

# Firma digitale pratica

Enrico Cherubini  
<[kevin@bestkevin.com](mailto:kevin@bestkevin.com)>

- Presidente del Linux User Group di Verona
- Lavora per Multilink Spa/Infracom Spa come amministratore dei server di produzione linux based
- E' libero professionista con la propria società InfoSysNet Snc

# Firma digitale pratica

Obiettivi: In questa presentazione non ci occuperemo degli aspetti matematici ma esclusivamente di quelli pratici legati all'uso della firma digitale per email e documenti elettronici

# Firma digitale pratica

Le comunicazione sicura agli albori

- Il problema del riconoscimento
  - scambio di una parola chiave face to face da tenere segreta
  - telex cifrati con chiave via snail mail di verifica.

# Firma digitale pratica

La soluzione: la chiave asimmetrica

- Cos'è la chiave asimmetrica
- Perché si usa (autenticità, integrità, non ripudiabilità)

# Firma digitale pratica

## Come funziona

➤ Alice e Bob si creano le loro accoppiate di chiavi pubbliche e private: rendono le pubbliche liberamente disponibili e tengono riservate la private.

# Firma digitale pratica

[integrita'] Alice vuole mandare un messaggio a Bob, ed essere sicura che nessuno lo possa leggere: dopo avere scritto il messaggio lo cifra con la chiave pubblica di Bob.

Bob riceve il messaggio ed usa la propria chiave privata per decifrarlo. Chiunque poteva creare un messaggio e spoofando ad esempio il mittente della mail, inviarla a nome di Alice a Bob. Lo scopo pero' era quello di impedire che qualcuno potesse alterare il messaggio inviato e cio' e' garantito dal fatto che solo Bob lo puo' decifrare.

# Firma digitale pratica

[autenticita'] Alice vuole mandare un messaggio a Bob e fare in modo che sia chiaro che sia stata lei ad averlo inviato: dopo avere scritto il messaggio lo firma con la propria chiave privata.

Bob riceve il messaggio e lo puo' aprire con la chiave pubblica di Alice. Essendo la chiave a disposizione di tutti, chiunque lo puo' aprire, ma lo scopo era solo quello di rendere chiaro il mittente.

# Firma digitale pratica

[autenticita'+integrita' == non ripudiabilita']  
Alice vuole mandare un messaggio a Bob ed essere contemporaneamente sicura che sia garantita la provenienza e che il suo contenuto non sia alterato durante la trasmissione: dopo avere scritto il messaggio lo firma con la propria chiave privata e poi con la chiave pubblica di Bob.

Bob riceve il messaggio, lo decifra con la propria chiave privata e controlla che il mittente sia Alice verificandolo con la sua chiave pubblica.

# Firma digitale pratica

Perche' non ripudiabilita' ? Perche' il messaggio ha un autore certo garantito dalla firma digitale, e la certezza che esso non sia stato modificato nel tragitto comporta che il contenuto sia attribuibile con altrettanta certezza proprio al firmatario

# Firma digitale pratica

Ma chi garantisce chi ? fino a questo punto abbiamo parlato di firmare, cifrare senza dire con cosa, con quali strumenti. Quello che abbiamo raggiunto si poteva ottenere con GPG ma c'e' il problema del riconoscimento dell'appartenenza della chiave pubblica all'effettiva persona che l'ha emessa (gpg-party, face to face meeting, etc...). Pur usando la chiave asimmetrica non abbiamo risolto i problemi iniziali.

# Firma digitale pratica

Importanza della Certification Authority (CA)

Supponiamo che Charlie voglia impersonare Bob e inviare messaggi ad Alice. Per prima cosa invia ad Alice un messaggio con la sua chiave pubblica che ha emesso a nome di Bob (self signed signature). D'ora in poi i messaggi che Charlie invierà ad Alice verranno ritenuti provenienti da Bob (signature spoofing)

# Firma digitale pratica

Supponiamo che Charlie riesca a intercettare lo scambio delle chiavi tra Alice e Bob, e mandi ad entrambi la propria chiave pubblica. In questo modo potrà aprire tutti i messaggi che Alice e Bob si invieranno, leggerli e/o modificarli e reinviarne una copia al destinatario originale: man in the middle attack

# Firma digitale pratica

La CA garantisce, tramite la sua firma digitale apposta a quelle di Alice e Bob, che esse siano realmente le loro, e lo fa, ad esempio, raccogliendo dati documentali. Charlie non può avere un documento che certifichi che lui è Bob quindi le sue firme saranno riconosciute come untrusted e quindi, volendo, rifiutate. In questo scenario, Bob può non conoscere personalmente Alice, né mai incontrarla, e nonostante questo essere sicuro di parlare con lei. Nel web: [www.sitobancario.it](http://www.sitobancario.it) noi siamo sicuri che sia effettivamente la banca grazie al certificato che contraddistingue il sito.

# Firma digitale pratica

Un'accoppiata firma digitale CA + firma digitale personale compongono un certificato digitale. Il certificato ha altri campi quali la scadenza, dati personali del possessore, campo di validita' etc.

# Firma digitale pratica

Chi certifica la CA ? La CA emettrice di un certificato e' come lo stato che emetta un documento: gli si deve credere. In realta' i grossi produttori di software (web browser, email, etc...) dichiarano "trusted" un elenco di societa' emettitrici.

# Firma digitale pratica

La Certificate Revocation List e' lo strumento con cui la CA, per propria iniziativa (scadenza contrattuale) o su richiesta del cliente (a causa ad esempio dello smarrimento o compromissione della chiave privata), invalida il certificato del cliente, in questo modo anche l'uso da parte di terzi del certificato verra' reso inutile.

I software possono connettersi ai server della CA per verificare di volta in volta la CRL

# Firma digitale pratica

L'insieme della CA, dei certificati, delle revocation list, formano la Public Key Infrastructure (PKI), X.509 e' lo standard che identifica le CA.

# Firma digitale pratica

L'ultimo baluardo: una password

Cio' che si frappone tra la compromissione del sistema informatico su cui e' depositato il vostro certificato ed il suo uso indebito e' una password. La prima cosa da fare quindi e' usare una password forte, la seconda, ancora piu' importante, e' usare sistemi operativi che limitino al massimo la possibilita' di compromissione.

# Firma digitale pratica

...ed ora passiamo ad aspetti piu' pratici con degli esempi d'uso...

# Firma digitale pratica

Domande ?!?

# Firma digitale pratica

Grazie ed arrivederci a presto.

Queste slide sono distribuite sotto licenza creative  
common Attribution-ShareAlike:  
<http://creativecommons.org/licenses/by-sa/2.0/it>