Come e perché difendere la riservatezza della posta elettronica

Leandro Noferini
Firenze Linux User Group
leandro@firenze.linux.it

giovedì 25 Aprile 2002

Sommario

Questa vuole essere una breve presentazione dei sistemi di protezione della riservatezza della posta elettronica con i mezzi a disposizione di tutti.

Il tutto anche a ricordo della Resistenza contro il fascismo e il nazismo.

La PE nella vita quotidiana

La PE sta diventando sempre più un media centrale nella vita di relazione di tutti i giorni, almeno per la parte ricca del pianeta.

Il suo uso è favorito dalla sua diffusione e dalle notevoli comodità che presenta: purtroppo però, a nostro avviso, non è altrettanto diffusa la coscienza della sua *intrinseca* debolezza per quanto concerne la riservatezza dei dati.

In verità tutto ciò che spediamo con la PE viene trasmesso in rete *in chiaro*, cosa che permette a chiunque con un *minimo* di necessità e/o voglia di leggere e archiviare tutto.

PE e posta ordinaria/cartacea

Nella posta ordinaria è uso comune spedire il proprio *messaggio* in busta chiusa a meno che non si voglia spedire una cartolina illustrata da qualche località di villeggiatura; questo nonostante che la tariffa delle cartoline postali sia più bassa delle buste chiuse.

Allo stesso modo è auspicabile che questo comportamento diventi usuale anche nella corrispondenza elettronica.

Ancora peggio

Intercettare la posta ordinaria è molto complicato perché necessita di lavoro diretto, concreto e in tempo reale, per realizzarla è necessario

- prendere fisicamente in mano la busta spedita
- aprirla
- leggerla (cosa che è difficilmente automatizzabile)
- prendere appunti

La PE è invece molto comoda

Il formato di memorizzazione della PE invece è quanto di più comodo ci possa essere perché possa essere memorizzato.

Con la PE è molto comodo e conveniente memorizzarla, farci ricerche anche incrociate, recuperarla nel tempo.

Siamo tutti sotto controllo

- Intercettare la nostra PE è semplice e conveniente
- I dati così ottenuti hanno un tale valore economico nonché sociale e politico

che dobbiamo presumere di essere tutti possibili oggetti di controllo da parte di terzi

Esempio

L’esempio che viene facile da presentare è la corrispondenza commerciale di una ditta medio/piccola che ha rapporti con i propri clienti, fornitori, dipendenti e dirigenti attraverso la PE.

Soluzioni - il cuore del mio intervento

Il problema di rendere il proprio messaggio illeggibile ad altri che non fosse il destinatario è vecchio probabilmente poco meno della possibilità di spedire messaggi

Molte soluzioni sono state pensate

Crittografia ed informatica

Una soluzione escogitata è quella della crittografia, cioè il rendere illeggibile il messaggio

Con l'informatica questo sistema ha ricevuto una spinta ulteriore dalla capacità di calcolo di queste macchine, capacità che benissimo si adattano al problema

Crittografia a chiave

In particolare qui parleremo della tecnica crittografica detta a chiave

```
Messaggio -> Algoritmo -> Messaggio
originale Chiave Crittato
```

- Algoritmo

  La descrizione del modo con cui si passa dal MO a quello crittato [1]

- Chiave

  un elemento che associato insieme all'algoritmo permetta di risalire al messaggio originario e tale che senza questo non sia possibile ottenere il MO

Ovviamente il tutto deve essere reversibile cioè dati l'algoritmo, la chiave e il MC si deve poter ottenere indietro il MO

[1] La questione dell'algoritmo è molto complessa e viene qui volutamente trlasciata per chiarezza e per il tono introduttivo di questo intervento

Messaggio -> Algoritmo -> Messaggio
originale Chiave Crittato

messaggio in chiaro

Questo è un esempio di messaggio in chiaro (i puntini sono al posto di alcuni header).

```
From flug-admin@firenze.linux.it  Sun Apr 21 20:31:52 2002
Return-Path: <flug-admin@firenze.linux.it>
Delivered-To: leandro@clementino.cybervalley.org
Received: from localhost (localhost [127.0.0.1])
        by clementino.cybervalley.org (Postfix) with ESMTP id
        for <leandro@clementino.cybervalley.org>; Sun, 21 Apr
Delivered-To: lnoferin@cybervalley.org
....
To: flug@firenze.linux.it
Subject: Re: [Flug] [carobene@systems.it: Notizie per inter.n
From: Leandro Noferini <lnoferin@cybervalley.org>
....
Date: Sun, 21 Apr 2002 08:28:14 +0200
....
Lines: 14
```

> ricevuta su info@f.l.i

Direi che gli potresti suggerire di scrivere direttamente a
così fa prima, lui a raggiungerci tutti, noi a segarlo se co
a rompere!

;-)

--
Ciao
leandro
Email: lnoferin@cybervalley.org
Quello che puoi, fallo. Quello che non puoi, simulalo.

---

messaggio crittato

Questo un esempio di messaggio crittato

```
....
Subject: Re: Due cose
....
From: Leandro Noferini <leandro@firenze.linux.it>
....
Date: Thu, 25 Apr 2002 13:59:02 +0200
In-Reply-To: <20020424101356.4ab63a0e.leonardo@firenze.linux.
 Giacomelli's message of "Wed, 24 Apr 2002 10:13:56 +0200")
Message-ID: <87662gj8ft.fsf@clementino.cybervalley.org>
User-Agent: Gnus/5.090006 (Oort Gnus v0.06) Emacs/21.1
 (powerpc-debian-linux-gnu)
MIME-Version: 1.0
Content-Type: multipart/encrypted; boundary="=-=-=";
        protocol="application/pgp-encrypted"
Lines: 40
Xref: clementino.cybervalley.org mail.2002-04:146
```

```
--=-=-=
Content-Type: application/pgp-encrypted

Version: 1

--=-=-=
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: Per informazioni si veda http://www.gnupg.org

hQEOA51zNbaxvAB/EAP/XVavvxd3GjOSHOyympg3fZl0SpdFzqXlOWRRlfOCQ
bHCPMk348/afS/aRxWOR5YFwYaJk7r6Frz6Wc6ObxSl82n6BgEVEIwNLabJ9O
yKqUAW9NtThQl+PLUII/NDNRS/64iHpuu5MCjYM1bGu7D/KJmf1Kx/8PzJdvx
AIacLet+yW1Cq2zCFkZMPNrf9YYT88JjWJeu8pDPiIw0Gh9JWkq76c4hr4YZw
VyPn3mo3kDPBSKvbuo1c1QiQcdn6jV1q1w7J0MRR6qMY/YRulaqupwtOLc5vD
qn7C8iTUVxMy8dqWDH2/NLhrF9uytfDbDtE9+MBL8TzJ0ukBzZbQ3v2vddKSg
uQjU18xwhW7m4r8GIAR2qLvNqQbIcovcz/cQpxdEnX9X6i0yUv+wihtXxwkM3
YocPxAAADg8Qsbclno3QF4VBlchOzYbEhH/LrBgoM0zBmRFJR72KZRtzslQj4
hEoeeu/ylyw1JmfWNWIvAvP+JBBPQdhLszy1OzT9qj24Tpkn8+jXDjp2HmblI
```

LvH2PQJDOANv4BScHzGRDr+1YcLTBEDlsjAfiJKoTIVKJjkrsKrjfy/WIDQTM
fTfR1VJ+v1erWaNgTW36TUjYNKIpdL3TyQLr3EoymZQvoNWEJha6/jCgPhbvf
Nto+fRx7aFzus0ZFOsQatYvJFQowtPyJRq+k8JEHyHeOFVHSZsLoiGKrlEULD
ang6LzfVxzWDoUeAUYS+YxE862SaY1B3R7POLVyhWnk1qFr9katr/z58483U4
+EMcpkuov9eGHm8xGSDI2E87Hd1F03BvuKUKgLJq0n/YjU06Jswb5WUbGWG+y
v3Yt68uOiA1+jUGFZothoLtok5jS1yH7o7tJAAqQth4ak3GBwU9+lkVx/OP8J
5+61oSDwMAAFcBr5/FeN9Olt85qNlG9WbLZir0zeH9hosuRKLFNPN+kVVZoj1
yeUkj+Kmgvc7Z3FMMIUYVNhmsMC5YFppWR8MwDraV77twktIfmqAVatmFEeSI
JLSN8bkt0vT7dxHz+2foLvkNoLhwDdq5bdUoEg+nzbENM/ONtutZxXzXxKN5b
MPTc4S3qK/A9FTK/ia2prIx2F/JWeZ1vgzlfuE6bv+HP3u+g2DlJEzQn8Ovp6
D8ByQCArnkPi+YEHsR0MesX+L0sfWp9CK4GpMl/crTSdZV1J4dAT0XsMcD/Qo
WK4DOGEIjjI95mnidMRR+UG9gabUKUe5UJDyZTx6j4tu8TmaK5CChwb/rc2Sa
ssmJd7DisZZmvESamVwMPzMNndrxHNUjKlIDgBAzNxeI5kCFPz05gvo02sZWO
23ZhT7nd6b8qedf4ukepMfN2+xXlPy5FotUXIRt5Urkn3ZoD8rtAcQNg1He9K
wICYRrjkt+UYwJiSCXEvXDC8T+ZnPxUvmwTlPbVuuvJ7UQSo5XLjfGc8Np50U
AMdI+xiR/7I41TQC5tE=
=c306
-----END PGP MESSAGE-----
--=-=-=--

Debolezze di questo sistema

Ce ne sono molte (che spiegherò più avanti) ma il principale problema sta nell'unicità della chiave

Con tutti i sistemi di questo tipo chiunque conosca la chiave (oltre all'algoritmo usato) può risalire al MO ragione per la quale diventa necessario scambiare la chiave usando canali sicuri

Ma se si hanno a disposizione canali sicuri per scambiarsi la chiave li potremmo anche usare per scambiarci i messaggi

Inoltre un altro grave problema è che questi canali sicuri dovrebbero essere usati per *tutte* le comunicazioni in atto e dovrebbero essere sempre diversi.

Disegnino di Alessandro e Barbara che si scambiano la posta con una chiave singola

Il PGP - doppia chiave

Nel 1987(?) Philip Zimmerman scrisse un programma che usava un altro approccio al problema istituendo la DOPPIA CHIAVE.

- una chiave *Pubblica*

  una chiave che serva esclusivamente per crittare i messaggi che così diventano leggibili solo conoscendo la

- chiave *Privata*

  che serve esclusivamente a decrittare i messaggi crittati con la precedente

Disegnino delle doppie chiavi

La pratica

Il tutto può sembrare complicato così come lo farò vedere adesso ma il tutto è stato reso sempre più semplice ed integrato, come vedremo più avanti

Facciamo un esempio:

Alessandro e Barbara mi hanno creduto e quindi hanno deciso di rendere la loro corrispondenza privata e illeggibile da parte di altri

Primo passo: la creazione delle due chiavi

Alessandro crea la sua coppia di chiavi: una chiave privata e una pubblica.

Queste due chiavi formano un binomio inscindibile: senza l'una l'altra è assolutamente inutile però particolare attenzione deve essere posta a quella privata (link ai problemi del pgp)

Secondo passo: la spedizione della chiave pubblica

A questo punto Alessandro spedisce la propria chiave pubblica a Barbara

Questo passo può essere eseguito anche usando canali non sicuri (come la PE non crittata) perché il possesso di questa chiave permette *soltanto di crittare* messaggi per la *chiave privata* di Alessandro

Un eventuale Carlo che segue la conversazione intercettando i messaggi scambiati non entrerebbe in possesso di alcun dato sensibile

Tanto che la cosa è stata resa ancora più *semplice* dall'istituzione di appositi server che servono proprio a scambiare chiavi pubbliche

Terzo passo: si comincia a crittare

A questo punto Barbara *inserisce* la chiave pubblica di Alessandro nel suo programma [2]

Barbara a questo punto scrive il messaggio per Alessandro e poi lo critta usando la chiave pubblica di questi e spedisce il messaggio così *trattato* usando i normali mezzi

Se il Carlo di cui sopra intercetta questo messaggio si trova una cosa sempre illeggibile perché non è in possesso della chiave privata di Alessandro

[2] questo passo cambia moltissimo a seconda del client di posta in uso e dalla versione di pgp/gpg usata

Quarto passo: il messaggio arriva

Alessandro a questo punto riceve il messaggio e lo può leggere perché lui (e lui solo) è in possesso della chiave privata atta a decrittare il contenuto

Notare due cose:

- tutta la corrispondenza è avvenuta usando canali “normali”, “non sicuri”
- nonostante quanto detto sopra non è mai avvenuto uno scambio di dati “delicati” senza la protezione della crittazione

Ovviamente se Alessandro vuole rispondere a Barbara usando la stessa tecnica deve aspettare che questa faccia la stessa trafila e renda disponibile la propria chiave pubblica

Problemi di questa soluzione

Evidentemente anche questa soluzione pone problemi dei quali

- alcuni sono risolvibili “direttamente” dall’utente
- altri sono risolvibili usando altri approcci
- altri usando altri programmi
- altri invece rimangono non risolti
- altri problemi nascono dalle differenti “implementazioni” di quest’idea
- altri dagli algoritmi usati

Proviamo ad elencarli

L'identità del corrispondente

In uno scenario, molto comune ormai, di comunicazione crittata diffusa è possibile per me spacciarmi per un altro

Il Carlo-spione, con notevole tempismo, spedisce a Barbara una chiave pubblica dicendole "Sono Alessandro e questa è la mia chiave privata", *questo prima che Alessandro spedisca la sua*

Barbara, non avendo altri mezzi per accertarsi dell'identità di chi le ha spedito la chiave, spedisce il messaggio crittato con la chiave fasulla ad Alessandro (il quale non potrà leggere il messaggio). Carlo sarà lì che intercetta e che diventa perciò in grado di leggere il messaggio

L'unica soluzione a questo problema è di accertarsi dell'identità del corrispondente:

- direttamente mediante i *PGP Party*
- indirettamente mediante la *fingerprint* della chiave che Alessandro curerà di rendere il più comune possibile e soprattutto il più associabile alla sua persona possibile (link al messaggio d'esempio)

- indirettamente attraverso il *web of trust* cioè le *firme* presenti nella chiave pubblica di Alessandro

Gli attacchi a forza bruta

I computer stanno diventando sempre più veloci e potenti per cui sta diventando sempre più possibile attaccare un messaggio crittato per trovare il contenuto originale senza avere nessun altro indizio

Questa tecnica funziona sempre, solo che con *chiavi ragionevoli* occorre troppo tempo per ottenere un qualche risultato

La soluzione a questo problema è quello di usare *chiavi più lunghe*: le chiavi possono avere lunghezza diversa (512, 1024, 2048 bit sono le dimensioni più comuni). Una maggiore lunghezza implica una maggiore difficoltà per un attaccante a *forza bruta*, comportando però un maggior carico di lavoro per il computer, oltre che una maggiore lunghezza dei messaggi spediti

Poiché la creazione di una coppia di chiavi è un atto da fare pensando ad una certa durata è importante prevedere l'aumento della potenza di calcolo nel futuro

Ora come ora usare chiavi da *1024 bit* è RAGIONEVOLMENTE SICURO; si consigliano perciò chiavi di *2048 bit*

Relazione fra chi scrive a chi

Con questo sistema è possibile per Carlo-spione stabilire che Barbara e Alessandro si scrivono

Evidentemente se voi userete PE crittata scrivendo *esclusivamente* a “basista@brigaterosse.rev” attirerete notevoli attenzioni

Da uno studio di una corrispondenza, anche crittata molti dati possono essere rivelati, studiando

- le dimensioni dei messaggi
- la frequenza di spedizione
- le ore e le date di spedizione

Anche questo problema non ha soluzioni “intrinseche” al metodo ma solo “scappatoie” date da altri approcci

- l’uso di remailer anonimi (prossimo intervento)

- usare PE crittata per *tutta* la posta personale

  maggiore è l'uso personale di queste tecniche più difficoltoso diventa uno studio dei comportamenti

- diffondere la conoscenza e l'uso di questi strumenti il più possibile

  più siamo ad usare questi strumenti meno tracciabili siamo

- "nascondere" il messaggio in "qualcos'altro" (steganografia)

Cura della chiave privata

Punto focale dell'affidabilità di questo sistema è la chiave privata

Questa viene normalmente memorizzata con una protezione crittografica (passphrase), però molti problemi lo stesso sono nati da questo

- mai tenere la chiave privata su computer in rete oppure dei quali non siamo *assolutamente* certi
- usare versioni di programmi che hanno risolto i problemi della residenza della chiave privata in file di swap e/o in memoria

Problemi legati alle implementazioni

Di software stiamo parlando e quindi con i “bachi” dobbiamo confrontarci

In particolare gli algoritmi usati devono essere ben provati

Ad esempio è importante non dare alcuna possibilità di poter risalire dalla chiave pubblica a quella privata

Problema dei sorgenti

Un grave problema (peraltro comune a tutti i programmi crittografici) è la *disponibilità dei sorgenti*

PGP è da molto tempo una ditta commerciale: però per lungo tempo (fino alla versione 6.5.3) i sorgenti del programma venivano resi disponibili. Ora non è più così e quindi il mio consiglio è quello o di usare il *GPG* oppure di usare la vecchia versione

Riferimenti