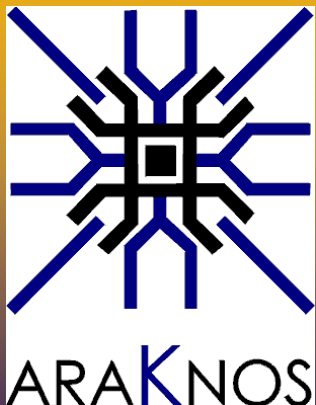


Problematiche di Sicurezza in reti TCP/IP ad alta velocità

Università di Modena e Reggio Emilia

Facoltà di Ingegneria

5 aprile 2006



Maurizio Dal Re
Amm.re Unico, Araknos Srl



Sicuri
di conoscere
l'interno della
vostra rete?



Sicurezza Informatica

- disponibilità di dati e servizi
- integrità dei dati
- confidenzialità dei dati



Metodi

- affidabilità dei sistemi
- controlli perimetrali
- controllo dall'interno



Strumenti di Protezione

◆ Firewall, Router, IDS

- Perimetrali e interni, Firewall personali

◆ Sistemi di Autorizzazione e Autenticazione

- Password, Smart Card, Fingerprint, ...

◆ Protocolli di comunicazione sicuri

- IPSEC, SSH, SSL, ..

◆ Antivirus

- Gateway Server, Personali

◆ Filtri Internet

- Proxy e Filtro dei Contenuti
-



Strumenti di Protezione e Traffico di Rete

◆ Analisi di grandezze caratteristiche del traffico di rete

(numero di byte/pacchetti/flussi per sorgente/destinazione, modelli di traffico, tipologia di protocolli, ...)

◆ Carico elaborativo dipendente da quantità e qualità del traffico di rete

(throughput, indirizzi/porte sorgente/destinazione, protocolli, ...)



Grandezze caratteristiche in “high speed”

Pacchetti TCP: 40-1500 byte

PPS: pacchetti per secondo

Data rate

	40 bytes pps	500 byte pps	1500 byte pps
155 Mbs	480K	38K	12K
1 Gbs	3.1M	250K	83K
40 Gbs	125M	10M	3.3M



Problematiche

◆ Acquisizione

◆ Analisi

◆ Memorizzazione



Problematiche: Acquisizione

◆ Buffer di interfaccia

(gestione picchi)

◆ IO Bus

(trasferimenti verso RAM e OS)



Problematiche: Analisi

◆ CPU

(analisi di header, classificazione dei pacchetti, deframmentazione e risquenzializzazione dei pacchetti, trasmissioni sovrapposte, flussi *idle*, ispezione)

◆ RAM

(strutture dati sotto analisi, trasferimenti verso sottosistemi)

◆ Storage locale

(strutture dati di contesto e per definizione di modelli)



Problematiche: Memorizzazione

◆ Memoria di massa

(oltre 2TB/g, ca 350 Mbps di picco)

◆ IO bus

(SCSI, FiberChannel, ...)

◆ Fault Tolerant

(garanzia di mantenimento dati nel tempo)



Soluzioni HW

◆ Micro Processori general-purpose

(compresi i Network Processor)

◆ ASIC

(Application Specific Integrated Circuit)

◆ FPGA

(Field Programmable Gate Array)



Soluzioni SW

◆ Sistemi Operativi general-purpose

(Windows, Unix/Linux, ...)

◆ Sistemi Operativi custom

(Unix/Linux custom hardened, ...)

◆ Sistemi Operativi Real Time

(LynxOS, QNX, ...)



Soluzioni Algoritmiche

◆ Sampling

◆ Elephant flows

◆ Bitmap counting



Araknos

Domande?

No??

Grazie!

www.araknos.it

info@araknos.it

