

Verba volant scripta manent.

Quando, come e soprattutto **quale** crittografia.

Marco Bodrato

Linux Day - Torino - 25 ottobre 2008
Cascina Roccafranca

- 1 Modelli di sicurezza
 - Cosa vuole dire sicurezza?
 - Quel che ci aspettiamo dalla posta
 - ... e da una chiacchierata tra amici
- 2 Vari programmi/paradigmi per la crittografia
 - HTTPS, SSL...
 - GPG o OpenPGP
 - E cosa succede su una chat?
- 3 Crittografia Off-the-Record
 - Cosa ci garantisce
 - Programmi che la implementano
 - Dimostrazione interattiva

Una citazione

... non prendiamoci sul serio ...

Mohamed el Baradei

Nobel per la pace 2005

Per molti popoli e nazioni la sicurezza resta una preoccupazione prioritaria. Ma in cosa essa consista, e quali siano le strategie per conseguirla, può variare molto.

Per miliardi di persone sicurezza è la speranza di vedere “garantiti” i propri bisogni fondamentali: cibo, acqua, un tetto, l’assistenza sanitaria.

Per altri, sicurezza è la speranza di vedere “garantiti” altri diritti umani fondamentali, quali la libertà d’espressione e dissenso, ...

...

Università di Firenze, 5 ottobre 2007

Sicurezza nella comunicazione

Per dire che un canale di comunicazione è sicuro ci aspettiamo almeno alcune garanzie:

- l'identità dell'interlocutore
- che non ci siano altri ad ascoltare
- messaggi non distorti

Per ogni forma di comunicazione tradizionale, *conosciamo il livello di sicurezza* e adeguiamo il tono e i contenuti della discussione. Non tutti i canali devono essere sicuri, ma vogliamo saperlo.

Posta e posta elettronica

Busta chiusa

Nessuno può leggere il contenuto senza manomettere l'involucro.
La grafia ci conforta sull'identità del mittente.

Posta elettronica

È paragonabile alle cartoline...
...scritte a macchina

Falsificare messaggi di posta elettronica è tecnicamente banale,
solo una questione di volontà.

Servono firma elettronica e cifratura, per questo si usano protocolli
come OpenPGP o SSL.

Chiacchiere e chat

Discussione a casa di amici

Vediamo i nostri interlocutori e possiamo immaginare che nessuno abbia un registratore in funzione: "... *che resti tra noi...*"

Chat via internet

Identità garantita in modo molto debole...
...quasi certezza che *il registratore* sia in funzione.

In ogni caso la trascrizione elettronica è un testo facilmente falsificabile.

Quindi crittografia sí, ma non basta... meglio *Off-the-Record*:
"immune alla registrazione".

Canali sicuri

https://..., SSL o TLS

Esistono degli standard abbastanza consolidati per creare connessioni *sicure*.

Le domande da porsi...

- Chi garantisce questa sicurezza? (2x)
- Che tipo di sicurezza è?
- È adeguata ai *miei* bisogni di sicurezza?

Ad esempio l'uso di HTTPS per leggere/spedire posta o per partecipare a chat. Sono protocolli adeguati?

Per la posta elettronica... GPG!

Se volete che la vostra posta elettronica non sia intercettabile e manipolabile, potete usare OpenPGP!

- Si basa sui concetti di cifratura asimmetrica (o a chiave pubblica).
- Vi permette di creare la vostra chiave, senza interventi esterni.
- Non esiste una autorità garante di cui vi dovete fidare.
- Ad oggi non è noto **nessun** attacco ai maggiori algoritmi che GPG usa.

Il programma libero piú noto che implementa il protocollo è GnuPG (o GPG). Reperibile sul sito <http://www.gnupg.org/>.

In pochi passi dalle *cartoline* alla posta blindata

Facilmente GPG è già installato nella vostra distribuzione Linux, in ogni caso il pacchetto da installare si chiama `gnupg` o `gpg`.

- 1 Create la **vostra** coppia di chiavi (privata e pubblica) con:
`gpg --gen-key`.
- 2 Firmate e fate firmare le chiavi pubbliche `gpg --edit-key`
- 3 Configurate il vostro programma di posta per usare GPG

e... il gioco è fatto.

Programmi di posta con GPG “di serie”: evolution, kmail, mutt...
...o con qualche aggiunta: enigmail (icedove, thunderbird), ...

Attenti a non perdere chiave privata e passphrase!

Chiave privata e la “frase chiave” *sono* la vostra identità digitale.

Per la posta elettronica... pro e contro.

Ed una volta che abbiate creato la vostra chiave GPG, ed imparato ad usare un poco di crittografia...

Vantaggi

- Se usate la cifratura, solo i destinatari potranno decifrare il messaggio.
- Se usate la firma, chiunque, in ogni momento, potrà verificare che siete stati voi a scrivere quello che avete scritto.

Per la posta elettronica... pro e contro.

Ed una volta che abbiate creato la vostra chiave GPG, ed imparato ad usare un poco di crittografia...

Vantaggi

- Se usate la cifratura, solo i destinatari potranno decifrare il messaggio.
- Se usate la firma, chiunque, in ogni momento, potrà verificare che siete stati voi a scrivere quello che avete scritto.

Svantaggi

- Se usate la firma, chiunque, in ogni momento, potrà verificare che siete stati voi a scrivere quello che avete scritto.

Ci son caratteristiche desiderabili in alcune occasioni e **non** in altre.

Cosa succede se uso i paradigmi precedenti su una chat?

Si possono firmare e cifrare tutti i messaggi.

Installazione su Debian di un plug-in per pidgin...

```
# apt-get install pidgin-encryption
```

In questo modo otterrò le garanzie di identità e riservatezza di prima, ma sono solo questi gli effetti? O ci sono *effetti collaterali* (effetti che nuocciono al marketing)?

Questo significa firmare ogni messaggio

Siete davvero disposti a mettere per scritto e firmare ogni vostra chiacchiera?

Bisogna inventarsi qualcosa d'altro...

▶ Cosa ci aspettavamo?

OTR: Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

Vediamo cosa ci garantisce la crittografia OTR:

- **Riservatezza: nessun'altro può leggere i nostri messaggi.**

OTR: Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

Vediamo cosa ci garantisce la crittografia OTR:

- Riservatezza: nessun'altro può leggere i nostri messaggi.
- Autenticazione: garantita l'identità del nostro interlocutore e l'integrità del messaggio.

OTR: Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

Vediamo cosa ci garantisce la crittografia OTR:

- Riservatezza: nessun'altro può leggere i nostri messaggi.
- Autenticazione: garantita l'identità del nostro interlocutore e l'integrità del messaggio.
- *Perfect forward secrecy*: una compromissione della chiave privata non fornisce informazioni sui messaggi passati.

OTR: Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

Vediamo cosa ci garantisce la crittografia OTR:

- Riservatezza: nessun'altro può leggere i nostri messaggi.
- Autenticazione: garantita l'identità del nostro interlocutore e l'integrità del messaggio.
- *Perfect forward secrecy*: una compromissione della chiave privata non fornisce informazioni sui messaggi passati.
- Rinnegeabilità: i messaggi **non** contengono una firma digitale verificabile da terzi. È facile falsificare la trascrizione della conversazione.

Programmi liberi che implementano la crittografia OTR

Per ora solo alcuni programmi per chat via rete:

- climm (ex mlCQ), centerIM, mcabber, . . . ,
- (via plug-in) kopete , Miranda, irss, . . . ,
- pidgin (via plug-in).

Quest'ultimo è l'implementazione migliore che potete sperare, visto che è curata ed aggiornata degli inventori del protocollo.

Installazione ed uso di pidgin-otr

Installazione su Debian (o Ubuntu)

```
# apt-get install pidgin-otr
```

Su altre distribuzioni (Fedora, Gentoo, ...) o sistemi (FreeBSD,...) il pacchetto si chiama comunque **pidgin-otr**.

La configurazione e l'uso in pochi passi ...lanciato pidgin

- 1 Tools→Plugins→Off-the-Record attivate il plugin
- 2 Durante la chat a 2: l'icona accanto al menù "OTR" mostra lo stato della sessione
- 3 Durante la chat a 2: "OTR"→Authenticate per verificare l'identità.

Al posto della dimostrazione "dal vivo" ...

The screenshot displays the Pidgin IM client interface. On the left is the 'Buddy List' pane showing 'Recent Buddies' (LD08TO, LDT008) and 'Plugins' (including 'Off-the-Record Messaging 3.2.0'). The main window shows a conversation with 'LD08TO'. The chat history includes messages from 'Secondo utente' and 'Primo utente', as well as system messages about private conversations and encryption. An 'Authenticating Buddy' dialog is open, showing a progress bar and 'Waiting for buddy...'. A second 'Authenticate Buddy' dialog is also open, displaying the question: 'Dove ci siamo conosciuti (evento luogo anno, e ricorda le maiuscole!)?' and the answer: 'Linux Day Torino 2008'. The dialog has 'Cancel', 'Authenticate', and 'Help' buttons.

... immagine con varie fasi di configurazione e uso.

Grazie

Domande?

Grazie per l'attenzione!

Domande?

Per informazioni aggiornate:

<http://www.cypherpunks.ca/otr/>

La presentazione (e il sorgente \LaTeX) è disponibile via web:

<http://bodrato.it/presentazioni/#LD2007>,

Rilasciata con licenza Creative Commons BY-NC-SA.

