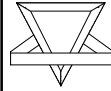


The Emerald IDS

Tysen Leckie – Security Group



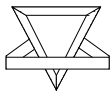
System Overview

Emerald = Event Monitoring Enabling Responses to Anomalous Live Disturbances

“An environment for anomaly and misuse detection and subsequent analysis of the behavior of systems and networks”.

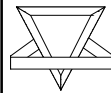
Created By:

Peter G. Neumann and Phillip A. Porras.
Computer Science Laboratory
SRI International, Menlo Park CA



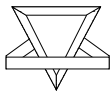
Detection Methods

- ✓ **Anomaly Detection** - Recognition of deviations from expected normal behavior.
- ✓ **Misuse Detection** - Involves the detection of various types of misuse.



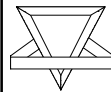
Concepts

- ✓ Targets both external and internal threats that attempt to misuse the system.
- ✓ Combines signature-based and statistical analysis components with a resolver that interprets the analysis results.
- ✓ A recursive framework for gathering data from the distributed monitors to provide a global detection and response capability that can counter attacks occurring across an entire network.
- ✓ Real-time detection of patterns in network operations to detect malicious activity, and responds to this activity through automated countermeasures.



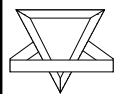
Concepts

- ✓ **Analysis Units**
 - **Profiler Engines** - Statistical profile-based anomaly detection given a generalized event stream of an analysis target.
 - **Signature Engines** - Requires minimal state-management and employs a rule-coding scheme to provide a distributed signature-analysis model.
 - **Resolver** - Coordinator of the monitor's external reporting system and implements the response policy.
- ✓ **Hierarchically Layered Approach**
 - **Service Analysis** - Misuse of individual components and network services within the boundary of a single domain.
 - **Domain Wide Analysis** - Misuse visible across multiple services and components.
 - **Enterprise Wide Analysis** - Coordinated misuse across multiple domains.



Main Components

- ✓ **Monitors**
 - Provides dynamic localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces).
 - Interacts passively (reading activity logs or network packets) or actively (via probing that supplements normal event gathering).
 - Produces analytical results, then disseminates these results asynchronously to other client monitors.
 - Well-defined interface for sharing and receiving event data and results.
 - Signature analysis and statistical profile-based anomaly detection on a target event stream.
 - Each monitor includes an instance of the resolver.



Emerald Monitor Architecture

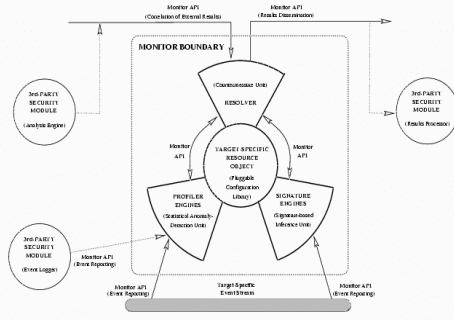
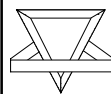


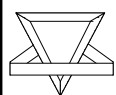
Figure 1: The Generic EMERALD Monitor Architecture



Main Components

Statistical Signal Analysis Subsystem

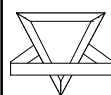
- Employs a variant of the P-BEST (Production-Based Expert System Tool).
 - A rule set to detect known “problem activity” occurring on the analysis target.
- Tracks subject activity via one of four types of statistical measures:
 - Categorical (e.g., discrete types).
 - Continuous (e.g., numerical quantities).
 - Traffic intensity (e.g., volume over time).
 - Event distribution (e.g., a meta-measure of other measures).
- Results are forwarded to the monitor’s resolver.



Main Components

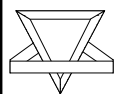
Service Monitors

- Independently distributed to analyze the activity of multiple network services (e.g., FTP, SMTP, HTTP) or network elements (router, firewall).
- Resource objects are developed for each analysis target. (e.g., an FTP resource object for FTP monitoring, and a BSM resource object for BSM Solaris kernel analysis).
- Information correlated by a service monitor can be disseminated to other EMERALD monitors through a *subscription*-based communication scheme.



Event Stream

- ✓ May be derived from a variety of sources including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion-detection instrumentation.
- ✓ Stream is parsed, filtered, and formatted by the target-specific event-collection methods provided within the resource object definition.
- ✓ Event records are then forwarded to the monitor’s analysis engine(s) for processing.



Trends in Alarm Sequences

Indicates a more Global Threat.

- **Commonality Detection** - search for common alarm indicators produced across independent event analyses (multiple monitors).
- **Multiperspective Reinforcement** - Independently analyze the same target from multiple perspectives (e.g., an analysis of a Web server’s audit logs in conjunction with Web network traffic).
- **Alarm Interrelationships** - Model an interrelationship (cause and effect) between the occurrence of alarms across independent analysis targets. An alarm regarding activity observed on one host or domain may give rise to a warning indicator for a different threat against a second host or domain.
- **Sequential Trends** - Seek to detect patterns in alarms raised within or across domains.