Sicurezza dei sistemi

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Sicurezza dei sistemi

- Sistemi operativi e infrastrutture virtuali
- Autenticazione, autorizzazione, identificazione
- Backup
- Dal monitoraggio all'intrusion prevention
- Crittografia
- Certificati e firma digitale

.....

Hardening

http://en.wikipedia.org/wiki/Hardening_(computing)

E' una tecnica di configuration management dei sistemi, che permette di analizzare e affinare la configurazione degli stessi con l'obiettivo di accrescerne la sicurezza intrinseca.

Ciascun tipo di server richiede tecniche di hardening proprie, che variano anche in funzione della sua visibilità e dell'informazione in esso contenuta.

“Less is better” lasciare solo i servizi indispensabili: quello che non c'è non può essere rotto!

Le tecniche di hardening includono:

- disattivazione di programmi e servizi non utilizzati
- controllo delle configurazioni del software
- controllo dei permessi e delle ACL sui file e verifiche di appropriatezza
- configurazione di parametri di sistema

Vale per il fisico ma anche per il virtuale, docker, serverless ecc.

Metodologie diverse fra ambienti fisici, virtuali,container e serverless

Ci sono basi comuni ma anche differenze fra “hardenizzare” server fisici, virtuali (compreso quindi lo strato di virtualizzazione), container (attenzione anche a quelli “standard” trovati in rete) e serverless (acquisto “pezzi di server” nel cloud su cui far girare pezzi di mie applicazioni, sicurezza rimane a tutti i livelli).

Obiettivo comune: ridurre superficie di attacco

https://thenewstack.io/security-differences-containers-vs-serverless-vs-virtual-machines

Autenticazione, autorizzazione, identificazione

Accesso implica:

Identificazione
Autenticazione
Autorizzazione

Identificazione è la verifica dell'identità di una persona o di una cosa (es. sito web) tramite uno o più informazioni: “Chi sei tu ?” (utente).

Autenticazione è l'atto di verificare la verità di un attributo di un dato o di una informazione: “Dimostramelo !” (password).

Autorizzazione è la verifica che tu sia autorizzato a fare quello che stai facendo: “OK, puoi fare queste cose” (profilo). Può essere statica (“tutti gli amministrativi possono usare il programma di contabilità”) oppure dinamica (“gli amministrativi possono usare il programma di contabilità solo dopo aver timbrato l’entrata e fino a quando non timbrano l’uscita”).

Autenticazione, autorizzazione, identificazione

Autenticazione semplice o mutua

Autenticazione a 1-2-3 fattori

Passaggio dal virtuale al fisico

Autenticazione semplice (ad esempio banconota) o mutua (certezza reciproca).
Autenticazione a 1-2-3 fattori:

- Qualcosa che so (password)
- Qualcosa che ho (tessera bancomat)
- Qualcosa che sono (impronta digitale)

Bisogna poi fare il passaggio successivo per associare il virtuale con il reale/fisico (es. documento all'atto del rilascio delle credenziali). Associare uno userid ad una persona del mondo reale.

Non ripudio

E’ un tema prettamente giuridico, posso ripudiare la mia firma (elettronica)? Posso negarne la validità?

Vari fattori che influenzano il non ripudio:

- sintassi (è la tua firma?)
- semantica (hai capito ciò che stavi firmando?)
- volontà (hai firmato volontariamente?)
- identificazione (sei stato tu a firmare?)
- tempo (quando hai firmato?)
- luogo (dove hai firmato?)

Autenticazione, autorizzazione, identificazione

Access Control

Mandatory
Discretionary

Access control.

Discretionary (DAC): politica standard, tipica dei sistemi commerciali. Il proprietario di un oggetto decide di assegnargli i diritti di accesso voluti. Errori di utenti o applicazioni mettono a rischio il sistema.

Mandatory (MAC): Il sistema viene rappresentato in termini di subjects (processi) e objects (devices, files, sockets, …). L'amministratore definisce esplicite policy su tutti gli accessi, ossia gli usi che i subjects fanno degli objects. Complesso da gestire.

Implementazione MAC= SeLinux (kernel modificato per supportare MAC)
https://selinuxproject.org/

Enterprise backup

http://en.wikipedia.org/wiki/Backup

Salvataggio strutturato dei dati/sistemi/macchine critici per l'azienda seguendo precise policy.

Può servire per:

- Proteggere i dati da un incidente (rottura dischi, attacco informatico ecc.)
- Consentire il ripristino di situazioni stabili precedenti (recupero di file cancellati o modificati per errore, ricostruzione di una situazione al momento X, ripristino di un sistema allo stato precedente una modifica ecc.)

Non è difficile fare i backup … il difficile è fare il restore che ci interessa !

Backup=salvataggio di dati dinamici, concetto di retention

Archive=archiviazione di copia statica e perenne.

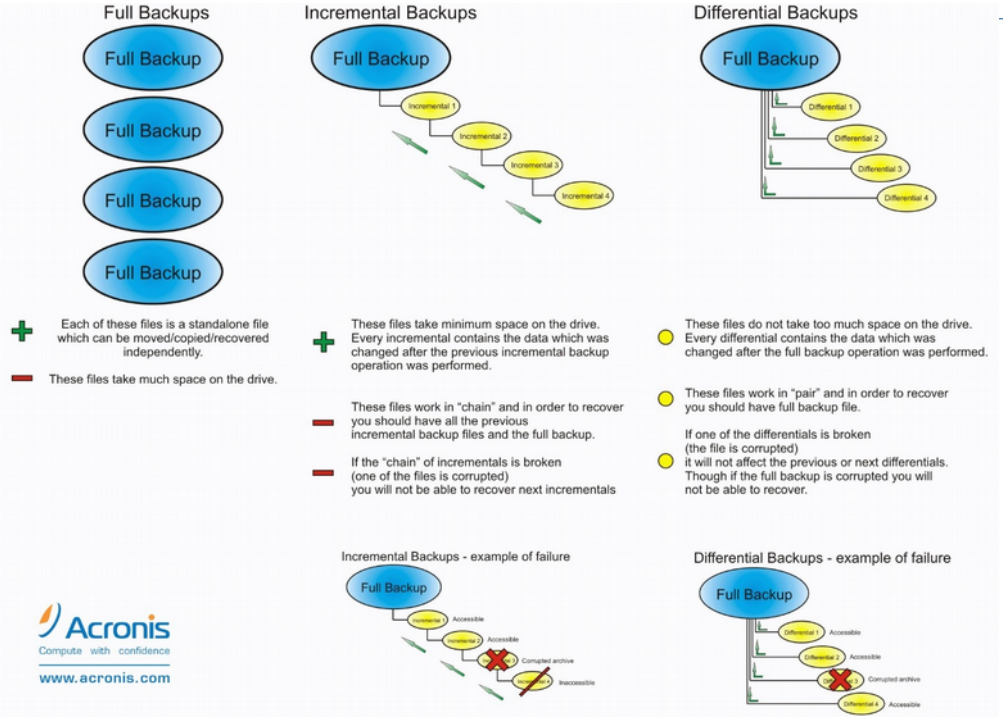
Enterprise backup

NB: Non è difficile fare i backup … il difficile è fare il restore che ci interessa!

http://en.wikipedia.org/wiki/Backup
Esempi di policy sono:

- Si effettua il backup notturno di tutti i sistemi server (non i client) e si tengono 2 copie di ciascun file; un file cancellato viene tenuto dal sistema per 60gg; settimanalmente si effettua una duplicazione dei nastri che viene trasportata e conservata in altro sito
- I database sono esportati su file ogni notte, il dump viene archiviato su nastro e l'archivio mantenuto per 15gg, cancellando a rotazione il più vecchio
- Di ogni sistema virtuale viene effettuato l'image backup differenziale ogni notte e consolidato ogni week-end; dall'insieme delle immagini differenziali accumulate durante la settimana si possono effettuare le procedure di restore

Backup e dintorni



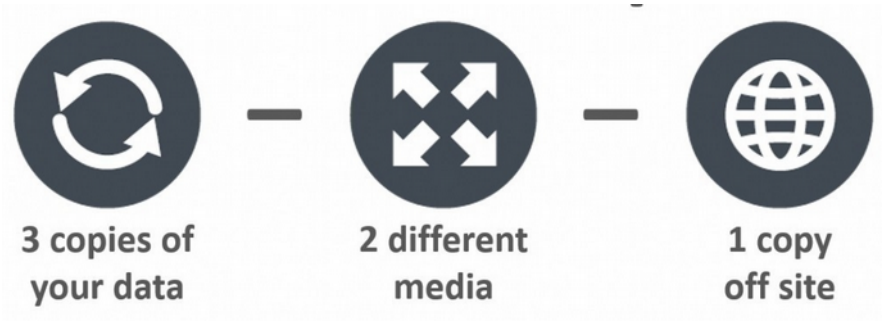
Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo 11

Backup full = salvo tutto tutte le volte

Backup incrementale = salvo quello che è cambiato dall'ultimo backup full oppure dall'ultimo incrementale

Backup differenziale = salvo quello che è cambiato dall'ultimo backup full

Backup 3-2-1



Regola del 3-2-1

Avere sempre almeno 3 copie dei propri dati: l'originale + due copie di riserva

Le copie debbono essere su almeno due media diversi (disco, nastro, CD, NAS, cloud ecc.)

Almeno una copia deve essere in un posto fisicamente distinto da quello dei dati originali (oppure nel cloud).

Business Continuity
Disaster Recovery

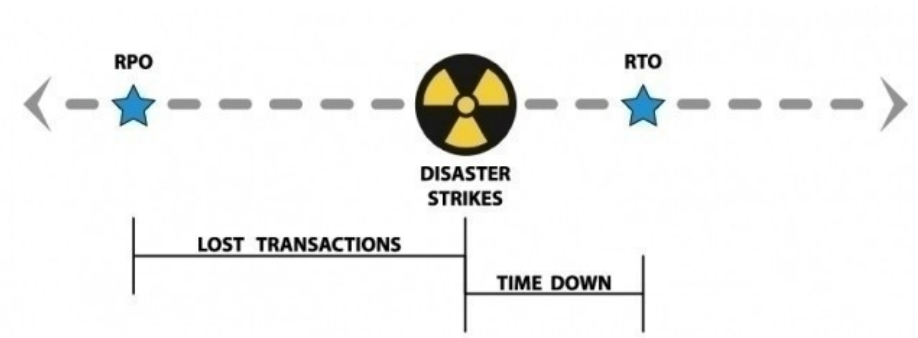
http://en.wikipedia.org/wiki/Business_continuity
http://en.wikipedia.org/wiki/Disaster_recovery

La Business Continuity non è un problema IT !

A che cosa serve infatti poter ripristinare tutte le risorse informatiche di supporto alla produzione e alla vendita se non si riescono a ripristinare le risorse primarie necessarie per svolgere queste funzioni (es. logistica, magazzino, linea di produzione)?

Per Disaster Recovery si intende normalmente il ripristino della struttura aziendale IT a fronte di un “disastro”. E' un “di cui” della Business Continuity.

RPO e RTO



RPO e RTO

Sono i parametri con cui si definiscono le performance di un sistema di backup adibito al Disaster Recovery: si riferiscono entrambi all'istante in cui avviene l'evento disastroso (perdita del sistema protetto).

Recovery Point Objective: tempo fra l'ultimo stato del sistema disponibile in una copia di backup e il momento del disastro.

Recovery Time Objective: tempo fra il momento del disastro e quello in cui il sistema alternativo comincia a essere disponibile

Sarebbe bello che fossero molto bassi ma, ovviamente, ha un costo.

Piano di Disaster Recovery

Disaster Recovery Site

L’elemento più importante di un progetto di Disaster Recovery non è tecnologico: Piano di Disaster Recovery.

Contiene la descrizione del sito di DR, le procedure necessarie per riattivare i sistemi remoti, indicando i responsabili di queste attività e i contatti delle ditte esterne da attivare (es. ISP).

Il piano di DR va mantenuto aggiornato con esplicite procedure di simulazione e test, tipicamente annuali.

Disaster Recovery Site

E’ un centro servizi remoto, dotato di sistemi, applicazioni e dati sufficienti e sufficientemente aggiornati per consentire a un’organizzazione di ripartire con le funzioni IT vitali in caso di grave disastro o indisponibilità prolungata nel tempo dei suoi sistemi principali

Esistono indicazioni sulla distanza fisica dal centro vitale IT.

Si stanno diffondendo soluzioni in cloud.

Backup e dintorni

.....

Ridondanze

Le caratteristiche di ridondanza costruttiva e di impiego dei dispositivi aumentano la sicurezza e la disponibilità dell'informazione:

- Doppia alimentazione
- Doppio allacciamento (su linee generali separate)
- Ventilazione ridondante (come numero di ventole e come controllo: sensori ecc)
- Alimentatori e ventole rimpiazzabili a caldo
- Data plane e Control plane separati (un fermo sul secondo non impedisce al dispositivo di funzionare almeno parzialmente)
- Hot/cold standby
- Ridondanza virtuale/reale
- Copie multiple dei dati
- Processi ridondati
- Data center replicati

Attenzione alle false ridondanze (es. rete mesh internet su singolo provider)

Systems & Networks Monitoring

Necessario per garantire e controllare la disponibilità dei dati.
Da non sottovalutare la sua funzione in chiave di identificazione di compromissioni della sicurezza.
E' necessario stabilire una baseline affidabile, poi ...

- Un server sta facendo traffico anomalo?
- Un client cerca di collegarsi ad altri client?
- Un client produce una quantità di traffico anomalo?
- Un utente crea numerose sessioni da/verso Internet?
- Un'applicazione varia il pattern delle sue transazioni?
- Una linea si satura improvvisamente?

Estremamente efficace nelle situazioni che richiedono una mente umana e non un algoritmo (ma vedi dopo SIEM).
Ovviamente non è semplice quanto sembra!

Intrusion Detection

- Host-based
- Network-based
- Statistical detection
- Pattern-matching detection
- Offline or online analytics

http://en.wikipedia.org/wiki/Intrusion_detection_system

Con Intrusion Detection si identificano metodologie e tecniche per scoprire attività anomale, scorrette o non appropriate nei sistemi e nelle reti.
Host-based, Network-based.
Statistical detection, pattern-matching detection, offline or online analytics.
E' necessario avere una baseline di cosa è “normale” sia sulla rete che sui server.
Autoapprendimento.
Facile avere falsi positivi o mancati rilevamenti.

Network-based IDS

Catturano il traffico che passa sulla rete.
Filtro di primo livello --> estrae il traffico da analizzare, con regole o campionamento
Secondo livello --> analizzatore (pattern matching o statistical: identifica anomalie e frequenza delle stesse)
Terzo livello --> modulo di intervento (logging, alerting)
Il traffico viene catturato tramite un adattatore di rete configurato in Promiscuous Mode (shared media) oppure collegato ad una porta di mirroring dello switch.

Monitoraggio e dintorni

Snort https://www.snort.org/
Suricata https://suricata-ids.org/
NIDS molto leggeri Open Source
Effettuano analisi e logging del traffico IP in tempo reale.
Hanno tre modi: sniffer, logger o NIDS.
L'analisi si basa sulla tecnica del pattern matching.
Quando analizza un pacchetto contenente certi pattern specificati nelle sue regole esegue l'azione ad essi associata (logging, alert…).

Host-based IDS

Fanno un auditing sistematico dei log di sistema e del filesystem.
Real-time vs scheduled auditing.
Tracciano I/O, Process, Port e Network activity.
Modulo di analisi, modulo di intervento.
I più sofisticati si agganciano oppure intercettano direttamente gli hook di sistema.

Debolezze
Intrusion Detection

Debolezze dell'Intrusion Detection

Nel tempo gli IDS si sono rivelati poco utilizzabili.

- NIDS sono come dei guardiani all'ingresso di una Banca cui è consegnato un pacco di fotografie di delinquenti: quando ne vedono uno suonano l'allarme ma lo lasciano entrare
- HIDS sono come guardiani all'interno del caveau della Banca, che controllano che il contenuto sia ancora lì, se sparisce suonano l'allarme (ma intanto è sparito)

Il danno non si può evitare, finché non si dotano i guardiani di strumenti per impedire l'intrusione.

Intrusion Prevention

- Network-based
- Wireless
- Network behavior analysis
- Host-based

http://en.wikipedia.org/wiki/Intrusion_prevention_system

Network-based intrusion prevention system (NIPS)
Wireless intrusion prevention systems (WIPS)
Network behavior analysis (NBA)
Host-based intrusion prevention system (HIPS)
Prima Detection poi Prevention (blocco delle porte sugli apparati di rete, blocco dei MAC Address, kill di processi, spostamento del traffico su LAN isolate ecc.).
Nascono grazie all'aumento della potenza di calcolo di apparati e server.
Esempio: sistema antivirus enterprise

Gestione dei log

http://en.wikipedia.org/wiki/Log_management
Spesso è l'elemento chiave per capire “cosa è successo?” oppure “cosa sta succedendo?”.
Raccolta dei log da vari sistemi chiave con aggregazione centralizzata (timestamp !).

- Per quanto tempo li tengo ?
- Debbo nasconderli agli utenti (privacy)
- Debbo proteggerli dagli attaccanti
- Debbo ruotarli
- Mi servono strumenti di analisi (in tempo reale o a posteriori)
- Mi serve una baseline (“che cosa è normale che ci sia nei miei log ?”)
- Mi servono strumenti di aggregazione e reporting

Insomma, non è semplice quanto sembra !
https://www.splunk.com/

Monitoraggio e dintorni

SIEM
Security Information & Event Management

https://en.wikipedia.org/wiki/Security_information_and_event_management

Unisce IPS+gestione dei log+logica:

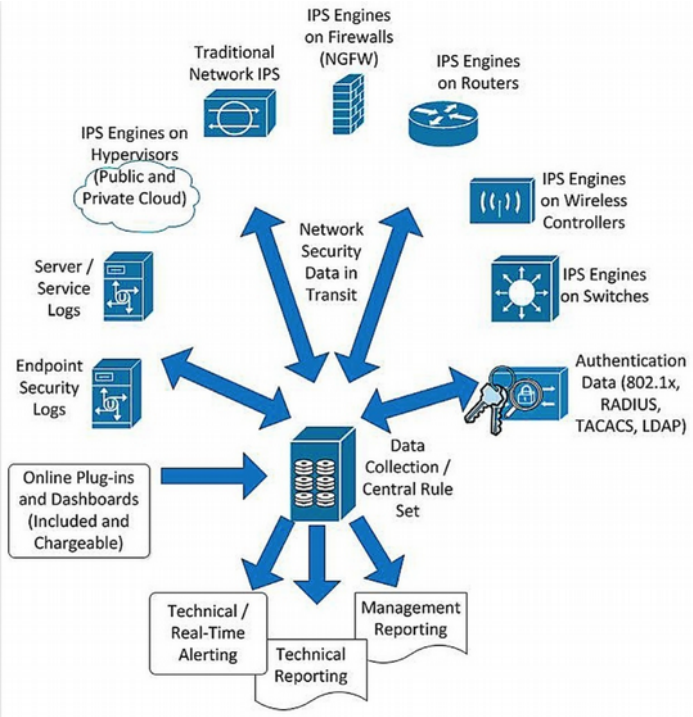
- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance (ad esempio amministratori di sistema)
- Retention
- Forensic analysis

Analisi Predittiva

https://en.wikipedia.org/wiki/Predictive_analytics

Un passo oltre il SIEM cerca di prevenire gli attacchi basandosi su informazioni e tendenze provenienti sia dall'interno che dall'esterno.
IPS ferma attacco appena iniziato, qui si cerca di identificarlo prima che cominci.
Big data, machine learning, AI ecc.
https://www.4iq.com/
Analisi comportamentali sui dipendenti/collaboratori
https://fortscale.com/ (RIP, Comperata da RSA, prodotto integrato nella loro suite)
https://www.crunchbase.com/organization/fortscale

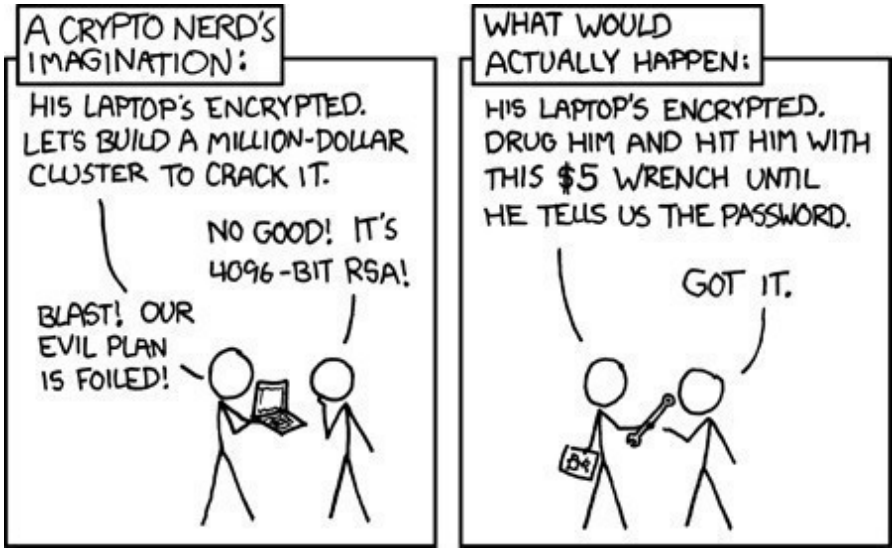
Monitoraggio e dintorni



Si tende ad un modello unico di controllo e di gestione della sicurezza.

Crittografia

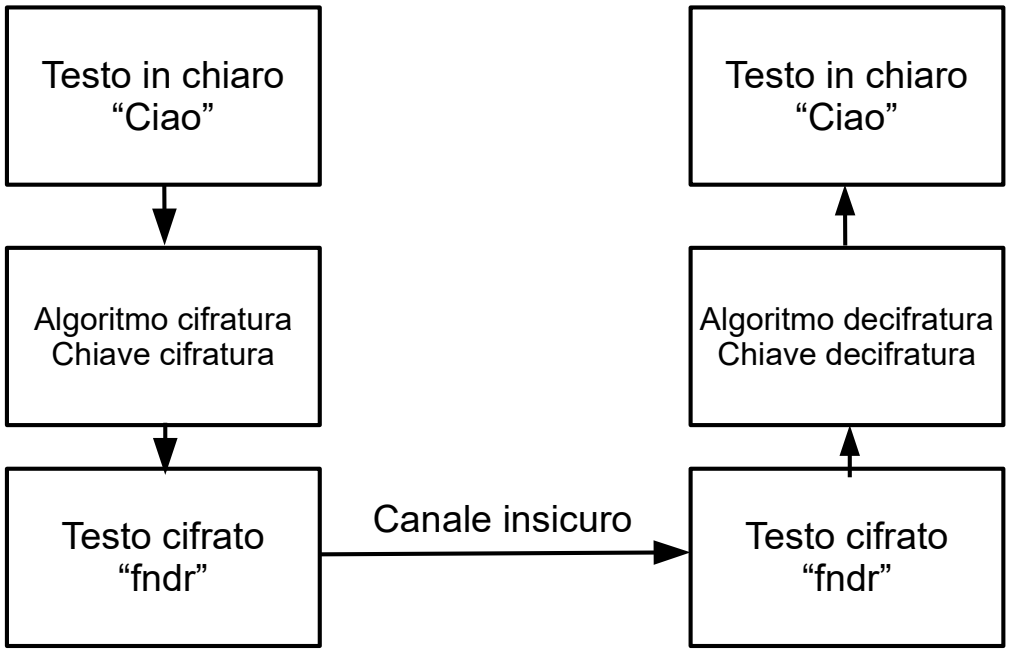
Crittografia



http://xkcd.com/538/

http://xkcd.com/538/

Crittografia



Principio di Kerckhoffs

“La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione.”

http://en.wikipedia.org/wiki/Kerckhoffs's_principle

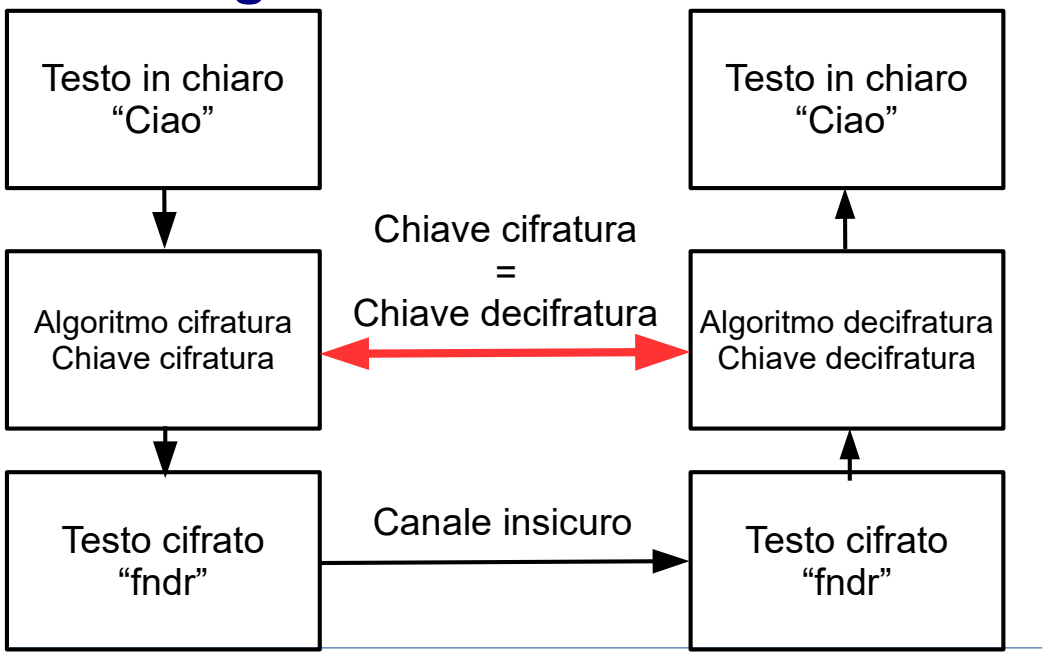
“La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione.”

“It should not require secrecy, and it should not be a problem if it falls into enemy hands”

Auguste Kerckhoffs, "La cryptographie militaire" Journal des sciences militaires, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883.

Il contrario di “Security by Obscurity”

Crittografia a chiave simmetrica



https://en.wikipedia.org/wiki/Symmetric-key_algorithm

Crittografia a chiave simmetrica

Vantaggi

- Algoritmi anche molto complessi ma veloci e con basso consumo di risorse
- Spazio delle chiavi molto ampio quindi più robusto
- Algoritmo di decifratura simmetrico a cifratura
- Sicurezza dipende solo dalla chiave
- Numero di chiavi cresce in modo esponenziale

Svantaggi

- Scambio della chiave

Esempi

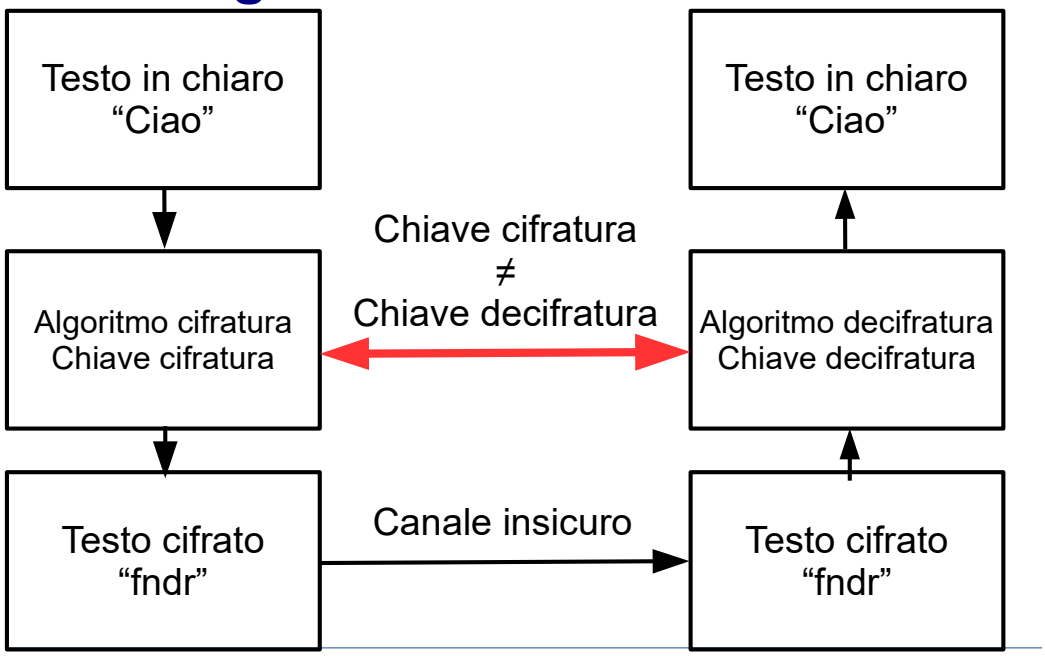
- Blowfish, 3DES

https://en.wikipedia.org/wiki/Blowfish_(cipher)

https://en.wikipedia.org/wiki/Triple_DES

20 colloqui = 19 chiavi per ogni utente = 190 chiavi da gestire (20*19/2)

Crittografia a chiave asimmetrica



https://en.wikipedia.org/wiki/Public-key_cryptography

Crittografia a chiave asimmetrica

Svantaggi

- Algoritmi molto complessi e lenti
- Spazio delle chiavi meno ampio
- Algoritmo di decifratura asimmetrico rispetto a quello di cifratura
- Introduce un ente terzo (CA)
- Numero di chiavi cresce linearmente

Vantaggi

- Lo scambio della chiave non è più un problema

Esempi

- RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

20 colloqui = 20 chiavi pubbliche e 20 chiavi private = 40 chiavi

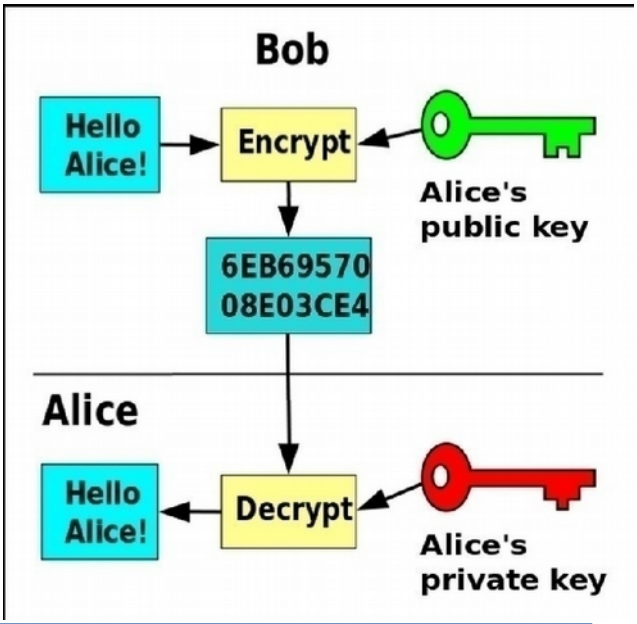
Quindi come ne esco ?

Uso l'algoritmo asimmetrico a chiave pubblica per scambiarmi la chiave segreta dell'algoritmo simmetrico, poi uso l'algoritmo simmetrico per la cifratura del resto.

Ma si capisce meglio con un esempio dal vero ...

Crittografia a chiave asimmetrica

- Coppia di chiavi
- Tecniche matematiche



http://en.wikipedia.org/wiki/Public-key_cryptography

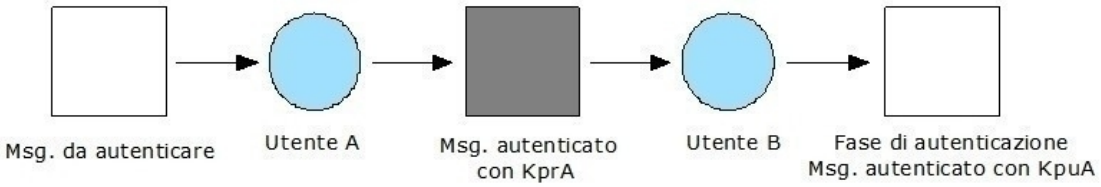
Coppia di chiavi: chiave pubblica (public key) per encryption e chiave privata (private key) per decryption

Utilizza tecniche di tipo matematico basate sulla teoria dei numeri, sulla teoria delle curve ellittiche, sull'asimmetria di alcune operazioni matematiche (es. fattorizzazione 127*157=19939) etc.

(ecco chi sono Alice e Bob, https://en.wikipedia.org/wiki/Alice_and_Bob)

Crittografia a chiave asimmetrica

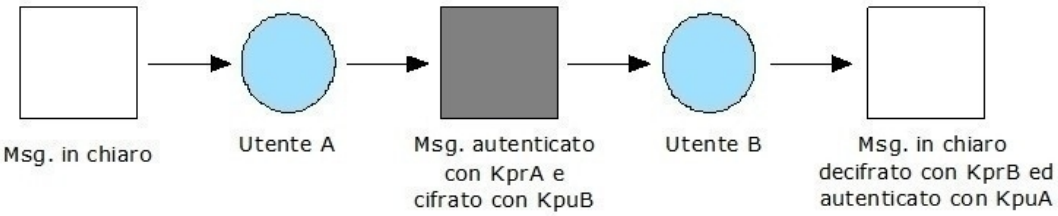
Posso usarla anche per fare autenticazione



KprA = chiave privata dell'utente A
KpuA = chiave pubblica dell'utente A

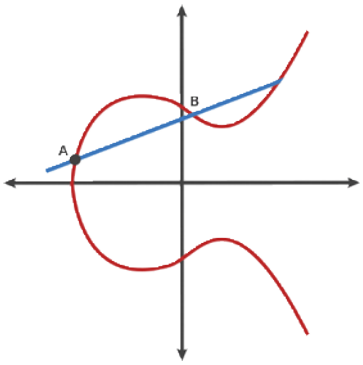
Crittografia a chiave asimmetrica

Oppure per fare autenticazione e crittografia



KprA = chiave privata dell'utente A
KpuA = chiave pubblica dell'utente A
KprB = chiave privata dell'utente B
KpuB = chiave pubblica dell'utente B

Crittografia ellittica



Crittografia ellittica (in inglese Elliptic Curve Cryptography o anche ECC). Asimmetrica.
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

A 256 bit key in ECC offers about the same security as 3072 bit key using RSA.
Starting at A:
A dot B = -C (Draw a line from A to B and it intersects at -C) Reflect across the X axis from -C to C
A dot C = -D (Draw a line from A to C and it intersects -D) Reflect across the X axis from -D to D
A dot D = -E (Draw a line from A to D and it intersects -E) Reflect across the X axis from -E to E

Public Key: Starting Point A, Ending Point E
Private Key: Number of hops from A to E
https://blog.goodaudience.com/very-basic-elliptic-curve-cryptography-16c4f6c349ed

Attacchi alla crittografia

Attacco esaustivo (o “brute force”)
→ numero tentativi pari a

$$2^N$$

Con N= lunghezza della chiave crittografica in bit.
Lunghezze ritenute “***sicure***” ***oggi***:
- Chiavi simmetriche: 192-256 bit
- Chiavi asimmetriche: 2048 bit

“Sicure” si intende a fronte di un attacco “normale” (no governi, servizi segreti, criminalità organizzata internazionale ecc.)

“Oggi” perché con i miglioramenti di hardware e software domattina potrebbe non essere più vero.

Utilizzo di GPU come potenza di calcolo per attacchi forza bruta.

Computer quantistici

Algoritmo di fattorizzazione di Shor

Fattorizzazione di un numero di 230 cifre

Computer tradizionale=1,68 anni

Computer quantistico=5,32 picosecondi

Computer quantistici in grado di cambiare completamente le carte in tavola. (descrizione out-of-scope).
Aumento esponenziale velocità con piccole operazioni altamente parallelizzabili.
Algoritmi specifici per sfruttarli al massimo: algoritmo di fattorizzazione di Shor
https://en.wikipedia.org/wiki/Shor%27s_algorithm
Servono nuovi algoritmi di crittografia: crittografia post-quantistica
https://en.wikipedia.org/wiki/Post-quantum_cryptography

Steganografia

https://en.wikipedia.org/wiki/Steganography

Steganografia è la crittografia nascosta. Se vedo un messaggio cifrato lo riconosco, obiettivo della steganografia è nascondere il fatto che ci sia un messaggio nascosto.

Affonda le radici nella storia (uovo, capelli).

Più recentemente applicata alle immagini sfruttando piccole modifiche ai bit di colore, indistinguibili all'occhio umano ma in grado di codificare un messaggio. In questo caso la chiave è l'immagine originale da cui, per differenze, ricavo il messaggio.

(immagine modificata usando OpenStego http://www.openstego.com/)

Steganografia

https://en.wikipedia.org/wiki/Steganography

Non solo immagini come vettore di trasporto, anche audio, video, pdf ecc.

https://www.darknet.org.uk/2017/07/openpuff-professional-steganography-tool/

Posso crittografare i dati prima di nasconderli, posso lavorare a più livelli (nascondo un messaggio non troppo segreto sopra ad uno più segreto in modo da fermare la ricerca dell'attaccante).

Steganografia

Document fingerprinting
(watermark nascosto)

Queste tre stringhe sono diverse
Queste tre stringhe sono diverse
Queste tre stringhe sono diverse

Posso usare la steganografia anche per fare un watermarking nascosto dei documenti (in caso di fuga dei documenti posso distinguere le diverse copie anche se apparentemente sono uguali, impronte digitali dei documenti).

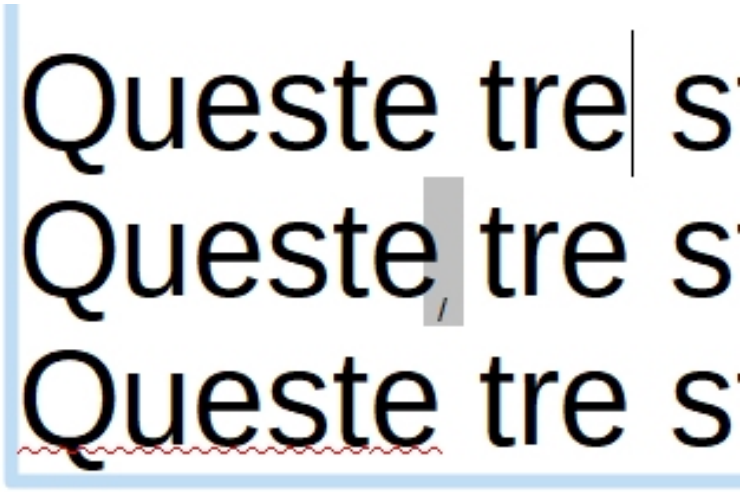
Tecniche steganografiche sulle immagini, uso di “spazi di lunghezza zero” (seconda riga dopo “queste”) oppure di caratteri di alfabeti non latini (terza riga seconda e) nei testi.

https://www.zachaysan.com/writing/2017-12-30-zero-width-characters

https://www.researchgate.net/publication/308044170_Content-preserving_Text_Watermarking_through_Unicode_Homoglyph_Substitution

http://blog.fastforwardlabs.com/2017/06/23/fingerprinting-documents-with-steganography.html

Steganografia



Posso usare la steganografia anche per fare un watermarking nascosto dei documenti (in caso di fuga dei documenti posso distinguere le diverse copie anche se apparentemente sono uguali).

Tecniche steganografiche sulle immagini, uso di "spazi di lunghezza zero" (seconda riga dopo "queste") oppure di caratteri di alfabeti non latini (terza riga seconda e) nei testi.

In alternativa posso usare minime perturbazioni della forma dei caratteri
https://www.youtube.com/watch?v=dejrBf9jW24

Certificazione della chiave pubblica

Certificato digitale

http://en.wikipedia.org/wiki/Public_key_certificate

Certificazione della chiave pubblica o più semplicemente “certificato digitale”.

E' l'associazione della chiave pubblica dell'utente alla sua identità fisica.

Unisce il mondo online con quello offline (non sempre, potrei anche certificare un'identità digitale o un indirizzo IP).

Serve un garante delle identità: Certification Authority

Le Certification Authority debbono avere una gerarchia.

Un certificato può essere revocato (CRL) sia dall'emettitore che dal richiedente.

Deve avere una scadenza temporale.

Formato dei certificati
X.509

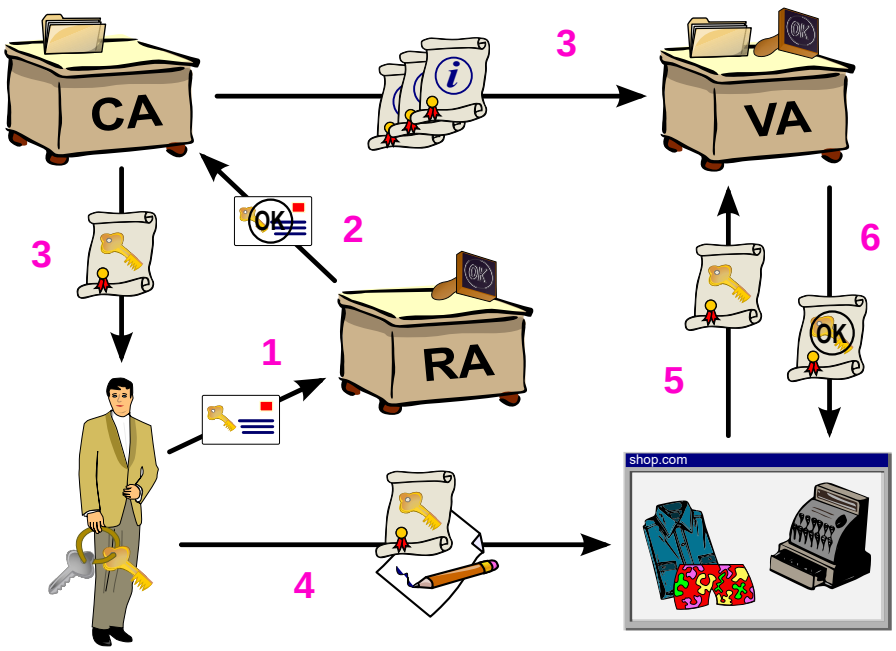
Formato standard dei certificati: X.509
http://en.wikipedia.org/wiki/X.509
Deve contenere:

- Periodo di validità
- Soggetto
- Nome dell'autorità emittente
- Chiave pubblica
- Firma digitale dell'autorità emittente

Più altri campi opzionali:

- Scopi di uso del certificato (validare sito web ecc.)
- Nomi alternativi del soggetto (esempio metto mail, IP, URL ecc.)
- Estensioni private utilizzabili, ad esempio, a livello di azienda

Certificati e firma digitale



PKI (Public Key Infrastructure)
https://en.wikipedia.org/wiki/Public_key_infrastructure
Certificate Authority (CA) Genera i certificati, garantendo la corrispondenza tra una chiave pubblica e un soggetto.
Registration Authority (RA):identifica il soggetto
Validation Authority (VA): valida il certificato al client

By Chris 論 - [1] and OpenCliparts.org, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2501151

Certificati e firma digitale

CA riconosciute nel browser.
Certificato a pagamento, dipende dal tipo, qualche centinaio di Euro/anno.
Certificati gratis per siti web: https://letsencrypt.org/
"Let's Encrypt is a free, automated, and open certificate authority brought to you by the non-profit Internet Security Research Group (ISRG)."

Motivi di revoca di un certificato prima della scadenza:
- Azienda non esiste più
• Compromissione di chiave privata
• Persa la passphrase associata alla chiave privata
• Cambio di informazioni nel certificato

Certificati e firma digitale

HACKING DEFCON 23'S IOT VILLAGE SAMSUNG FRIDGE

Posted on Tuesday, August 18th, 2015 by Pedro Venda.

pwned?

As well as running the Village this year (more challenge:

"Can you own our #IoT

As a team we're doing opportunity to work on

It was a full-on team ef here.

Se non controllo che il certificato presentato sia valido … il nemico può annidarsi ovunque … il tuo frigorifero può rivelare le tue credenziali Gmail con un attacco "Man in the Middle".

http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/

Funzioni di hash

- Da testo a stringa di lunghezza fissa
- Algoritmi unidirezionali
- Variazione produce modifica non correlabile
- Basso costo computazionale
- Non ci debbono essere collisioni
- Usato per verificare che un testo non sia stato modificato
- MD5
- SHA-*

http://en.wikipedia.org/wiki/Cryptographic_hash_function

Trasformano un testo in una stringa di lunghezza fissa (message digest o riassunto)
Algoritmi unidirezionali (è praticamente impossibile risalire dalla stringa al testo originale)
Una piccola variazione al testo originale produce una modifica non facilmente correlabile alla stringa
Basso costo computazionale
Non ci debbono essere collisioni
Usato per verificare che un messaggio/documento non sia stato modificato
Esempio: MD5 http://en.wikipedia.org/wiki/MD5
SHA-1 (old) SHA-3 (Ethereum) SHA-256 (bitcoin)
https://en.wikipedia.org/wiki/Secure_Hash_Algorithms
https://medium.com/@rauljordan/the-state-of-hashing-algorithms-the-why-the-how-and-the-future-b21d5c0440de

Funzioni di hash

Utilizzate per salvare le password sul server (meglio aggiungere un po' di sale)

Utente scrive la password, il server calcola hash della password e lo confronta con quello che ha memorizzato. Se uguali autenticazione OK. Se hash non è reversibile e non ha collisioni posso fare autenticazione sicura senza memorizzare la password in chiaro.

Se algoritmo di hash noto posso fare attacco a dizionario o a tabella (conosco tutti gli hash di quell'algoritmo).

Per evitare aggiungo un valore alla password (salt).

Per ogni utente genero un salt diverso (lungo e con caratteri poco usati). Calcolo hash=(password + salt). Memorizzo sul server: utente, hash, salt. Faccio stesso calcolo per verificare password. Password uguali hanno hash-salted diverso. Rende molto più difficili gli attacchi dizionario.

https://en.wikipedia.org/wiki/Salt_(cryptography)

Funzioni di hash

Varianti specifiche per la protezione delle password: **bcrypt**, PBKDF2

AMD Radeon HD 7970, 500$
258.7M SHA1 Hash per second

Con l'aumento delle velocità di crack gli algoritmi tradizionali (MD5, SHA*) sono diventati attaccabili anche con salt.

Meglio passare ad algoritmi più lenti da applicare ma anche molto più lenti da attaccare.

https://en.wikipedia.org/wiki/Bcrypt

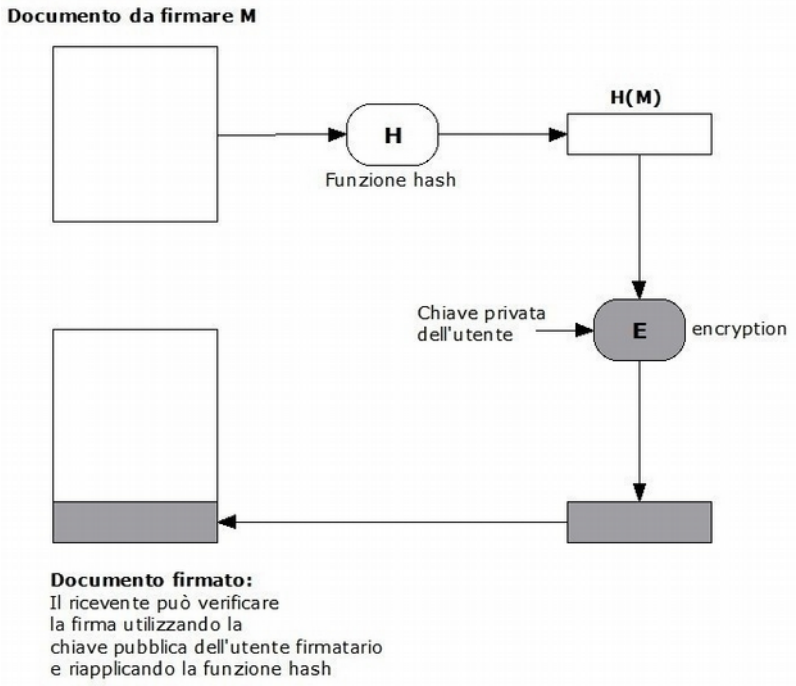
https://www.troyhunt.com/our-password-hashing-has-no-clothes/

Firma digitale

http://en.wikipedia.org/wiki/Digital_signature

Uso crittografia asimmetrica, certificati digitali e funzioni di hash per firmare digitalmente un documento.

Certificati e firma digitale



Chiave privata su dispositivo di firma sicuro a garanzia dell'"Identità digitale" (ad esempio smart card protetta da PIN).

Il documento non è crittografato, viene nascosto solo l'hash.

Decodificando l'hash con la chiave pubblica del mittente ne verifico l'identità.

Confrontando l'hash decodificato con quello calcolato verifico l'integrità del documento.

Vale anche come "non ripudio" (con tutte le cautele giuridiche del caso: volontà della firma, consapevolezza della firma).

Time stamp Protocol

Uso crittografia asimmetrica, certificati digitali e funzioni di hash + un servizio di time stamp online (TSA Time Stamping Authority, Marca temporale) per datare digitalmente un documento (ad esempio per poterne stabilire in seguito la paternità).

“La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell’Amministrazione Digitale Dlgs 82/2005).”

https://www.pec.it/marche-temporali.aspx