Intelligent logging server

“SIEM for the poor”

Jan Vykopal, Martin Juřen, Daniel Kouřil
Tomáš Kubina, Michal Procházka, Martin Drašar

Masaryk University, Brno, Czech Republic

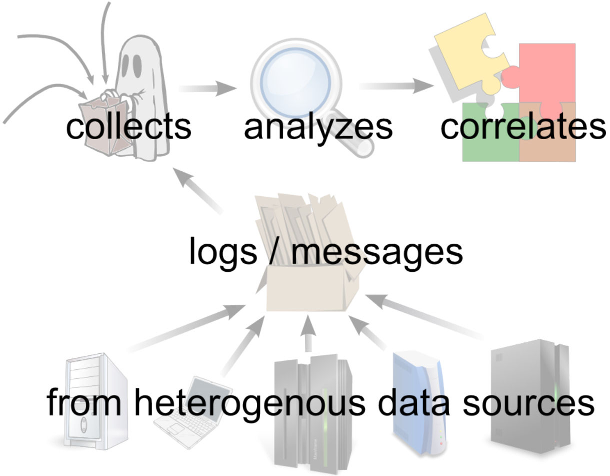
CYTER 2010
Prague, June 23–24, 2010

Introduction

Use case: cyber attack detection

Intelligent logging server (ILS)

useful tool for intrusion detection and forensic analysis that:



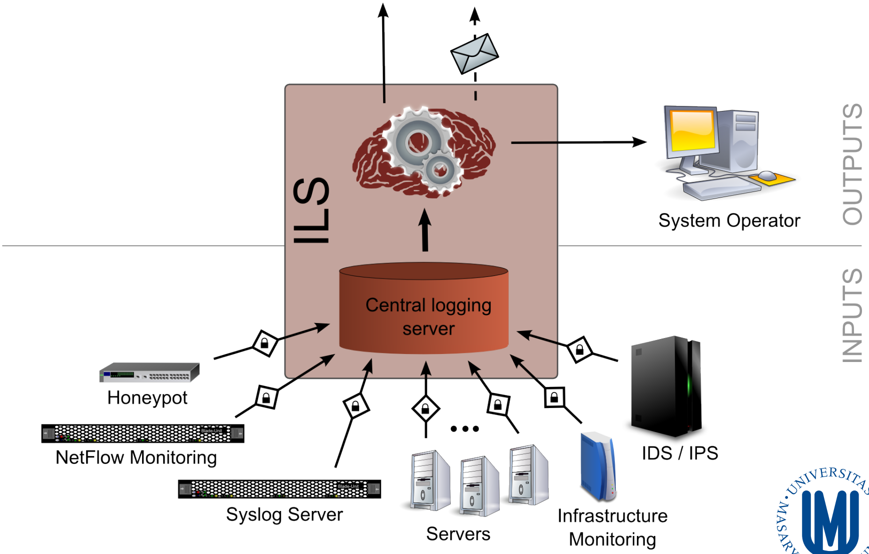
Intelligent logging server (ILS)

- Enables earlier and more accurately detection of cyber attacks.
- Integrates outputs from separate ICT monitoring systems.
- **Based on free (and open-source) components.**
- Reduces total count of relevant messages and eventual false positives.
- Supports network hierarchy – suitable for large networks.
- Detects also system misconfiguration.

ILS as a central monitoring point I

- Supervises network infrastructure:
  servers, IDS, honeypots . . .
- Centrally stores log files destroyed by attackers at compromised hosts (allows forensic analysis).
- Can reveal malicious activities invisible at host level (e. g., distributed attacks).
- Uses additional data sources such as public blacklists.
- Logs are sent via secure channel to ensure message integrity and authentication.

ILS as a central monitoring point II



ILS development as a project I

- Small project funded by Development Fund of CESNET and Masaryk University.
- Our prototype is aimed at the Linux operating system family.
- Should be **easy to deploy in real-life network infrastructure**.
- Project period: 09/2009–11/2010.
- Output available under BSD license:
  software package and deployment guide incl. probes configuration.

ILS development as a project II

- Done:
  - project specification:
    ”core” protocol: Syslog, correlation: Simple Event Correlator
  - central log storage deployment (Linux server with RAID)
  - honeypot deployment (honeyd, VMware + Sebek + database of attempted passwords)
  - deployment of public blacklist correlation engine
  - integration of flow-based IDS
  - attack detection modules
- In progress:
  - presentation layer
  - deployment of the whole system in the Masaryk University network

Use case: Unauthorized access to computer system

- network reconnaissance by attacker
- online distributed dictionary attack
- successful breach
- destruction of evidence
- ...

Incident handling without ILS

Somebody or some devices reports **several alerts = cyber attacks.**

Incident handling without ILS

Somebody or some devices reports **several alerts = cyber attacks.**

- (distributed) port scanning captured by firewall/IDS

Incident handling without ILS

Somebody or some devices reports **several alerts = cyber attacks.**

- (distributed) port scanning captured by firewall/IDS
- (distributed) dictionary attack (not) detected at host

Incident handling without ILS

Somebody or some devices reports **several alerts = cyber attacks**.

- (distributed) port scanning captured by firewall/IDS
- (distributed) dictionary attack (not) detected at host
- breach is locally logged as well as many other events

Incident handling without ILS

Somebody or some devices reports **several alerts = cyber attacks.**

- (distributed) port scanning captured by firewall/IDS
- (distributed) dictionary attack (not) detected at host
- breach is locally logged as well as many other events
- attacker stealthily destroys local log files

Incident handling without ILS

Somebody or some devices reports **several alerts = cyber attacks**.

- (distributed) port scanning captured by firewall/IDS
- (distributed) dictionary attack (not) detected at host
- breach is locally logged as well as many other events
- attacker stealthily destroys local log files

We do not know any connection between these events.

Incident handling with ILS

ILS reports only **one alert = cyber attack.**

Incident handling with ILS

ILS reports only **one alert = cyber attack.**

- port scanning is reported to ILS

Incident handling with ILS

ILS reports only **one alert = cyber attack.**

- port scanning is reported to ILS
- ILS creates *context*

Incident handling with ILS

ILS reports only **one alert = cyber attack.**

- port scanning is reported to ILS
- ILS creates *context*
- assigns other reported events to this context

Incident handling with ILS

ILS reports only **one alert = cyber attack.**

- port scanning is reported to ILS
- ILS creates *context*
- assigns other reported events to this context
- destroyed logs can be accessed later in ILS data storage

Incident handling with ILS

ILS reports only **one alert = cyber attack.**

- port scanning is reported to ILS
- ILS creates *context*
- assigns other reported events to this context
- destroyed logs can be accessed later in ILS data storage

Events are correlated, one incident is reported
and all evidence is kept.

Summary: incident handling without ILS

- Events are correlated
- Only one dashboard
- Utilization of public blacklists
- Retaining all logs for forensic analysis

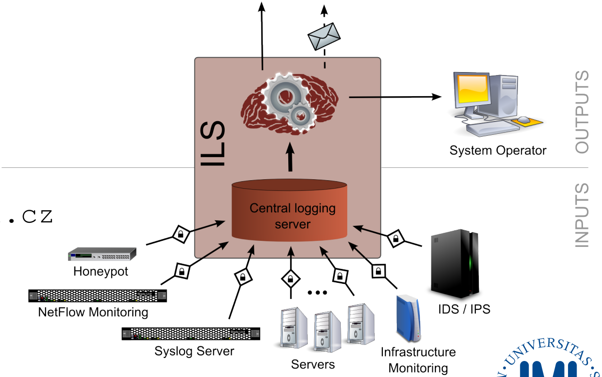
- Several alerts relevant to one attack
- Several different systems
- Local logs prone to destruction

Questions&Answers

Intelligent logging server

Jan Vykopal et al.

vykopal@ics.muni.cz


ILS
Central logging server
System Operator
OUTPUTS
INPUTS
Honeypot
NetFlow Monitoring
Syslog Server
...
Servers
Infrastructure Monitoring
IDS / IPS