Sicurezza nei WIS

Prof.ssa E. Gentile
a.a. 2011-2012

Definizione di sicurezza

- Si intende l'insieme delle misure (organizzative e tecnologiche) tese ad assicurare a ciascun utente autorizzato tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste
- I requisiti da garantire sono la disponibilità, l'integrità, la riservatezza e l'autenticità

Requisiti di Disponibilità

- Il sistema deve rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere nei tempi e nei modi previsti
- Requisiti legati alla disponibilità sono quelli di prestazioni e di robustezza

Requisiti di Integrità

- Il sistema deve impedire l'alterazione diretta o indiretta delle informazioni sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali

Requisiti di Riservatezza

- Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere

Requisiti di Autenticità

- Le informazioni in transito e memorizzate devono essere integre
- L'autenticità impedisce che avvenga il ripudio dell'invio di messaggi o di informazioni

Requisiti di Autenticazione

- Ogni agente deve essere identificato prima di poter interagire con il sistema
- L'autenticazione deve essere mutua, anche il client deve autenticare il server con cui interagisce prima di iniziare uno scambio di informazioni

Attacchi a livello fisico

- Furto
  - Dei dischi o di interi server: è un attacco alla disponibilità e alla riservatezza
- Danneggiamento
  - Condotto contro apparecchiature e cavi di rete: è un attacco alla disponibilità ed alla integrità

Attacchi a livello logico

- Livello interfaccia
- Livello applicazione
- Livello dati
- Livello main-frame

Classificazione degli attacchi

- Intercettazione e deduzione
  - attacco alla riservatezza
- Intrusione
  - attacco alla integrità ed alla riservatezza
- Disturbo
  - attacco alla disponibilità

Attacchi di intercettazione

- Gli attacchi di intercettazione possono richiedere un attacco preventivo a livello fisico per installare dispositivi pirata o per agganciarsi alla rete, e di intrusione (livello logico), per installare software di supporto alla intercettazione
- Le tecniche comunemente utilizzate sono basate su:
  - analizzatori di traffico su rete (locale o geografica);
  - applicazioni di analisi del traffico su rete (sniffing);
  - server pirata che si spacciano come router (spoofing);
  - programmi che emulano servizi del sistema (tipicamente il login, durante il quale l'utente digita username e password) registrando al contempo le informazioni riservate digitate dall'utente
- Gli attacchi di intercettazione possono sfruttare debolezze intrinseche di protocolli e software di rete, o poco accorte configurazioni del sistema operativo

Attacchi di deduzione

- Gli attacchi basati sulla deduzione sono condotti incrociando informazioni tratte dall'osservazione del sistema con informazioni ottenute per altre vie.
- Alcuni esempi sono gli attacchi condotti:
  - a partire dal fatto stesso che un certo servizio o una certa informazione sia negata dal sistema
  - a partire dal monitoraggio dei volumi di traffico nella comunicazione fra componenti del sistema
  - confrontando informazioni presenti nel sistema, individualmente configurate come poco riservate

Attacchi di intrusione

- L'accesso al sistema tramite password illegale è uno degli attacchi di intrusione più frequenti
- Una volta ottenuti in qualche modo (anche temporaneamente) i diritti di amministratore, è possibile installare nel sistema un meccanismo, detto **backdoor**, che permetta anche in seguito di mantenere un accesso privilegiato
- Questa tecnica rientra fra quelle indicate come "cavallo di Troia"

Attacchi di disturbo

- Gli attacchi che fanno uso di queste tecniche non sono tesi ad accedere a servizi ed informazioni, ma semplicemente a degradare la operatività del sistema
- Sono considerabili come atti di sabotaggio, e minacciano tipicamente la integrità e la disponibilità dei dati, più raramente (e indirettamente) la riservatezza

Attacchi di disturbo tramite virus

- I virus sono programmi auto-replicanti, spesso inseriti nel sistema come cavalli di Troia, generalmente pericolosi per la integrità del file-system e per la disponibilità dei servizi.
- I virus sono principalmente caratterizzati da:
  - logica del payload
  - modalità di infezione
  - modalità di mimetizzazione

Logica del payload

- logica del payload, cioè del modo in cui arrecano danno al sistema, il payload è la parte del codice virale che arreca direttamente il danno;
- la logica del payload può essere piuttosto complessa, e variare il comportamento del virus in funzione di variabili come:
  - data ed ora,
  - presenza di determinati file nel file-system infettato,
  - nome, tipo o dimensione dei file da alterare;
- gli effetti del payload sono spesso resi volutamente pseudo-casuali al fine di camuffare i danni causati come problemi nell'hardware o nel software di base del calcolatore colpito

Modalità di infezione

- Dal modo in cui si inseriscono e si duplicano nel sistema;
- Ad esempio abbiamo virus:
  - parassiti
  - Boot-Sector
  - Gemelli
  - multi-partiti, etc.

Modalità di mimetizzazione

- Dal modo in cui si sottraggono alla identificazione da parte dei programmi anti-virus
- Abbiamo ad esempio virus:
  - Stealth
  - Polimorfici
  - Armoured
  - tunneling, etc.

Attacchi di disturbo tramite worm

- I worm sono virus particolari che si limitano a degradare le prestazioni del sistema, ad esempio lanciando molte immagini di uno stesso processo.
- Quando il rallentamento del sistema supera una certa soglia, alcuni servizi possono risultare di fatto inutilizzabili, ed in questo caso si ha una violazione dei requisiti di disponibilità.
- L'attacco con worm è particolarmente subdolo su sistemi batch, nei quali è più probabile che il degrado delle prestazioni sia rilevato con un ritardo inaccettabile.

Attacchi di disturbo "denial of service"

- Si tratta di una famiglia di tecniche tese a fare in modo che il sistema neghi l'accesso a servizi ed informazioni anche ad utenti regolarmente autorizzati.
- Gli attacchi che usano queste tecniche minacciano quindi i requisiti di disponibilità del sistema.
- Due tipiche tecniche "denial of service" consistono nel paralizzare il traffico sulla rete generando falsi messaggi di errore o intasandola con traffico di disturbo generato appositamente.

Contromisure

- **preventive** o **correttive**
- **informatiche** o **organizzative**
- **a livello fisico** o **logico**

Contromisure informatiche a livello di applicazione

- Le contromisure operanti a livello di applicazione sono particolari funzioni inserite nelle applicazioni ai fini della sicurezza, e possono essere utilizzate da esse solo quando effettivamente necessario.
- Le contromisure a livello di applicazione sono spesso caratterizzate da una efficacia elevata ma relativa ad un insieme tipicamente ristretto di eventi indesiderati che è quello specificamente previsto per l'applicazione che vanno a proteggere.

Contromisure informatiche di base (DBMS, sistema operativo, rete)

- Le contromisure che operano a livello di DBMS, sistema operativo o rete hanno carattere più generale, rispetto a quelle di livello applicativo, e indipendente dalla particolare applicazione eseguita.
- Di conseguenza, sono spesso meno sofisticate di quelle a livello applicazione, ma dotate in compenso di un più ampio grado di copertura rispetto alla gamma degli eventi indesiderati che vanno a contrastare.

Protezione dalle false autenticazioni

- Imporre che a ciascun login name sia associato una persona fisica.
- Disabilitare o eliminare i login name non più utilizzati per qualunque motivo.
- Mantenere una lista degli utenti cancellati.
- Imporre che a ciascun login name sia associata una password.
- Imporre agli utenti di cambiare periodicamente (eventualmente ad ogni sessione) la password, impedendo il riuso di password utilizzate in precedenza.
- Utilizzare tecniche avanzate di autenticazione (smart-card, riconoscimento della retina, etc.).
- Verificare che tutti i serventi della rete siano fra loro reciprocamente autenticati.

Protezione dagli accessi illegali

- Limitare il numero delle connessioni simultanee di ciascun utente
- Rilevare i login falliti e disabilitare i login name al terzo tentativo.
- Limitare gli intervalli temporali in cui è possibile utilizzare la rete.
- Limitare gli indirizzi MAC di rete delle stazioni di lavoro da cui consentire l'accesso agli utenti.
- Disabilitare e rimuovere fisicamente lettori di dischetto e di CD-ROM dalle stazioni di lavoro e dai server.
- Educare gli utenti a chiudere la sessione ogni volta che abbandonano la propria stazione di lavoro.
- Verificare periodicamente i diritti di accesso di ogni utente.
- Limitare l'accesso fisico alle postazioni di lavoro ai soli utenti autorizzati.
- Utilizzare esclusivamente prodotti certificati.
- Installare le applicazioni di rete in modo conforme alle specifiche della casa produttrice.

Protezione degli attacchi via rete ed alla rete stessa

- Configurare il sistema in modo che tutti i nodi firmino ogni pacchetto trasmesso (8% di sovraccarico).
- Definire esplicitamente un utente cui assegnare i diritti di amministratore di rete (eliminando un eventuale utente di default).
- Utilizzare Hub dotati di meccanismi anti-intercettazione.
- Installare Hub e router in locali protetti, e far passare i cavi della rete in canaline murate.
- Bloccare il traffico non autorizzato su una rete locale (firewall, packet-inspecting routers, etc.);
- Cifrare il traffico riservato a livello applicativo oppure a livello di router;

Protezione dagli attacchi ai server

- Isolare i server in un locale sicuro e proteggerne l'eventuale impianto di condizionamento.
- Definire una politica precisa per la gestione e la distribuzione delle chiavi di accesso ai locali protetti.
- Registrare gli accessi ai locali dove si trovano server e dispositivi di rete.
- Bloccare la console dei server con una password diversa da quella dell'amministratore di rete.
- Imporre una password per ciascun server di stampa.
- Limitare il caricamento dei serventi applicativi in directory predefinite.
- Disabilitare tutti i servizi di console remota.
- Duplicare le unita di alimentazione e di raffreddamento
- Rendere a sola lettura tutte le directory in cui sono installate applicazioni.

Protezione dai virus

- Verificare periodicamente le dimensioni di tutti i file eseguibili.
- Installare solo software originale prelevato da confezioni sigillate.
- Acquisire, installare ed aggiornare periodicamente un sistema anti-virus per le stazioni di lavoro in rete.

Protezione dalle perdite di dati

- Definire una politica di backup periodico.
- Abilitare la funzione di controllo automatico del backup.
- Effettuare prove a campione di lettura dei dati su backup.
- Isolare nastri e dischi di backup in un luogo sicuro, separato da quello che ospita i server.
- Utilizzare array ridondanti di dischi

Algoritmi di crittografia

- Sono algoritmi matematici in grado di trasformare (cifrare) reversibilmente un insieme di dati, ad esempio un documento, in modo da renderlo non intelligibile.
- Affinché questi algoritmi siano di qualche utilità pratica occorre che soddisfino le seguenti condizioni fondamentali:
  - la cifratura e la decifratura deve avvenire in funzione di una variabile detta *chiave* e costituita da una sequenza di bit di lunghezza variabile in funzione dell'algoritmo e del livello di sicurezza che si desidera ottenere;
  - le operazioni di cifratura e decifratura sono relativamente semplici nel caso in cui si conosca la chiave; in caso contrario risultano laboriose al punto da risultare praticamente inattuabili;
  - risulta egualmente laborioso dedurre la chiave con cui è stato cifrato un documento confrontandolo con la sua versione in chiaro (cioè non cifrata).
- Gli algoritmi di crittografia possono essere classificati come **simmetrici**, anche detti "a chiave privata", ed **asimmetrici**, anche detti "a doppia chiave" o "a chiave pubblica".

Algoritmi simmetrici

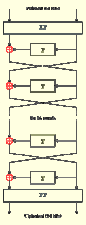
- Gli algoritmi simmetrici utilizzano la stessa (ed unica) chiave privata, per cifrare e decifrare. Conviene evidenziare da subito che gli algoritmi simmetrici non si prestano bene a garantire la riservatezza nella comunicazione continuativa fra N soggetti indipendenti, in quanto:
  - occorre una chiave privata per ogni coppia di soggetti;
  - ogni soggetto è costretto a possedere N-1 chiavi, a mantenerle segrete ed a ricordare la chiave da utilizzare per comunicare con ciascuno degli altri soggetti;
  - nel caso in cui la chiave sia generata autonomamente dal soggetto che avvia la comunicazione, è necessario che venga trasmessa al destinatario affinché questo possa decifrare i messaggi che riceve, e durante il trasferimento la chiave potrebbe essere intercettata.
- Uno degli algoritmi simmetrici utilizzati al momento è il **DES** (Data Encription Standard) con chiavi di 56 o 112 bit.

Algoritmo DES (Data Encryption Standard)

- Il DES è l'archetipo della cifratura a blocchi, un algoritmo che prende in ingresso una stringa di lunghezza fissa di testo in chiaro e la trasforma con una serie di operazioni complesse in un'altra stringa di testo cifrato della stessa lunghezza.
- La dimensione del blocco è di 64 bit.
- Il DES usa una chiave per modificare la trasformazione in modo che l'operazione di decifratura possa essere effettuata solo conoscendo la chiave stessa.
- La chiave è lunga 64 bit ma solo 56 di questi sono effettivamente utilizzati dall'algoritmo.
- Otto bit sono utilizzati solo per il controllo di parità e poi scartati, per questo la lunghezza della chiave effettiva è riportata come di 56 bit.

Passi dell'Algoritmo DES

- È composto da:
  - 16 fasi identiche di processo dette *round*, o cicli
  - una permutazione iniziale ed una finale dette *IP* e *FP*, che sono tra di loro inverse (IP "disfa" l'azione di FP e viceversa)
  - Prima del ciclo principale, il blocco è suddiviso in due metà di 32 bit e processato alternativamente (rete di Feistel)

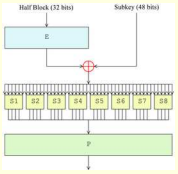


Funzione Feistel

- La *funzione Feistel* mescola metà del blocco con una parte della chiave.
- Il risultato della funzione Feistel è poi combinato con l'altra metà del blocco, e le due metà sono scambiate prima del ciclo successivo.
- Dopo il ciclo finale, le metà non sono scambiate per rendere le fasi di cifratura e decifratura più simili.

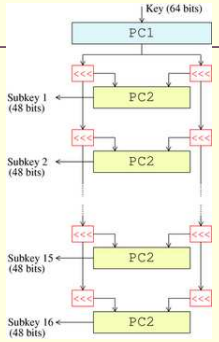
Passi della Funzione Feistel

1. ***Espansione***
2. ***Miscelazione con la chiave***
3. ***Sostituzione***
4. ***Permutazione***



Gestore della chiave per la cifratura

- Inizialmente, vengono selezionati 56 bit della chiave dagli iniziali 64 bit mediante la funzione *Permuted Choice 1* (*PC-1*) - i rimanenti 8 bit sono scartati o utilizzati come bit di controllo della parità.
- I 56 vengono poi suddivisi in 2 metà di 28 bit; ogni metà è poi trattata separatamente.
- Nei cicli successivi entrambe le metà vengono fatte slittare verso sinistra di 1 o 2 bit (per i round 1, 2, 9, 16 lo shift, cioè lo slittamento, è di 1 bit, per gli altri è di 2) e quindi vengono scelti 48 bit per la sottochiave mediante la funzione *Permuted Choice 2* (*PC-2*) - 24 bit dalla metà di sinistra e 24 bit da quella di destra.
- La rotazione significa che in ogni sottochiave è usato un insieme differente di bit; ogni bit è usato più o meno in 14 delle 16 sottochiavi.
- Il *gestore delle chiavi per la decifratura* è simile - deve generare le chiavi nell'ordine inverso quindi la rotazione è verso destra invece che verso sinistra.



Algoritmi asimmetrici

- Gli algoritmi asimmetrici sono di concezione recente (1976) ed utilizzano due chiavi distinte per cifrare e decifrare, con alcune proprietà fondamentali:
  - un documento cifrato con una chiave può essere decifrato con l'altra e viceversa;
  - le chiavi vengono generate in coppia da uno speciale algoritmo ed è di fatto impossibile ottenere una chiave a partire dall'altra;
  - una qualsiasi delle due chiavi viene detta pubblica, è può essere distribuita; l'altra, detta privata, deve essere mantenuta segreta.
- L'algoritmo RSA, è attualmente considerato come standard per la crittografia a chiave pubblica. Esistono varie implementazioni di RSA, che utilizzano coppie di chiavi di 512 o di 1024 bit.

Algoritmo RSA

- Per semplificare il funzionamento immaginiamo che A debba spedire un messaggio segreto a B. Occorrono i seguenti passaggi:
  1. B sceglie due numeri primi molto grandi (per esempio da 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
  2. B invia il numero che ha ottenuto ad A. Chiunque può vedere questo numero.
  3. A usa questo numero per cifrare il messaggio
  4. A manda il messaggio cifrato a B, chiunque può vederlo ma non decifrarlo
  5. B riceve il messaggio e utilizzando i due fattori primi che solo lui conosceva lo decifra.
- A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe troppo tempo per scoprire i due fattori primi, con cui si può decifrare il messaggio.

Algoritmi asimmetrici

- Nella comunicazione fra N soggetti, gli algoritmi asimmetrici risultano decisamente più utili dei simmetrici in quanto:
  - occorre una sola coppia di chiavi per ciascun soggetto.
  - ogni soggetto genera autonomamente una propria coppia di chiavi, ed è tenuto a mantenere segreta una sola di esse, quella privata, mentre può, anzi deve, pubblicare l'altra;
  - le chiavi private non devono essere scambiate, dunque non sussiste pericolo di intercettazioni.

Algoritmi di hashing sicuro

- Questi algoritmi permettono di creare, a partire da un documento D, una sequenza di bit, detta *digest*, strettamente correlata a D e di lunghezza fissa (cioè indipendente dalla dimensione di D).
- Un algoritmo di questo tipo generalmente utilizzato dai servizi sicurezza è lo SHA (Secure Hash Algorithm).

SHA (Secure Hash Algorithm)

- Per generare una firma:
  - si estrae un digest SHA dal documento da firmare;
  - si cifra RSA il digest con la chiave privata del firmatario.
- Chiunque può verificare la validità della firma:
  - decifrando la firma con la chiave pubblica del firmatario;
  - generando a parte un digest SHA del documento firmato;
  - confrontando il digest ottenuto dalla firma con quello ottenuto dal documento.

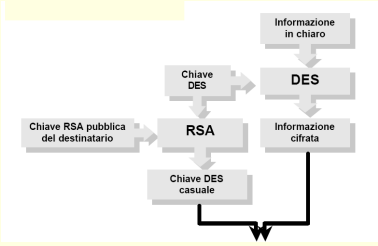
Introduzione di riservatezza

- Obiettivo di questo servizio è quello di rendere un documento, o più genericamente una informazione, leggibile solo da parte di un destinatario prefissato, cioè senza possibilità che terze parti possano interpretarlo.
- Sebbene questo servizio possa essere realizzato, sul piano teorico, con l'utilizzo del solo RSA, la lentezza di tale algoritmo (come di tutti quelli asimmetrici) rende necessario l'utilizzo congiunto di un algoritmo simmetrico quale il DES.

Passi per il servizio

1. Viene generata una chiave DES in modo pseudo-casuale.
2. L'informazione che si vuole rendere riservata viene cifrata con DES utilizzando la chiave pseudo-casuale.
3. La chiave pseudo-casuale, che se intercettata permetterebbe di decifrare l'informazione originale, viene a sua volta cifrata con RSA utilizzando la chiave pubblica del destinatario, cioè dell'interlocutore al quale si desidera comunicare l'informazione in modo riservato.

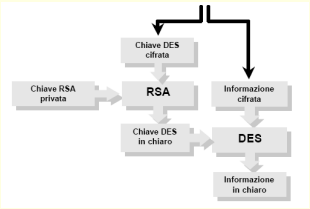
Introduzione di riservatezza



Rimozione di riservatezza

- Obiettivo di questo servizio è quello di permettere al destinatario di una informazione a lui riservata di riportare in chiaro, cioè in forma leggibile, l'informazione stessa.
  1. Viene ricevuta la informazione cifrata e, in allegato, la relativa chiave DES (cioè la chiave con cui l'informazione stessa è stata cifrata). La chiave DES è a sua volta cifrata RSA con la chiave pubblica del destinatario.
  2. Il destinatario decifra la chiave DES applicando su di essa RSA con la propria chiave privata. Essendo tale chiave nota solo al destinatario, nessun altro può decifrare la chiave DES e quindi l'informazione originale.
  3. L'informazione cifrata viene riportata in chiaro, cioè in forma intelligibile, applicando su di essa DES con la chiave decifrata.

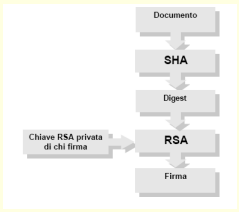
Rimozione di riservatezza



Apposizione di Firma digitale

- Obiettivo di questo servizio è quello di generare, dato un documento e la chiave privata di un soggetto che chiameremo firmatario, una sequenza di bit detta firma digitale che provi in modo non ripudiabile il possesso del documento "firmato" da parte del soggetto firmatario.
  1. Al documento viene applicato SHA al fine di ottenere un digest, La stretta correlazione fra il documento ed il suo digest, assicurata da SHA, garantiscono con sufficiente sicurezza che la firma generata dal servizio sia stata effettivamente apposta sul documento originale.
  2. Il digest viene cifrato RSA con la chiave privata del firmatario. Il fatto che il risultato della cifratura, cioè la firma, sia decifrabile solo con la chiave pubblica del firmatario garantisce circa la identità del firmatario stesso.

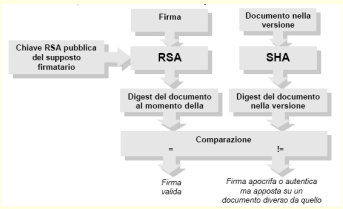
Apposizione di firma digitale



Verifica di firma digitale

- Obiettivo di questo servizio è quello di verificare l'autenticità di una firma digitale, rispetto al documento firmato ed al soggetto firmatario. In particolare, dato un documento, un soggetto (o meglio la sua chiave pubblica) ed una firma, il servizio verifica che quel soggetto (e non altri) abbia effettivamente apposto la firma sul quel documento (e non su altri o sullo stesso modificato in qualche sua parte).
  1. La firma viene decifrata con RSA utilizzando la chiave pubblica del soggetto firmatario. In questo modo, se la firma è autentica, si ottiene il digest del documento al momento della firma.
  2. Il documento nella versione corrente viene sottoposto ad SHA e ne viene generato il digest che, se il documento non ha subito modifiche e se la firma è autentica, dovrebbe coincidere con quello ottenuto al passo precedente decifrando la firma con RSA.
  3. Il digest ottenuto applicando SHA sul documento viene confrontato con il digest ottenuto applicando RSA sulla firma. Se i digest coincidono la firma è valida, altrimenti la firma è apocrifa (cioè apposta da un soggetto diverso da quello considerato) e/o il documento è stato modificato dopo la firma.

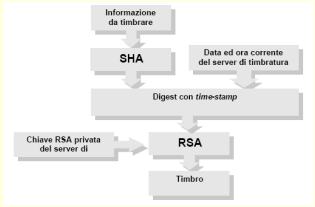
Verifica di firma digitale



Timbratura

- Obiettivo di questo servizio è quello di associare in modo incontestabile un riferimento temporale (data ed ora esatta) ad un dato documento. Affinché questo servizio sia di qualche utilità è essenziale che venga svolto da un soggetto al di sopra degli altri e da tutti ritenuto autorevole e fidato. Questo soggetto, spesso indicato come terza parte fidata, dovrà naturalmente gestire autonomamente ed in modo sicuro un orologio di sistema.
  1. Alla informazione da timbrare viene applicato SHA al fine di ottenerne il digest. Questa operazione è tipicamente compiuta dal soggetto che richiede il servizio di timbratura.
  2. La terza parte fidata accoda al digest la data e l'ora dell'orologio di sistema da essa gestito autonomamente.
  3. La terza parte fidata cifra RSA il digest e la sequenza temporale utilizzando la propria chiave privata. Il risultato della cifratura è il timbro, la cui validità è verificabile da chiunque semplicemente decifrando il timbro stesso con la chiave pubblica della terza parte fidata.

Timbratura



Servizi di Notariato

- I servizi di notariato sono offerti da una Autorità di certificazione che sia riconosciuta come fidata ed autorevole da tutti gli utenti del sistema informativo.
- Come ogni altro utente, anche l'Autorità dispone di una coppia (privata, pubblica) di chiavi asimmetriche.
- I principali servizi di notariato offerti dall'Autorità sono:
  - la certificazione delle chiavi pubbliche
  - la gestione delle chiavi pubbliche sospese o revocate
  - la certificazione temporale, (timbratura)

Certificazione di chiave pubblica

- Con la certificazione di una chiave pubblica l'Autorità garantisce la sua effettiva corrispondenza con il soggetto che la espone. A tal fine, l'Autorità pubblica mantiene, in un apposito registro, certificati firmati con la propria chiave privata. Tali certificati includono il nome dell'Autorità, la data di emissione del certificato, la data di scadenza del certificato, il nominativo univoco del soggetto (cioè reso non ambiguo da dati aggiuntivi, nel caso di omonimie) e la chiave pubblica del soggetto.

- Vale la pena di osservare la estrema importanza che ha la certificazione delle chiavi pubbliche nella verifica di una firma digitale. Per tale verifica occorre infatti:
  - conoscere la chiave pubblica del soggetto firmatario al momento della firma; questo é possibile richiedendo all'Autorità il relativo certificato;
  - essere certi della reale appartenenza della chiave al soggetto firmatario; la firma dell'Autorità garantisce la validità del certificato e quindi la effettiva corrispondenza fra chiave pubblica e soggetto.
- Tale sequenza di operazioni viene tipicamente svolta in modo automatico dal software che gestisce le firme digitali, a partire da informazioni contenute nella firma stessa.

Gestione delle chiavi pubbliche sospese o revocate

- Le chiavi pubbliche possono essere sospese o revocate (ad esempio a seguito di furto o smarrimento delle corrispondenti chiavi private). L'Autorità deve quindi gestire un registro storico delle chiavi pubbliche revocate, al fine di garantire nel tempo la verificabilità delle firme generate utilizzando le corrispondenti chiavi private.

Gestione del tempo di riferimento e timbratura ufficiale

- Il servizio base di timbratura ricade fra i servizi di notariato in quanto richiede che il time-stamp sia generato ed apposto da una Autorità riconosciuta da parte tutti gli utenti del sistema. come detentrice affidabile del riferimento temporale.

Tecniche avanzate di autenticazione

- La autenticazione degli utenti é generalmente basata su una combinazione di tre tipi di elemento:
  - conoscenze dell'utente (per esempio una **password**);
  - oggetti posseduti dall'utente (per esempio una **card** o una **smart-card**);
  - caratteristiche biometriche dell'utente (per esempio l'impronta di un polpastrello o l'immagine di una retina).

Password

- La tecnica di autenticazione tramite password é quella più diffusa, ma presenta vari problemi legati al fatto che, tendenzialmente, gli utenti:
  - impostano password troppo brevi, che quindi possono facilmente essere individuate attraverso tentativi ripetuti, o prevedibili (per esempio il proprio nome);
  - impostano password appropriate ma poi le scrivono in luoghi non sicuri, per non doverle imparare a memoria;
  - impostano password appropriate, impiegano del tempo per impararle a memoria, ma proprio per questo non le cambiano mai

Card

- Le card sono tessere che memorizzano in modo non duplicabile o alterabile la chiave privata dell'utente. La card dialoga con la stazione di lavoro attraverso un apposito lettore, ed software applicativo può interrogarla per ottenere la chiave privata dell'utente.
- La card fornisce la chiave privata solo se riceve dalla applicazione (e quindi dall'utente) un PIN (Personal Identification Number) segreto.
- In definitiva, analogamente a quanto avviene con il Bancomat, l'utente é identificato sia per il fatto di conoscere il PIN, sia per il fatto di possedere la card. Il punto debole delle card é insito nel fatto che la chiave privata dell'utente viene trasferita sulla stazione di lavoro, ove potrebbe essere intercettata.

Smart-Card

- A differenza delle semplici card, le smart-card non si limitano a memorizzare in modo inalterabile la chiave privata dell'utente, ma dispongono di firmware, micro-processore e memoria con caratteristiche sufficienti a eseguire autonomamente un algoritmo asimmetrico di crittografia.
- Il principale vantaggio delle smart-card, rispetto alle card semplici, é che non richiedono il trasferimento della chiave privata dell'utente sulla stazione di lavoro. La chiave rimane sempre stabilmente memorizzata nella card, che resta peraltro inutilizzabile senza il PIN associato.
- La presenza di un micro-processore a bordo, permette inoltre alle card interessanti funzionalità accessorie, quali ad esempio la generazione e la memorizzazione automatica di una one-time password ad ogni sessione di lavoro.

Valutazione del costo e dell'efficacia di una contromisura

- La considerazione, almeno qualitativa, del rapporto costo/efficacia di ciascuna contromisura, permette di valutarne il grado di adeguatezza, evitando in particolare quelle contromisure con un costo ingiustificato rispetto al rischio dal quale proteggono.
- L'**efficacia** di una contromisura può essere valutata, in prima analisi, come funzione del rischio dal quale protegge, cioè dal rischio complessivamente legato agli eventi indesiderati che neutralizza.
- Il **costo** di una contromisura deve essere valutato ponendo la dovuta attenzione sui cosiddetti *costi nascosti*. Oltre al lavoro necessario per individuare ed attuare le contromisure, infatti, occorre tenere presenti le limitazioni che esse impongono e le operazioni di controllo che introducono nel flusso di lavoro del sistema informatico e dell'organizzazione nel suo complesso. Il costo di una contromisura, insomma, deve essere valutato su vari fronti, sia tecnologici che organizzativi.

Valutazione del costo e dell'efficacia di una contromisura

- un costo di messa in opera della contromisura: si tratta di un costo "una tantum" che assume particolare rilevanza laddove la contromisura imponga un riassetto logistico della organizzazione (adeguamento di locali, trasloco di apparecchiature, etc.);
- un peggioramento dell'ergonomia della interfaccia utente: aumentare la sicurezza di un sistema informatico impone generalmente la introduzione o la complicazione delle procedure di autenticazione degli utenti; l'utente che viene costretto a digitare una password ogni volta che accede ad un servizio riservato, ad esempio, troverà il sistema informatico meno piacevole da utilizzare;

Valutazione del costo e dell'efficacia di una contromisura

- un decadimento delle prestazioni del sistema nell'erogare i servizi: allo scopo di validare le autorizzazioni di accesso, o di cifrare le informazioni riservate, un sistema informatico può spendere una parte anche consistente della sua potenza elaborativa; ne consegue un decadimento prestazionale che, superati certi limiti, si traduce in un calo nella produttività degli utenti;
- un aumento nella complessità di procedure e norme comportamentali come la registrazione delle presenze o le richieste di intervento tecnico.

Contromisure: Completezza

- **completezza**: il sotto-insieme delle contromisure scelte deve comunque far fronte a tutti gli eventi indesiderati individuati per il sistema in esame;

Contromisure: Omogeneità

- **omogeneità**: le contromisure che si decide di adottare devono essere compatibili ed integrabili tra loro in modo da minimizzare il costo della loro attuazione congiunta; a fronte di eventi indesiderati con analogo livello di rischio, inoltre, le rispettive contromisure dovrebbero avere costo comparabile;

Contromisure: Ridondanza

- **ridondanza controllata**: la ridondanza delle contromisure ha un costo e deve quindi essere rilevata e vagliata accuratamente; può accadere, ad esempio, che più contromisure siano inutilmente ridondanti, che ad esempio neutralizzino un medesimo evento valutato a basso rischio; d'altra parte, è anche possibile che un evento ad alto rischio, che potrebbe e dovrebbe essere neutralizzato da più di una contromisura, di fatto non lo sia;

Contromisure: Attuabilità

- **effettiva attuabilità**: l'insieme delle contromisure deve rispettare vincoli di tipo logistico (per esempio la distribuzione dei locali), di tipo amministrativo (per esempio limitazioni nella assunzione di nuovo personale), di tipo giuridico (per esempio vincoli su formato e disponibilità delle informazioni).