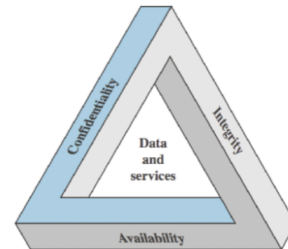


Protezione Delle Risorse

D: Quali risorse (Asset) vogliamo proteggere?

- **Hardware:** sicurezza “fisica”
- **Software:** sistema operativo e applicativi
- **Dati:** file e database
- **Reti:** collegamenti e apparati di rete



“**Proteggere**” vuol dire garantire le proprietà di *confidenzialità, integrità, disponibilità, autenticità e tracciabilità*.

Confidenzialità:

Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è tenuto a conoscere.

Integrità:

Bisogna impedire l’alterazione diretta o indiretta delle informazioni, sia dalla parte degli utenti, sia dalla parte dei processi non autorizzati, che a seguito di eventi accidentali.

(Se i dati vengono alterati è necessario fornire uno strumento per verificarlo)

Disponibilità:

Rendere disponibile a ciascun utente le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti (include prestazione e sicurezza)

Autenticità:

Ciascun utente deve poter verificare l’autenticità di un’informazione e si può richiedere di verificare se un’informazione è stata manipolata.

Tracciabilità:

Ogni azione delle entità devono essere tracciate in un modo univoco in modo tale da supportare la non-ripudiabilità e l’isolamento delle responsabilità

	Confidenzialità	Integrità	Disponibilità
HW			Calcolatore rubato
SW	Copia non autorizzata	Eseguibile modificato	Eseguibili cancellati
Dati	Lettura non autorizzata	File modificati	File cancellati
Rete	Lettura messaggi inviati	Messaggi modificati / ritardati / duplicati	Messaggi distrutti Rete fuori uso

Minacce e Attacchi

- Una **minaccia** è una possibile violazione della sicurezza
- Un **attacco** è una violazione effettiva del sistema

Gli attacchi possono essere di tipo:

Attivi: Tentativi di alterare le risorse o modificare il funzionamento dei sistemi

Passivi: Tentativi di capire le risorse e utilizzarle senza intaccare i sistemi e le risorse

Interni: Iniziati da un'entità all'interno del sistema

Esterni: Iniziati da un'entità esterna, tipicamente attraverso la rete

Classi di attacco:

Disclosure: Accesso non autorizzato alle informazioni

Deception: Accettazione di falsi dati

Disruption: Interruzione o prevenzione di operazioni corrette

Usurpation: Controllo non autorizzato di alcune parti del sistema

Principi Fondamentali

Aspetti Economici: la progettazione delle misure di sicurezza deve essere il più semplice possibile

Fail-Safe Default: i comportamenti non specificati devono prevedere un caso di default sicuro

Sorgente Pubblico: è preferito a un sorgente privato

Tracciabilità Delle Operazioni: qualsiasi operazione può essere riconosciuta in un sistema ripristinato

Separazione dei Privilegi: bisogna differenziare gli accessi alle risorse e ai file

Separazione delle Funzionalità: distinzione dei ruoli nel sistema fisico e logico

Isolamento dei Sottosistemi: un sistema compromesso non ne deve compromettere altri

Una **politica di sicurezza** è un'indicazione di cosa è e cosa non è permesso. Le regole possono riguardare dati, utenti e operazioni possibili.

Un **meccanismo di sicurezza** è un metodo (procedura) per garantire una politica di sicurezza.

- Data una politica, i meccanismi possono **prevenire, recuperare o scoprire** un attacco.

Crittografia

La crittografia è una scienza che si occupa di proteggere l'informazione rendendola sicura, in modo che se un utente ne entri in possesso non sia in grado di comprenderla.

Algoritmo Crittografico:

Un algoritmo crittografico è una funzione che prende in ingresso un messaggio e come parametro una **chiave**, e produce in uscita un messaggio trasformato.

- Cifratura: *plaintext* --> *ciphertext*
- Decifratura: *ciphertext* --> *plaintext*

→ Le chiavi possono essere **uguali**, quindi l'algoritmo è **simmetrico** (le chiavi devono essere segrete)
→ Le chiavi possono essere **diverse**, quindi l'algoritmo è **asimmetrico** (una chiave è pubblica e una è privata)

Robustezza Crittografica:

→ **NON** deve essere possibile dato un testo cifrato risalire (facilmente) al testo in chiaro
→ **NON** deve essere possibile dato un testo cifrato e decifrato, risalire alla chiave

In generale, nessun algoritmo crittografico è completamente sicuro, si dice quindi che un **algoritmo crittografico è computazionalmente sicuro se:**

- Il costo per decifrarlo è superiore al valore dell'informazione cifrata
- Il tempo di decifratura è superiore al tempo di vita dell'informazione cifrata

Crittoanalisi:

La crittoanalisi tenta di decifrare un testo senza conoscere la chiave di decifratura. L'attacco più banale è il *Brute-Force*.

Principio di Kerckoffs : la segretezza deve essere nella chiave e non nell'algoritmo!

Crittografia Simmetrica

La **crittografia simmetrica**, detta anche crittografia a chiave segreta, utilizza una chiave comune e il medesimo algoritmo crittografico per cifrare e decifrare la risorsa.

Due utenti che desiderano comunicare con la crittografia simmetrica devono concordarsi su che algoritmo e chiave usare (*la chiave deve essere scambiata su un canale sicuro*)

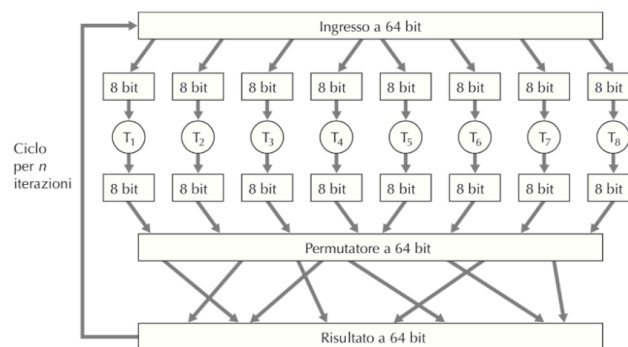
Alcuni Algoritmi Simmetrici:

- **Cifrario di Cesare**
- **Cifratura Monoalfabetica**
- **Cifrari a Blocchi:**

Sono usati in molti protocolli sicuri di Internet, compreso PGP (posta elettronica), SSL (connessione TCP) e IPSec (trasmissione a livello di rete). Sono anche chiamati cifrari a flusso.

→ Dati K bit, 2^K ingressi vengono permutati

→ Le permutazioni possono essere combinate per creare schemi più complessi



DES (Data Encryption Standard) [56 bit] :

DES è il più noto algoritmo crittografico simmetrico. Utilizza chiavi a 56 bit ed è ormai considerato obsoleto.

TRIPLO-DES [112 – 168 bit] :

Per aumentare la sicurezza del DES, si triplica in cascata l'algoritmo con chiavi diverse. Esistono due varianti:

- Con chiave da 112 ($\times 2$)
- Con chiave da 168 ($\times 3$)

AES (Advanced Encryption Standard) [128 – 192 – 256]

Negli **algoritmi simmetrici** la chiave è la stessa in cifratura e decifratura. Deve quindi essere segreta e deve essere scambiata su un canale sicuro. Per questo **Diffie** e **Hellman** propongono uno schema che supera questa limitazione: crittografia a chiave pubblica (asimmetrica)

Crittografia Asimmetrica

Nella crittografia **asimmetrica** ogni utente ha una chiave pubblica e una privata: la chiave pubblica viene resa nota, mentre quella privata deve rimanere segreta.

→ La risorsa viene cifrata con la **chiave pubblica** del destinatario, il quale dovrà usare la propria **chiave privata** per decifrarlo

Vantaggi:

- Non è più necessario incontrarsi per scambiare le chiavi
- La stessa chiave pubblica può essere usata da più utenti

Requisiti:

- La generazione della chiave privata e pubblica deve essere semplice
- L'operazione cifratura e decifratura deve essere semplice quando è nota la chiave
- Deve essere computazionalmente impossibile ricavare la chiave privata da quella pubblica
- Deve essere computazionalmente impossibile ricavare il testo in chiaro avendo il testo cifrato e la chiave pubblica

Algoritmo RSA

RSA è un algoritmo che si basa sulla difficoltà di **scomporre un numero in fattori primi**. La chiave ha di solito dimensioni di 2^{10} bit (*300 cifre decimali*).

→ Il bruteforce su RSA non prova tutte le chiavi possibili, ma prova solo a fattorizzare il prodotto di numeri primi.

Come funziona:

Scelti due numeri primi p, q si calcola:

- $n = p \cdot q$
- $z = (p-1) \cdot (q-1)$
- un numero $1 < e < n$ relativamente primo a z
- un numero d tale che $(e \cdot d - 1)$ sia multiplo di z

[...]

Sintesi Algoritmi Asimmetrici:

- Richiedono molte risorse computazionali (dalle 100 alle 1000 volte più lenti dei simmetrici)
- Vengono utilizzati per scambiare le chiavi di sessioni (simmetrici)
- Con RSA ciò che viene cifrato con la chiave pubblica può essere decifrato con la chiave privata ma anche l'incontrario! In questo modo si può garantire l'autenticità

Integrità E Autenticazione

L'obiettivo crittografia è garantire la privacy

L'integrità garantisce che un messaggio non sia stato modificato da terzi. Per fare ciò ci appoggiamo alle funzioni HASH.

Funzioni HASH:

Le funzioni HASH permettono di risolvere il problema di autenticità e integrità del messaggio. Se un utente mi invia un messaggio come faccio a sapere che è suo?

Una **funzione hash** trasforma un qualsiasi messaggio in una lunghezza predefinita (*digest*)

Per stabilire la sicurezza, le condizioni gli algoritmi che eseguono hashing devono avere:

- **Coerenti:** Input uguali devono corrispondere ovviamente ad output uguali
- **Casuali** (o apparire tali): bisogna impedire l'interpretazione del messaggio originale
- **Univoci:** due messaggi non dovrebbero generare lo stesso *digest*
- **Non Invertibili:** non deve essere possibile risalire al messaggio originale

Gli HASH **non invertibili** vengono di solito utilizzati per assegnare un'**impronta digitale** alle risorse.

Le funzioni HASH più comuni sono MD5 e SHA. *E' possibile offrire Autenticità senza scambiare la chiave?* Sì grazie agli algoritmi asimmetrici: **firma digitale**

Autenticità: Firma Digitale

E' l'equivalente informatico di una firma convenzionale, generalmente non ripudiabile

Nella crittografia asimmetrica on si cifra l'intero messaggio con gli algoritmi asimmetrici, ma si usano per scambiare la chiave di sessione (di un alg. simmetrico) e poi utilizzo la chiave appena creata per andare a cifrare il messaggio. Questo però non permette di confermare l'autenticità. Per essere sicuri che il mittente sia quello pensato si utilizza la firma digitale.

Si utilizza la cifratura asimmetrica nel senso inverso:

Ad esempio, in RSA viene utilizzato nel seguente modo:

- L'algoritmo di cifratura diventa l'algoritmo di verifica
- L'algoritmo di decifratura diventa l'algoritmo di firma

→ Firmare l'intero documento diventa oneroso, quindi si firma l'HASH del documento

Non è garantito che l'utente che si dichiara bob, sia realmente bob. Per risolvere si utilizza il **certificato elettronico**: associa la chiave pubblica e privata univocamente a un'identità. Il certificato viene rilasciato dalla **CA** (*Certification Authority*)

Autenticazione

E' un processo che avviene tra due interlocutori

Gli interlocutori possono essere utenti o computer dove la proprietà primaria è la richiesta di un **corretto controllo di accesso**.

Tipologie di autenticazione:

- **Locale:** l'utente accede in locale al servizio che effettua l'autenticazione. (*i.e. acceso allo smartphone*)
- **Diretta:** l'utente accede da remoto al servizio che effettua l'autenticazione. (*i.e. accesso alle macchine del laboratorio Delta*)
- **Indiretta:** il servizio di autenticazione è separato
- **Offline:** i certificati elettronici

Fattori di autenticazione:

- **Conosce** (PIN, password, ...)
- **Possiede** (carta, tessera, ...)
- **E'** (impronta digitale, iride, ...)

#Autenticazione: Qualcosa che si conosce: **username e password**

Vantaggi	Svantaggi
<ul style="list-style-type: none">- Semplice- Economico- Non richiede di salvare dati (client)	<ul style="list-style-type: none">- Password deboli scelte dall'utente- Metodi di autenticazione deboli

Gli attacchi possibili alle password possono essere:

- Intercettazione (MITM/Sniff)
- Cracking (Brute Force)
- Social Engineering, Trojan, Keylogger, ...

#Autenticazione: Qualcosa che si possiede: **One Time Password**

One Time Password è un sistema in cui viene generata una password ogni volta per evitare il problema dell'intercettazione. Le password "monouso" vengono generate seguendo un contatore o l'istante temporale.

Altri esempi:

- Smart Card
- Carte Magnetiche

Spesso queste si combinano con dei PIN.

#Autenticazione: Qualcosa che si è:

E' il possesso di caratteristiche univoche che forniscono l'autenticità:

- **Fisiche**: impronta digitale, iride, ...
- **Comportamentali**: firma, timbro della voce, scrittura, ...

Punto debole:

- Misure imprecise basate su dei template
- Possibilità di falsi positivi e falsi negativi

Autenticazione DIRETTA:

Le modalità di autenticazione viste fin ora si possono usare in **locale**, se l'autenticazione viene da **remoto** (*autenticazione diretta*) ci possono essere altri problemi: un intruso potrebbe intercettare e registrare le informazioni (*MITM*)

Soluzione: l'autenticazione viene su un canale sicuro, oppure si aggiunge una “*sfida*”.

Autenticazione INDIRETTA:

Le informazioni degli utenti vengono salvati su in sistema unico, e viene offerto anche ad altri servizi per autenticare. Due esempi di autenticazione indiretta sono:

- **RADIUS** (*Remote Authentication Dial in User Service*) nato per accesso remote dial-up
- **Kerberos** utilizzato per l'autenticazione *Single Sign-On (SSO)* all'interno di un dominio amministrativo.

Autenticazione OFF-LINE:

E' basata sui certificati: emessi da un'**autorità di certificazione (CA)** e distribuiti da un'infrastruttura a chiave pubblica (**PKI**).



Autorità di Certificazione (CA)

I 10 compiti di una CA

- 1) Identificare con certezza la persona fisica che fa richiesta della chiave pubblica
- 2) Rilasciare e rendere pubblico il certificato
- 3) Garantire l'accesso telematico al registro delle chiavi pubbliche
- 4) Informare i richiedenti sulle tecniche di accesso e di registrazione
- 5) Dichiarare la propria politica di sicurezza
- 6) Attenersi alle norme sul trattamento dei dati personali
- 7) Non rendersi depositario delle chiavi private
- 8) Procedere alla revoca in caso di problemi con l'intestatario
- 9) Rendere pubblica la revoca e sospensione delle chiavi
- 10) Assicurare una corretta manutenzione delle chiavi pubbliche

Come ottenere un certificato digitale:

- 1) L'utente genera una **coppia di chiavi**
- 2) L'utente **invia alla CA una richiesta di certificato** insieme alla chiave generata (a meno che non sia la CA che ha generato le chiavi)
- 3) **La CA autentica l'utente** chiedendoli di recarsi allo sportello *LVP (Local Validation Point)* collegato con la CA
- 4) Quando è verificata l'autenticità **la CA emette il certificato** e lo invia al richiedente tramite posta elettronica e inserisce la chiave nel registro delle chiavi pubbliche

L'intera procedura accade nell'ambito di una **PKI (Public Key Infrastructure)**

PKI

Public Key Infrastructure

La struttura mini ma è **CA+LVP**. Si può avere una struttura gerarchica di chiavi pubbliche:

- E' una struttura ad albero
- La root certifica le CA di primo livello
- Le primo livello certificano le CA di secondo livello
- Le CA di ultimo livello certificano l'utente

Utilizzo dei certificati:

- Bob invia ad Alice il certificato firmato dalla CA
- Alice controlla la firma ed estrapola la chiave pubblica di Bob
- Alice ha la chiave pubblica di bob garantita dalla CA

Problemi dei Certificati:

- E' necessario ottenere in modo sicuro il certificato dalla CA per controllare la firma
- Un certificato può essere revocato, ma il match della firma può avere comunque successo
- Il sistema implica una fiducia nella CA, ma chi lo garantisce?

Problemi comuni a tutti gli schemi:

Alice vuole inviare una coppia di chiavi pubblica e privata, ma:

- Come la **genera**?
- Come la **conserva**?
- Come la **trasporta**?

Autorizzazione: Controllo degli Accessi

Garantisce che il servizio sia limitato a solo a chi ne ha diritto

- Le **politiche** di accesso definiscono l'attribuzione dei privilegi sugli oggetti
- I **meccanismi** di accesso definiscono come le relazioni tra i soggetti e gli oggetti sono rappresentati

Due principi utili:

- **Privilegio minimo**: Ad un soggetto dovrebbero essere concessi solo i privilegi minimi necessari a compiere l'azione che deve compiere
- **Separazione dei compiti**: Nessun soggetto dovrebbe avere abbastanza potere per sovvertire il sistema

Meccanismi di controllo dell'accesso:

- Matrice di controllo: nelle righe ho i soggetti, nelle colonne gli oggetti, e nel contenuto i permessi.
- Ho problemi di scalabilità: Posso raggruppare la matrice per righe e colonne e i permessi in modo omogeneo.

ACL (Access Control List):

Memorizzo la matrice di accesso per colonne. Ciascuna risorsa viene memorizzata con la lista dei soggetti che possono interagire con essa. (es. file system unix)

→ Sono adatte in un contesto in cui la protezione è **orientata ai dati**: è semplice gestire gli accessi a un oggetto

→ Non sono adatte se voglio gestire centralmente i dati e introdurre meccanismi di delega.

Politiche di controllo dell'accesso:

Si distinguono in:

- **DAC**: Discretionary Access Control
- **MAC**: Mandatory Access Control

Gli accessi possono essere combinati con una suddivisione di utenti e ruoli:

- Un gruppo è una lista di soggetti
- Un ruolo è un insieme prefissato di permessi di accesso

DAC

In un modello *DAC* gli utenti possono a loro discrezione concedere e revocare i permessi sugli oggetti sotto il loro controllo

- Ogni oggetto ha un proprietario e il soggetto ne definisce i permessi di accesso
- Il DAC è flessibile e usato in diversi contesti
- Il DAC non permette di controllare la diffusione delle informazioni

MAC

In un modello *MAC* la politica di accesso è determinata centralmente dal sistema, utilizzato ad esempio in ambito militare

i.e. nel modello Bell-LaPadula, il sistema segue le seguenti regole:

- **No read-up:** non è possibile leggere informazioni dei livelli più alti rispetto al proprio
- **No write-down:** non è possibile scrivere informazioni nei livelli più bassi al proprio

Il MAC è meno flessibile, ma più robusto del DAC.

Firewall

I **firewall** di rete sono apparecchiature o sistemi che controllano il flusso del traffico tra due reti con diversi livelli di sicurezza:

- Per prevenire accessi non autorizzati a una rete privata
- Per prevenire l'esportazione di dati dall'interno all'esterno
- Schermare alcune reti interne da nascondere ad altri
- Bloccare alcuni accessi e/o servizi a degli utenti
- Monitorare (e logging)

Problemi del firewall:

- Gli attacchi possono arrivare dall'esterno ma anche dall'interno di una rete
- Non difende da bug non aggiornati nei protocolli
- I filtri sono difficili da impostare e mantenere, sono un difficile compromesso tra libertà e sicurezza
- Può degradare le performance della rete

Default Deny	Default Permit
<u>Tutto quello che non è espressamente ammesso è proibito:</u> <ul style="list-style-type: none">- I servizi sono abilitati caso per caso dopo un'analisi- Gli utenti sono molto ristretti	<u>Tutto quello che non è espressamente proibito è ammesso:</u> <ul style="list-style-type: none">- Il sys admin deve procedere velocemente ogni volta che appare un bug nel protocollo- Vengono aggiunti/rimossi servizi quando vengono scoperti pericolosi- Gli utenti sono meno ristretti

I firewall si suddividono in 3 tipologie:

- Packet Filtering Router (1° Gen)
- Statefull Inspection (2° Gen)
- Gateway a liv. di applicazione (o gateway) (3° Gen)

I filtri a **livello 3** sono:

- Source e destination del pacchetto IP
- Tipo di traffico (IP, ICMP, ...)
- Possibilmente anche alcune caratteristiche di liv. 4 (porta sorgente e destinazione)
- Alcune volte informazioni del router (i.e. interfacce di sorgente e destinazione)

Vantaggi del firewall:

- E' trasparente (non ostacola il normale utilizzo della rete)
- Poco costoso
- E' disponibile in molti router

Svantaggi:

- Può avere bug, e può essere difficile da configurare

STATEFULL PACKET FILTERING:

→ Quando viene stabilita una connessione, se le regole di filtraggio non la bloccano, le informazioni relative ad essa diventano delle entry in una tabella di stato.

→ I successivi pacchetti saranno valutati in base all'appartenenza di una delle connessioni appartenenti alla tabella.

→ Quando la connessione viene chiusa, la entry viene eliminata.

Vantaggi	Svantaggi
<ul style="list-style-type: none">- Rapporto prestazioni/sicurezza buono perché non effettua troppi controlli sulla connessione- Protegge da IP Spoofing (non si limita a controllare il singolo IP o porta)	<ul style="list-style-type: none">- Difficile da testare il firewall- Mancano tutti i servizi aggiuntivi a liv. applicativo

I filtri a **livello 7** sono:

- Il routing tra due interfacce è effettuato dal sw del firewall
- C'è la possibilità di *authentication* (U/Pwd, HW/SW, biometric, ...)
- Si possono eseguire i filtri sui comandi (es blocco la *GET*)

Vantaggi	Svantaggi
<ul style="list-style-type: none">- Più sicuri del packet filter- Deve solo controllare un numero limitato di applicazioni (http, ftp...)- Log facile, idem controllo del traffico	<ul style="list-style-type: none">- Overhead su ogni connessione- Posso controllare solo un numero limitato di applicazioni

PROXY SERVER DEDICATI:

→ Sono specifici per ogni applicazione

→ Aiutano il proxy gateway nell'inspection

→ Il loro tipico uso è per

- Antivirus
- Codice malevolo
- Web Proxy, Email Proxy

PERSONAL FIREWALL:

→ Proteggono solo la macchina di dove sono installati

→ Necessario, specie per i mobile users

IDS *Intrusion Detection System*

E' uno strumento sw, o hw, che automatizza il processo di monitoraggio impiegato per individuare eventi che rappresentano un'intrusione non autorizzata

→ Si può fare a livello di host (**HIDS**) e a livello di network (**NIDS**)

IDS vs FIREWALL:

IDS può essere visto come un sistema di antifurto, cioè rilevare delle intrusioni, mentre il Firewall può essere visto come una porta blindata che serve per bloccare le eventuali connessioni

→ Un IDS perfetto può individuare tutte le **reali** intrusioni.

Principali problemi sono:

- Falsi positivi: IDS rileva un'anomalia, ma non ci sono problemi
- Falsi negativi: IDS non rileva un'intrusione avvenuta

Requisiti per un IDS ottimale:

- Scoprire una ampia gamma di intrusioni conosciute e non
- Scoprire un'intrusione in tempo reale
- Presentare un report semplice e comprensibile, ma accurato

Principio di Base:

→ Distinguo le situazioni normali da quelle anormali

→ L'utente in condizioni normali si comporta in un modello prevedibile: non compie azioni che compromettono la sicurezza e i suoi processi sono protetti dai permessi

Modelli per l'IDS:

- Detection di anomalie: delle sequenze di azioni non normali possono presentare un'intrusione
- Detection di uso malevolo: Si conosce quali sequenze possono essere malevole
- Detection in base alle specifiche: Si conoscono intrusioni in base a delle conseguenze

→ I modelli possono essere statici o adattivi

DETECTION DI ANOMALIE:

Si analizzano insiemi di caratteristiche del sistema confrontando i valori con quelli attesi segnalando quando non sono uguali:

- Metriche a soglia
- Momenti statici
- Modelli di Markov

METRICHE A SOGLIA:

→ Conta il numero di volte che un evento si presenta: ci si aspetta da m a n eventi, se sfiora c'è un'anomalia. **Problema**: è difficile trovare l'intervallo perfetto. (es. utenti francesi che usano la tastiera americana per effettuare il login su windows)

MOMENTI STATICI:

L'analizzatore calcola i due momenti, se sono fuori di un certo intervallo c'è un'anomalia.

MODELLI DI MARKOV:

Ipotesi: la storia passata influenza il prossimo passo. Le anomalie sono riconosciute da delle sequenze di eventi e non dalla frequenza degli eventi.

→ Il sistema deve essere addestrato per rilevare queste sequenze:

- L'addestramento è svolto con utenti non anomali
- Più ho dati, più è efficace
- I dati dovrebbero coprire tutte le sequenze di sistema

DETECTION USO MALEVOLO:

Si controlla se una sequenza di istruzioni da eseguire è già nota al sistema come malevola. Non posso ricoprire intrusioni non note in precedenza.

DETECTION IN BASE ALLE SPECIFICHE:

Si determina se una sequenza di azioni viola una specifica di come programma dovrebbe funzionare.

Architettura di un *IDS*

E' un sistema di auditing sofisticato (verifica sofisticata). Ha 3 attori principali:

- **AGENTE** (*logger*):
 - o Ottiene le informazioni e le invia al direttore
 - o Può mettere le informazioni in altri modi
 - o Può cancellare informazioni non necessarie
 - o Il direttore può richiedere all'agente maggiori informazioni
 - o Si distinguono in agenti host e agenti network
- **DIRETTORE** (*analizzatore*):
 - o Collezione le informazioni ricevute
 - o Analizza le info. Per determinare se si è sotto attacco
 - o Gira su un sistema separato
- **NOTIFICATORE** (*esecutore*):
 - o Ottiene i risultati dal direttore
 - o Prende le decisioni appropriate (Notifica, Riconfigura, Risponde all'attacco)

Combinazione *DIDS*

Il monitoraggio dell'host e della network non sempre è sufficiente:

- Mallory fa attacchi con telnet: IDS di rete lo rileva, di host no.
Mallory fa attacchi senza la password: IDS di host lo rileva, di rete no

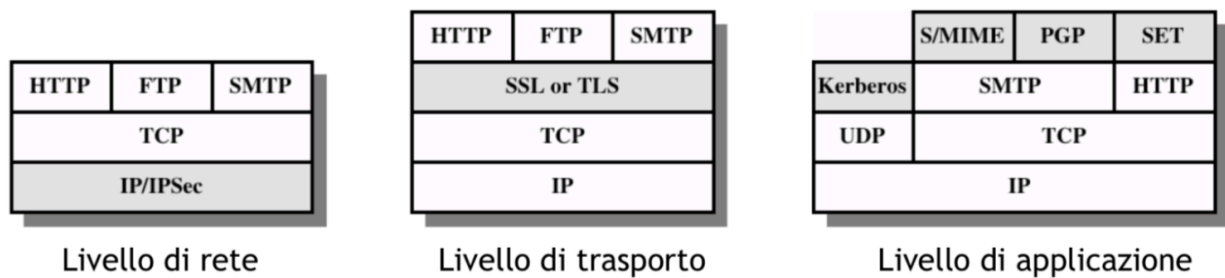
DIDS usa gli agenti host e un monitor di rete per controllare.

Risposte Agli attacchi:

→ L'attacco deve essere scoperto prima del completamento.

→ Una tecnica è il *jailing*: far credere all'attaccante che il suo attacco è andato a buon fine e limitarlo in una zona limitata.

Scurezza nello stack protocollare TCP/IP



A livello applicativo:

Ogni applicazione implementa già all'interno della sua logica la sicurezza. I messaggi di livello applicativo che vengono generati sono già cifrati. Il TCP quindi quando riceve i dati, non gli interessa la semantica (significato) e non ne capisce il contenuto perché è già cifrato.

Chi sviluppa l'applicazione si prende in carico di sviluppare anche la parte legata alla cifratura (può essere oneroso e inutile inglobare un algoritmo di cifratura già esistente in ogni applicazione differente)

A livello di trasporto:

A livello di trasporto il messaggio è già cifrato con SSL o TLS, quindi TCP non vede il contenuto (e non gli interessa), ma questo strato è utilizzato da più di un'applicazione per rendere più sicura la connessione (i.e. HTTPS); quindi il protocollo a liv. Applicativo non cambia, è uno in più strato che cifra i dati in mezzo.

A livello di rete:

Fa la cifratura avviene direttamente a livello del pacchetto IP. Se la cifratura la faccio a livello di trasporto, significa che quando viaggia sulla rete, oltre all'*header IP* chi intercetta il pacchetto riesce a leggere anche parte del pacchetto del contenuto *payload* del pacchetto IP e quindi vede parte del pacchetto TCP.

Per ovviare a ciò si cifra a livello IP (ci sarà l'*header IP* perché è necessario), ma c'è subito dopo un secondo header che è dell'*IPSEC* che contiene le informazioni utilizzate per la cifratura e da lì in poi è cifrato (e quindi non vedo le porte usate a liv. di trasporto)

A livello di collegamento (i.e. WLAN):

Viene cifrato il pacchetto usato nelle Wireless Lan, si cifra solo il tratto condiviso dall'host all'AP, (si fa solo in casi particolari come questo).. si possono anche combinare le cifrature dei liv. Superiori.

Sicurezza delle e-Mail

Livello Applicativo

Perché ci interessa?

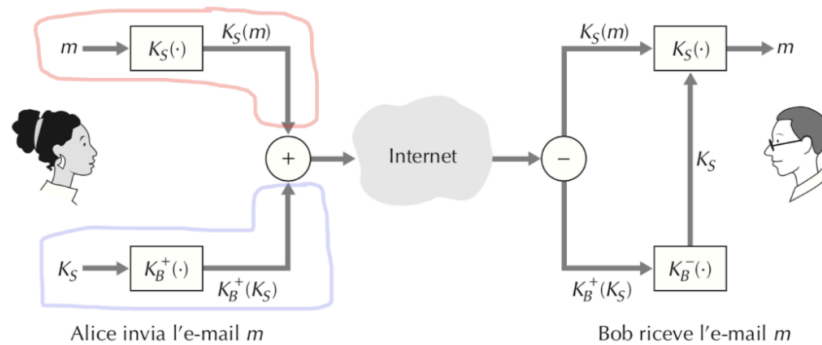
Perché la cifratura può garantire l'autenticazione del mittente, del destinatario, farla leggere solo al destinatario o garantirne l'integrità. Per poter ottenere queste proprietà si applicano i meccanismi seguenti:

Esempio Cifratura Delle Email Garantendo Le (4) Proprietà

Step 1: Alice utilizza una chiave simmetrica, K_S , per inviare una e-Mail a bob:

K_S è la simmetrica chiave di sessione (usata per quello specifico messaggio)

K_b è chiave asimmetrica pubblica del destinatario (viene usato per cifrare la K_S)



- (rosso) Alice cifra il messaggio con una chiave K_S , in questo modo ottiene il messaggio cifrato
- (blu) Alice cifra la sua chiave di sessione K_S con la chiave pubblica di bob K_b , in questo modo cifra la sua chiave di sessione e solo Bob con la chiave privata potrà decifrare la chiave di sessione K_S per decifrare poi il contenuto del messaggio.

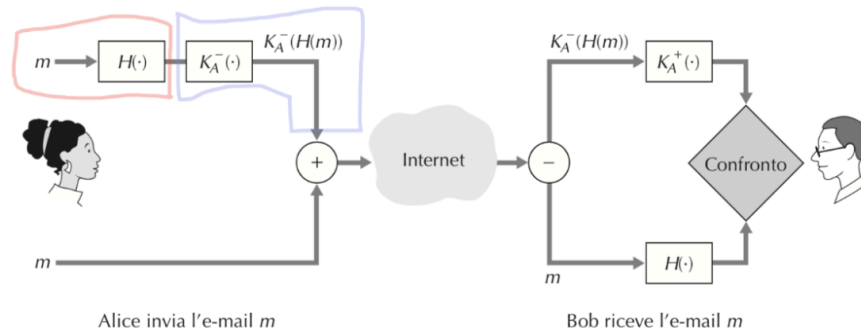
Il tutto viene poi unito e inviato a Bob

- Non ho integrità del messaggio e autenticazione del mittente. Garantisco solo la sicurezza e l'autenticazione destinatario

Step 2: Alice utilizza una funzione *HASH* e firma digital per garantire l'autenticità del messaggio:

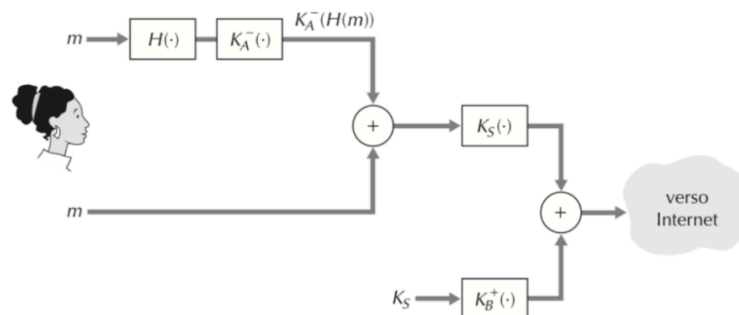
***H** è la funzione di HASH per garantire l'integrità*

***Ka** è la chiave privata di Alice*



- (rosso) Alice utilizza una funzione di HASH per garantire l'integrità del messaggio.
- (blu) Alice cifra il risultato della funzione di HASH con la sua chiave privata Ka per garantire l'autenticità.

L'unione di questi due step permette ad Alice di inviare una e-Mail a Bob garantendo le (4) proprietà della sicurezza:



PGP

Pretty Good Privacy

PGP stato implementato fine anni '90 e poi reso disponibile come software libero ed è lo schema citato sopra.

Un problema riscontrato in *PGP* è che *SMTP* è un protocollo testuale, quindi non posso inviare i binari che ottengo con le funzioni di cifratura e devo trasformare il contenuto di *PGP* in testo. (Risolvo ciò con conversione a base64)

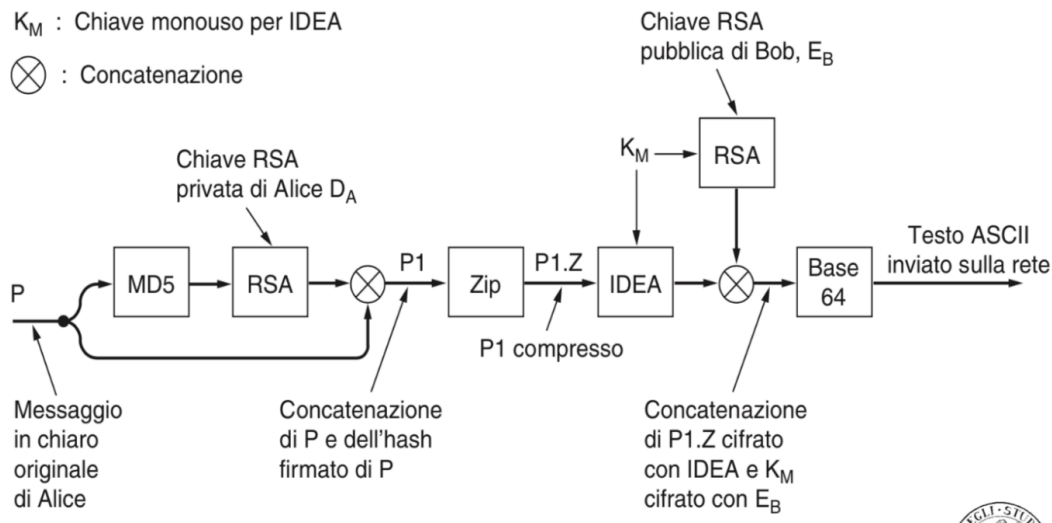
[base64]

Ho 64 simboli: a-zA-Z0-9+/. ... Dato un file binario come input lo divido in gruppi da 6 bit e gli traduco in caratteri

I servizi che PGP offre sono:

- Autenticazione (*SHA-1*, *RSA*, *firme*)
- Confidenzialità (*CAST*, *IDEA*, *triplo-DES*)
- Compressione
- Codifica per compatibilità (*Radix-64*)
- Segmentazione

Esempio funzionamento PGP:



PGP si basa anche l'uso della fiducia:

- L'utente assegna un livello di fiducia ad ogni utente e intermediario
- PGP assegna un livello di fiducia nell'abbinamento chiave-utente

SSL / TLS

Sicurezza livello di trasporto

SSL & TLS offrono confidenzialità e integrità. SSL è stato principalmente stato progettato per rendere sicure le transazioni nella rete, poi è diventato uno standard con TLS.

Handshake SSL/TLS:

La fase di handshake prevede ad

- Autenticare (*se richiesto*) solo il server o anche il client
- Accordare le parti su che algoritmi cifrari usare
- Generare le chiavi di cifratura da usare

Wireless LAN

Sicurezza livello di collegamento

WEP: Wired Equivalent Privacy (802.11)

È un protocollo utilizzato per proteggere le reti wireless e fornisce una minima autenticazione per evitare che chiunque si collegasse alla WLAN.

Serve per cifrare i dati tra utente e AP: la chiave usata è comune a tutti gli utenti. Ogni utente ha la stessa chiave, se intercetto la chiave catturo il traffico di tutti gli utenti.

WEP - Autenticazione:



Sebbene usi una *secret key*, e un check-sum per garantire l'autenticità, WEP offre una protezione minima.

WPA / WPA2: Wifi Protected Access

WPA e WPA2 forniscono le seguenti caratteristiche crittografiche:

- Integrità e cifratura dei dati con gli standard 802.1x
- Protezione da attacchi “replay”
- Operano a livello Media Access Control

Tipologie di Cavi

Supporto agli apparati di rete

Tra le tecnologie di fili si possono trovare:

- Doppino **UDP**: non schermato
- Doppino **STP**: schermato
- Connettore **RJ45**: cavo ethernet (4 coppie)
- Connettore **RJ11**: cavo telefono (2 coppie)
- Fibra Ottica

Con i cavi RJ45 è possibile utilizzare la tecnologia **PoE** (*Power on Ethernet*) che permette di non utilizzare due coppie di cavo per dati ma bensì per la corrente (o più/meno coppie).

La **Fibra Ottica**:

- E' utilizzata in ambienti molto rumorosi
- Può essere monomodale o multimodale (LED)

Apparati di Rete

Tipologie di Apparati di Rete

SWITCH:

- Permette la comunicazione tra le porte (*Store&Forward*)
- Elimina le PDU errate e in collisione
- Utilizza l'algoritmo **selective flooding** se non conosce l'associazione *porta/MAC*
- Utilizza l'algoritmo **backward learning**
- Spezza il dominio di collisione ma non di broadcast e multicast

Algoritmo *selective flooding*:

- 1) Le PDU che arrivano su una certa porta vengono trasmesse sulle altre
- 2) Non viene trasmessa sulla stessa porta da cui è arrivata

Algoritmo *backward learning*:

- 1) Lo switch impara quali indirizzi MAC hanno le stazioni attaccate su una certa porta guardando il campo source MAC dei frame che arrivano su quella porta
[*L'associazione MAC-porta è multi-uno perché si possono raggiungere più MAC da una porta*]
- 2) Le associazioni imparate si aggiornano automaticamente nel tempo
- 3) Non è richiesto nessun intervento umano

Sicurezza negli switch: **debole**

- Il *flooding* iniziale rileva le interfacce MAC dei dispositivi collegati
- Furto di identità (*MAC Spoofing*)
- Furto di informazioni : falso l'algoritmo di backward learning inviando PDU con il MAC falso

VLAN

Virtual Lan

→ Gli switch separano i domini di collisione ma non di broadcast / multicast: ARP e i malfunzionamenti generano traffico di banda.

- Ho problemi di poisoning, e flooding

Soluzione: pariziono una LAN in tante LAN da collegare tramite un router IP. Posso avere LAN diverse collegate allo stesso switch:

- L'amministratore decide il LAN assignment tramite le porte
- L'assegnazione è facile da cambiare via sw

Per poter suddividere più LAN è necessario scrivere un LAN-ID nella trama ethernet (nel TAG)