Selective and early threat detection in large networked systems

Michele Colajanni, Mirco Marchetti and Michele Messori
WebLab, University of Modena and Reggio Emilia, Italy

Bradford - 29 June 2010
10th IEEE International Conference on Computer and Information Technology
Selective and early threat detection in large networked systems
Selective and early threat detection in large networked systems

Goals

Avoid common drawbacks of Centralized and Hierarchical architectures.

- Single point(s) of failure
- Load unbalance
- Poor or no scalability

We propose:

- Hybrid communication scheme
  - Hierarchical at intra-department level
  - Peer-to-peer at inter-department level
- Distributed alert ranking scheme
Goals

Avoid common drawbacks of pure P2P architectures.

- Complex algorithms
- Sharing/disclosure of sensitive data

We propose:

- Hybrid communication scheme
  - Hierarchical at intra-department level
  - Peer-to-peer at inter-department level
- Selective alert sharing service
Selective and early threat detection in large networked systems

Distributed IDS with hybrid architecture
Alert ranking system

External source 1 → HTTP interface → Custom wrapper 1
External source 2 → HTTP interface → Custom wrapper 2
External source n → HTTP interface → Custom wrapper n

External sources crawler → DB interface

Vulnerable software DB → Alert ranking server
CMDB
Alert Ranking Request
< Targeted IP, Vulnerability ID >
Alert Ranking Reply
Critical, Inconclusive, Not critical
Alert ranking components

- External source crawler:
  - Gathers vulnerability updates from external sources
  - Normalizes data

Alert ranking server

- Alert Ranking Request
- Critical
  - Inconclusive
  - Not critical

Vulnerable software DB

CMDB
Alert ranking components

**Vulnerable software DB:**
- Provide fast access to vulnerable software

**Configuration Management Database (CMDB):**
- **Authoritative** information on devices, software and services
- **Complete** information of all IT infrastructure
- **Directly managed** by the administrator
Alert ranking components

Alert ranking server:

- Searches software vulnerable to the received NIDS alert
- Retrieves list of software installed on the targeted machine
- Compares results and ranks the alert:
  - Match → Critical
  - No Match → No Critical
  - Insufficient information → Inconclusive
Selective and early threat detection in large networked systems

Distributed ranking scheme

Root Department Manager:
- receives already ranked alerts

Local alert managers:
- Receive and process raw alerts
- Forward ranked alerts

Distributed NIDS:
- Monitor all network segments
Selective and early threat detection in large networked systems

Selective alert sharing

**Critical CMDB (CCMDB):**
- Small subset of **critical machines** belonging to the IT infrastructure
- Populated on a **voluntary base**

**Root Department Manager:**
- Processes received alerts using CCMDB
- Forwards to others Departments only **Critical alerts**
Supported *External sources*: 
- CVE and Snort's SID

*Alert ranking server* written in Python

*Local alert manager* based on Prelude:
- Simple implementation of hierarchical architecture
- *Correlator module* modified to invoke the *alert ranking server*

*Root department manager:*
- Similar to Local alert manager
- Implements a publish/subscribe module based on Scribe (Pastry routing scheme)
- Graphical front-end based on Prewikka
Conclusions and future work

Conclusions

- Innovative architecture
- Fit to realistic information systems
- Provide distributed alert ranking
- Enable selective alert sharing

Future works

- Automatic populating of the CMDB
- Increase supported external sources