

Verba volant scripta manent.

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

Marco Bodrato

Linux Day - Pisa - 27 ottobre 2007

- 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

# 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. . .

## 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.

Qui serve la crittografia *Off-the-Record*, "immune alla registrazione".

# Canali sicuri

https://...o SSL

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 o SSL per leggere/spedire posta o per partecipare a chat. Sono protocolli adeguati?

## Per la posta elettronica...

Per usare in modo sicuro la posta elettronica conviene crearsi una chiave GPG. Ed imparare 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...

Per usare in modo sicuro la posta elettronica conviene crearsi una chiave GPG. Ed imparare 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?

**Questo significa firmare ogni messaggio**

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

Bisogna inventarsi qualcosa d'altro...

# Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

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

# Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

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

# Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

- 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.

# Cosa ci garantisce?

Quello che ci aspettiamo da una chiacchierata privata...

- 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.
- Rinneghiabilità: i messaggi **non** contengono una firma digitale verificabile da terzi. È facile falsificare la trascrizione della conversazione.

# Programmi liberi

Per ora solo alcuni programmi per chat via rete:

- climm (ex m1CQ),
- kopete (via plug-in),
- pidgin (via plug-in).

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

## Installazione su Debian

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

# Configurazione ed uso di pidgin-otr

## La configurazione e l'uso in pochi passi...

- 1 Tools→Plugins→Off-the-Record attivate il plugin
- 2 Durante la chat a 2: il tasto "OTR" in basso inizia la sessione protetta
- 3 Mouse-destro sul tasto "OTR" →Authenticate per verificare l'identità.

Grazie

Domande?

Grazie per l'attenzione!

Domande?

Per informazioni aggiornate:  
<http://www.cypherpunks.ca/otr/>

La presentazione è disponibile via web:  
<http://bodrato.it/presentazioni/#LD2007>,  
Rilasciata con licenza Creative Commons BY-NC-SA.



## E per la posta?

È teoricamente possibile un protocollo del genere anche per la posta, ma è piú complicato. Per ora non esistono implementazioni. Tra i problemi:

- la interattività necessaria per attivare il protocollo,
- ritardo tra un messaggio e un altro.

## E per la voce?

A parte il fatto che potrebbe essere illegale cifrare la voce, e a quanto mi risulta in Italia lo è, tecnicamente è fattibile, ma...

La solita domanda:

La sicurezza data dal protocollo OTR è adeguata al caso della trasmissione vocale?

**NO!**

Come possiamo garantire la rinnegabilità della voce?  
La registrazione analogica di una frase detta col nostro accento, timbro, pronuncia, cadenza... può risultare incontestabile.

Le parole dette viaggiano in volo, incontrollabili; ciò che è scritto rimane, passibile di correzione. Ciò che è per l'uno non è per l'altro.