si puedes determinar cual es la fuente real.

9.3 Utilización Segura del Correo Parte 2: Enviando

El envío de correo es un poco más cuidadoso. Existen algunos puntos que puedes considerar para cerciorarte de que la conversación es segura. El primer punto es asegurarte de que la conexión es segura (para mayor información ver sección **9.4 Seguridad en las Conexiones**). También existen métodos que te permiten firmar de manera digital tus mensajes, lo que garantiza que el mensaje proviene de tí y que no ha sido modificado durante el trayecto. Y para mayor seguridad, puedes encriptar tus mensajes a fin de que nadie pueda leerlos.

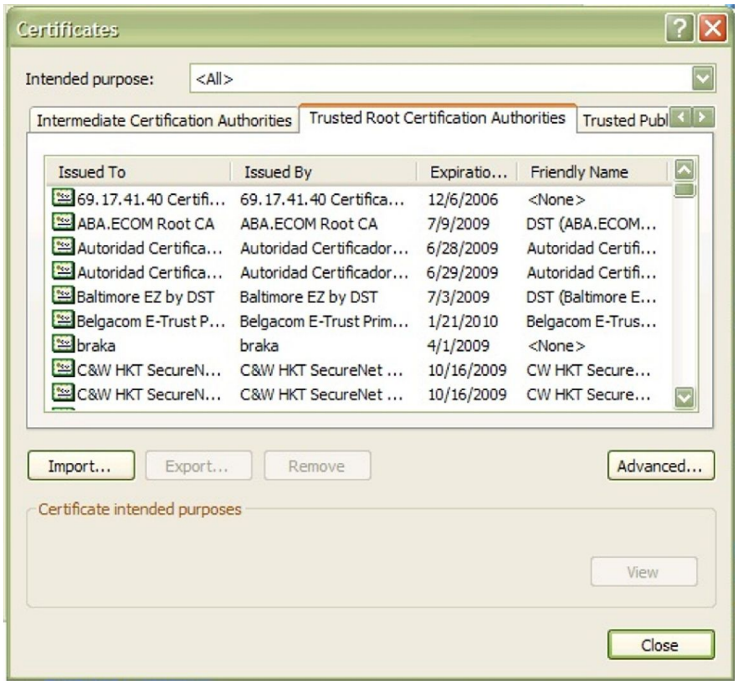
Las firmas digitales prueban de dónde viene el correo, y que no ha sido alterado en el trayecto. Si adoptas el hábito de utilizar firmas digitales para correos importantes, tendrás mucha credibilidad en caso de que en alguna ocasión tengas que negar algún correo falseado que aparente ser tuyo. PGP en particular ofrece niveles de encriptación tan complejos que requieren computadoras de gran potencia para ser descifrados.

9.3.1 Certificados Digitales

Un certificado digital es único para cada individuo, como si fuese una licencia para conducir o un pasaporte, el cual se compone de 2 partes, una llave pública y una privada. El certificado es único para una persona y típicamente los certificados son expedidos por una Autoridad Certificadora confiable o CA. La lista de Autoridades Certificadoras en quien confías es distribuida automáticamente (si eres un usuario Microsoft Windows) a través de la actualización de Windows, y la lista es accesible en tu explorador a través de:

Herramientas>opciones de internet>contenido>certificados.

Puedes ir a éste apartado para ver los certificados instalados en tu máquina (tuyos o de otros) y otras autoridades certificadoras en las cuales confías.



Puedes deshabilitar la actualización automática de CAs, y elegir quitar todos los CAs de la lista, aunque no es recomendable. Las instrucciones de cómo hacer esto se encuentra disponible en el sitio web de Microsoft.

9.3.2 Firmas Digitales

Una firma digital es generada por tu software de correo usando tu llave privada a fin de garantizar la autenticidad del correo. El propósito de la firma es doble. El primero es certificar que proviene de ti: es lo que se llama "**no repudio**". El segundo es asegurar que el contenido no ha sido alterado, lo que se llama "**integridad de datos**". La manera en que un programa de correo cumple con este cometido es mediante la ejecución de un proceso que, a partir del contenido de tu mensaje, genera un resumen del mismo –message digest-. Éste último, si el algoritmo matemático que se utiliza es lo suficientemente fuerte, posee los siguientes atributos.

- El mensaje original no puede ser reproducido a partir del resumen.
- Cada resumen es único.

Después de que el resumen ha sido creado, es cifrado con tu llave privada. El resumen cifrado es anexado al mensaje original junto con tu llave pública. El recipiente abre el mensaje, y el resumen es desencriptado con tu llave pública. El resumen es comparado con el resumen idéntico generado por el programa de correo del recipiente. Si concuerdan, es correcto. Si no, tu cliente de correo te avisará que el mensaje ha sido modificado.

Existen 2 tipos de función de firma/cifrado, S/MIME y PGP. S/MIME es considerada como la mejor opción para el gobierno y corporaciones, tal vez por que utiliza menos recursos del modelo de autenticación de la autoridad certificadora, y porque es de fácil implantación a través del cliente de Microsoft Outlook Express. PGP es muy común dentro de las comunidades de usuarios finales, debido a que está basada en un esquema web de confianza no-centralizado, en donde la confianza de los usuarios es validada a través de un sistema "amigo del amigo", en el cual acuerdas que, si tu confías en mí, entonces puedes confiar en aquellos que yo confío, y porque los miembros de las comunidades no les interesa si toma cuatro horas el saber como funciona PGP con Thunderbird – ellos consideran este tipo de retos como recreación.

9.3.3 Obteniendo un certificado

Si estás interesado en obtener un certificado digital o un ID digital, necesitas contactar a una Autoridad Certificadora (Verisign y thawte son las más conocidas, a pesar de que algunos buscadores pueden encontrar otras). Ambas requieren que les proveas de tu identificación a fin de comprobarles que eres tú quien dices ser. Puedes obtener un certificado gratuito de thawte, pero requiere una cantidad significativa de información personal, incluyendo identificación oficial (como el pasaporte, identificación para pago de impuestos o licencia de manejo). Verisign pide una cuota por su certificado y requiere que pagues esta cuota a través de una tarjeta de crédito, sin embargo pide menos información. (Presuntamente, Verisign reenvía los datos con la compañía de la tarjeta de crédito a fin de validar tu información personal). Estas peticiones de información pueden parecer intrusivas, pero recuerda, estás pidiendo a éstas compañías que certifiquen tu confianza e identidad. Y – como siempre – chequea con tus familiares o representantes antes de proveer cualquier tipo de información (si no, tendrán grandes cargos en sus tarjetas de crédito).

La mayor desventaja al utilizar una autoridad certificadora es que tu llave privada está disponible para un tercero: la autoridad certificadora. Y si la autoridad certificadora se ve comprometida, entonces tu ID digital está comprometido.

9.3.4 Encriptación / Cifrado

Como una medida adicional de seguridad, puedes cifrar tu correo electrónico. El cifrado puede convertir el texto de tu correo en un lío mutilado de números y letras que sólo pueden ser interpretados por aquellos recipientes confiados. Tus secretos más profundos y tu peor poesía estarán escondidos para todo el mundo excepto para aquellos ojos en quien confías.

Sin embargo, debes recordar que, mientras esto te suene atractivo –y para todos nosotros que no deseamos ser expuestos a la pésima poesía –algunos gobiernos no lo aprueban. Sus argumentos pueden o no ser válidos (puedes discutir esto entre tus amigos), pero la validez no es el punto. El punto es que, dependiendo de las leyes del país en el que vives, el envío de correo cifrado puede ser un crimen, independientemente del contenido.

9.3.5 ¿Cómo funciona?

La encriptación o cifrado es un poco complicada, por lo que intentaré explicarlo de una manera no muy técnica:

Jason desea enviar un mensaje cifrado, por lo que lo primero que hace Jason es ir con una Autoridad Certificadora y obtener un Certificado Digital. Este Certificado tiene dos partes, una llave pública y una llave privada.

Si Jason desea recibir y enviar mensajes cifrados con su amiga Kira, ambos deberán intercambiar sus llaves públicas. Si tú obtienes una llave pública de una Autoridad Certificadora, en la cual has decidido confiar, la llave puede ser verificada de manera automática a esa autoridad certificadora. Esto significa que tu programa de correo verificará que el certificado es válido, y que no ha sido revocado. Si el certificado no proviene de una autoridad en la que confías, o es una llave PGP, entonces necesitarás verificar la huella de la llave. Típicamente esto se hace por separado, mediante el intercambio cara a cara de la llave o por la huella de los datos.

Asumamos ahora que tanto Kira como Jason están utilizando esquemas de cifrado compatibles, y han intercambiado mensajes firmados. Esto significa que ambos poseen la llave pública del otro.

Cuando Jason desea enviar un mensaje cifrado, el proceso de cifrado comienza convirtiendo el texto del mensaje de Jason en un código pre-enmascarado. Éste código es generado utilizando una fórmula matemática llamada algoritmo de encriptación. Existen varios tipos de algoritmos, sin embargo, para el correo, el S/MIME y el PGP son los más comunes.

El código enmascarado del mensaje de Jason es cifrado por el programa de correo utilizando la llave privada de Jason. Entonces, Jason utiliza la llave pública de Kira para cifrar el mensaje, por lo que sólo Kira podrá desencriptarlo con su llave privada, terminando así el proceso de encriptación.

9.3.6 Desencriptación

Ahora, Kira ha recibido el mensaje cifrado de Jason. Esto típicamente se indica con un icono de un candado en la bandeja de entrada de ella. El proceso de desencriptación es manejado por el software de correo, pero lo que hay detrás es algo como esto: el programa de correo de Kira utiliza su llave privada para descifrar el código encriptado pre-enmascarado y el mensaje encriptado. Entonces el programa de correo de Kira obtiene la llave pública de Jason donde estaba almacenada (recuerda, intercambiamos llaves anteriormente). Esta llave pública es utilizada para desencriptar el código pre enmascarado del mensaje. Si el posteo del código enmascarado es igual al código pre enmascarado, el mensaje no ha sido alterado durante su trayecto.

Nota: si pierdes tu llave privada, todos tus archivos encriptados no te serán útiles, por lo que es importante que tengas un procedimiento para realizar el respaldo (backup) tanto de tu llave privada como pública.

9.3.7 ¿Es el cifrado irrompible?

De acuerdo a los números el nivel de encriptación ofrecido por, por ejemplo, PGP es irrompible. Aunque seguramente un millón de computadoras trabajando para romperlo podrían eventualmente romperlo de manera exitosa, pero no antes de que el millón de chimpancés terminaran el guión para *Romeo y Julieta*. El número teórico detrás de este tipo de encriptación involucra la descomposición en factores de los productos de un gran número de números primos y el desafío del hecho de que los matemáticos han estudiado los números primos por años, por lo que no hay una manera fácil de hacerlo.

Pero la encriptación y la privacidad es más que sólo números. Sin embargo, si alguien tiene acceso a tu llave privada, tendrá acceso a todos tus archivos encriptados. La encriptación sólo funciona si y sólo si es parte de un esquema grande de seguridad, el cual ofrece protección tanto a tu llave privada como a tu pass-phrase o contraseña de encriptación/desencriptación.

Ejercicios:
1. ¿La encriptación de correo es legal en el país donde vives? Encuentra otro país donde sea legal y otro donde no lo sea.

2. Los escritores de ciencia ficción han imaginado dos tipos de futuros, uno en donde la gente vive de manera transparente, es decir, sin secretos, y otro en donde tanto los pensamientos como las comunicaciones de todos son completamente privadas. Phil Zimmerman, creador de PGP, cree en la privacidad como una fuente de libertad. Lee sus pensamientos en ¿porqué necesitas PGP? en http://www.pgpi.org/doc/whypgp/en/. Luego, del escritor de ciencia ficción David Brin, en su artículo titulado 'A Parable about Openness' que puedes encontrar en http://www.davidbrin.com/akademos.html, hace referencia a una serie de puntos donde aboga por la franqueza como una fuente de libertad. Discute éstos dos puntos de vista. ¿Cuál prefieres? ¿Cuál crees que tendrá mayor aceptación? ¿Cómo crees que será el futuro de la privacidad?

9.4 Seguridad en las Conexiones

Lo último, pero no menos importante, es la seguridad en las conexiones. Para el correo web, asegúrate de utilizar una conexión SSL hacia tu proveedor de correo. Un pequeño candado deberá aparecer en la barra de la parte inferior de tu explorador. Si estás utilizando POP y un cliente de correo, asegúrate de que has configurado tu cliente de correo para utilizar SSL con POP en el puerto 995 y SMTP en el puerto 465. Esto encripta tu correo desde tu máquina hasta el servidor, además de proteger tu usuario y contraseña POP / SMTP. Tu proveedor deberá tener un how-to en su sitio web para saber como configurarlo. Si no te ofrecen una conexión segura de POP / SMTP, ¡cambia de proveedor!

Ejercicio:
Si tienes una cuenta de correo electrónico, averigua si tu cuenta está utilizando una conexión SSL. ¿Cómo verificarías esto en tu cliente de correo? ¿Tu proveedor proporciona información sobre una conexión SSL?

Lecturas Recomendadas

¿Alguien puede leer mi correo electrónico?
http://www.research.att.com/~smb/securemail.html
Página libre de PGP del MIT
http://web.mit.edu/network/pgp.html
Noticias generales sobre aspectos de privacidad en la Internet:
Centro de Información de Privacidad Electrónica
http://www.epic.org/
y
Electronic Frontier Foundation
http://www.eff.org/
Más acerca de PGP
http://www.openpgp.org/index.shtml
¿Cómo el leer un E-mail puede comprometer tu Privacidad?
http://email.about.com/od/staysecureandprivate/a/webbug_privacy.htm
Evitando los Virus del E-mail
http://www.ethanwiner.com/virus.html
Una breve descripción de preguntas de seguridad en E-mail (con un pequeño aviso al final)
http://www.zzee.com/email-security/
Una breve descripción de preguntas de seguridad en E-mail (sin aviso)
http://www.claymania.com/safe-hex.html
Precauciones de E-mail basado en Windows
http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html
http://computer-techs.home.att.net/email_safety.htm
Diferencias Entre Virus de Linux y Windows (con información sobre porqué los programas de E-mail de Linux son más seguros)
http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses/