Convenzione Interbancaria per i Problemi dell'Automazione

(CIPA)

Convegno su "I servizi digitali"

Contributo del prof. Antonio LIOY

Politecnico di Torino

Frascati, 4 marzo 2003

I servizi digitali sono già da tempo usati all'interno delle aziende per conseguire vari benefici. La vera sfida oggigiorno è esportare questi benefici anche nei confronti degli utenti esterni e – più in generale – dei cittadini. Ciò comporta un'apertura del sistema informativo verso realtà non controllate e non controllabili e può quindi generare dei rischi.

Il Ministro Stanca ha recentemente detto che una delle caratteristiche non positive dell'adozione dell'informatica in Italia è il suo uso semplicemente come strumento per automatizzare una data attività già esistente, ma non per fare vera innovazione. A me pare che nel campo dei servizi digitali spesso ciò capiti anche per la sicurezza. Le tecnologie ed i prodotti di sicurezza vengono talvolta applicati in modo quasi automatico, senza riflettere adeguatamente su quali siano veramente i nuovi scenari e quindi i nuovi rischi a cui ci sottoponiamo. A questo proposito sono sicuramente illuminanti alcune statistiche: gennaio 2003 è stato un mese record per gli attacchi ai sistemi informatici, in un solo mese ci sono stati circa 20.000 attacchi a livello mondiale, con danni per almeno 8 miliardi di euro. Ciò non dovrebbe sorprendere: l'attacco alle Poste Italiane nei primi mesi del 2003 è stato riportato da tutti i giornali ed ha destato grande scalpore, ma negli anni passati i virus Nimda e Red Code avevano bloccato i sistemi informativi di mezzo mondo, inclusi quelli di primari istituti bancari e di istituzioni di ricerca. In precedenza, il primo grande attacco su larghissima scala è stato quello contro Yahoo, nel febbraio 2000. Sono quindi almeno tre anni che stiamo osservando questi eventi, ma non abbiamo ancora imparato veramente come comportarci per prevenire questi attacchi invece che per reagire semplicemente ad essi. Ciò è preoccupante perché chi non impara dai propri errori è condannato perpetuamente a ripeterli. Occorre quindi domandarsi perché questi servizi digitali siano così terribilmente insicuri e che cosa possiamo fare per migliorarli.

Per rispondere a questa domanda possiamo prendere spunto dall'analisi condotta da un gruppo di esperti statunitensi dopo l'attacco a Yahoo, in quanto tale analisi non è specifica del mondo USA ma applicabile ai sistemi informativi di qualunque nazione industrializzata.

Il primo punto di questa analisi rileva che le tecnologie con cui vengono condotti gli attacchi si sviluppano in un ambito open-source e quindi si evolvono rapidamente. In altre parole quando un malintenzionato vuole sviluppare un nuovo strumento di attacco non deve cominciare da zero ma ne prende uno esistente e lo migliora aggiungendogli nuove caratteristiche. Viceversa le strategie usate per difendere i sistemi informativi sono di tipo reattivo: solo dopo essere stati vittima di un attacco implementiamo le contromisure necessarie a proteggerci da questo specifico attacco.

Un tipico esempio di questo approccio è il problema dei virus: l'aggiornamento settimanale, quando non addirittura giornaliero, delle firme virali è dato per scontato da tutti gli amministratori di sistema perché bisogna saper reagire ai nuovi virus che vengono inventati quotidianamente. Questo approccio è fondamentalmente sbagliato: il sistema informativo dovrebbe essere insensibile ai virus per costruzione. Esistono infatti sistemi ed applicazioni insensibili ai virus ma dispiace rilevare quanti servizi, anche di rilevante importanza, vengano sviluppati su piattaforme attaccabili da virus e worm.

Un secondo punto dell'analisi statunitense osserva come la diffusione di Internet possa costituire un'arma a doppio taglio, specialmente quando l'accesso a Internet avviene tramite un sistema a banda larga. In questo caso gli utenti casalinghi diventano un obiettivo ghiottissimo per i malintenzionati che si inseriscono nei loro computer (tipicamente poco protetti) per usarli come teste di ponte per condurre l'attacco verso un determinato obiettivo finale. Questo è proprio quello che è capitato nell'attacco a Yahoo in cui migliaia di sistemi casalinghi a bassa sicurezza sono stati usati per condurre l'attacco all'insaputa del legittimo proprietario.

L'analisi citata rileva anche che l'esplosione dell'uso di Internet ha messo alla frusta lo scarso livello tecnico degli amministratori di sistema, il cui livello medio è decresciuto drammaticamente negli ultimi cinque anni. Se ciò è vero per gli USA credo che, a maggior ragione, sia applicabilissimo anche all'Italia. Con un po' di ironia, potremmo chiamare i nostri amministratori – tutti rigorosamente certificati – amministratori "point and click" perché hanno seguito corsi che insegnano quasi esclusivamente come svolgere un determinata attività selezionando una ben precisa sequenza di icone o menù all'interno di un'interfaccia grafica. Ma pochi di loro comprendono il funzionamento del sistema che stanno amministrando, mentre gli attaccanti comprendono benissimo il funzionamento e le debolezze degli attuali sistemi informativi. Si potrebbe obiettare che per guidare un'automobile non è necessario comprenderne il funzionamento ma io credo che i sistemi informativi non abbiano ancora raggiunto una maturità tecnologica paragonabile a quella di un autoveicolo e sia quindi indispensabile – almeno per gli amministratori di sistema – comprendere a fondo il funzionamento dei servizi che gestiscono.

Un altro problema di base legato alla sicurezza dei servizi digitali è che sono sviluppati da programmatori che scrivono software complicatissimo senza avere ricevuto alcun tipo di addestramento su come si scrive codice sicuro. Si noti che parliamo di codice sicuro, non codice di sicurezza: non è necessario che tutti i programmatori sappiano implementare la firma digitale o la crittografia dei dati, ma ogni programmatore dovrebbe sapere come evitare i "buffer overflow", i puntatori "sporchi" ed altri problemi di questo genere. Purtroppo queste cose non si insegnano nei corsi e non sono richieste nelle specifiche di progetto: l'attenzione è tutta concentrata

sull'interfaccia grafica e sulla rapidità di sviluppo; non dobbiamo quindi poi stupirci se i servizi che ne risultano sono facilmente attaccabili.

Il governo statunitense è rimasto profondamente impressionato dall'attacco condotto contro Yahoo nel febbraio 2000, nonostante si trattasse di un servizio commerciale e non militare o governativo. Poiché l'infrastruttura tecnologica di Yahoo era molto sofisticata (decine di server web ed un collegamento ad Internet attraverso provider diversi, con una banda totale di più di 2 gigabit/s), l'attacco ha dimostrato un'elevata capacità di pianificazione e di conduzione dell'attività da parte degli attaccanti. A fronte di questa analisi, il governo USA ha investito e continua ad investire miliardi nella creazione di centri di eccellenza per la ricerca nel campo della sicurezza informatica. Ma in Italia sentiamo spesso dire che è inutile approfondire gli aspetti tecnologici dell'informatica perché per erogare servizi digitali è sufficiente acquistare e configurare prodotti standard: in altre parole, la tecnologia è solo uno strumento docile nelle mani dei creatori di servizi digitali. Io non credo che la tecnologia sia solo uno strumento da usare in modo cieco ed asettico. Credo piuttosto che la tecnologia debba essere uno strumento che noi comprendiamo molto bene, molto a fondo, per non correre il rischio di creare servizi sofisticati e complessi ma che sfuggono al nostro controllo. In particolare la sicurezza è proprio uno dei campi in cui limitarsi ad usare la tecnologia senza comprenderla può originare rischi inaccettabili. A questo proposito, non si può fare a meno di evidenziare che i sistemisti ed i programmatori adibiti a queste attività sono pochi e poco (e male) addestrati rispetto alla complessità del compito, con poco tempo da dedicare alla comprensione approfondita del sistema e dei suoi problemi. In altre parole, spesso siamo noi stessi i nostri peggiori nemici, perché non poniamo abbastanza cura in quello che facciamo. Frequentemente i sistemi informativi sono sovradimensionati perché – non comprendendone appieno il funzionamento – aggiungiamo risorse (ad esempio, memoria o una CPU più veloce) nel tentativo di mitigare l'effetto dei problemi o ritardarne la comparsa. Ma ciò significa aver rinunciato a governare il sistema informativo, significa subire il *technology push*, significa contraddire una delle leggi fondamentali dell'ingegneria: "ogni sistema non deve essere più complesso del necessario". Più acceleriamo l'innovazione tecnologica come mera acquisizione di hardware o di software e meno comprendiamo e controlliamo il sistema risultante.

Per correggere questa situazione potremmo sfruttare l'attuale periodo di flessione economica per prepararci alla ripresa. Molte aziende affrontano i periodi di crisi riducendo i costi fissi ed in particolare il personale, senza ricordarsi che è proprio il personale la vera ricchezza di un'azienda. Sarebbe invece opportuno intraprendere due attività chiave: riconsiderare in modo critico i sistemi informativi e soprattutto addestrare in modo adeguato il personale, dando agli

amministratori ed agli sviluppatori il tempo di pensare, di sperimentare e quindi di capire veramente i sistemi che hanno sotto il loro controllo, senza l'assillo di un progetto da finire in fretta.

In generale un concetto chiave che vorrei sottolineare è che la complessità è nemica della sicurezza. Più un oggetto è complesso, meno lo comprendiamo, meno lo governiamo e quindi maggiori saranno i problemi di sicurezza che può generare. La nostra comprensione dei sistemi informativi tende a diminuire, a cominciare dal sistema operativo. Per me l'adozione del modello open-source non è tanto una questione di risparmio economico quanto una possibilità di analizzare e quindi capire a fondo il funzionamento del sistema, non limitandosi all'interfaccia grafica. Ciò vale non solo in piccolo (il sistema operativo) ma anche in grande (l'architettura del sistema informativo nella sua globalità): non tutte le aziende hanno finito di implementare le reti ed i sistemi client-server che già arrivano altre tecnologie (i web service, XML ed altro ancora). Dovremmo domandarci se tutto ciò è utile per l'azienda e per i servizi che intende erogare o se è solo una moda che genera complessità non solo non necessaria, ma anche nemica della sicurezza. Ecco allora che forse considerare il modello open-source come un aiuto nella comprensione dei sistemi non è così sbagliato.

La sicurezza dei servizi digitali ha due aspetti. Da una parte ci sono gli sviluppatori ed i gestori dei servizi, con le soluzioni che possono mettere in campo per cercare di proteggere i loro sistemi, ma dall'altra parte ci sono gli utenti dei servizi, che sempre più frequentemente sono persone non esperte di informatica ed in particolare di sicurezza. Eppure bisogna riconoscere che queste persone – col loro comportamento – fanno parte integrante del sistema di sicurezza. Ne consegue che bisogna sviluppare sistemi di sicurezza che siano usabili facilmente anche da persone non esperte. L'usabilità è uno dei fattori critici per il successo di un sistema di sicurezza e non è che un altro aspetto della complessità.

Per gli utenti spesso la sicurezza nell'accesso ad un servizio si esaurisce nel dimostrare la propria identità digitale: questo è e sarà sicuramente sempre di più uno dei problemi fondamentali dei servizi erogati in rete. Tipicamente oggi l'accesso ad un servizio è regolato da username e password, che dovrebbero essere conservate con cura e non rese note ad estranei. Ma purtroppo gli utenti hanno troppe password perché ogni servizio insiste nell'assegnare una propria password (alcuni servizi non permettono neanche di cambiarla, perché chi ha progettato il sistema presume di saper generare una password forte, difficile da indovinare, e quindi obbliga l'utente a mantenere questa password). Questo approccio genera troppe password (una per ogni servizio) e gli utenti, dopo un po', cominciano a non custodirle con cura, a scriverle e – quando possibile – a duplicarle. Quindi anche l'ipotesi che esista una password diversa per ogni servizio diverso è sbagliata: l'utente tende a rendere tutte le password uguali, se può, oppure a scriverle tutte nelle stesso posto, senza

distinzione tra password forti e deboli. I malintenzionati possono quindi attaccare l'utente non quando si collega al sistema forte ma quando si collega a quello debole, ne catturano la password e poi la usano anche sul sistema forte: in pratica è stato l'utente a creare la falla per penetrare nel sistema.

Su questo tema dell'identità digitale ci sono requisiti fortemente contrastanti. E' sicuramente indispensabile dimostrare la propria identità digitale quando si desidera accedere ad un servizio, ma ciò non deve generare complicazioni eccessive per l'utente. D'altra parte questa richiesta di semplicità contrasta col desiderio dei fornitori di servizi che vogliono proteggere i loro servizi ed identificarne gli utenti, per far pagare loro l'accesso e per raccogliere informazioni sui loro comportamenti. Il quadro è fortemente sbilanciato perché le conoscenze tecnologiche stanno tutte da una parte, quella dei fornitori di servizi: essi dovrebbero usare la tecnologia per semplificare la vita degli utenti invece di complicarla. Invece in questo momento ci sono tante, troppe tecnologie che finiscono col confondere l'utente: le password statiche, le password "usa-e-getta", gli autenticatori hardware, la firma digitale. Consideriamo la firma digitale, che – con qualche avvertenza – potrebbe essere la soluzione di questo problema. Innanzitutto sarebbe opportuno cambiarle nome, perché la firma digitale è una tecnologia che serve sia per firmare i documenti elettronici sia come sostituto di username e password. Purtroppo la firma digitale è standard, ma gli standard hanno così tante opzioni che di fatto due implementazioni standard possono essere incompatibili tra loro. Ne consegue che, anche in questo campo, c'è una tendenza – da combattere assolutamente – a fornire agli utenti un diverso sistema di firma digitale per ogni servizio a cui devono accedere. In pratica, è in corso la moltiplicazione degli strumenti di firma digitale esattamente come prima avveniva la moltiplicazione delle password. Ciò capita perché gli sviluppatori hanno una mentalità centrata sul servizio. Invece il sistema dovrebbe essere centrato sull'utente perché è lui che non ha grosse conoscenze tecnologiche ed è a lui che bisogna rendere l'accesso facile e sicuro. Se c'è un aggravio di tecnologia, una complessità, questa deve essere sopportata dai fornitori di servizi e non ribaltata sugli utenti. In altre parole mi oppongo ad avere sistemi di identificazione imposti dal fornitore del servizio, a cui gli utenti devono necessariamente adeguarsi perché alla fine risultano troppi sistemi di identificazione diversi e gli utenti non fanno più caso all'effettivo grado di sicurezza dei servizi che usano.

Un esempio concreto e reale di questi problemi è offerto da un sito di commercio elettronico molto frequentato che richiede l'introduzione della password in una pagina web apparentemente non protetta tramite un canale sicuro. Alla richiesta di spiegazione di un utente preoccupato, i responsabili del sito hanno risposto che – per motivi di efficienza – la pagina di introduzione dei dati non è protetta, ma il trasferimento dei dati lo è. Quindi l'utente non deve

preoccuparsi ed introdurre con fiducia la propria password in una pagina apparentemente non protetta. Pur essendo questa risposta tecnicamente corretta, è mia opinione che sia un approccio da deplorare perché produce cattiva educazione nei confronti dell'utente. Infatti l'utente si convince che può inserire la password anche se la pagina è non protetta (visivamente il lucchetto presente in basso nella finestra del browser web è aperto). Stiamo quindi diseducando l'utente e lo stiamo preparando all'attacco di un malintenzionato, che può creare un sito fantasma con il *look and feel* del servizio reale e presenta anch'esso una mancanza di sicurezza (il lucchetto aperto) ma l'utente non nota alcuna differenza col sito reale, introduce quindi tranquillamente la sua password che viene catturata ed usata per scopi illeciti.

L'esistenza di tante diverse identità digitali è dovuta ad un approccio sbagliato al problema. Molti gestori di servizi digitali sfruttano username e password per realizzare in un colpo solo due funzioni che in realtà sarebbero distinte: autenticazione ed autorizzazione.

Autenticazione vuol dire identificare l'utente, mentre autorizzazione vuol dire decidere quali azioni questo utente può svolgere. Per cercare di scindere questo legame, che crea i problemi citati, bisognerebbe rompere il legame tra password e servizio, ribaltando il paradigma da centrato sul servizio (*service-centric*) a centrato sull'utente (*user-centric*), permettendo all'utente di scegliere il sistema di autenticazione e quindi l'identità con cui presentarsi ad un servizio, scegliendo tra una delle identità che già possiede (uno strumento di firma digitale oppure la password di un servizio che usa frequentemente). Ogni cittadino dovrebbe avere poche identità elettroniche da gestire, una, due o tre al massimo: una lavorativa, una di privato cittadino ed una per l'accesso anonimo. Al momento dell'accesso ad un servizio, l'utente dovrebbe poter scegliere l'identità con cui presentarsi, in una filosofia di semplicità e di rispetto della privacy. Per realizzare un sistema di gestione delle identità di questo tipo occorrono formati e protocolli comuni tra i diversi fornitori di servizi, oppure la creazione di punti di mediazione (*clearing house*). Ad esempio a Torino si sta sperimentando una clearing house comune per la gestione delle identità elettroniche negli scambi documentali tra Comune, Provincia, Regione, Università, Politecnico ed Anagrafe. Ogni volta che un dipendente di uno qualunque di questi enti ha bisogno di dati forniti da un altro, si presenta con l'identificativo del proprio ente di appartenenza e la clearing house attesta la sua validità nei confronti dell'ente destinatario della transazione. In questa realizzazione non sono importanti i dettagli tecnologici dell'implementazione quanto la volontà di accordarsi per trovare una soluzione di sicurezza che semplifichi l'operatività degli utenti. La volontà di accordarsi è proprio quella che spesso manca perché molti fornitori di servizi vedono l'assegnazione di un proprio specifico meccanismo di identificazione come un modo di fidelizzare il cliente. Io sostengo che il meccanismo di identificazione dovrebbe essere unico, mentre la competizione dovrebbe

essere sulla tipologia e sulla qualità del servizio fornito. La creazione di tanti meccanismi di autenticazione diversi disorienta gli utenti che non sono invogliati ad accedere ai servizi oppure che inavvertitamente contribuiscono a minarne la sicurezza.

In conclusione lo sviluppo di servizi digitali sicuri richiede sia un investimento nello sviluppo dei servizi (centrato soprattutto sulla comprensione dei meccanismi, sulla semplicità architetturale e sulla correttezza di sviluppo) sia una maggiore attenzione alla semplicità d'uso dei servizi da parte degli utenti (con particolare riferimento alla gestione dell'identità digitale).

Alcune riflessioni sulla sicurezza nei servizi digitali

Antonio Lioy

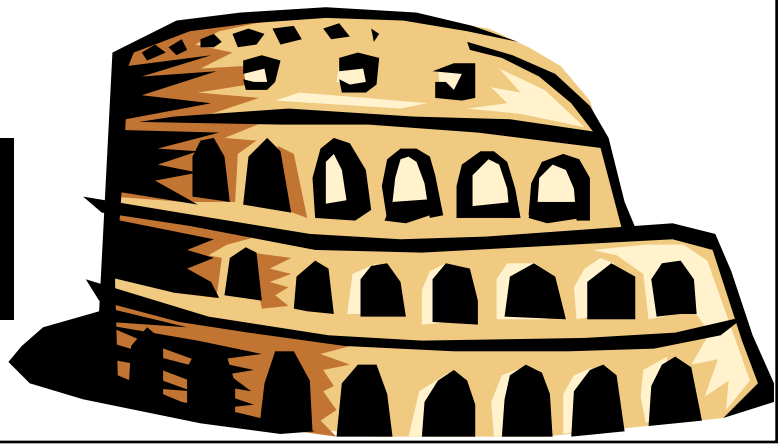
(lioy @ polito.it)

Politecnico di Torino
Dip. di Automatica e Informatica

La storia si ripete …

- **gennaio 2003 è stato un mese record:**
  - 20.000 attacchi
  - danni per 8 G Euro
- **l'attacco alle Poste Italiane …**
- **il NIMDA che bloccò mezzo mondo …**
- **l'attacco a Yahoo (feb 2000)**

"nil sub sole novi"



"chi non impara dai propri errori è condannato a ripeterli"

Insicurezza: le cause profonde (I)

- “Attack technology is developing in a open-source environment and is evolving rapidly”
- “Defensive strategies are reactionary”
- “Thousands - perhaps millions - of system with weak security are connected to the Internet”
- “The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrators … has decreased dramatically in the last 5 years”

Insicurezza: le cause profonde (II)

- **“Increasingly complex sw is being written by programmers who have no training in writing secure code”**
- **“Attacks and attack tools trascend geography and national boundaries”**
- **“The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that … prosecution of computer crime is unlikely”**

da “Roadmap for defeating DDOS attacks” (feb. 2000, after Clinton meeting at White House)

Il Politecnico di Torino sta sbagliando

- è quello che molti AD ripetono nelle conferenze ai nostri studenti
- “l’Italia non ha bisogno di sviluppare tecnologia, basta comprarla ed usarla: noi siamo commercianti, venditori, fornitori di servizi, …”
- ne siamo certi?

I nostri sistemisti (e programmatori)

- pochi
- poco addestrati
- male addestrati
  (le famose “certificazioni” …)
- con poco tempo da dedicare
  ai problemi

- es: lucchetto “disegnato”
  sulla pagina web !!!

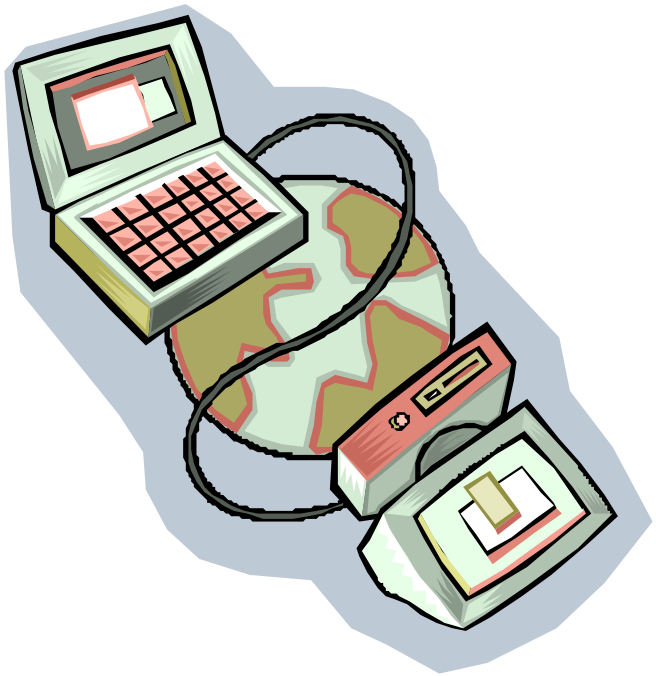
I nostri nemici …

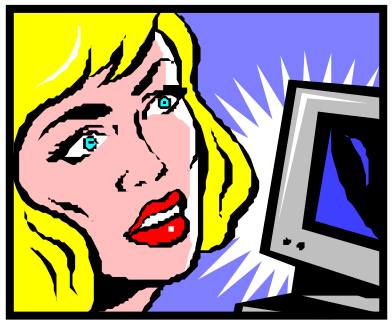
- **… siamo noi stessi (!)**
- **rightsizing o oversizing?**

- **siamo in un periodo di flessione economica**
- **usiamolo per:**
  - riconsiderare in modo critico i nostri sistemi
  - addestrare il personale (senza l'assillo di un progetto da finire in tre giorni …)

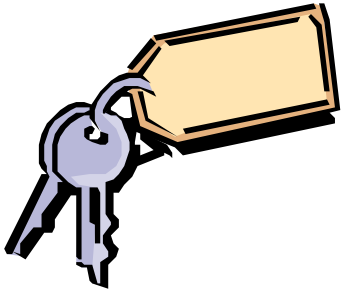
La complessità è nemica della sicurezza

- noi non comprendiamo più i nostri sistemi …
- … sia nel piccolo
  (il sistema operativo)
- … sia nel grande
  (il sistema globale)
- il modello open-source
  ci può aiutare?

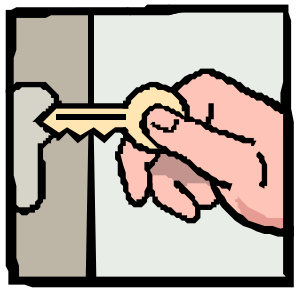




Usabilità



- **è un altro aspetto della complessità**
- **esempio tipico (per gli utenti):**
  - la gestione della propria identità elettronica
  - mediante username / password
  - una password va bene, ma due sono già troppe
  - ogni sistema insiste nel far usare la PROPRIA password
  - … ma ci pensa l'utente a renderle tutte uguali!



Requisiti contrastanti

- **gli utenti vogliono accedere ai servizi:**
  - in modo semplice (perché hanno scarse conoscenze tecnologiche)
  - in modo sicuro
  - proteggendo la propria privacy
- **i fornitori di servizi vogliono:**
  - proteggere l'accesso ai propri servizi
  - far pagare per l'accesso ai servizi
  - raccogliere informazioni sugli utenti
  - hanno ottime conoscenze tecnologiche

Identità digitale

- **tante (troppe?) tecnologie**
- **password (una per ogni sistema diverso)**
- **autenticatori hardware (one-time password)**
- **firma digitale**
  - sia per firmare documenti sia per autenticarsi (sistema a sfida)
  - sottili incompatibilità (nei formati, nelle smart-card, nei certificati)
  - molteplicità di supporti (la carta elettronica d'identità, dei servizi, sanitaria, bancaria, assicurativa, …)

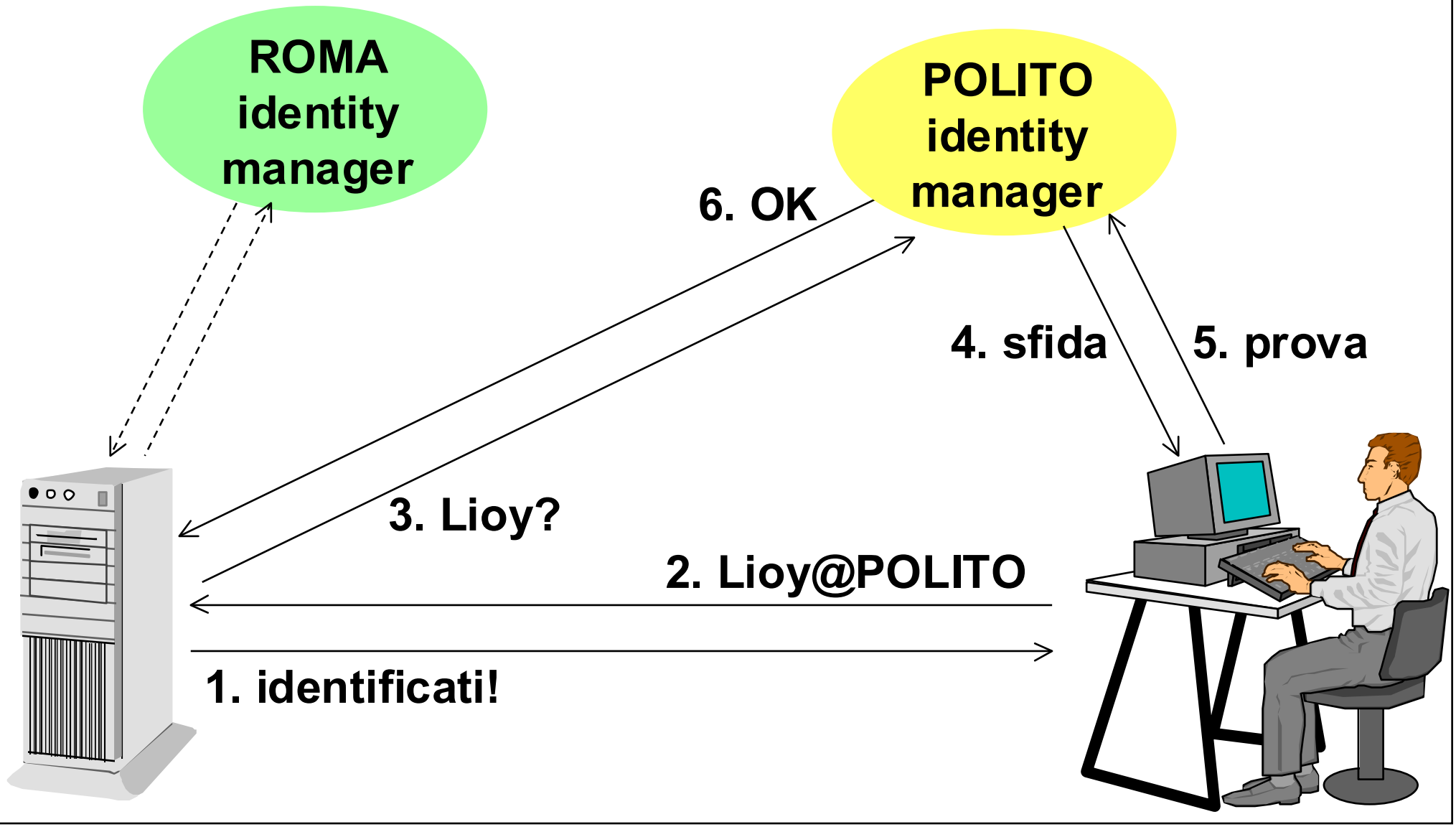
Sistemi di identificazione

- **il sistema di identificazione è imposto dal fornitore del servizio**
- **gli utenti devono adeguarsi ed alla fine hanno:**
  - troppi sistemi di identificazione
    - li smarriscono
    - non li sanno usare
    - si scrivono i dati rilevanti
  - non fanno più caso all'effettivo grado di sicurezza dei servizi che usano
    - es. pagina web con lucchetto “disegnato”
    - es. pagina web con lucchetto “aperto”

Autenticazione o autorizzazione?

- sono due concetti correlati ma diversi …
- … spesso mischiati in modo improprio

Verso servizi di gestione dell'identità



Gestione dell'identità

- **per comodità dell'utente, con rispetto della privacy:**
  - deve essere possibile l'anonimato!
- **occorrono:**
  - formati e protocolli comuni
  - clearinghouse (es. enti Torinesi)
- **ma soprattutto VOLONTA' DI ACCORDARSI**
  - per una reale interoperabilità delle carte elettroniche
  - facendo un sistema veramente aperto

LA COMPETIZIONE E' SUI SERVIZI,
NON SULLE PASSWORD