

# Italian Cyberspace Law Conference

Bologna, 21 novembre 2003

## Hacking della firma digitale e attacco ai contenuti delle smartcards. Alcune casistiche.



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

**Relatore: Igor Falcomatà - [igor@infosec.it](mailto:igor@infosec.it)**



Hacking della firma digitale e attacco ai contenuti delle smartcards. Alcune casistiche

Italian Cyberspace Law Conference – Bologna, 22 novembre 2003 - © 2003 Igor Falcomatà, tutti i diritti riservati

# Hacking della firma digitale e attacco ai contenuti delle smartcards. Alcune casistiche

**audience: livello tecnico medio-basso**

**requisiti: conoscenza del meccanismo di firma digitale**

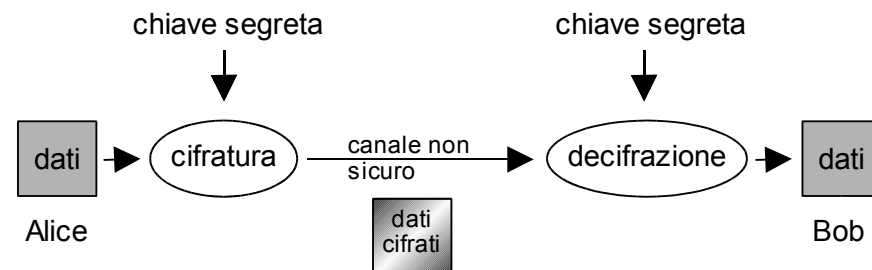
- **in questa presentazione analizzeremo le principali problematiche di sicurezza legate alla firma digitale ed al suo utilizzo**
- **anche utilizzando supporti "sicuri" (smartcard & co) per la firma "forte"**
- **con l'obiettivo di fornire una panoramica, sfatare alcuni miti ed elencare alcune risorse utili per approfondimenti**
- **si presuppone una conoscenza dei principi alla base del meccanismo di firma digitale**

# Ragioni della crittografia

- **confidenzialità**  
il messaggio può essere interpretato solamente dal mittente e dal destinatario (o anche solamente dal destinatario)
- **integrità**  
il messaggio non è stato alterato; quanto ricevuto corrisponde a quanto inviato
- **autenticazione**  
il ricevente e/o il mittente possono essere identificati con certezza
- **non ripudiabilità**  
il mittente non deve poter negare di aver trasmesso il messaggio (ed eventualmente il destinatario di averlo ricevuto)

# Crittografia a chiave segreta

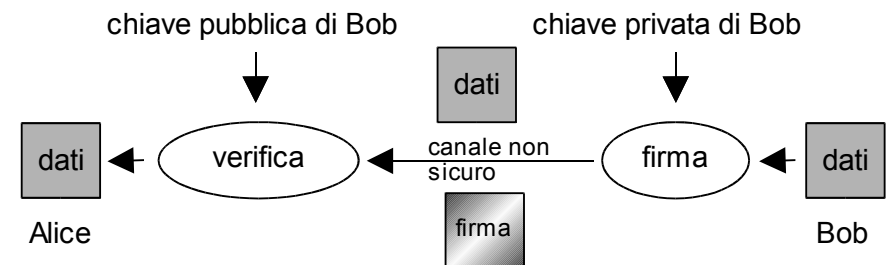
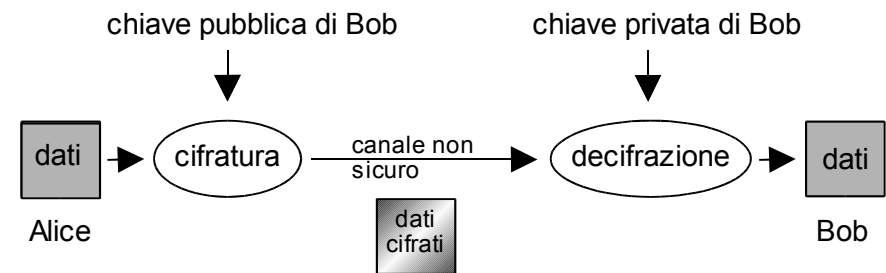
- gli algoritmi a chiave segreta (secret-key algorithms) utilizzano una chiave uguale sia per la cifratura che per la decifrazione; questi algoritmi sono detti anche "single-key" o "one-key"; vengono anche chiamati "algoritmi simmetrici"
- la sicurezza dei dati cifrati dipende principalmente dalla chiave; chiunque sia in possesso della chiave o sia in grado di ricavarla, può leggere i dati cifrati
- sono considerati molto sicuri anche con chiavi di lunghezza limitata (128 bit, etc.)
- sono molto veloci (fino a 1000 volte più veloci degli algoritmi a chiave pubblica)
- è molto difficile gestire la distribuzione delle chiavi; per esempio attraverso canali non sicuri oppure quando i soggetti coinvolti nella transazione non si conoscano o non siano fidati;
- è praticamente impossibile utilizzare metodi veloci di autenticazione o di verifica dell'integrità con la sola cifratura simmetrica
- spesso si usano algoritmi a chiave pubblica per le autenticazioni e per scambiare le chiavi che verranno poi utilizzate con algoritmi simmetrici



# Crittografia a chiave pubblica

- gli algoritmi a chiave pubblica (public-key algorithms, detti anche a chiave pubblica/privata), introdotti a metà degli anni 70, hanno rivoluzionato i concetti della crittografia; vengono anche chiamati "algoritmi asimmetrici"
- utilizzano una coppia di chiavi, correlate da una relazione matematica; una chiave pubblica, da distribuire liberamente, ed una chiave privata, da mantenere segreta
- è possibile, utilizzando la chiave pubblica di qualcuno, cifrare dei dati in modo che egli solamente possa decifrarli con la propria chiave privata
- è possibile utilizzando la propria chiave privata, "firmare" dei dati in maniera che chiunque possa verificarne l'autenticità

- la segretezza dipende principalmente dalla chiave privata, possedendo la chiave privata di qualcun'altro, è possibile impersonarlo e/o decifrare dati diretti a lui



# Obiettivi degli attacchi al meccanismo di firma:

- "rottura" degli algoritmi crittografici**
- accesso/modifica contenuto smartcard**
- debolezze delle PKI**
- sovversione del procedimento di firma e/o verifica**
- compromissione delle stazioni degli utenti**
  
- falsificazione dell'identità dei soggetti coinvolti**
  - mittente, destinatario, terze parti**
  
- falsificazione o modifica di dati firmati digitalmente**
  - documenti, atti, archivi, e-mail, flussi, login & auth**

## in pratica...

***[..] infatti la falsificazione di una firma autografa è quasi sempre verificabile con una perizia calligrafica, mentre una firma digitale è sempre "vera". [..]\****

FAQ: Domande e risposte sulla firma digitale, di Manlio Cammarata e Enrico Maccarone  
<http://www.interlex.it/docdigit/faq/faq42.htm>

- emettere documenti a nome di qualcun altro
- fornire false credenziali di identificazione
- alterare/invalidare documenti, timestamps

\* qualora la chiave privata utilizzata per emettere la firma digitale contraffatta sia la stessa utilizzata per firmare i documenti legittimi

# "rottura" degli algoritmi crittografici [1/2]

**attacco tramite tecniche di crittoanalisi agli algoritmi ed alle chiavi utilizzate per proteggere i dati**

- **forzatura delle chiavi di sessione (crittografia simmetrica)**
- **forzatura delle chiavi private (crittografia a chiave pubblica)**
- **sovversione degli algoritmi di hash crittografico**

# "rottura" degli algoritmi crittografici [2/2]

in passato è stata dimostrata la debolezza di sistemi che utilizzino una lunghezza di chiavi non adeguata  
gli algoritmi e le chiavi adottate per la firma "forte" sono considerati pubblicamente "sicuri" (qualora correttamente implementati)

- questi attacchi richiedono elevate conoscenze crittografiche e notevoli risorse hardware
- non sono alla portata "dell'uomo della strada" e generalmente "sono molto costosi"
- nella crittografia vengono generalmente utilizzati algoritmi che siano pubblicamente considerati "sicuri"

spesso esistono metodi più vantaggiosi (tempo, risorse, denaro, ..)

# accesso/modifica contenuto smartcard [1/4]

uno dei punti più deboli della crittografia a chiave pubblica (e quindi del meccanismo di firma digitale) è la confidenzialità della chiave privata

- per evitare che la chiave privata possa essere "rubata" facilmente, la firma digitale "forte" prevede:

*1. La generazione della coppia di chiavi deve essere effettuata mediante apparati e procedure che assicurino, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.*

Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999

Art. 5 - Generazione delle chiavi

<http://www.interlex.it/testi/regtecn.htm#5>

# accesso/modifica contenuto smartcard [2/4]

per ovviare a questa debolezza si utilizzano dei supporti "hardware" (smartcard, token USB) dotati di microchip

- questi dispositivi effettuano autonomamente le operazioni di crittografia a chiave pubblica
- sono previsti meccanismi di protezione dalla modifica hardware ("tamper proof")
- sono previsti meccanismi di protezione della chiave privata: la chiave privata non lascia mai la smart card, né sono disponibili funzioni per estrarla



# accesso/modifica contenuto smartcard [3/4]

esistono (e sono ben documentate) numerose metodologie di attacco "fisico" o "logico" alle smart-card

- **attacchi invasivi**  
**con sottrazione della stessa e distruzione**
- **attacchi non invasivi**  
**senza sottrazione (o con restituzione dopo il furto)**

**l'accesso alla chiave privata potrebbe non essere l'unico obiettivo...  
pensiamo ad un sistema di moneta digitale dove i dati relativi al  
credito siano contenuti nel supporto...**

Introduzione alle tipologie di attacco (ita):

Smart Card (Java Card), Francesca Fiorenza

<http://www.blackhats.it/it/eventi/24012002/smartcard.pdf>

Panoramica e riferimenti (eng):

SMART CARD CONTENT SECURITY, Stefano Zanero

<http://www.elet.polimi.it/upload/zanero/papers/scsecurity.pdf>

# accesso/modifica contenuto smartcard [4/4]

**nell'utilizzare queste metodologie, l'attaccante valuterà l'impegno necessario in relazione ai risultati:**

**un conto è forzare un meccanismo di sicurezza di una pay-tv o di un sistema di digital cash,  
un altro è firmare documenti a nome del dott. Rossi.**

- questo attacchi richiedono elevate conoscenze crittografiche e dell'hardware**
- richiedono anche risorse e laboratori attrezzati**
- non sono alla portata "dell'uomo della strada" e generalmente "sono piuttosto costosi"**

**spesso esistono metodi più vantaggiosi (tempo, risorse, denaro, ..)**

# debolezze delle PKI (Public Key Infrastructure)

una terza parte "fidata" (Certification Authority) emette un certificato digitale (firmato) che garantisce la corrispondenza tra una certa chiave pubblica ed un certo soggetto, nonché definisce gli utilizzi e gli attributi

- debolezze nel processo di verifica dell'identità legato alla emissione del certificato
- compromissione della sicurezza delle chiavi private della CA e/o della sua struttura informatica
- lentezze nel processo di emissione delle revoche (CRL)
- timestamp (marca temporale)
- queste problematiche sono affrontate e regolamentate nella normativa italiana inerente la firma digitale "forte"

Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure, C. Ellison and B. Schneier  
<http://www.schneier.com/paper-pki.html>

# Quando a rischio non e' la smart-card (ma quello che ci sta intorno)

assumiamo che le smartcard, i relativi lettori, nonché le infrastrutture di PKI dei certificatori ed i loro sistemi informativi non siano attaccabili praticamente con i metodi visti fin qui...

- rimangono sempre da valutare gli anelli deboli della catena:
  - gli utenti  
buonafede, mancata conoscenza dei meccanismi alla base della firma digitale, scarse competenze informatiche in genere, ..
  - le loro stazioni  
scarse procedure di sicurezza, carenza di hardening, utilizzo di privilegi elevati, vulnerabilità, ..
  - i software di firma  
sovversione delle procedure di firma e di verifica, ..

# debolezze nella verifica dei documenti e dell'identità dei soggetti coinvolti

la sicurezza del meccanismo di firma digitale non è legato solamente alla sicurezza dei certificatori e della loro struttura di PKI

- **sovversione delle chiavi pubbliche utilizzate per la verifica (sulla stazione dell'utente)**
  - **chiavi di CA che non risiedono sul supporto "sicuro"**
  - **sovversione dell'ordine di verifica**
- **mancata verifica della validità del certificato (CRL)**
  - **mancanza di collegamento ad Internet**
  - **Denial of Service**
- **cattiva implementazione dei software di verifica**
- **sovversione del processo di verifica**
  - **sostituzione del software di verifica con una versione contraffatta**

# implementazione dei software di firma: un esempio concreto

**From: Stefano Zanero <s.zanero@securenetwork.it>**

**Subject: Sconfinati CAMPI di Cavoli Amari**

**Date: Fri, 6 Sep 2002 15:11:15 +0200**

**<http://www.sikurezza.org/ml/msg05957.html>**

Tra i "banchi" delle norme e quelli dei programmi, Manlio Cammarata,  
<http://www.interlex.it/docdigit/banchi.htm>

- **cosa succede se il software visualizza sul video dell'utente un contenuto che possa variare dinamicamente in base al contenuto di certe "macro" o campi variabili?**
  - **senza avvertire l'utente della presenza di questi campi**
  - **senza nemmeno avvertirlo della potenziale pericolosità di certi formati**

**l'utente firma il documento basandosi su quando visualizza a video, ma alla successiva verifica il contenuto potrebbe essere diverso!**

# implementazione dei software di verifica: un altro esempio concreto

From: "Hotmail" <buubby<at>hotmail.com>

Subject: Sconfinati CAMPI di CAVOLI AMARI 2- LA VENDETTA

Date: Thu, 20 Feb 2003 17:25:52 +0100TA

[http://www.sikurezza.org/ml/02\\_03/msg00159.html](http://www.sikurezza.org/ml/02_03/msg00159.html)

Una notizia ai limiti dell'incredibile, Manlio Cammarata,  
<http://www.interlex.it/docdigit/bachi10.htm>, 2003, Interlex

- **cosa succede se il software importa, direttamente dal documento inviato per essere verificato, il certificato "root" di una Certification Authority fittizia?**
  - **senza chiederne conferma esplicita all'utente**
  - **senza nemmeno visualizzarlo in modo evidente**

**tutti i documenti firmati con certificati emessi da quella  
CA saranno visualizzati come correttamente verificati!**

# altri attacchi dell'uomo della strada: furto/sottrazione della smartcard

**chiunque possa utilizzare la smartcard e conosca il PIN del dott. Rossi  
può emettere documenti firmati digitalmente e con firma valida**

- **smartcard (personali) affidate ad altri  
segretaria, commercialista, ...**
- **smartcard incustodite  
possibile sottrazione (anche temporanea)**

**come può essere sottratto il PIN?  
fogliettini, magari custoditi insieme alla smartcard  
durante la digitazione  
attraverso software o hardware di "snooping"**

# compromissione delle stazioni degli utenti

**Providing Authentication to Messages Signed with a Smart Card in Hostile Environments**  
**Tage Stabell-Kulo, Ronny Arild, and Per Harald Myrvang, University of Tromsø**  
<http://www.usenix.org/publications/library/proceedings/smartcard99/stabell.html>

[..]

- The problem is that there is no authenticated ``channel'' from the card to the user. The card is unable to ``tell'' P what it is about to sign, and P can not verify that X has been received for signing [1]. The problem is well known [4,14]. Authenticated channels can be obtained by means of, for example, more powerful hardware, such as contemporary PDAs. With this type of hardware, integrity is obtained since the PDAs have a (small) display on which X can be shown. However, smart cards are prevalent and we seek a solution using this technology.

[..]

1. M. Abadi, M. Burrows, C. Kaufman, and B. Lampson.  
Authentication and delegation with smart-cards.  
Science of Computer Programming, 21(2):93-113, October 1993.
4. H. Gobiuff, S. Smith, J. D. Tygar, and B. Yee.  
Smart Cards in Hostile Environments.  
In Proceedings of the Second USENIX Workshop on Electronic Commerce, Oakland, CA, November 1996.
14. B. Yee and D. Tygar.  
Secure Coprocessors in Electronic Commerce Applications.  
In Proceedings of The First USENIX Workshop on Electronic Commerce, New York, New York, July 1995.

# il gioco delle tre carte

**vedi quello che vuoi firmare...**

**firmi (anche) quello che vuole l'attaccante**

- **anche utilizzano smartcard o token (la chiave privata non e' fisicamente estraibile dal supporto)**
- **un attaccante che prendesse il controllo della stazione potrebbe (facilmente) sovvertire il processo di firma**
- **intromettendosi nel meccanismo qualora l'utente voglia firmare un documento**
  - **visualizzando un certo contenuto e firmando qualsiasi altra cosa a suo piacimento**
- **eventualmente catturando anche il pin di accesso alla chiave, per riutilizzarlo (qualora la smartcard/token sia inserita) quando piu' gli aggrada**

# attacchi alle stazioni dell'utente: un esempio concreto

## Firma digitale: un attacco simulato rileva alcune debolezze del sistema

PuntoSicuro, [http://www.puntosicuro.it/language,1/page,1.php/articolo\\_3092/](http://www.puntosicuro.it/language,1/page,1.php/articolo_3092/)

- procedura sviluppata dal DICO, gruppo sicurezza, Università di Milano (<http://dico.unimi.it>)
- attraverso un worm mirato ad attaccare la stazione dell'utente
- sviluppato per colpire uno specifico prodotto di firma ma potrebbe essere "puntato" verso altri prodotti
- permette di sovvertire i procedimenti di firma e produrre "documenti falsi con firma vera"
- non è ancora pubblicamente disponibile il "proof of concept" [sarà rilasciato a breve]
- un attaccante con un sufficiente bagaglio tecnico e pochissime risorse (un lettore di smartcard, il software da attaccare ed un computer) potrebbe replicarlo

# gli attacchi alle stazioni degli utenti sono un pericolo reale/concreto al meccanismo di firma?

**la risposta è indubbiamente sì**

- **le stazioni "client" vengono generalmente meno "mantenute" dei server (che a loro volta sono spesso attaccati con successo)**
- **i sistemi operativi "client" sono insecure by default**
- **vengono scoperte (e spesso rese pubbliche) continuamente nuove tipologie di attacco e vulnerabilità**
- **continuamente = quotidianamente**
- **le stazioni utilizzate per la firma vengono spesso utilizzate (anche) per attività potenzialmente "pericolose"**  
**accesso ad Internet, lettura della posta, esecuzione di applicazioni slegate dalle procedure di firma**
- **spesso con privilegi elevati (amministratore della macchina)**

# perché indubbiamente sì?

(con tutti i sistemi operativi attualmente utilizzati)

- l'amministratore del sistema ha il controllo completo di tutto quello che transita (memoria, schermo, file, connessioni, periferiche, etc.)
- la smartcard impedisce che possa comunque accedere alla chiave privata
- la smartcard **NON** impedisce che l'amministratore possa far visualizzare sul monitor un certo documento ed inviare alla smartcard un **ALTRO** documento
- la smartcard non ha "strumenti" per comunicare cosa sta firmando all'utente
- non ha neanche strumenti per comunicare che sta firmando qualcosa...
- e se amministratore = attaccante?

# come affrontare le problematiche? conoscere i limiti della tecnologia

- utilizzare per la firma digitale "forte" stazioni dedicate, possibilmente separate dal resto della rete
- o prevedere quantomeno procedure di messa in sicurezza, corretta manutenzione e monitoraggio
- utilizzare sistemi operativi che garantiscano un livello di sicurezza sufficiente\*
- utilizzare software di firma e verifica che garantiscano un livello di sicurezza sufficiente\*
- il "buon senso" informatico in ottica di sicurezza ("best practices")
- preservare dal furto le smart card ed i pin
- utilizzare formati di documento non modificabili

\* stabilire livello di sicurezza sufficiente non è banale

Relatore: Igor Falcomatà - [igor@infosec.it](mailto:igor@infosec.it)

a breve potrete scaricare queste slide:

<http://www.infosec.it/risorse.html>

# Domande?

## Altri riferimenti utili:

- Interlex, sezione dedicata:  
<http://www.interlex.it/docdigit/indice.htm>
- Sito Avv. Andrea Monti, sezione dedicata  
<http://www.ictlaw.net/internal.php?sez=art&IdT=3&IdTA=14&IdA=75&lang=1>

<http://www.sikurezza.org> - Italian Security Mailing List  
</free advertising>

