SWAMP: Software Assurance Marketplace

Smitha Sam James Obert Christopher C. Lamb
Science & Engineering Information Systems
Sandia National Laboratories
{ssam, jobert, cclamb}@sandia.gov

Abstract - *abstract*

Services Interface

Keywords: Intelligent Agents, System of Systems.

1 Introduction

The nations critical infrastructure, businesses, and utilities are extensively controlled and enabled by software. These software systems, and their associated hardware platforms, must perform in a predictable and reliable manner. As the complexity of software systems increase, the demands and sophistication of the techniques and tools necessary to test, evaluate, and demonstrate assurance also increase. The development of these tools and approaches is an area of ongoing and active research. It has been noted that the research community could benefit from a facility architected such that access to securely configured and controlled hardware platforms, rules and vulnerabilities databases, and threat descriptions are readily available to the community in a real-time manner.

A federated test bed and analysis environment is proposed to facilitate the creation of new approaches and tools for software assurance activities. This test bed and analysis environment, referred to as a Software Assurance Marketplace (SWAMP) will provide both open source and proprietary services and infrastructure to test new assurance algorithms on software systems in heterogeneous environments with access to hardware ranging from desktop to high performance computing systems. The SWAMP will be installed in a secure, isolated environment at Sandia to enable the evaluation of assurance techniques that need to be protected.

This SWAMP will dramatically accelerate the development of assurance tools and techniques that can be quickly applied to critical software components and systems. It is expected that application of the advanced tools developed within the SWAMP will significantly raise software assurance levels, reduce costs, and positively impact critical infrastructure software throughout its lifecycle.

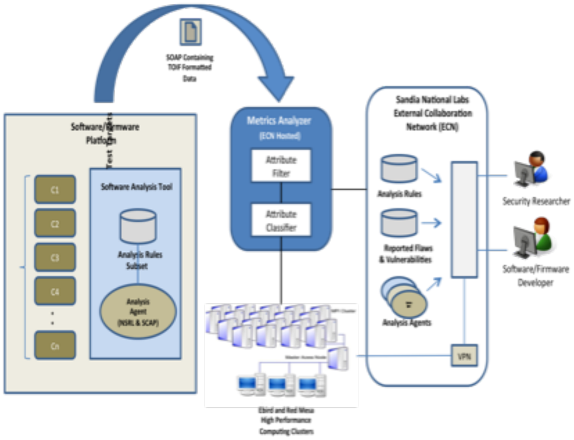

Figure 1. Conceptual Architecture.

1.1 Previous Work

2 Technical Approach

Sandia National Laboratorys primary mission is to maintain and provide failsafe nuclear weapon systems. In support of our mission a large number of software/firmware assurance modeling and simulation techniques and tools have evolved. Achieving failsafe assurance levels in our systems requires the use of extremely capable computing platforms executing complex modeling and simulation scenarios. One of many such systems available at Sandia is Red Storm consisting of 38,000 processor cores with an effective massively parallel processing speed of 204.2 TFLOPS. In addition to Red Storm, Sandias Service Oriented Architecture (SOA) contains a Core Enterprise web services platform of-

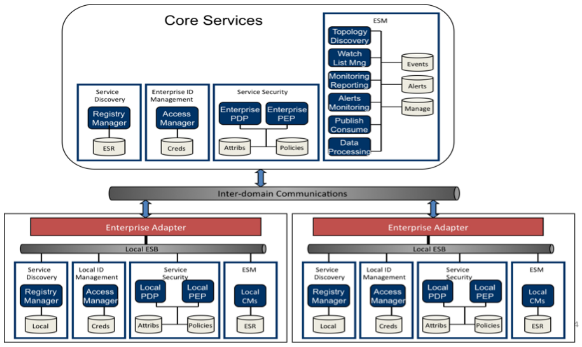

Figure 2. Federated SOA Infrastructure.

fering federated secure web service capabilities in support of distributed test analysis agents and web based user interfaces. The following sections describe a high-level design for a Sandia hosted Software Assurance MarketPlace (SWAMP) that enables:

Research into new forms of software analysis and testing in secure, reliable and repeatable workflows. Expansion into new forms of testing including static, dynamic, and binary analysis. Compatibility as a plug-in to DHS specified software analysis tools. Interoperability as specified by the Homeland Open Security Technology (HOST) program.

2.1 Sandia SWAMP Infrastructure

The proposed Sandia SWAMP infrastructure as shown in the figure below provides web services and VPN interfaces such that security researchers, software developers, and other pertinent staff members are able to analyze collected test data, develop/configure analysis agents and data classifiers.

User access is provided on a 24 by 7 basis utilizing Sandias existing External Collaboration Network (ECN) which allows users to develop and configure deployable National Software Reference Library (NSRL) and Secure Content Automation Protocol (SCAP) compliant analysis agents as plug-ins to DHS designated software analysis tools. Access via the Sandia ECN also allows users to develop and configure data collection Attribute Filters and Classifiers within a central Metrics Analyzer. Deployed analysis agents utilizing a platform specific rules subset, collect test metrics, format the metrics into TOIF form and periodically transmits it via The Simple Object Access Protocol (SOAP) over HTTPS to the Metrics Analyzer. Analysis Agents software updates to target test platforms, and test data transmissions to the Metrics Analyzer are securely and reliably transmitted utilizing Sandias WS-SecureMessaging and WS-ReliableMessaging compliant Inter-domain messaging service as shown in the SOA Infrastructure diagram below. In order to ensure that all deployed Analysis Agents are up to date and properly recognized each is registered in a UDDI Enterprise Service Directory located at Sandia. Additionally, access control is maintained within each domain of the federated system via Service Security Policy Decision Points (PEP), and Policy Enforcement Points (PDP). All PDP and PEP decision and enforcement logic is stored in domain level WS-Security Policy repositories that map Individual access policies on a per Analysis Agent or system user basis.

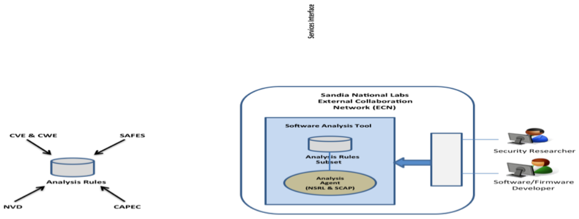

Figure 3. Analysis Agent Configuration.

Figure 1 2: Sandia Federated SOA Infrastructure

2.2 Analysis Agent

As shown in the figure below, a master Analysis Rules database derived from standards, capabilities, and vulnerability databases (CVE, CWE, SAFES, NVD and CAPEC) is assembled and maintained by participating security research and development organizations. Research members of security organizations first perform comprehensive threat analysis of target test systems. The resulting threat analysis findings guide which rules are extracted from the master database and included in the subset deployed with the Analysis Agent.

Figure 1 3: Analysis Agent Configuration

Each Analysis Agent contains a rules interpreter capable of inspecting each rule and translating the rules into testing scripts native to the hosting software analysis tool. Each test scenario tests security-specific software architecture and design elements which effectively measure attack resistance, tolerance, and resilience.

2.3 Metrics Analyzer

The Metrics Analyzer consists of an Attribute Filter and Classifier which in combination are capable of parsing, trending and classifying the large amount of incoming Analysis Agent data. The Attribute Filter conditions Analysis Agent messages by removing message protocol constructs, and performing data compression. The Attribute Classifier uses machine learning and statistical methods to recognize specific software flaws and vulnerabilities. The classifier is capable of decomposing learning and statistical algorithms for parallel task execution on Sandias EBird and

Red Mesa High Performance Clusters. Flaws and vulnerabilities identified during the classification process are stored in a database made available to security researchers through ECN hosted web services.

3 Conclusion

References