“Un nuovo modello di sistema di identificazione delle intrusioni informatiche: il Router-IDS”

Tesi di laurea di primo livello di Balduzzi Marco, Matr. 33248
Sessione straordinaria estiva A.A. 2003/2004
Facoltà di Ingegneria, Università degli Studi di Bergamo

Il paradigma C.I.D.

Descrive gli obiettivi della Sicurezza Informatica in termini di:

- confidenzialità: capacità di un sistema di offrire i propri servizi soltanto a chi ne ha l'autorità per farlo;
- integrità: capacità di un sistema di rendere possibile solo alle persone autorizzate la modifica delle sue risorse e dei suoi dati, in modo da mantenere una consistenza tra questi dati e le funzioni svolte dal sistema;
- disponibilità: capacità del sistema informatico di offrire sicuramente, tempestivamente e in ogni circostanza l'accesso alle persone che possiedono il diritto di farlo

Sicurezza dell'informazione: dall'approccio tradizionale a quello moderno

- approccio tradizionale: "Who are you? What can you do?"

  il sistema chiede all'utente di identificarsi e gli assegna dei privilegi; meccanismi di sicurezza basati su associazione utente–privilegio.

  due limiti evidenti: - trade-off tra sicurezza e disponibilità;
  - password: credenziali di autenticazione deboli

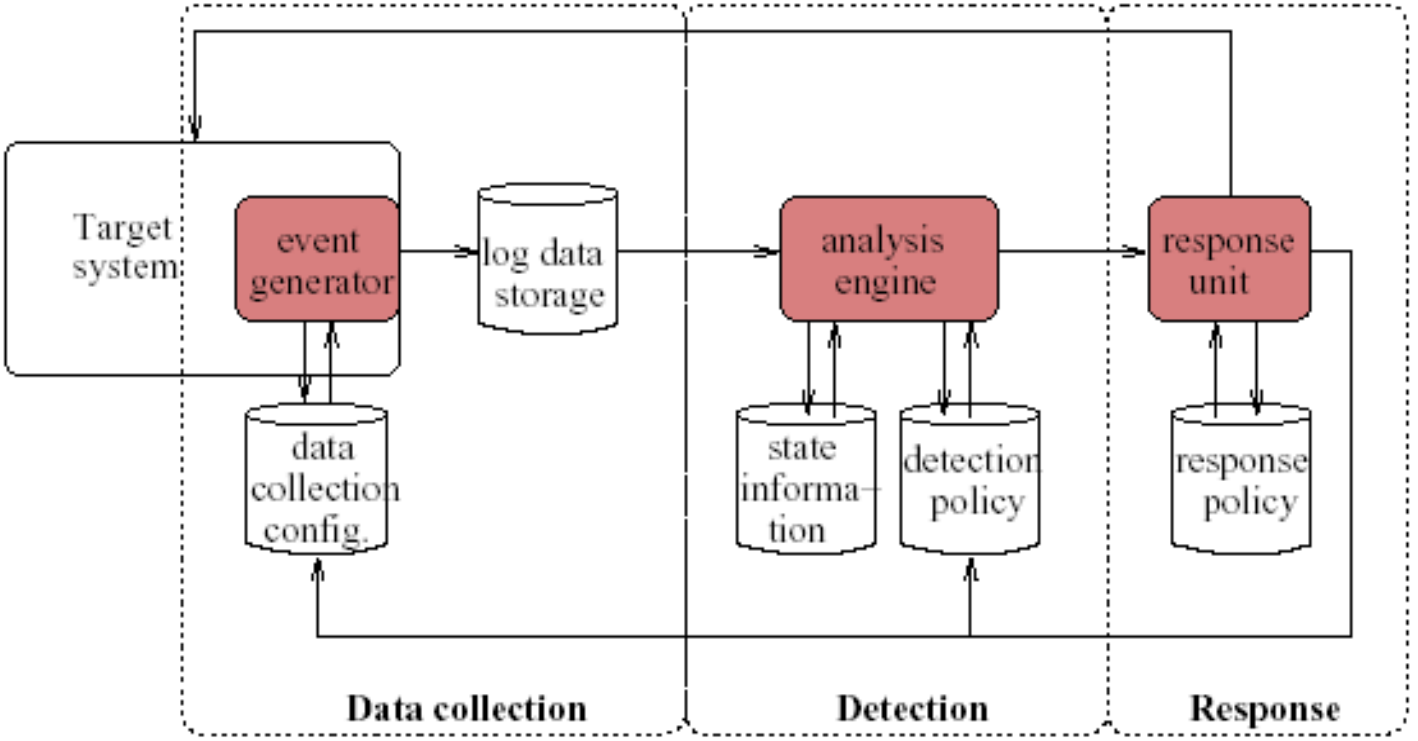
  NON ESISTE SICUREZZA ASSOLUTA!

- approccio moderno: "Che cosa stai cercando di fare? Perché stai operando in questo modo?"

  N.B: l'approccio moderno è complementare a quello tradizionale

Cos'è un Intrusion Detection System?

- funzione di antifurto
- Anderson 1980: "Intrusion detection systems analize information about the activity performed in a computer system or network, looking for evidence of malicious behaviours".



Tassonomia degli Intrusion Detection System

- per “approccio”
  - anomaly detection: il sistema calcola statisticamente e reagisce a deviazioni “significative” dal comportamento normale del soggetto;
  - signature detection (misuse detection): il sistema ricerca l'evidenza di una intrusione nei dati che corrispondono a firme (signatures) note di un comportamento intrusivo o anomalo

- per “sorgente dati”
  - host-based: controllo in loco di log, syscall, file e qualsiasi altra funzione/variabile caratteristica del soggetto;
  - network-based: architettura a layer
    - il sensore di cattura del traffico di rete
    - unità d'analisi: funzione di decodifica, normalizzazione e analisi

Limiti degli attuali Intrusion Detection System

1. sorgente dati povera, semplice e generica;
2. mancanza di contesto;
3. elevato carico computazionale;
4. traffico crittografato;
5. routing asimmetrico;
6. molti altri...

ALTO NUMERO DI FALSI POSITIVI E NEGATIVI!

Approccio context-based

Tre principi:

- focus: capacità dell'IDS di adattare il proprio comportamento a contesti di tipo e dimensione diversa (dispositivo, comunità, scenario);
- conoscenza a priori: la configurazione dell'IDS è modellata secondo la tipologia dell'infrastruttura di rete, del contesto operativo e dei rischi a cui è esposto il soggetto;
- correlazione: tra eventi provenienti da più IDS -> arricchisce il contenuto informativo sintetizzando ricche informazioni sulla rilevazione delle intrusioni e riducendo il numero di falsi positivi/negativi

Il modello Router-IDS

- basato sui tre principi dell'approccio context-based:
  - focus: router, comunità di router, scenario eterogeneo;
  - conoscenza a priori: configurazione dipendente dalle caratteristiche del router (marca e modello, tipo e versione del S.O., componenti hardware presenti, funzioni presenti e abilitate) e del contesto di operatività;
  - correlazione: utilizzo di una architettura distribuita e a layer

- nuova famiglia di IDS
  - estende la tassonomia host-based vs. network-based;
  - presuppone l'integrazione con altri modelli di IDS (Switch-IDS, Firewall-IDS, Server-IDS)

- approccio ibrido: anomaly-based + misuse-based

Una implementazione di prova: RIDS

- sviluppato come esempio di Router-IDS (licenza Opensource);
- controllo remoto via SNMP (protocollo di network management);
- due fasi di funzionamento:
  - tuning: creazione della configurazione e definizione statistica del comportamento normale;
  - normale: - flusso dati sincrono e asincrono;
    - archiviazione configurazioni;
    - analisi anomaly-based;
    - correlazione storica (con configurazioni precedenti);
    - correlazione tra variabili della stessa configurazione
- controlli specifici per i dispositivi di routing

RIDS: esempio di funzionamento (1)

- utilizzo gli Object ID ifAdminStatus e ifOperStatus per verificare lo stato amministrativo e operativo delle interfacce;
- anomalie identificate: disabilitazione di una interfaccia, perdita di link, modifica della configurazione delle interfacce;
- output:

```
DEBUG: Administrative state (IF-MIB::ifAdminStatus.1): 1
DEBUG: Operational state (IF-MIB::ifOperStatus.1): 2
ALERT: FastEthernet0/0: Operational status is wrong (is 2, should be 1)
ALERT: FastEthernet0/0 has been modified in 2:03:36.96

ALERT: FastEthernet0/0: AdminStatus has changed from 1 to 2
ALERT: FastEthernet0/0 has been modified in 0:03:46.51
ALERT: FastEthernet0/0 has been modified in 0:04:06.82
```

RIDS: esempio di funzionamento (2)

- connessioni dal router all'esterno: tcpActiveOpens (“The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state”);
- un attaccante potrebbe utilizzare l'accesso al router per mascherare il proprio indirizzo internet;
- output:

```
Router#telnet 172.16.0.50 21
Trying 172.16.0.50, 21 ... Open
220 ProFTPD 1.2.9 Server (ProFTPD)[portatile.too.fun]

ALERT: Discovered 1 connection from router to outside
```

RIDS: esempio di funzionamento (3)

- numero di pacchetti con flag RST uscenti dal router: tcpOutRsts ("The number of TCP segments sent containing the RST flag");
- il protocollo tcp-ip ammette varie situazioni in cui utilizzare il flag RST, in particolare per annulalre i tentativi di connessioni (3 handshake) verso porte chiuse;
- è possibile controllare attività di portscanning e di flooding

```
# nmap -p 1-65000 -sS router.too.fun

DEBUG: Outbound RST packets (TCP-MIB::tcpOutRsts.0): 5559
ALERT: Transport layer (tcp): high tcpOutRsts value (187 packets/sec.
Causes could be:
   1) Connection (connect()) against closed ports
   2) Halt-open portscan (-sS) to closed port
   3) Stealth FIN (-sF), Xmas Tree (-sX) or Null (-sN)   portscan modes
   4) Random tcp flood to closed port
```

Riferimenti

- Tesi di primo livello su "Un nuovo modello di sistema di identificazione delle intrusioni informatiche: il Router-IDS", Marco Balduzzi. Liberamente scaricabile, modificabile e distribuibile nei termini della GNU Free Documentation License, http://www.madlab.it/URL
- RIDS Router-IDS v. 0.1-public, Marco Balduzzi. Licenza GPLv2, http://www.madlab.it/codes/rids-0.1-public.tar.gz
- "Intrusion Detection System: stato dell'arte e ricerca", Hackmeeting 2004 Genova - 2 Aprile, Marco Balduzzi e Valerio Genovese, http://www.madlab.it/slides/ids_hkm04.pdf
- Per critiche e suggerimenti: marco.balduzzi@madlab.it