Fiducia e consapevolezza: riflessioni sull'utilizzo delle tecnologie per la sicurezza

Marco Prandini
DEIS – Università di Bologna

Seminario per il corso di Tecnologie per la Sicurezza LS
Facoltà di Ingegneria – Università di Bologna
6 marzo 2006

Il problema della fiducia

- Cosa differenzia i sistemi che utilizziamo per gestire dati sensibili dagli altri?
  - Le conseguenze nel caso non facciano quel che desideriamo
- Cosa differenzia i sistemi informatici da quelli “tradizionali”?
  - Non siamo in grado di verificare di persona il loro operato

Quando le cose non sono come sembrano

- Funzionalità nascoste:
  parlare troppo senza accorgersene
- La firma digitale:
  una catena con molti anelli
- Phishing:
  errori di rotta navigando sul WWW

Dati che passano inosservati

- Metadati
  - Word
  - PDF
- Canali Esotici:
  - keysniffing audio
  - keylogging hardware

Firma digitale

- Caratteristiche desiderabili
  - Autenticità
  - Integrità
  - ***Non ripudio***
- Requisiti necessari ad ottenerle
  - Protezione della "identità digitale"
    - Dispositivo di firma sicuro (smart card)
  - Volontà di firmare
  - Consapevolezza di ciò che si firma

L'onere della prova

- Nel caso siano rispettate tutti i requisiti la FD sembra "migliore" della firma autografa, cioè impossibile da contraffare
- Una firma digitale contraffatta non è distinguibile in alcun modo da una autentica

Pare ragionevole che l'onere della prova ricada sul firmatario (firma non ripudiabile), che ha gli strumenti tecnici per difendersi dai falsari, e non sul verificatore, che al contrario non può provare se vi sia stato un uso fraudolento dei dispositivi di firma...

Il problema dell'interfaccia

... ma è davvero così semplice difendere il proprio dispositivo di firma?

1) prendo visione del documento (consapevolezza)

2) inserisco il PIN (volontà)

3) la chiave privata viene utilizzata per firmare (identità)

Il problema dell'interfaccia

... ma è davvero così semplice difendere il proprio dispositivo di firma?

1) prendo visione del documento consapevolezza???

2) inserisco il PIN (volontà)

3) la chiave privata viene utilizzata per firmare (identità)

Per firmare... COSA?

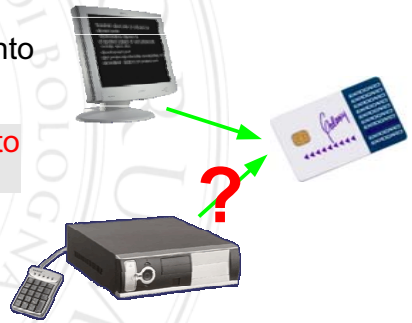
Il problema dell'interfaccia

... ma è davvero così semplice difendere il proprio dispositivo di firma?

1) prendo visione del documento (consapevolezza)

2) Il PIN può essere intercettato volontà???

3) la chiave privata viene utilizzata per firmare (identità)



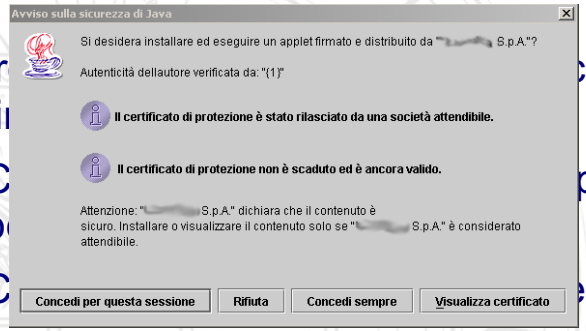
E quando non guardo ?

Il problema dell'interfaccia

Il problema della reale certezza di ciò che si firma rimane irrisolto

- Chi garantisce che il SW si “comporti bene”?
- Chi verifica che non sia stato alterato?
- Chi è in grado di comprendere le domande poste all'utente da molti sistemi al sorgere di potenziali problemi di ***fiducia***, e di apprezzare pienamente le conseguenze della propria risposta?

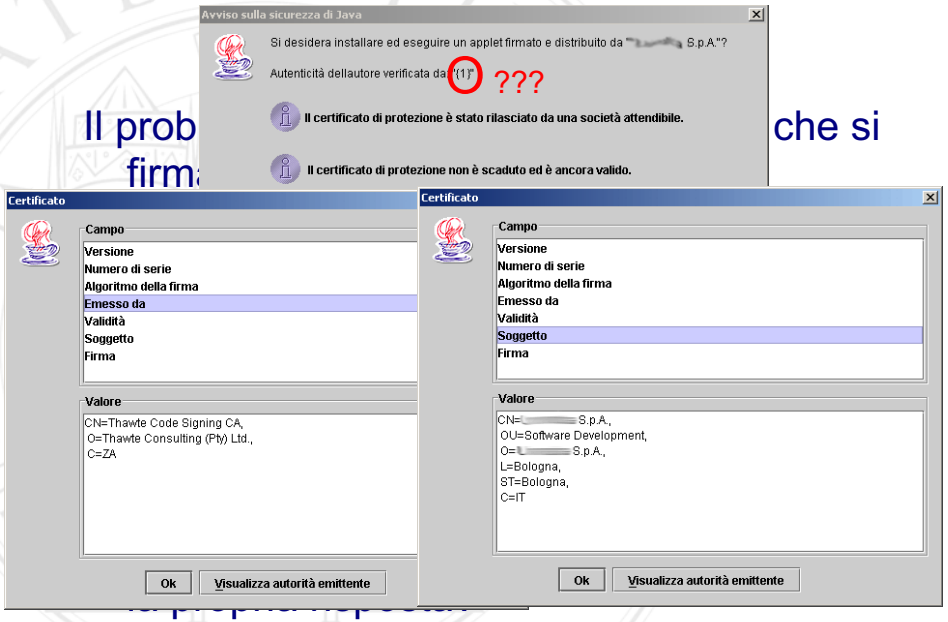
Il problema dell'interfaccia



Il pr… …ciò che si fi…

- C… …porti b…
- C… …erato?
- Chi è in grado di comprendere le domande poste all'utente da molti sistemi al sorgere di potenziali problemi di ***fiducia***, e di apprezzare pienamente le conseguenze del-la propria risposta?

Il problema dell'interfaccia



Il prob… …che si firm…

Dall'altro lato

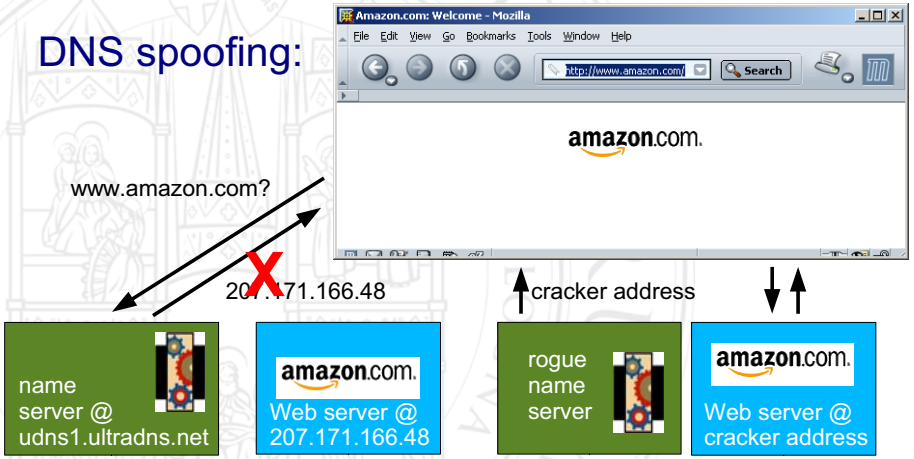
Problemi analoghi si possono riscontrare anche quando il nostro interesse è verificare l'identità altrui anziché attestare la nostra.

Esempi:

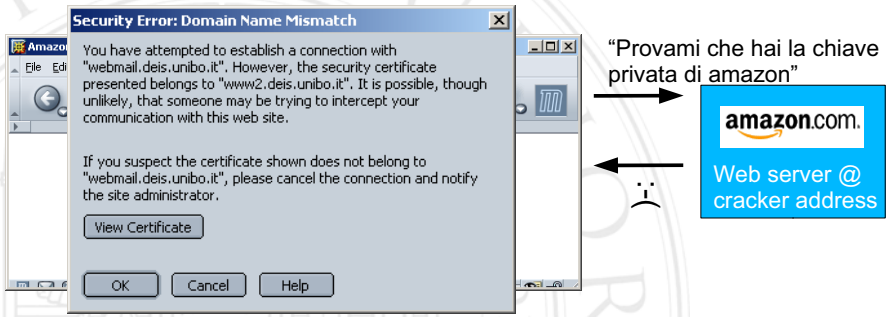
- URL spoofing
- DNS spoofing
- Certificati per HTTPS

HTTP senza autenticazione

DNS spoofing:



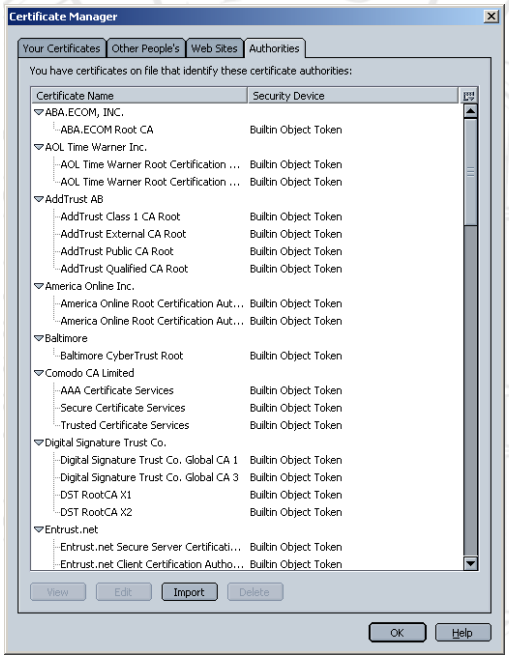
HTTPS: autenticazione del server



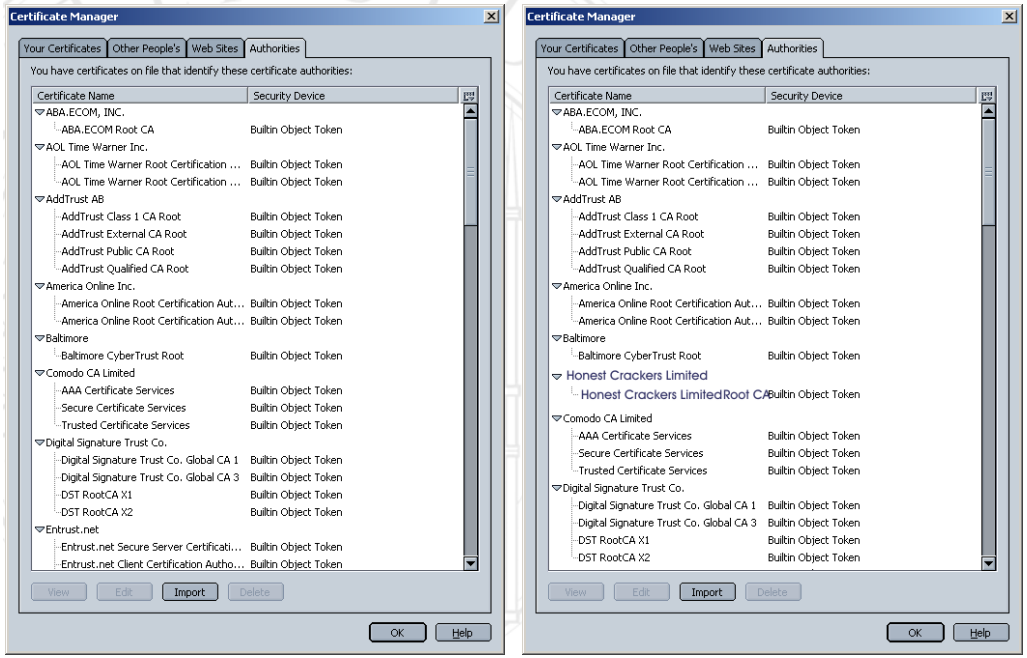
Come fa il browser a verificare la prova fornita dal web server?

- Certificate store
- Trusted CAs

Certificate store



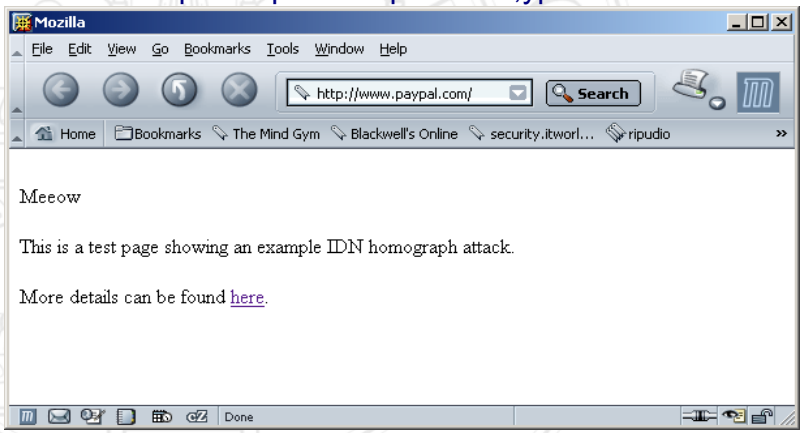
Certificate store



Ma anche più semplicemente...

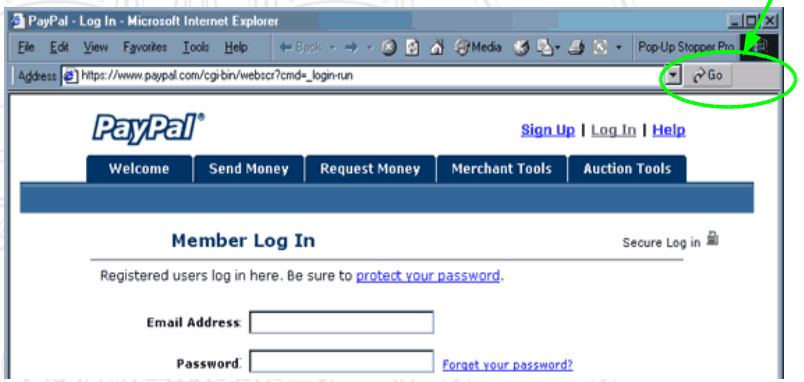
RFC3490/1/2: International Domain Names

ad esempio: http://www.pаypal.com/



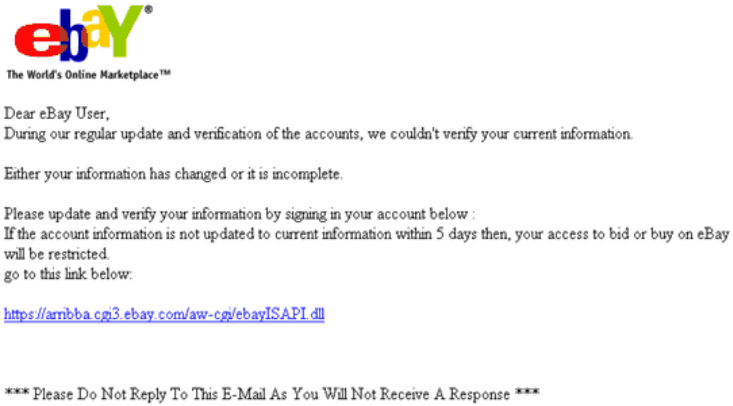
Ma anche più semplicemente...

Qualche riga di codice js o activeX

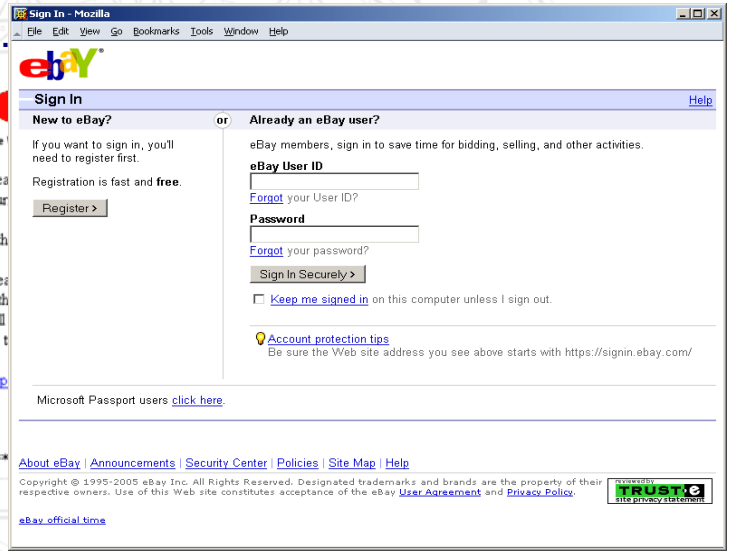


Ma anche più semplicemente...

... senza nemmeno intervenire sul DNS



Ma anche più semplicemente...



Ma anche più semplicemente...

IE tech support:
"The most effective step that you can take to help protect yourself from malicious hyperlinks is not to click them. !!! (nda)
Rather, type the URL of your intended destination in the address bar yourself. By manually typing the URL in the address bar, you can verify the information that Internet Explorer uses to access the destination Web site."

Problematiche di realizzazione dei sistemi sicuri

Qualche statistica

- Circa 4000 nuove vulnerabilità ogni anno dal 2002 al 2004, quasi 6000 nel 2005
- Crescita esponenziale degli incidenti denunciati (quasi 140.000 nel 2003)
  - La comparsa di strumenti automatici richiede metodi di conteggio più intelligenti
  - Gli incidenti denunciati sono una frazione del totale

Carnegie Mellon Software Engineering Institute CERT Coordination Center

Qualche statistica

- Provenienza degli attacchi
  - 81% esterni
  - 37% interni
- Tipologia di attacco
  - Più comune: Virus, worm e trojan horses (64% del totale)
  - Più dannosa economicamente: DDoS (50% dei costi totali per incidenti)
- Costo medio: 150k$
  - Fortemente dipendente dal tipo di attacco

Vulnerabilità - origini

- Codice di scarsa qualità
  - "Remotely exploitable buffer overflow vulnerabilities continue to be the number one issue that affects Windows services."
- Reazioni inadeguate dei produttori
  - "In many cases, the vulnerabilities were 0-days i.e. no patch was available at the time the vulnerabilities were publicly disclosed."

Vulnerabilità - origini

- Attacchi data-driven/cross-platform
  - Cross-site scripting
  - Condivisione e backup di file
  - DNS
  - Database
  - Media players

La componente umana

- La fase progettuale
  - Non esistono metodi formali che consentano una verifica completa delle caratteristiche di sicurezza di un sistema
  - Purtroppo la pigrizia dei progettisti tipicamente va ben oltre
    - Buffer overflow
    - WEP

La componente umana

- Dei lavoratori intervistati da ICM Research
  - Il 21% lascia usare il portatile o il PC aziendale ad amici e parenti
  - Il 51% vi collega i propri dispositivi
  - Il 60% vi memorizza dati privati
  - Il 62% ammette di non avere alcuna nozione di sicurezza informatica
  - Il 10% ammette di utilizzarlo per scaricare contenuti pur sapendoli esplicitamente proibiti
  - Il 5% ammette di accedere ad aree del SI teoricamente precluse

La componente umana

- Esigenze contrastanti: più sicurezza o più funzionalità?
  - WiFi: fin troppo semplice connettersi
  - RFID: semplice come usare un cellulare
  - Bluetooth: 4 cifre per guidare sicuri

Esigenze contrastanti

- Wireless: così vicino, così lontano

802.11, 125 miglia senza ampli
(DEFCON WiFI Shootout 2005
Team iFiber Redwire)

BT, 1 miglio
(John Hering, Flexilis
BlueSniper Rifle)

Esigenze contrastanti

- RFID nasce per sostituire badge e barcode, ma può essere facilmente impiegato per ledere la privacy
- Problemi tecnologici
  - Solito problema del raggio di ricezione (record: 20m)
  - Varianti più comuni prive di protocolli sicuri
- Ovvio coro di promesse, però...
  - Brevetti IBM e BellSouth per tracciare i consumatori
  - Applicazioni “cuneo” per installare lettori in casa
  - Progetti governativi: Sorting Door

Tunnel vision

- Implementazione di tecnologie innovative senza valutazione dell'impatto complessivo
  - Biometria, o come sventare un furto d'auto e provocare mutilazioni e rapimenti
  - Libertà senza fili, o come rendersi visibili anche chiusi in un baule
  - Chip and Pin, l'anello debole cambia, la catena che si rompe è sempre quella

Politiche di configurazione

- Accesso consentito di default
  - Esempi:
    - regole dei firewall
    - assenza di segmentazione
    - signature-based IDS e antivirus
  - Eredità delle origini dei sistemi multiutente e delle reti
  - Tuttora diffusissimo per favorire l'usabilità
  - Effetti:
    - Rincorsa continua e spesso inefficace (finestra di vulnerabilità)

Politiche di individuazione e contrasto di azioni dannose

- Caso particolare dello scenario precedente: affrontare le vulnerabilità invece di consentire solo azioni fidate
- Tipico approccio degli antivirus, nonostante l'evidente inefficienza
  - Il “computer medio” viene utilizzato per eseguire poche decine di applicazioni, note all'utilizzatore
  - I virus, spyware, trojan horses in circolazione sono quasi 100.000, ed ogni giorno ne appaiono di mai visti prima

Politiche di individuazione e contrasto di azioni dannose

Un aneddoto paradossale.
Dopo tutta questa fatica per evitare infezioni...

- 31 ottobre 2005: scoperto il S*** rootkit
  - Si installa senza informare l'utente all'inserimento del CD audio nel PC
  - Consente accesso remoto completo
  - Si nasconde all'ispezione del sistema

Politiche di individuazione e contrasto di azioni dannose

- Le beffe...
  - Affermazione che il rootkit non contatta la casa: falsa
  - “La gente non sa nemmeno cos'è un RK, perché dovrebbe preoccuparsi se glie ne installiamo uno”
  - Un prodotto per difendere il copyright che contiene software copiato dalla comunità open
- ... i danni
  - Danneggia Windows se si tenta di rimuoverlo
  - Primo tool per rimuoverlo: toglie solo il cloaking
  - Seconda versione: apre una falla più grossa

Politiche di individuazione e contrasto di azioni dannose

La morale

- Una certa classe di industrie evidentemente ha una certa influenza
  - Infetta gravemente i PC del DHS ma non è perseguita
  - Per 6 mesi nessun antivirus è stato aggiornato per rilevare il RK
  - Il RK destabilizza seriamente Windows e Microsoft tace
- I sistemi di DRM saranno sempre più invasivi, sia legalmente (DMCA) che tecnologicamente: entra in scena il Trusted Computing

Politiche di individuazione e contrasto di azioni dannose

- Trusted computing: il fine dichiarato è quello di rendere più fidati i computer
- Predecessori sfortunati: il code signing
  - Firma digitale per riconoscere il codice autentico
  - Problema: la certificazione delle chiavi
  - Problema: l'autenticità del software è verificata da altro software

↓

TC: Far partire la chain of trust dall'hardware

Trusted computing

- Trusted Computing Group:

  Microsoft, Intel, IBM, HP, AMD (SUN, Sony, minori)
- Dalla FAQ di Ross Anderson:

  La funzione principale di questo sistema è di fornire una piattaforma informatica che non permetta di modificare i programmi utilizzati dall'utente.

  Le applicazioni che gireranno su questo sistema, inoltre, saranno in grado di comunicare in modo sicuro col produttore.

  L'obiettivo originale era quello di gestire il copyright per i beni digitali.

Trusted computing

- Architettura
  - Chip “Fritz”
  - Memoria separata nella CPU
  - Kernel di sicurezza “Nexus” del S.O.
  - Kernel di sicurezza in ogni applicazione
  - Server on-line gestiti dai produttori SW

Trusted computing

- Motivazioni
  - Governative: garanzia di rispetto della classificazione dei documenti
  - Economiche: licenze software e DRM (multimedia = killer app per produttori HW e SW)
- Rischi
  - Censura dei contenuti
  - Lock-in

Trusted computing

- Tutele: TC Best Practices
  - Conformità alle legislazioni sulla privacy
  - Assenza di ostacoli all'interoperabilità
  - Assenza di ostacoli alla portabilità dei dati
  - Scelta sull'utilizzo e sulla configurazione dei componenti TC in mano all'utente
  - Funzionamento trasparente e report accessibili
  - Facilità d'uso e comprensione del funzionamento anche da parte di utenti non tecnici

Trusted computing

- In pratica...
  - Distinzioni artificiose tra HW e SW
  - Ritardo nella diffusione del documento

Elusione in Vista?

E perché non in altri prodotti?