# Hacker Highschool
## SECURITY AWARENESS FOR TEENS

# LEZIONE 9
# SICUREZZA DELLA POSTA ELETTRONICA

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.

# Informazioni sulla licenza d'uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo "non-commerciale" verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo "doposcuola".

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L'erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all'indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

# Indice

# Hanno contribuito

Stephen F. Smith, Lockdown Networks

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Per la versione in lingua italiana:

Raoul Chiesa (ISECOM)

Doriano Azzena (centro CSAS del progetto Dschola IPSIA Castigliano - Asti )

Sophia Danesino (centro CSAS del progetto Dschola ITIS Peano – Torino )

Nadia Carpi (centro CSAS del progetto Dschola ITIS Peano – Torino )

Claudio Prono (@ Mediaservice.net Srl. Torino – ISECOM Authorized Training Partner)

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

mediaservice.net
CORPORATE SECURITY & IMAGE

# 9.0 Introduzione

Tutti usano la posta elettronica. E' la seconda applicazione più utilizzata in Internet dopo il browser web. Tuttavia spesso non ci si rende conto che una parte significativa degli attacchi provenienti dalla rete avviene proprio tramite la posta. Per quanto riguarda la privacy, il cattivo uso della posta elettronica può rendere accessibile il contenuto dei vostri messaggi o fornire informazioni su di voi ad uno spammer.

Lo scopo di questo modulo è quello di dare informazioni su come funzionano le e-mail, su come usare la posta correttamente, descrivere gli attacchi basati su mail e in generale le strategie rivolte a rendere sicuro l'uso della posta elettronica.

# 9.1 Come funziona la posta elettronica

Esattamente come la posta aerea viene inviata con un aereo, le 'e'-mail vengono inviate attraverso la 'e' – la 'e' in questo caso è il web fatto di connessioni elettroniche e delle reti da cui è composta Internet. Quando spedite una e-mail, i dati vengono inviati dal vostro computer ad un server SMTP. Il server SMTP cerca il server POP3 corretto e invia la vostra mail a quel server, dove verrà memorizzata fino a quando il destinatario non la scaricherà sul proprio computer.

## 9.1.1 Account di posta

E' possibile ottenere un account di posta da molti fornitori diversi. Potete riceverne uno dalla vostra scuola, dal lavoro o attraverso il vostro ISP. Quando ottenete un account di posta, vi viene assegnato un indirizzo e-mail composto da due parti, del tipo *username@domain.name*. La prima parte, *username* vi identifica sulla vostra rete, differenziandovi da tutti gli altri utenti. La seconda parte, *domain.nam,e* è utilizzata per identificare la vostra rete.

Lo username deve essere unico all'interno della vostra rete, così come il nome di dominio deve essere unico tra tutte le reti in Internet. Gli username non sono univoci al di fuori delle loro reti; è possibile che due utenti su due reti diversi abbiano lo stesso nome. Ad esempio se un utente ha l'indirizzo pippo@granderete.net non esisterà un altro utente su granderete.net il cui nome è pippo. Tuttavia pippo@granderete.net e pippo@piccolarete.net sono entrambi indirizzi e-mail validi e possono fare riferimento a utenti diversi.

Una delle prime cose che farete per configurare il servizio di posta è quella di inserire il vostro indirizzo nel client di posta. Il programma client è quello che si usa per inviare e ricevere le e-mail. Il più noto è Microsoft's Outlook Express (dal momento che viene fornito gratuitamente insieme ad ogni copia di un sistema operativo Microsoft), ma ne esistono molti altri sia per Windows che per Linux, inclusi Mozilla, Eudora, Thunderbird e Pine.

## 9.1.2 POP e SMTP

Dopo aver inserito il vostro indirizzo e-mail, dovete specificare da dove scaricare le mail in arrivo e dove inviare quelle in uscita.

Le e-mail in ingresso si trovano su un computer detto *server POP*. Il server *POP* – generalmente chiamato con un nome simile a *pop.piccolarete.net* o *mail.piccolarete.net* – contiene un file associato al vostro indirizzo e-mail che contiene le e-mail che vi sono state inviate. *POP* è acronimo di *post office protocol*.

Le vostre e-mail in uscita vengono inviate ad un computer detto *server SMTP* . Questo server – chiamato *smtp.piccolarete.net* – esaminerà il *nome di dominio* contenuto nell'indirizzo di posta delle mail in uscita, effettuerà un *DNS lookup* per determinare a quale server POP3 inviare la e-mail. *SMTP* è acronimo di *simple mail transfer protocol*.

Quando avviate il vostro client di posta, vengono eseguite le seguenti operazioni:

1 il client apre una connessione di rete con il server POP

2 il client invia la password segreta al server POP

3 il server POP invia le vostre e-mail in ingresso al vostro computer locale

4 il client invia le vostre e-mail in uscita al server SMTP .

La prima cosa da notare è che non è necessario inviare la password al server SMTP. SMTP è un server vecchio, progettato ai primordi del servizio di posta, in tempi in cui quasi tutti in Internet si conoscevano personalmente. Il protocollo è stato scritto con l'assunto che chiunque l'avesse usato sarebbe stato degno di fiducia, quindi SMTP non effettua verifiche su chi lo sta usando. La maggior parte dei server SMTP utilizza altri metodi per autenticare gli utenti, ma - in teoria – chiunque può usare qualunque server SMTP per inviare e-mail (per ulteriori informazioni si veda la sezione **9.2.4 Intestazioni contraffatte**).

La seconda cosa da notare è che, quando si invia la password segreta al server POP, essa viene trasferita in chiaro. Può essere nascosta con piccoli asterischi sullo schermo del vostro computer, ma viene trasmessa in rete in un formato facilmente leggibile. Chiunque stia monitorando il traffico sulla rete – utilizzando un *packet sniffer*, ad esempio – sarà in grado di rilevare chiaramente la vostra password. Potete essere certi che la *vostra* rete sia sicura, ma avete poco controllo su quello che avviene nelle altre reti attraverso cui passano i dati.

La terza cosa, probabilmente la più importante, che dovete sapere sulle e-mail è che vengono trasmesse e memorizzate in chiaro – esattamente come la vostra password. E' possibile che vengano esaminate ogni volta che vengono trasferite dal server al vostro computer.

Questo porta ad una conclusione: *la posta elettronica non è un metodo sicuro per trasferire le informazioni*. Certamente è formidabile per inviare scherzi o avvertimenti "esca" (spunkball warnings), ma a meno che non vogliate gridare qualcosa al vostro vicino attraverso la finestra, allora dovreste pensarci due volte prima di inserirlo in una mail.

Questo vi sembra paranoico? Certo è un po' paranoico, ma questo non lo rende necessariamente non vero. La maggior parte delle vostre comunicazioni via mail riguardano dettagli insignificanti. Nessun altro eccetto voi, Bob e Alice, si occupano dei vostri progetti per la cena del prossimo martedì. E, anche se Carol volesse disperatamente sapere dove voi, Bob e Alice andrete a cena il prossimo martedì, ci sono poche probabilità che abbia un packet sniffer in esecuzione su una delle reti attraverso cui viaggia la vostra mail. Tuttavia, se è noto che un'azienda utilizza e-mail per effettuare transazioni con carta di credito, non è improbabile che qualcuno abbia, o cerchi di impostare, un meccanismo per rilevare i numeri delle carte di credito dal traffico di rete.

## *9.1.3 Web Mail*

Una seconda opzione per gestire la posta elettronica è utilizzare un account di posta basato sul web. Questo premette di usare un browser per controllare la posta. Dal momento che le mail per questo genere di account sono memorizzate sul server web di posta – non sul vostro computer locale - è conveniente utilizzare questi servizi da computer diversi. E' possibile che il vostro ISP vi consenta di accedere alla posta sia tramite POP che web.

Tuttavia, dovete ricordare che le pagine web scaricate vengono memorizzate sul computer locale (in memoria *cache*), talvolta per parecchio tempo. Se verificate le vostre mail attraverso un sistema basato sul web presente sul computer di qualcun altro, c'è una buona possibilità che le vostre mail siano accessibili a qualcun altro che utilizzi quel computer.

Gli account di posta basati sul web sono spesso gratuiti e facilmente ottenibili. Questo significa che vi offrono l'opportunità si avere varie identità online. Potete, ad esempio, avere un indirizzo di posta che utilizzate solo per gli amici e un altro solo per i parenti. Questo è generalmente considerato accettabile, fino a quando non volete intenzionalmente defraudare qualcuno.

**Esercizi:**

1 Potete imparare molto su come vengono rintracciate le mail POP utilizzando il programma telnet. Quando usate telnet invece che un client di posta, dovete inserire a mano tutti i comandi (comandi che il programma client di posta di solito inserisce automaticamente). Utilizzando un motore di ricerca, trovate le istruzioni e i comandi necessari per accedere ad un account di posta utilizzando il programma telnet. Quali sono gli svantaggi di utilizzare questo metodo per recuperare la posta? Quali sono alcuni dei vantaggi potenziali?

2 Trovate tre organizzazioni che offrono servizi di mail basati sul web. Quali servizi vi offrono? Quali garanzie di sicurezza delle mail inviate o ricevute offrono i loro servizi? Fanno qualche tentativo per autenticare i loro utenti?

(Possibilmente compito a casa) Determinate il server SMTP dell'indirizzo di posta che usate più frequentemente.

## 9.2 Utilizzo sicuro della posta Parte 1: Ricezione

Tutti utilizzando le e-mail e, con stupore di molte persone, le vostre e-mail possono essere usate contro di voi. Le e-mail dovrebbero essere considerate come cartoline, nel senso che chiunque le vede può leggerne il contenuto. Non dovreste mai inserire in una mail ordinaria qualcosa che non volete venga letta. Detto questo, esistono strategie per rendere sicure le mail. In questa sezione tratteremo l'uso sicuro e assennato delle e-mail e spiegheremo come proteggere la vostra privacy online.

### 9.2.1 Spam, Phising e Frodi

A tutti piace ricevere mail. Molto tempo fa, in una galassia molto molto lontana si ricevevano mail solo da persone che si conoscevano e su argomenti di nostro interesse. Ora si ricevono mail da persone mai sentite che vi chiedono di comprare software, medicine e beni immobili, senza menzionare chi chiede aiuto per far uscire dalla Nigeria 24 milioni di dollari. Questo tipo di pubblicità non sollecitata viene chiamata *spam*. Sorprende molte persone il fatto che le mail che ricevono possono fornire una gran quantità di informazioni ad un mittente, quale quando la mail è stata aperta e quante volte è stata letta, se è stata inoltrata, ecc. Questo tipo di tecnologia –chiamata web bug – è usata sia dagli spammers che dai mittenti legittimi. Inoltre, la risposta ad una e-mail o la selezione di un link può indicare al mittente che è stato raggiunto un indirizzo attivo.

Un'altra invasione della privacy riguarda un attacco sempre più comune detto "*phishing*". Avete mai ricevuto una mail che vi chiede di effettuare un login e verificare le informazioni relative al vostro account bancario? State in guardia perchè è un tentativo di rubarvi le informazioni di accesso. Per proteggervi da questo tipo di attacchi esistono semplici strategie, di seguito illustrate.

### 9.2.2 E-Mail HTML

Uno degli aspetti che riguardano la sicurezza relativa alle mail basate su HTML è l'uso dei *web bugs*. I web bugs sono immagini nascoste nelle vostre e-mail che si collegano al server web del mittente e che forniscono la notifica del fatto che voi avete ricevuto o letto la mail. Un altro difetto è che il mittente può inserire nella mail dei collegamenti che identificano la persona che li seleziona. Questo può dare al mittente informazioni sullo stato del messaggio. Come regola, si dovrebbe usare un client di posta che consenta di disabilitare il download automatico delle immagini allegate o inserite nella mail. Un altro problema è associato agli script nella mail che possono lanciare un'applicazione se al browser non è stato applicato il pacchetto (la *patch*) per coprire le falle di sicurezza.

Per i client di posta basati sul web si può disabilitare il download automatico delle immagini o vedere il messaggio come testo. Entrambe le soluzioni sono buone norme. Il modo migliore di proteggervi dagli attacchi che si basano su mail HTML è quello di usare mail di solo testo. Se dovete usare mail HTML, fate attenzione!

### 9.2.3 Sicurezza degli allegati

Un altro problema legato alla sicurezza della posta ricevuta è quello degli allegati. Gli allegati sono un veicolo per malware, virus, cavalli di Troia e tutti i tipi di programmi di attacco. La miglior difesa contro tutto questo è non aprire gli allegati provenienti da chi non si conosce.

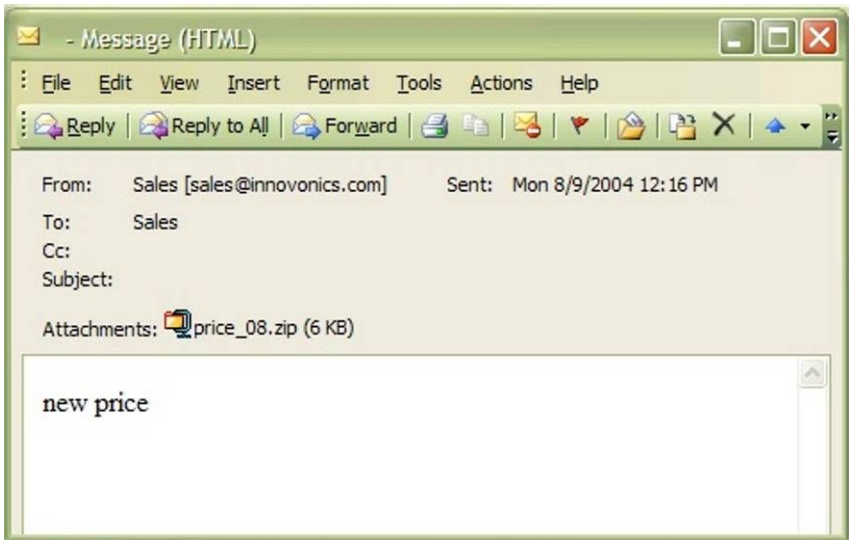
Non aprite mai un file con estensione .exe o .scr, poichè si tratta di estensioni che mandano in esecuzione file eseguibili che, a loro volta, possono infettare il computer con un virus. Come precauzione qualunque file riceviate dovrebbe essere salvato sul disco fisso e esaminato da un antivirus. Fate attenzione a file che assomigliano a tipi conosciuti, come i file zip. Qualche attaccante può mascherare un file cambiandone l'icona e nascondendone l'estensione in modo tale da non far capire che si tratta di un eseguibile.

## 9.2.4 Intestazioni contraffatte

Occasionalmente potreste ricevere mail che sembrano essere state inviate da qualcuno che voi conoscete come "Amministratore" o "Postmaster" o "Gruppo per la sicurezza" della vostra scuola o ISP. L'oggetto può essere "Returned Mail" o "Hacking Activity" o altre informazioni interessanti. Spesso c'è anche un allegato. Il problema è che contraffarre un indirizzo di mail non richiede particolari conoscenze tecniche e occupa circa 10 secondi di lavoro (a seconda di dove vivete può anche essere molto illegale).

Per fare questo, fate una semplice modifica alle impostazioni nel vostro software client di posta. Dove vi viene chiesto di inserire il proprio indirizzo e-mail (*Opzioni*, *Impostazioni* o *Preferenze*) inserite qualcos'altro. Da qui in uscita tutti i vostri messaggi avranno un indirizzo di ritorno falso. Questo significa che siete sicuri di non essere identificati? No, non esattamente. Chiunque sia in grado di leggere un'intestazione di e-mail e procurarsi un mandato di perquisizione può probabilmente ricavare la vostra identità dall'informazione contenuta nell'intestazione. Questo significa che uno spammer può mostrarsi come vuole. Così se Fannie Gyotoku [telecommunicatecreatures@cox.net] vi invia un'antenna per telefono cellulare che si rivela una scatola di cereali coperta con carta stagnola, potete anche reclamare alla cox.net, ma non siate sorpresi quando vi dicono che tale utente non esiste.

La maggior parte degli ISP autenticano i mittenti e evitano l'inoltro, ciò significa che dovete essere chi dite di essere inviando una mail tramite il loro server SMTP. Il problema è che gli hacker e gli spammer spesso agiscono su un server SMTP sul loro PC e quindi non devono autenticarsi per inviare una mail e possono simulare di essere chi vogliono. L'unico modo sicuro per sapere se una mail sospetta è legittima, è conoscere il mittente e chiamarlo. Non rispondete mai ad un messaggio che sospettate sia stato contraffatto, poichè questo fa sapere al mittente che ha raggiunto un indirizzo attivo. Potete anche esaminare l'intestazione per determinare da dove proviene la mail come nell'esempio seguente:



Questa è una e-mail proveniente da qualcuno che non conosco con un allegato sospetto. Normalmente lo eliminerei, ma questa volta voglio sapere da dove proviene. Così esamino l'intestazione del messaggio. Uso Outlook 2003 come client di posta ed esamino l'intestazione con Visualizza>Opzioni: vengono visualizzate le seguenti informazioni:

```
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—
```

Ora la parte a cui sono interessato è evidenziata sopra. Notate che il mittente è (si veda *Received from*) è kara.org, da un IP che appare essere una linea DSL xo.net, che è in disaccordo con innovonics.com, il mittente dichiarato.

Non solo, se esaminate il server di posta nnovonics.com utilizzando nslookup, il suo indirizzo risulta il seguente:

```
C:\>nslookup innovonics.com
Server:  dc.mycompany.com
Address:  192.168.10.54

Non-authoritative answer:
Name:    innovonics.com
Address:  64.143.90.9
```

Così, il mio sospetto era corretto e questa mail trasporta malware in un file eseguibile presentato come file zip. Il malware ha infettato il computer della persona sulla linea DSL, che ora è uno zombie e invia copie del malware a tutti coloro sono presenti nel suo indirizzario. Sono contento di aver evitato tutto ciò!

**Esercizi:**

1. Citbank e PayPal sono due degli obiettivi più comuni delle email *phishing*. Cerca cosa fanno per controllare / combattere il *phishing*.
2. Verificate se il vostro gestore di carta di credito o la vostra banca abbia delle regole sull'uso delle e-mail e informazioni personali.
3. (Possibilmente compito a casa) Cercate una mail di spam che avete ricevuto e cercate di risalire al mittente reale.

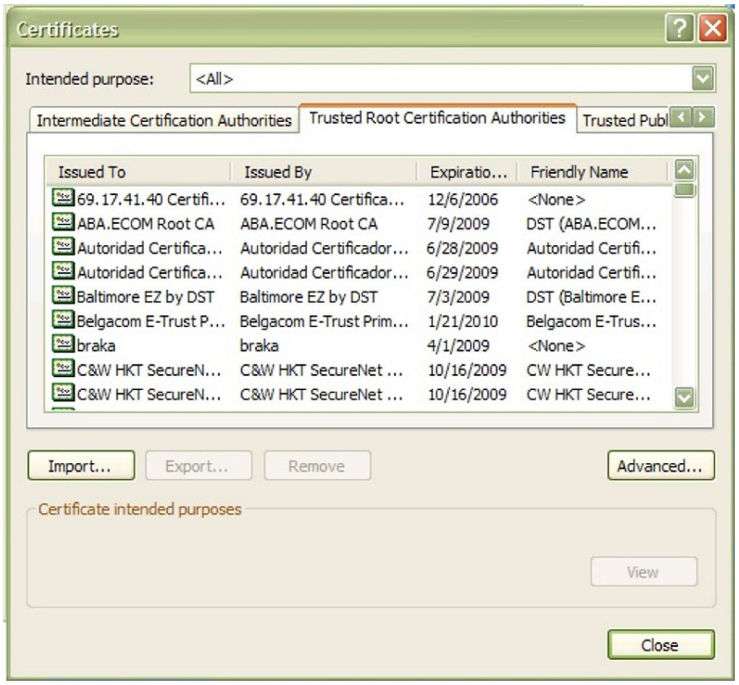
# 9.3 Uso sicuro delle E-mail Parte 2: Invio

L'invio di posta è un po' meno rischioso. Tuttavia ci sono alcune cose che potete fare per rendere più sicura la vostra conversazione. La prima è di assicurarvi che la vostra connessione sia sicura (si veda la sezione **9.4 Sicurezza della connessione** per ulteriori informazioni). Ci sono anche alcuni metodi per firmare digitalmente i vostri messaggi, che garantiscono che il messaggio proviene realmente da voi e non è stato manomesso lungo il trasferimento. Per ottenere la massima sicurezza potete crittografare i messaggi per essere sicuri che nessuno li legga.

La firma digitale attesta la provenienza del messaggio e il fatto che non sia stato alterato. Se prendete l'abitudine di utilizzare la firma digitale per le e-mail importanti, avrete molta credibilità se mai aveste bisogno di disconoscere una mail contraffatta che sembra provenire da voi. Vi consente anche di crittografare le mail in modo tale che nessun altro oltre al destinatario possa leggerle. PGP in particolare offre livelli di crittografia che solo la potenza computazionale del governo potrebbe scoprire.

## 9.3.1 Certificati Digitali

Un certificato digitale è associato univocamente ad un individuo, come la patente o il passaporto ed è composto da due parti. Queste parti sono una chiave pubblica ed una privata. Il certificato è associato univocamente ad una persona e tipicamente viene erogato da una CA (Certificate Authority) fidata. La lista delle Autorità di Certificazione è distribuita automaticamente (se siete un utente Microsoft Windows) con il Windows Update e la lista è accessibile nel vostro browser sotto Strumenti>Opzioni Internet>Contenuti>Certificati. Potete esaminare i certificati installati sulla vostra macchina (vostri e di altri) e le autorità certificate di cui vi fidate.




Potete disabilitare l'aggiornamento automatico delle CA, e scegliere di rimuovere tutte le CA dalla lista, nonostante non sia raccomandato. Le istruzioni su come fare questo si trovano sul sito web della Microsoft.

## 9.3.2 Firma digitale

Una firma digitale è generata dal software di posta con la vostra chiave privata per assicurare l'autenticità della vostra mail. Lo scopo della firma è doppio. Il primo è certificare che provenga realmente da voi. Questo è chiamato non ripudiabilità. La seconda è assicurare che i contenuti non siano stati alterati. Questo è chiamato integrità dei dati. Per effettuare ciò il programma di posta applica una funzione di hash al contenuto del messaggio. Questo produce un output di lunghezza fissa chiamato digest del messaggio. Il digest è un valore univoco e, se l'algoritmo matematico che lo produce è forte, ha i seguenti attributi:

- non si può ottenere il messaggio originale dal digest
- ogni digest è univoco.

Dopo aver creato il digest, viene crittografato con la vostra chiave privata. Il digest crittato è allegato al messaggio originale insieme alla vostra chiave pubblica. Il destinatario apre il messaggio e decifra il digest con la chiave pubblica. Il digest viene confrontato con un digest generato dal programma di mail del destinatario. Se sono uguali il controllo è terminato. Altrimenti il client di posta avvisa che il messaggio è stato alterato.

Ci sono due tipi di funzioni di firma/crittografia, S/MIME and PGP. S/MIME è considerato una scelta aziendale e di governo, perchè utilizza per l'autenticazione il modello "less labor intensive certificate authority model for authentication", e perchè si implementa più facilmente con il programma di posta Microsoft's Outlook Express. PGP è più spesso la scelta della comunità di utenti perchè si basa sul *web of trust* non centralizzato per l'autenticazione, dove l'affidabilità di un utente è validata tramite il sistema "l'amico dell'amico", dove si conviene che, se tu ti fidi di me, allora puoi anche fidarti delle persone di cui io mi fido e perchè ai membri della comunità degli utilizzatori non importa passare quattro ore per capire come far funzionare PGP con Thunderbird – essi considerano questi tipi di sfide un modo per *svagarsi.*

## 9.3.3 Ottenere un certificato

Se siete interessati ad ottenere un certificato digitale o digital ID, è necessario contattare una *Certificate Authority* (Verisign e Thawte sono i più conosciuti, anche se con una ricerca con un motore di ricerca se ne possono trovare altri). Entrambi chiedono al richiedente di identificarsi in modo da verificare che sia realmente chi dice di essere. Potete avere un certificato gratuitamente da Thawte, ma è richiesta una gran quantità di informazioni personali, incluso un numero di identificazione governativo (come un passaporto o patente). Verisign chiede un pagamento tramite carta di credito per i suoi certificati, ma chiede meno informazioni personali (presumibilmente Verisign si basa sulla compagnia di carta di credito per verificare le vostre informazioni personali). Queste richieste di informazioni possono sembrare invasive, ma ricordate che state chiedendo a queste società di garantire la vostra attendibilità. E -come sempre – effettuate approfondite verifiche con i vostri genitori o con i custodi prima di fornire qualunque informazione personale (o aggiungete grandi saldi sulle loro carte di credito).

Il principale svantaggio nell'uso dell'uso di un'autorità di certificazione è che la vostra chiave privata è disponibile a qualcun altro – l'autorità di certificazione. Se l'autorità di certificazione è compromessa, allora anche il vostro ID digitale lo è.

## 9.3.4 Crittografia

Come livello aggiuntivo di sicurezza, potete *crittografare* la vostra posta. La crittografia trasformerà la vostra e-mail in un insieme confuso di numeri e lettere che possono essere lette solo dal destinatario corretto. I vostri segreti più nascosti e le vostre poesie peggiori saranno nascoste a tutti tranne agli occhi più fidati.

Tuttavia, dovete ricordare che, mentre questo può sembrarvi una cosa buona – e anche a tutti noi che non desideriamo essere sottoposti a brutte poesie - alcuni governi non lo approvano. Le loro motivazioni possono essere più o meno valide (potete discuterlo tra voi), ma il punto non è se è corretto. Il punto è che, a seconda delle leggi della nazione in cui vivete, l'invio di mail crittografate può essere un crimine, indipendentemente dal contenuto.

## 9.3.5 Come funziona?

La crittografia è abbastanza complicata, così cercherò di spiegarla in modo meno tecnico:

Jason vuole mandare un messaggio crittografato. Così la prima cosa che Jason fa è andare ad una Autorità di certificazione e ottenere un Certificato Digitale. Questo certificato ha due parti, una chiave pubblica ed una chiave privata.

Se Jason vuole ricevere e inviare messaggi crittografati con la sua amica Kira, devono prima scambiarsi le chiavi pubbliche. Se ricavate una chiave pubblica da una autorità di certificazione di cui avete scelto di fidarvi, la chiave può essere verificata automaticamente da quella Autorità di Certificazione. Questo significa che il vostro programma di posta verificherà che il certificato sia valido e che non sia stato revocato. Se il certificato non viene da un'autorità di cui vi fidate o è una chiave PGP, allora dovete verificare l'impronta della chiave. Tipicamente questo viene fatto separatamente o con uno scambio faccia-faccia della chiave o dell'impronta.

Ora supponiamo che sia Kira e Jason stiano usando schemi di crittografia compatibile e abbiano scambiato messaggi firmati, così hanno ciascuno la chiave pubblica dell'altro.

Quando Jason vuole inviare un messaggio crittografato, il processo di crittografia inizia convertendo il testo del messaggio di Jason in un codice pre-hash. Questo codice viene generato utilizzando una formula matematica chiamata algoritmo di crittografia. Ci sono molti tipi di algoritmi, ma per le e-mail i più comuni sono S/MIME e PGP.

Il codice hash del messaggio di Jason viene crittografato dal programma di posta, così solo Kira può decifrarlo con la sua chiave privata, e questo completa il processo di crittografia.

## 9.3.6 Decifrazione

Così Kira ha ricevuto un messaggio cifrato da Jason. Questo tipicamente è indicato da un icona a forma di lucchetto sul messaggio nella sua cartella di posta in entrata. Il processo di decifrazione è gestito dal software di posta, ma ciò che avviene dietro le scene è qualcosa simile a questo: il programma di posta di Kira usa la sua chiave privata per decifrare il codice pre-hash crittografato e il messaggio crittografato. Il programma di posta di Kira trova la chiave pubblica di Jason in memoria (se ricordate avevano precedentemente scambiato le chiavi). Questa chiave pubblica è usata per decifrare il codice pre-hash e verificare che il messaggio provenga da Jason. Se il programma di posta di Kira genera un codice post-hash uguale al pre-hash il messaggio non è stato alterato lungo il percorso.

Nota: se perdete la vostra chiave privata, i vostri file criptati diventano inutili, così è importante avere una procedura di basckup della vostra chiave privata e di quella pubblica.

## 9.3.7 La crittografia è impenetrabile?

Basandoci sui numeri, il livello di crittografia offerto dal PGP, ad esempio, è impenetrabile. Certamente un milione di computer che eseguano programmi per scoprire un messaggio alla fine ci riuscirebbero, ma non prima che milioni di scimmie finiscano la loro sceneggiatura di *Romeo e Giulietta*. Il numero di teorie dietro questo tipo di crittografia coinvolge la fattorizzazione del prodotto di numeri primi molto alti e, nonostante molti matematici abbiano studiato i numeri primi per anni, non esiste un maniera semplice per farlo.

Ma la crittografia e la segretezza sono più che semplici numeri. Tuttavia se qualcuno ha accesso alla vostra chiave privata, allora ha accesso a tutti i vostri file crittografati. La crittografia funziona solo se è parte di un complesso di norme di sicurezza più ampio che offre protezione sia alla vostra chiave privata che alla password di accesso.

**Esercizi:**

1 La crittografia della posta elettronica è legale nel paese in cui vivete? Trovate un altro paese in cui sia legale e un paese in cui non lo sia.

2 Gli scrittori di fantascienza hanno immaginato due tipi di futuro uno in cui le vite delle persone sono trasparenti, cioè, non hanno segreti, e uno in cui i pensieri e le comunicazioni di tutti sono completamente privati. Phil Zimmerman, creatore del PGP, crede nella segretezza come fonte di libertà. Leggete i suoi pensieri sul motivo per cui serve PGP su http://www.pgpi.org/doc/whypgp/en/. Poi leggete l'articolo dello scrittore di fantascienza David Brin '*A Parable about Openness*' su http://www.davidbrin.com/akademos.html in cui evidenzia alcuni motivi per cui liberalità è fonte di libertà. Discutete questi due differenti punti di vista. Quale preferite? Quale pensate avrà maggior successo? Quale pensate sarà il futuro della privacy?

## 9.4 Sicurezza della Connessione

Ultima, ma non meno importante è la sicurezza della connessione. Per i server di posta, assicuratevi di usare una connessione SSL verso il vostro ISP. Comparirà una piccola icona di un lucchetto nella barra al fondo del vostro browser. Se state usando il POP e un client di posta, assicuratevi di aver configurato il client in modo che usi SSL con POP sulla porta 995 e SMTP sulla porta 465. Questo crittografa la vostra posta dal vostro computer al vostro server, così come protegge il vostro username e password POP/SMTP. Il vostro ISP dovrebbe avere un how-to sul loro sito web per configurare questo. Se non offrono una connessione sicura POP/SMTP, cambiate ISP!

**Esercizio:**

Se avete un account di posta verificate se utilizza SSL per la connessione. Come si può verificare questo nel vostro client di posta? Il vostro ISP fornisce informazioni riguardanti una connessione SSL?

# Letture di approfondimento

Può qualcun altro leggere le mie e-mail?

http://www.research.att.com/~smb/securemail.html

Pagina del PGP freeware del MIT

http://web.mit.edu/network/pgp.html

Notizie generali sulle pubblicazioni relative alla privacy in Internet:

Electronic Privacy Information Center

http://www.epic.org/

e

Electronic Frontier Foundation

http://www.eff.org/

Approfondimenti su PGP

http://www.openpgp.org/index.shtml

Come la lettura di una Email può compromettere la vostra privacy

http://email.about.com/od/staysecureandprivate/a/webbug_privacy.htm

Evitare i virus delle E-mail

http://www.ethanwiner.com/virus.html

Una breve panoramica delle domande sulla sicurezza della posta (con un piccolo avveritmento al fondo)

http://www.zzee.com/email-security/

Una breve panoramica delle domande sulla sicurezza della posta (senza avvertimento)

http://www.claymania.com/safe-hex.html

Precauzioni relative alla posta basata su Windows

http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html

http://computer-techs.home.att.net/email_safety.htm

Differenze tra i virus per Linux e Windows (con informazioni sul motivo per cui i programmi di posta per Linux sono più sicuri)

http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses/