EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances

Conceptual Overview

December 18, 1996

Phillip A. Porras
porras@csl.sri.com
Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

Peter G. Neumann
neumann@csl.sri.com
Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances

December 18, 1996

Conceptual Overview

We introduce the conceptual design of EMERALD, a scalable surveillance and response architecture for large distributed networks. The architecture is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployed at various abstract layers in the network. EMERALD's analysis scheme is hierarchically layered and extensible, providing a range of security coverage from the localized analysis of key domain services and assets, to coordinated global attacks against multiple domains and network infrastructure. EMERALD targets external threat agents who attempt to subvert or bypass network interfaces and controls to gain unauthorized access to domain resources. In addition, EMERALD provides a framework for correlating the results from its distributed analyses to provide a global detection and response capability to network-wide coordinated attacks.

The EMERALD architecture is composed of a collection of interoperable analysis and response units called *monitors*, which provide localized protection of key assets throughout an enterprise network. EMERALD monitors are computationally independent, providing a degree of parallelism in their analysis coverage, while also helping to distribute computational load and space utilization. By deploying monitors locally to the analysis targets, EMERALD helps to reduce possible analysis and response delays that may arise from the spatially distributed topology of the network. In addition, EMERALD introduces a hierarchically composable analysis scheme, whereby local analyses are shared and correlated at higher layers of abstraction.

EMERALD's composable analysis scheme begins from the network interface layer of individual administrative domains. Monitors are deployed sparingly throughout each domain to analyze the operation of network services and other externally accessible domain components. Each monitor includes an analysis target-specific set of response handlers that it invokes as it detects possible misuse. These service-layer monitors also disseminate their distributed analyses to other EMERALD monitors that perform domain-wide correlation. Domain monitors provide a more global perspective to the profiling and modeling of vulnerabilities that may arise from interdependencies among network services and other assets within the domain. Lastly, EMERALD implements an enterprise-wide analysis to correlate the activity reports produced across the set of monitored domains. Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain. Through this correlation and sharing of analysis results, reports of problems found by one monitor may propagate to other monitors throughout the network.

The EMERALD monitor architecture is intended to be very small, very fast, and general enough to be deployed at any layer in EMERALD's hierarchical analysis scheme. The initial design of the EMERALD monitor architecture is illustrated in Figure 0.1. EMERALD monitors demonstrate a streamlined, decentralized intrusion detection design that combines signature analysis with statistical profiling to provide localized real-time protection of network

services and infrastructure. The monitor consists of three computational units: a signature-based engine, a statistical profiling engine, and countermeasure unit called the resolver. Monitors incorporate a versatile application programmers' interface that enhances their ability to interoperability with the analysis target, and with other third-party intrusion-detection tool suites.

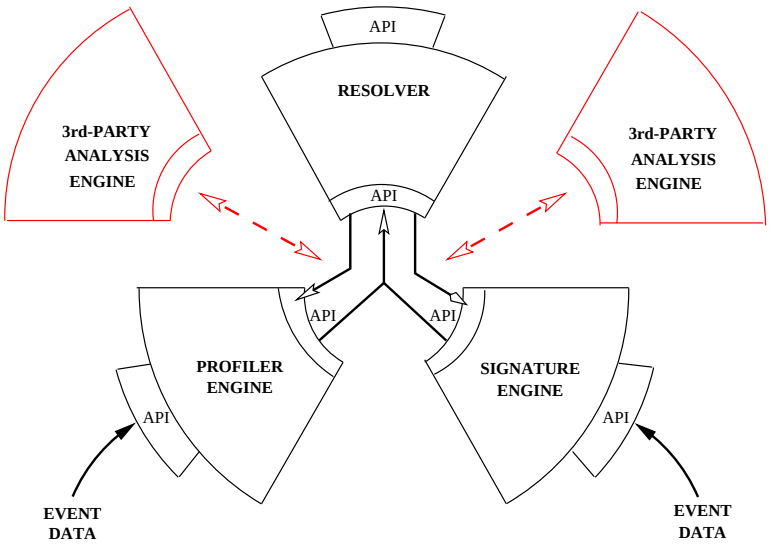

Figure 0.1: The EMERALD Monitor Architecture

EMERALD represents a considerable extension to past research and development in anomaly and misuse detection to accommodate the monitoring of large distributed systems and networks. Because the real-time analysis itself can be distributed and applied where most effective at different layers of abstraction, EMERALD has significant advantages over more centralized approaches in terms of event detectability and response capabilities, and yet can be computationally realistic. It is intended to detect not only local attacks, but also coordinated attacks such as distributed denials of service or repeated patterns of attack against multiple domains. The EMERALD design addresses interoperability within its own scope, and in so doing enables its interoperability with other analysis platforms as well. Its inherent generality and flexibility in terms of what is being monitored and how the analysis is accomplished suggest that EMERALD can be readily adapted to evolving threats as the system and network infrastructure change.