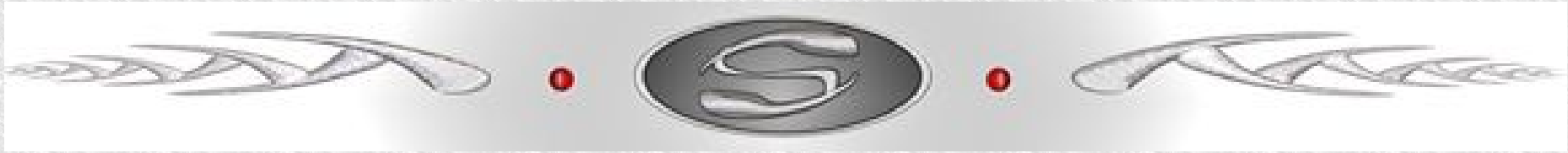


Tecniche di prevenzione, protezione e identificazione degli attacchi informatici

Relatori:

Marco Balduzzi, Paolo Carpo

30 Settembre 2004

Il paradigma C.I.D.

- Descrive gli obiettivi della sicurezza informatica:

- confidenzialità: capacità di un sistema di offrire i propri servizi soltanto a chi ne ha l'autorità
- integrità: rendere possibile solo alle persone autorizzate la modifica delle risorse e dei dati di un sistema, in modo da mantenere una consistenza tra dati e funzioni
- disponibilità: capacità di offrire sicuramente, tempestivamente e in ogni circostanza il servizio

Sicurezza dell'informazione
(l'approccio tradizionale)

- Basato sul meccanismo autenticazione/autorizzazione

  (chi sei? ecco cosa puoi fare..)

- Associazione: utente (gruppo) - privilegi

- Implementazioni di sicurezza
  - credenziali di identificazione: password, token fisici e soluzioni biometriche

Sicurezza dell'informazione (2)

- password: lunghezza appropriata, scadenza periodica, non prevedibili, personali
- token fisici: non falsificabili, difficili da smarrire

- gestione accurata dei profili utente
  - identificazione dei profili (amministratore, operatore, utente)
  - cosa è autorizzato a fare l'utente o il gruppo?
- gestione permessi su filesystem
  - identificazione e protezione dei dati crititici (file delle password, binari di sistema, log, directory di sistema, etc)
  - identificazione e protezione dei dati personali (/home)

Sicurezza dell'informazione (3)

- installare solo il software indispensabile!
- aggiornare periodicamente il sistema
- gestione corretta dei demoni (processi in background)
  - quali servizi vogliamo offrire? a chi?
  - tenere bassi i privilegi di esecuzione
  - nasconde i banner dei demoni
  - creare ambienti chroot (esecuzione in “jail”)
- ACL (Access Control List)
  - dove possibile porre dei filtri sull'utenza del servizio (login via ssh, elevazione di privilegi con su e sudo, etc..)

Sicurezza dell'informazione (4)

- protezione fisica
  - rendere difficoltoso l'accesso alla macchina
  - utilizzare di screensaver con password
  - UPS, sistema anti-incendio, sistema antifurto
  - soluzioni RAID e backup periodici
  - etc..
- crittografia e stenografia
- firewall
- log e intrusion detection system

Cos'è la Crittografia

- Deriva dal greco kryptos (nascosto) e graphos (scrivere). E' quindi l'arte delle scritture nascoste.
- E' oggi una scienza che si basa sulla matematica e sull'informatica.
- Usata fin dall'antichità per nascondere le informazioni, in special modo quelle di origine militare.
- Cifrario di Cesare (es: ROT3)

Cos'è la Crittografia(2)

- Cifratura: preso un testo in chiaro **t** e applicata su di esso una funzione **f1** , ottengo un crittogramma **c.**
- Decifratura: preso un crittogramma **c** e applicata su di esso una funzione **f2,** ottengo il testo in chiaro **t**.
- Matematicamente: **f1** e **f2** devono essere funzioni una inversa dell'altra. **f1**, inoltre, deve essere iniettiva, cioè a testi diversi corrispondono crittogrammi diversi.

Principio di Kerckhoffs

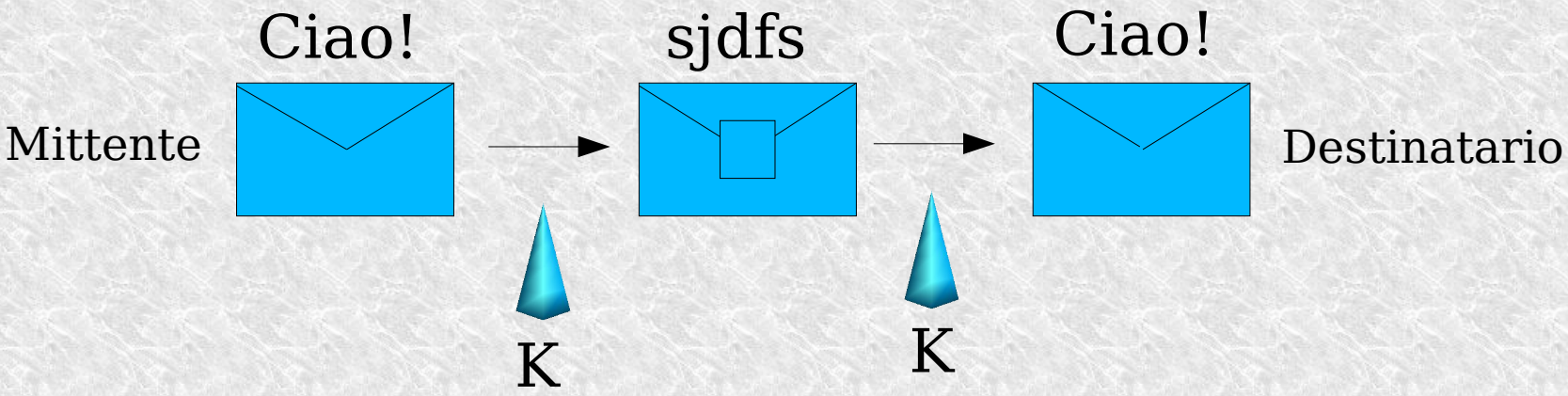
- se le chiavi:
  - sono tenute segrete
  - sono gestite solo da sistemi fidati
  - sono di adeguata lunghezza
- allora
  - ...non ha importanza che gli algoritmi di crittografia e decrittografia siano tenuti segreti
  - ...anzi è bene che siano pubblici affinchè siano studiati accuratamente e siano evidenziate aventuali debolezze
  - **DIFFIDARE** dalla Security Through Obscurity (STO)

Crittografia simmetrica

- Chiave comune a mittente e destinatario (unica chiave quindi)
- Algoritmi simmetrici
- Basso carico di elaborazione
- Principali algortimi:
  - DES (obsoleto), 3DES
  - IDEA
  - RC2...
  - Blowfish
  - AES

Crittografia simmetrica(2)

- Si basa sul presupposto che i due estremi della comunicazione abbiano la chiava comune **K.** La robustezza del cifrario dipende quindi solo dalla segretezza di **K**.



Crittografia simmetrica(3) Problemi

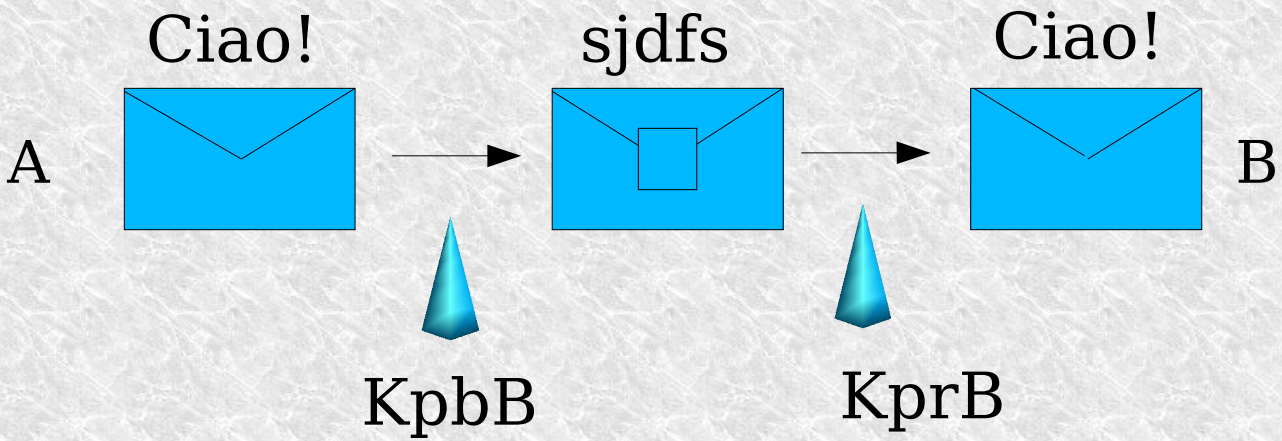
- Se anche il destinatario, come visto, deve conoscere la chiave di cifratura, allora il problema è evidente: come trasmettere la chiave se il canale non è sicuro?!
- Un malintenzionato potrebbe intercettare la chiave e quindi decifrare i messaggi o spacciarsi per uno dei due estremi della comunicazione!
- Si usa la crittografia a **chiave pubblica.**

Crittografia a chiave pubblica

- Si basa su una coppia di chiavi: pubblica e privata.
- La pubblica (**public key**) è usata per la crittazione
- La privata (**private key**) per la decrittazione
- Non ho più, come si vedrà, il problema della trasmissione delle chiavi su canali insicuri
- Principali algoritmi:
  - Diffie-Hellman
  - RSA
  - DSA

Crittografia a chiave pubblica(2)

- Esempio di comunicazione:
- **A** vuole mandare un messaggio cifrato a **B**



KpbB = public key di B
KprB = private key di B

Crittografia a chiave pubblica(3)

- Per poter intraprendere una comunicazione, A deve conoscere la public key di B. Una volta che ne viene a conoscenza, anche tramite canale insicuro, potrà crittare il testo in chiaro.
- Non ha importanza che il canale sia insicuro dal momento che la public key serve solo per crittare e non per decrittare!
- Si evince quindi che public e private key hanno una relazione matematica che le lega.
- La chiave privata quindi non dovrà MAI essere distribuita.
- La chiave pubblica, invece, il più possibile.

Crittografia a chiave pubblica(4)

- Ma chi mi garantisce la corrispondenza tra chiave pubblica e legittimo proprietario?
- Nascita dei **Public Key Infrastructure (PKI)**
- Sono server contenenti chiavi pubbliche
- Occorre però qualcuno che nuovamente garantisca la corrispondenza delle chiavi...
- Nascono i **Certification Authority (CA)**
- Convalida i certificati emessi...mi devo fidare!

Firma digitale

- Occorre un meccanismo che mi garantisca che il documento che ho tra le mani appartenga veramente all'autore e che non sia stato modificato da agenti esterni.
- L'autore codificherà il proprio documento con la sua chiave privata, in modo che chiunque possa decifrarlo con la sua chiave pubblica e verificarne quindi la paternità
- Sorge il problema per i documenti molto grossi -> tempi di elaborazione lunghi!
- Si autentica quindi solo una parte, utilizzando una funzione di Hash sicura

Firma digitale(2)

- Una funzione di Hash accetta in ingresso documenti di dimensione variabile e ne estrapola “un' impronta digitale” di dimensione sempre fissa.
- Questa viene cifrata con la propria chiave privata.
- Il ricevente ricalcola l'Hash sul documento ricevuto.
- Decritta tramite la chiave pubblica del mittente l'Hash allegato
- Effettua il confronto tra i due codici ottenuti.

Applicazioni crittografiche

- SSH (Secure Shell)
- SSL e TLSv1 (Secure Socket Layer)
- PGP e GnuPG (Pretty Good Privacy)

OpenSSH

- E' la controparte Open Source del protocollo SSH ed è nata all'interno del progetto OpenBSD
- Permette accesso remoto ad host in modo sicuro -> vuole sostituire rsh e rlogin.
- Si basa su scambio di chiavi pubbliche.
- Features: è libero, offre forte crittografia (si basa su algoritmi liberi quali Blowfish e 3DES), permette la redirezione sicura di sessioni X11 e molto altro.

SSL (Secure Socket Layer) e TLSv1

- Protocollo usato per la comunicazione sicura tra client e server nel mondo web (https://...).
- Il server invia un certificato di autenticità al client.
- Questi risponde, una volta verificato, con una chiave di sessione crittata dalla chiave pubblica del server (contenuta nel certificato).
- La chiave di sessione verrà utilizzata durante la connessione usando un algoritmo simmetrico (DES, RC4...)
- TLSv1 è il futuro di SSL, sottoposto a standardizzazione dal 1998. OpenSSL è l'implementazione Open Source.

PGP e GnuPG

- PGP (Pretty Good Privacy) e la sua controparte Open GnuPG sono tool per proteggere i propri dati tramite l'uso della crittografia (e-mail, messaggi...).
- GnuPG si basa su algoritmi pubblici

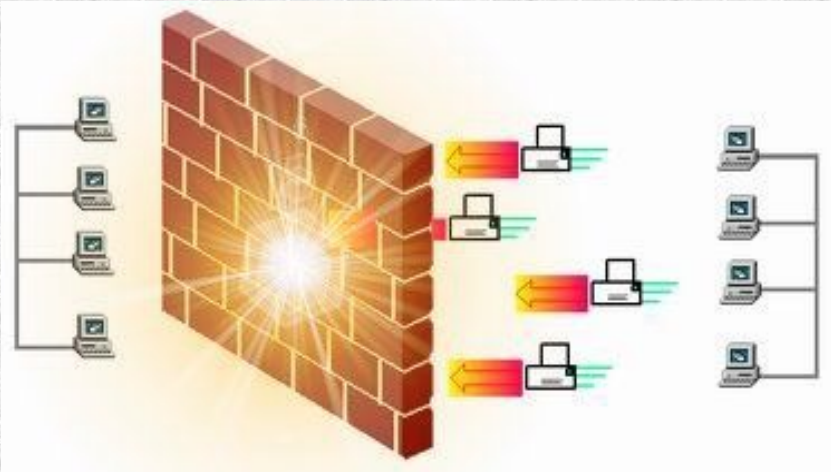
  (N.B. Sicurezza = Trasparenza)
- Usa la tecnica della chiave pubblica.
- Disponibile su diverse piattaforme (Linux, Windows ecc).

Steganografia

- Di cosa si tratta?
  - Arte del nascondere le informazioni all'interno di strutture dati non convenzionali quali
    - audio
    - video
    - immagini
  - Le informazioni significative del container non vengono alterate
- Outguess: steganografa un messaggio all'interno di un'immagine jpeg senza alterarne l'aspetto visivo

Firewall

- Un firewall è un dispositivo di protezione della rete
- E' una sorta di “dogana”... controlla che chi passa abbia il “passaporto”
- E' di fondamentale importanza la sua corretta configurazione!
  - Si basa su regole
  - Può (meglio: dovrebbe) essere integrato con un IDS



Firewall(2)

- Cosa protegge?
  - Rete perimetrale
  - Da attacchi esterni
- Da cosa NON protegge?
  - Attacchi interni alla rete
  - Attacchi ad applicazioni che offrono un servizio pubblico (HTTP, FTP...)

Firewall(3)

- Contesti in cui viene utilizzato:
- Packet Filtering: controlla fino a layer 4 (TCP). Si occupa di controllare i pacchetti in base alle regole impostate dall'amministratore. Controlla i vari campi dei protocolli (sorgente e destinazione, porte ecc).
  - Vantaggi: ottime prestazioni (può essere implementato in hardware in router), scalabilità.
  - Svantaggi: Non controlla il contenuto dei pacchetti (strati superiori)

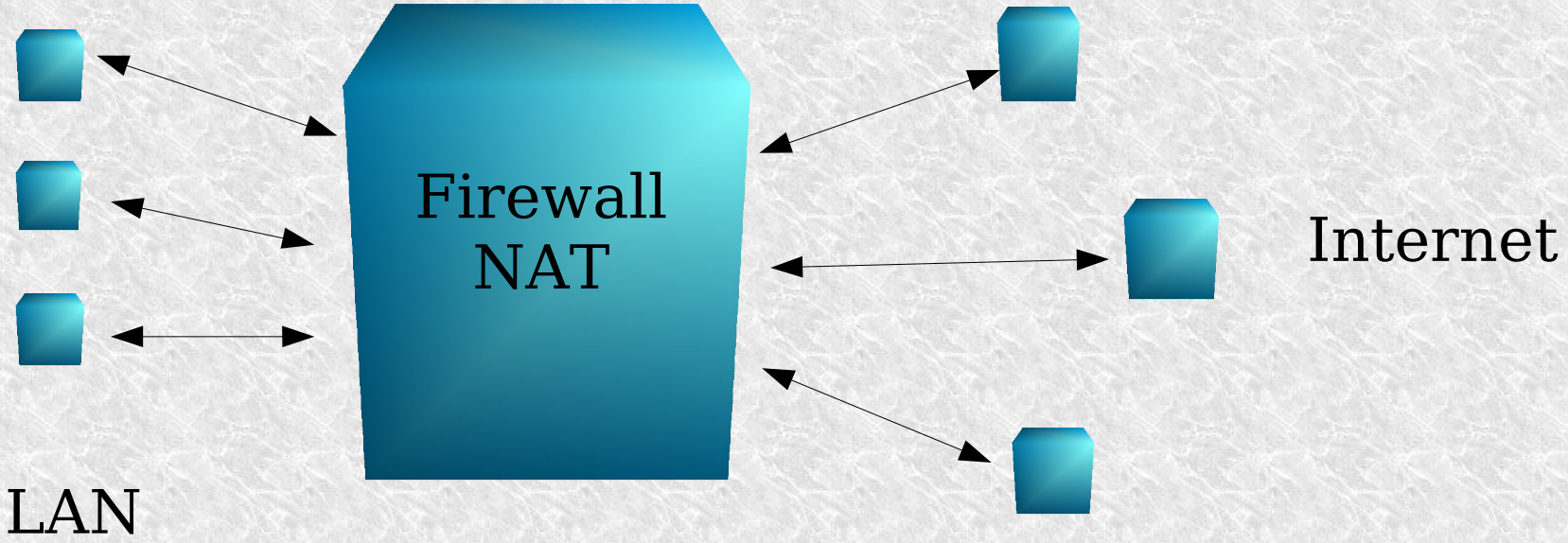
- Introdotto lo **Stateful Inspection**

Stateful Inspection

- Si occupa di tener traccia delle connessioni che attraversano il firewall, basandosi, potenzialmente, su tutti i 7 strati della comunicazione.
- Verifica lo stato della connessione in corso.
- Decide come comportarsi dinamicamente (Connessioni da e verso la rete interna...)

NAT

- Network Address Translation: si occupa di “tradurre” gli indirizzi IP di una rete privata in indirizzi IP pubblici e viceversa.



Sicurezza dell'informazione
(dall'approccio tradizionale a quello moderno)

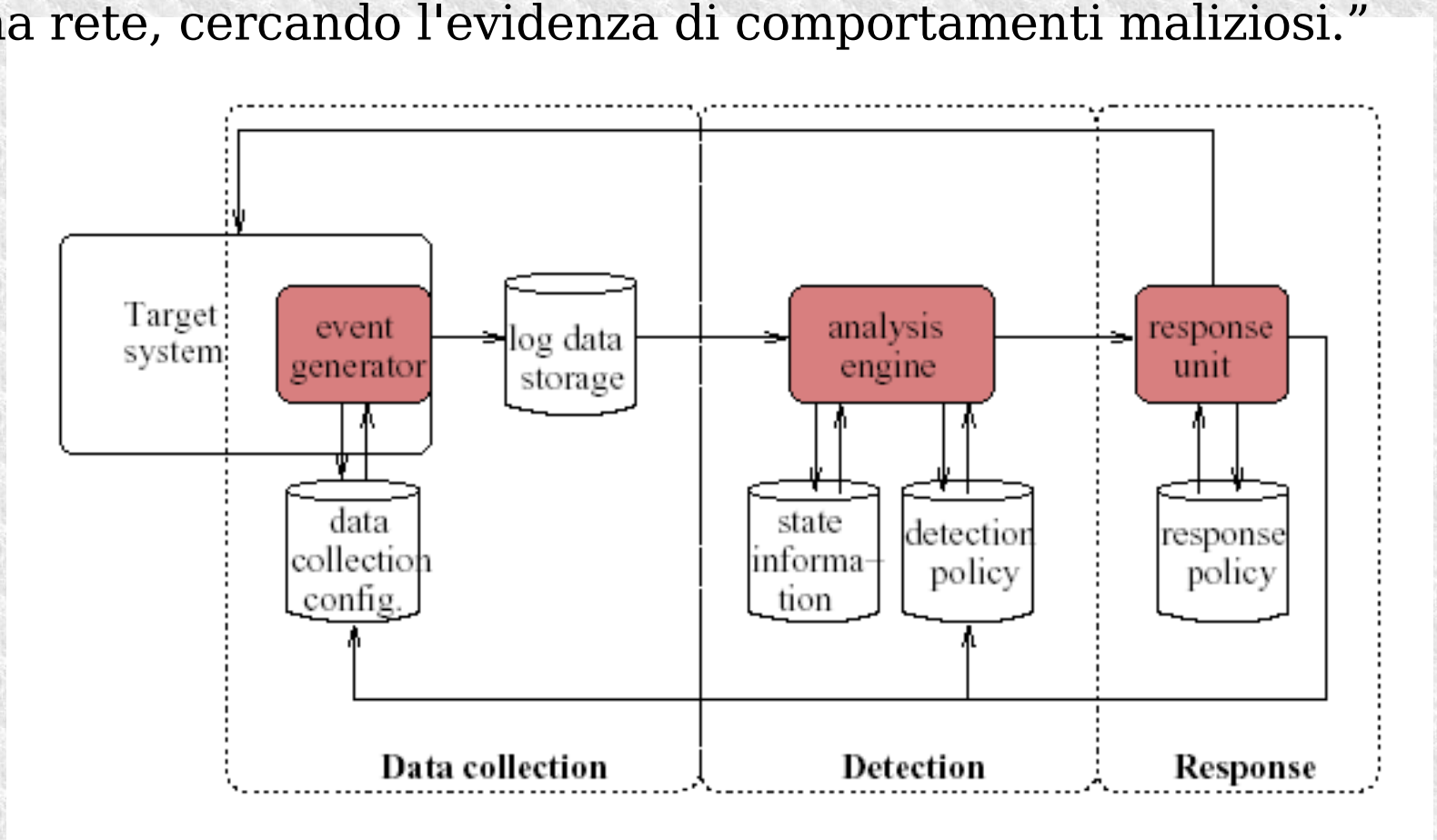
- approccio tradizionale: “chi sei? ecco cosa puoi fare”
- limiti
  - credenziali di autorizzazione deboli
  - restringente tradeoff sicurezza/disponibilità
  - natura booleana

non esiste sicurezza assoluta!

- approccio moderno degli IDS: “che cosa stai cercando di fare? perchè stai operando in quel modo?”

Cos'è un Intrusion Detection System?

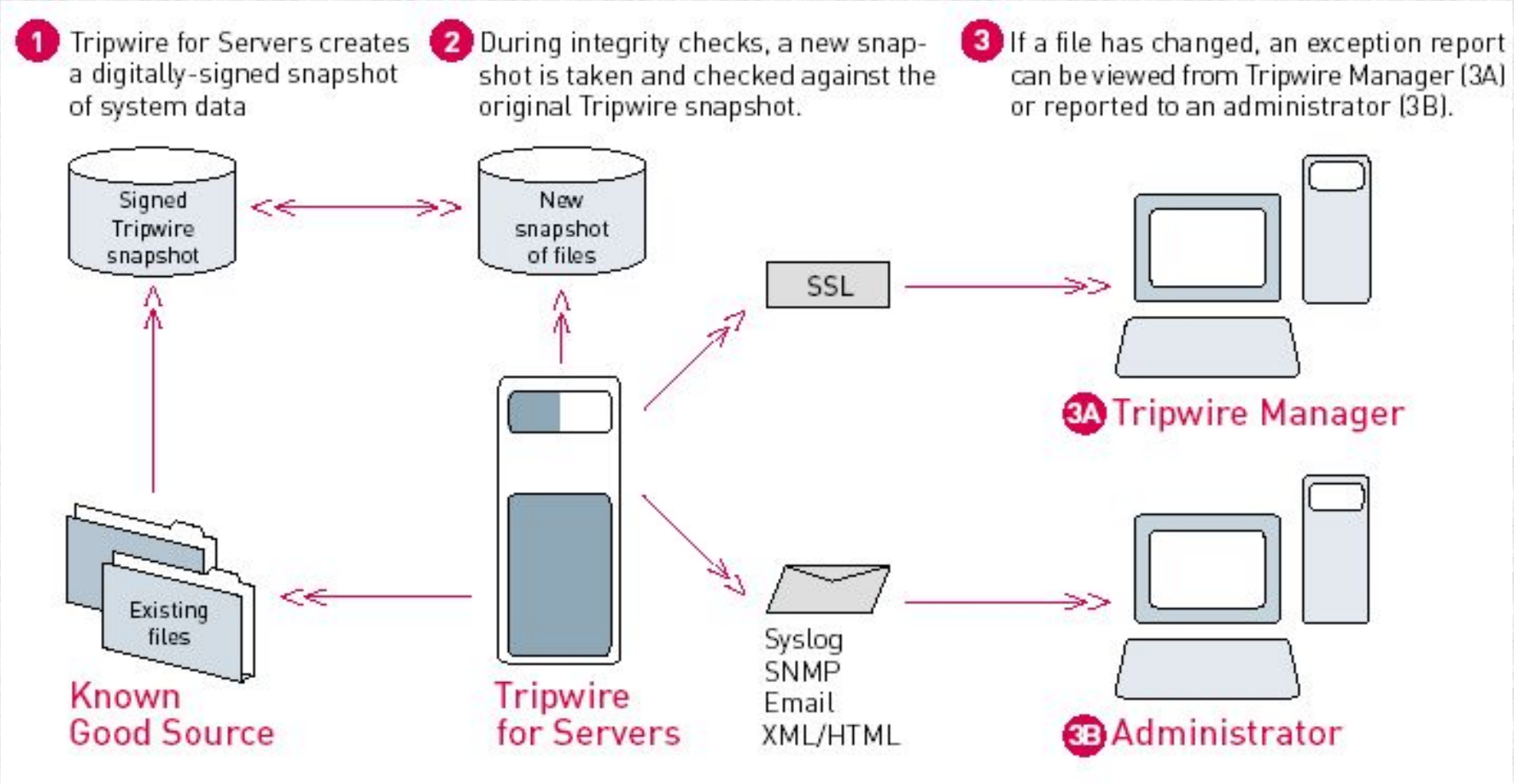
- Funzione di antifurto
- Anderson J. P. 1980: “I sistemi di rilevamento delle intrusioni analizzano le informazioni relative all'attività di un computer o di una rete, cercando l'evidenza di comportamenti maliziosi.”



Tassonomia degli IDS

- per “approccio”
  - anomaly detection: deviazioni "significative" dal comportamento normale
  - signature detection (o misuse detection): confronto con firme di attività intrusive/anomale
- per “sorgente dati”
  - host-based: controllo locale
  - network-based: controllo del traffico di rete
- per tempistica
  - on-line: analisi realtime delle informazioni
  - off-line: analisi periodica dei log a posteriori

Tripwire: Host-based IDS Opensource per il controllo del filesystem



Snort: il Network IDS Opensource

- Di cosa si tratta?
  - Network-based IDS con approccio signature detection
  - Dati d'analisi provenienti dal traffico di rete (sniffing)
  - Posizionamento strategico dei sensori
  - Database di conoscenza basato sulla tassonomia degli attacchi
  - Funzionalità di patter matching e riconoscimento del flusso dati
  - Controlli specifici per particolari attacchi (portscan..)
  - IDS di tipo on-line

- Reperibile da http://www.snort.org

Screenshot

Snort

```
D:\Snort\bin>snort -v
Running in packet dump mode
Log directory = log
Initializing Network Interface \Device\NPF_{BB392819-BEC3-4531-8F6F-B8256F4D120D
}
        --== Initializing Snort ==--
Initializing Output Plugins!
Decoding Ethernet on interface \Device\NPF_{BB392819-BEC3-4531-8F6F-B8256F4D120D
}
        --== Initialization Complete ==--
-*> Snort! <*-
Version 2.1.0-ODBC-MySQL-WIN32 (Build 10)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)
1.7-WIN32 Port By Michael Davis (mike@datanerds.net, www.datanerds.net/~mike)
1.8 - 2.1 WIN32 Port By Chris Reid (chris.reid@codecraftconsultants.com)

02/04-21:15:40.014856 ARP who-has 10.0.0.1 tell 10.0.0.170

02/04-21:15:40.017576 ARP reply 10.0.0.1 is-at 0:10:DB:C:23:10

02/04-21:15:40.017588 10.0.0.170 -> 10.0.0.1
ICMP TTL:128 TOS:0x0 ID:49492 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:13312  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/04-21:15:40.026394 10.0.0.1 -> 10.0.0.170
ICMP TTL:64 TOS:0x0 ID:16270 IpLen:20 DgmLen:60
Type:0  Code:0  ID:512  Seq:13312  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/04-21:15:41.017503 10.0.0.170 -> 10.0.0.1
ICMP TTL:128 TOS:0x0 ID:49493 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:13568  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/04-21:15:41.022164 10.0.0.1 -> 10.0.0.170
ICMP TTL:64 TOS:0x0 ID:16271 IpLen:20 DgmLen:60
Type:0  Code:0  ID:512  Seq:13568  ECHO REPLY
...
...
...
===============================================================================
Snort analyzed 26 out of 26 packets, dropping 0(0.000%) packets

Breakdown by protocol:                Action Stats:
    TCP: 0          (0.000%)          ALERTS: 0
    UDP: 16         (61.538%)         LOGGED: 0
   ICMP: 8          (30.769%)         PASSED: 0
    ARP: 2          (7.692%)
  EAPOL: 0          (0.000%)
   IPv6: 0          (0.000%)
    IPX: 0          (0.000%)
  OTHER: 0          (0.000%)
DISCARD: 0          (0.000%)
===============================================================================
Wireless Stats:
Breakdown by type:
    Management Packets: 0          (0.000%)
    Control Packets:    0          (0.000%)
    Data Packets:       0          (0.000%)
===============================================================================
Fragmentation Stats:
Fragmented IP Packets: 0          (0.000%)
    Fragment Trackers: 0
```

Intrusion Prevention System (IPS)

- IDS vs IPS
  - v Modalita' di intervento attiva in rapporto a quella di un IDS secondo l'applicazione di opportuni algoritmi
  - v Collaborazione tra firewall e IDS coordinate appunto dall'IPS
  - v Più appetibili dal punto di vista commerciale ormai quasi tutti i vendor propongono
  - x IPS Intervenire automticamente non sempre puo' essere una valida soluzione
  - x In caso di falsi positivi doppio fallimento
  - x Alta generazione di traffico

snort-inline IPS

- Da http://snort-inline.sourceforge.net/ : “Snort_inline is basically a modified version of Snort that accepts packets from iptables, via libipq, instead of libpcap. It then uses new rule types (drop, sdrop, reject) to tell iptables whether the packet should be dropped, rejected, modified, or allowed to pass based on a snort rule set. Think of this as an Intrusion Prevention System (IPS) that uses existing Intrusion Detection System (IDS) signatures to make decisions on packets that traverse snort_inline”.

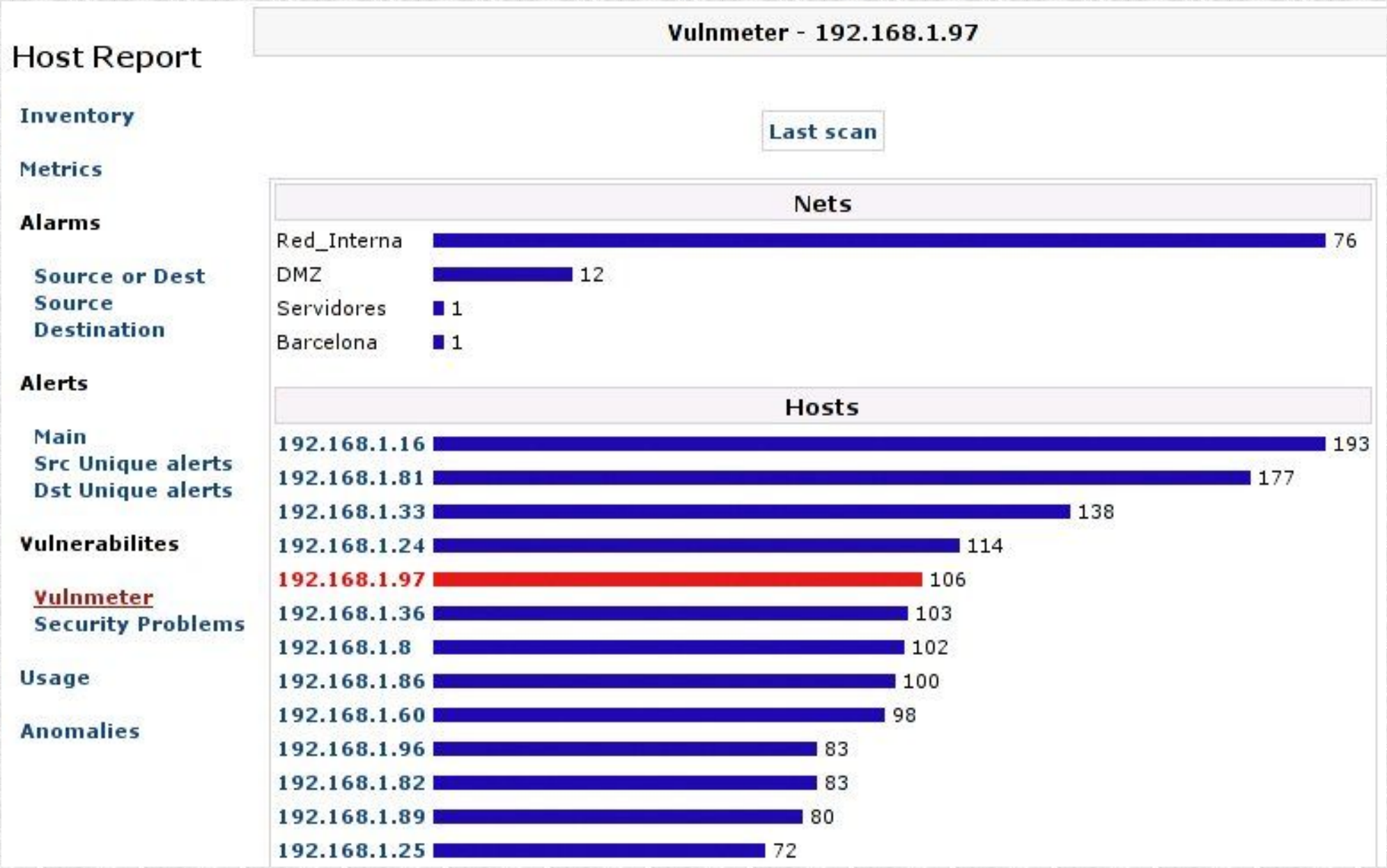
- Esempio pratico di “collaborazione” tra IDS e firewall, integrati insieme a livello logico

Security Information Management (SIM)

- Come gestire gli allarmi generati da molteplici dispositivi e sistemi sicurezza presenti nella rete?
- SIM: automatizzano la raccolta degli eventi gestendo
  - normalizzazione e aggregazione
  - correlazione
  - risk assestment
  - visualizzazione e reporting

- OSSIM: SIM Opensource reperibile da http://www.ossim.net

Screenshots OSSIM (1)



Screenshots OSSIM (2)

<- Last 25 (650-675 of 1120) Next 25 ->

Alarm	Risk	Date	Source	Destination	Description	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	5	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.7:0	Forbidden and Not Found	Delete
WEB cmd.exe access	5	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.7:0	Forbidden and Not Found	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	5	2004-02-19 19:18:05	192.168.1.153:0	192.168.1.6:0	Attack-Response WEB cmd.exe access	Delete
WEB cmd.exe access	5	2004-02-19 19:18:05	192.168.1.153:0	192.168.1.6:0	Attack-Response WEB cmd.exe access	Delete
Successful DCOM exploit	10	2004-02-19 19:18:05	192.168.1.6:0	192.168.1.153:0	Windows cmd.exe attack response	Delete
WEB cmd.exe access	8	2004-02-19 19:18:05	192.168.1.6:0	192.168.1.153:0	Attack-Response WEB cmd.exe access	Delete
WEB cmd.exe access	5	2004-02-19 19:18:05	192.168.1.153:0	192.168.1.6:0	Attack-Response WEB cmd.exe access	Delete

Contatti e riferimenti

- La presentazione sarà disponibile sul sito dello S.P.I.N.E. Group

  http://www.spine-group.org

- Potete contattarci via mail
  - Marco Balduzzi <embyte@spine-group.org>
  - Paolo Carpo <snifth@spine-group.org>

- Domande?