

***** I rischi della TUA casella di posta elettronica: consigli *****

Sommario:

1. Sulla privacy
 2. I rischi della TUA casella di posta elettronica: consigli.
 - . il percorso delle email.
 - . leggere la posta, il confine tra il bene e il male.
 3. Accorgimenti tecnici e crittografia.
 4. Ancora qualche spunto sulla crittografia: piccoli approfondimenti.
-

***** sulla privacy *****

Nell'ordinanza di custodia cautelare consegnata agli arrestati di Cosenza si fa esplicito riferimento alle discussioni degli indagati circa la possibilita' di cifrare le proprie missive e si valuta questo fatto come una precisa indicazione della loro volonta' di compiere azioni illegali.

La stessa inchiesta ha condotto all'intercettazione di 60.000 email. Non possiamo accettare che la tutela della propria privacy cada a colpi di ragion di stato, tra teoremi inquisitori e lo spauracchio del terrorismo.

In un sistema di cose nel quale il controllo viene sempre piu' imposto come la panacea di tutti i mali, vorremmo cercare di fare chiarezza sui pericoli che la comunicazione via email comporta, e le contromisure che e' possibile adottare.

Il percorso delle email.

La tua posta elettronica e' a rischio in vari modi: quando spedisce un messaggio, per prima cosa il client di posta che usi contatta un server attraverso un protocollo detto SMTP e trasferisce a quest'ultimo il messaggio. Questo trasferimento - di solito - avviene in chiaro (nessun tipo di cifratura viene applicato al messaggio). Il server SMTP a sua volta contatta il server di destinazione, e il passaggio attraverso la rete e' di nuovo in chiaro.

A questo punto il messaggio e' passato da una macchina all'altra, e risiede presso il tuo fornitore di casella postale.

Normalmente i fornitori di questo tipo di servizi mantengono traccia (i famosi log) di queste operazioni, quindi e' possibile risalire alle mail che hai spedito un certo giorno, ad una certa ora, ad una certa persona, o viceversa a quelle che hai ricevuto.

Leggere la posta, il confine tra il bene e il male.

Quando scarichi e leggi la posta presso la tua casella postale utilizzi solitamente uno di questi due metodi:

- 1) attraverso il web, da un semplice browser.
- 2) con un programma apposito utilizzando i protocolli POP3 o IMAP.

Sia nel primo caso che nel secondo, senza particolare accorgimenti, tutto il traffico e' di nuovo in chiaro, la tua password passera' in chiaro ed i messaggi passeranno dalla macchina del tuo fornitore di servizio al tuo pc in chiaro.

Il rischio si articola dunque su due livelli:
In primo luogo, durante le sue peregrinazioni attraverso la rete, il messaggio puo' essere intercettato e letto.
In secondo luogo, durante le soste nei vari server, il messaggio e' accessibile a chi ne abbia il controllo.

***** Accorgimenti tecnici e crittografia *****



Per quanto riguarda il primo problema, puoi utilizzare canali di comunicazione cifrati fra te ed i server che usi (SMTP con supporto SSL, POP3s, IMAP su SSL).

Per quanto riguarda il secondo problema, la soluzione e' utilizzare programmi per la cifratura del contenuto delle email. Nella scelta del programma da utilizzare e' critica la disponibilita' del codice sorgente. Solo tale disponibilita' puo' garantire che il programma faccia esattamente quello che sostiene di fare, e non contenga ad esempio una backdoor che modifichi ogni vostro messaggio crittato rendendolo visibile al possessore di una chiave predefinita (ad esempio la ditta realizzatrice del programma stesso).

Date queste premesse puoi utilizzare **GnuPG** (www.gnupg.org) che e' un programma a codice aperto distribuito con licenza GPL, oppure **PGP** (www.pgpi.org) ma con alcune limitazioni: vanno bene le prime versioni (fino alla 6.5.8 compresa) distribuite con il codice sorgente con una licenza simile alla gpl, mentre per le successive la societa' che ha preso la gestione del programma ha prima modificato le condizioni d'uso e poi impedito l'accesso ai sorgenti.

L'ultima versione (8.0) ha reso nuovamente disponibile il sorgente per verifiche (ma non per modifica e redistribuzione, come da licenza gpl) ma il programma supporta soltanto Windows e MacOS.

ricapitolando

Quindi utilizza un software di crittografia per scrivere i messaggi personali e configura il tuo programma di posta affinche' riceva ed invii posta in modo sicuro (SMTP con supporto SSL, POP3s, IMAP su SSL).

Su http://www.autistici.org/howto/mail_ht.php trovi tutte le informazioni su come configurare la tua posta.

Su http://www.autistici.org/howto/keyserver_ht.php come utilizzare il nostro keyserver pgp e gpg per rendere disponibile la tua chiave pubblica e cercare quelle degli altri.

Inoltre vi segnaliamo:

<http://crypto.spialaspia.org>

<http://www.winstonsmith.info/>

***** Ancora qualche spunto sulla crittografia *****

Le proprie email viaggiano solitamente in chiaro datosi che nessuno dei protocolli che stanno alla base dello scambio di missive e' stato concepito con un supporto crittografico, ovvero dei meccanismi in grado di rendere indecifrabile il contenuto delle proprie mail. Quest'ultimi sono stati ideati in seguito con il crescere della consapevolezza della fragilita' dei protocolli iniziali. E non hanno ancora trovato piena applicazione.

Sistemi di controllo generalizzato come il tanto discusso Echelon, ed in generale chiunque intenda per i motivi piu' diversi leggere il contenuto di una mail, puo' sfruttare a proprio vantaggio questa debolezza. Una decina di anni fa si incomincio' a parlare di crittografia applicata all'invio delle mail ed in modo piuttosto rocambolesco fu creata

la prima versione del **PGP**, il Pretty Good Privacy di Philips Zimmermann. Per un'introduzione all'uso ed ai concetti che stanno alla base di PGP si consiglia di consultare Kryptonite. (<http://www.kyuzz.org/anon/critto.html>)

Oggi la società che gestisce questo prodotto non gode più della fiducia della comunità informatica e l'unica versione del PGP il cui utilizzo è consigliabile è la **2.6.3i** (www.ecn.org/crypto/soft/pgp.phtml), prodotta circa 10 anni fa.

La PGP Inc., la società fondata da Zimmerman, è di recente stata rilevata dalla NAI, un cartello formato dalla TIS (Trusted Information Systems), e la McAfee anti-virus, ed ha cessato la vendita del PGP.

Esiste però un software che ne ricalca e migliora le caratteristiche e che raccoglie in pieno la fiducia della comunità informatica: **GPG**, il Gnu Privacy Guard. Questo software si basa sul lavoro di standardizzazione compiuto dall'**IETF** (www.ietf.org) e pubblicato nel rfc 2440 per la creazione di uno standard aperto e non proprietario per la gestione sicura della propria corrispondenza elettronica. Il sito ufficiale è tradotto in italiano ed esistono degli ottimi tutorials per l'apprendimento dei concetti base e avanzati (www.gnupg.org)

Sono stati sviluppati numerosi frontends per agevolare l'utilizzo di GPG, su www.gnupg.org/fronteds.html sono riportati alcuni dei progetti più interessanti.

Questa categoria di software permettono di spedire una mail che soltanto il reale destinatario possa decifrare, ma il solo fatto che il mittente della mail debba essere obbligatoriamente identificabile mina alla base il concetto di privacy. Per questo motivo sono stati creati una serie di strumenti conosciuti come **anonymous remailer** in grado di celare il mittente di una mail.

Un buon riferimento è di nuovo Kryptonite al capitolo 5. In generale gli anonymous remailer sono dei server che funzionano da intermediari tra il mittente ed il destinatario

nella fase di consegna della mail. Per cui il reale mittente viene sostituito dall'intermediario. Usando in catena più intermediari si realizza un livello di sicurezza accettabile e si può affermare che la propria mail sia stata spedita in maniera anonima. Un utilizzo intelligente implica la fusione di anonymous remailer e PGP o GPG. Per raggiungere un buon livello di sicurezza è infatti necessario prima cifrare il messaggio e quindi spedirlo attraverso una catena di remailer. Esistono diversi client grafici per l'uso di remailer. Per un elenco conviene consultare <http://www.ecn.org/crypto/soft/remailer.phtml>

È inoltre possibile presso alcuni server che ospitano questi servizi trovare delle interfacce web che ne rendono più intuitivo l'utilizzo. Ad esempio <https://mixmaster.autistici.org/cgi-bin/mixemail-user.cgi>

Rendere anonima la spedizione non significa comunque rendere anonima anche la ricezione. Per ottenere un circuito di scambio posta completamente sicuro esiste un servizio detto **nym server**, in grado di ricevere una mail e rigirla sulla proprio account attraverso una serie di remailer. In questo modo chi risponde non conosce il reale indirizzo del destinatario, ma soltanto un alias, un'identità fittizia creata ad hoc sulla macchina che si pone da intermediario tra la propria casella email ed il mittente. La posta potrà quindi essere spedita presso ad esempio `zorro@nome_dominio_nym` e solo in seguita inoltrata al reale indirizzo di posta di zorro.

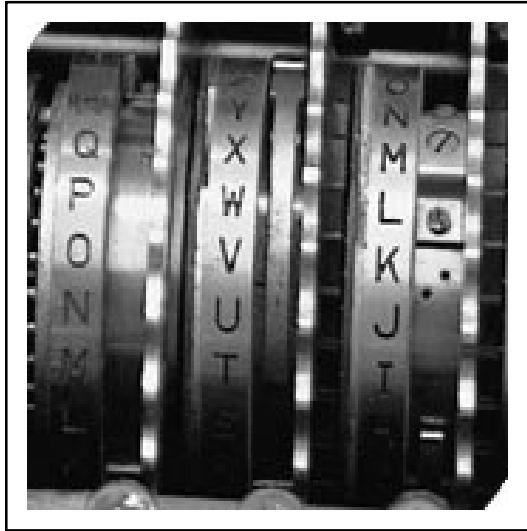
Rendere anonima e non decifrabile la propria posta potrebbe però non essere sufficiente. I protocolli che vengono solitamente utilizzati per scaricare le mail dal proprio provider contemplano, ma solitamente non utilizzano la possibilità di cifrare la connessione. Quindi la propria password transita in chiaro nel percorso che separa il vostro computer dal provider, il che potrebbe permettere ad un ipotetico ascoltatore nascosto di scaricarla al vostro posto. Sarebbe abbastanza frustrante prestare tanta attenzione nello spedire o ricevere un'email, che però non raggiungerà mai il reale destinatario. La maggior

parte dei server e dei client di mail ormai possiedono il supporto per il protocollo SSL o per TLS. Entrambi aggiungono un livello crittografico utile ad esempio a non far passare la propria password in chiaro per Internet. E' piuttosto semplice abilitarli dal lato client, non e' pero' detto che il proprio provider li supporti.

Per una trattazione approfondita del protocollo SSL si veda <http://telemat.die.unifi.it/book/Internet/Security/>

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

Autistici / Inventati



Pillole di paranoia

...cenni su crittografia e sicurezza della tua posta elettronica...

Autistici / Inventati

<http://www.autistici.org>

<http://www.inventati.org>

