INFORMATION ASSURANCE ASSET MANAGEMENT ARCHITECTURE USING XML FOR SYSTEM VULNERABILITY

Namho Yoo, Hyeong-Ah Choi
Department of Computer Science, The George Washington University,
801 22nd Street, N.W., Room 730, Washington, DC 20052, USA

Keywords: Asset Management, XML, Vulnerability, Information Assurance, System Engineering, Risk Management.

Abstract: This paper suggests an XML-based IA asset management architecture for system vulnerability. Once an information assurance vulnerability notice is given for a system, it is important for reducing massive system engineering efforts for IA asset management. When systems are updated by security patch for mitigating system vulnerability, asset management based on vulnerability update and request is trivial, in order to increase accuracy, efficiency and effectiveness of software processes. By employing XML technology, we can achieve seamless and efficient asset management between heterogeneous system format as well as data formats in analysing and exchanging the pertinent information for information assurance vulnerability. Thus, when a system is updated to improve system vulnerability, we proposed XML-based IA asset management architecture. Then, an executable architecture for implementation to verify the proposed scheme and testing environment is presented to mitigate vulnerable systems for sustained system.

1 INTRODUCTION

Information Assurance (IA) issues are one of hot areas among information technology management. IA asset management have become increasingly important because there are continuous changes in components of IA management. IA assets should contain all components such as objects or artefacts associated with IA. Among IA issues, system vulnerability management is addressed specifically in this paper. The basic intensions are to recognize the components of systems for IA asset management and propose IA asset management framework for system vulnerability.

In a sustained system, IA asset management architecture aims to help solve engineering issue of reducing efforts and producing better approach for mitigating system vulnerability. If IA asset management requirement for system vulnerability has an ongoing feature to be considered, even after implementing the change, the management efforts are still required for continued decision-making. (Yoo, 2004)

To maintain systems vulnerability is challenged efforts to the System Engineer and Information Assurance Specialist. All these activities are manually labor intensive and can consume several minutes to hours of time and effort, especially in sustained systems. Therefore it is necessary to build simple and powerful way to handle this.

In order to use asset data proactively, to build negotiable data using designated format is used more quickly that are less costly. Thus, in this paper, asset management architecture using XML is suggested. XML offers the advantages of the ease of displaying data in electronic or printed form and enhanced transportability of the asset data. For example, these XML files hold information regarding the system administration support personnel information such as name , contract status, scope of access, and so on. It is proposed to build IA asset management architecture using XML for managing system vulnerability notice more efficiently and effectively.

This approach is based on XML representation, with improving the impact analysis for IAVM with applying IAVN. The analysis uses a case study in the globally deployed health systems, which were analyzed manually by IA Engineers. An efficient scheme impact analysis scheme using IA vulnerability is discussed whether or not a vulnerability notice can be applied to the systems without causing any negative impact.

The rest of this paper is organized as follows: Section 2 briefly describes background and problem statement. Section 3 presents asset management

Yoo N. and Choi H. (2006).
INFORMATION ASSURANCE ASSET MANAGEMENT ARCHITECTURE USING XML FOR SYSTEM VULNERABILITY.
In *Proceedings of the Eighth International Conference on Enterprise Information Systems - ISAS*, pages 534-537
DOI: 10.5220/0002457105340537

steps. Based on the concepts we defined in Section 2 and Section 3. Section 4 describes basic architecture to handle vulnerability management using cube and implementation. Section 5 addresses conclusion.

2 BACKGROUND AND PROBLEM STATEMENTS

Figure 1 depicts the IA asset management model regarding system vulnerability.

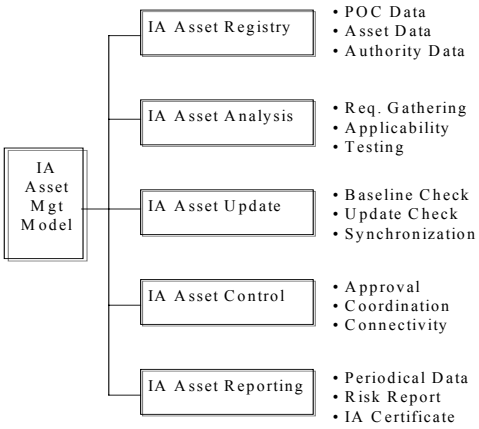

Figure 1: IA Asset Management Model.

This model shows a conceptual view of total IA asset management. With a given changing requirement, a System Engineer and an IA Engineer should be involved in the asset management architectural process. In the case of large-scale and globally deployed systems, engineering evaluations for IA asset management with vulnerability notice rely upon the test results of development testing. IA management on the system interfaces is dependent upon knowledge about interface details based on system resource information. If changing vulnerability management requirement is not a one-time request, it is necessary to involve engineers for continued analysis with more objective evidence from the system resource and build a stronger foundation (MIL, 1997)

In this paper, an applicable vulnerability management requirement, are focused during the process for analysis (DoD, 2004). This security requirement is an appropriate example of an applied to entire systems on an ongoing basis(Yoo, 2004).

Even though System Engineers have sufficient knowledge on each system asset, it will be difficult to trace all the detailed records on the system engineering efforts for IA asset management. Thus, this paper suggests an XML-based IA asset architecture, which is a good vehicle for improving the efficiency by managing the vulnerability information systematically during the process for asset management.

This approach is based on XML representation, with improving the IA asset management for information assurance vulnerability with applying security notice. The analysis uses a case study in the globally deployed US health systems, which were analyzed manually by System Engineers. An efficient scheme based on asset management scheme using XML is discussed.(Yoo, 2005)

Despite the recommendations of the process for conducting asset management process results using site information, relevant difficulties exist. This poses several questions for IA Engineers that are responsible for supporting asset management in the presence of IA vulnerability: 1) How to communicate each other between systems for effective IA asset management? 2) How can we track the status of updating specifications of asset management? 3) How can we minimize efforts for asset management? 4) How to increase the accuracy of asset management decision? 5) Is there any simple and powerful way to follow for asset management?

3 IA ASSET MANAGEMENT STEPS

The example shown in Figure 2 is the information assurance vulnerability notice for database.

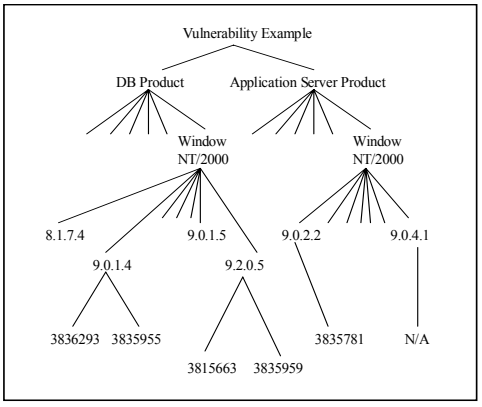

Figure 2: IA Vulnerability Information.

The leaf nodes indicate the patch number identified and parent nodes of those are version numbers. The IA asset management is essential for good decision support. In this paper, we propose an XML-based representation of gathered

specification.Figure 3 is an example of demonstrating a specification described with XML format

Figure 3: Vulnerability Notice XML And ECP XML.

In the column, an example of IA vulnerability information is given, and the ECP submittal form based on XML representation is given in the right column. Using proposed lightweight XML representation; we generate a simple, powerful, and customized model for enhancing the model for configuration management for mitigating IA vulnerability.

Also, as some resource information may exist without specification gathered, gathering specification and verifying it with comparison of the current status is another difficult problem to specify the Engineering Change Proposal (ECP) for Configuration Management (CM), as a common vehicle for final decision making. Figure 4 shows us the response policy and process of IA vulnerability for applicability.

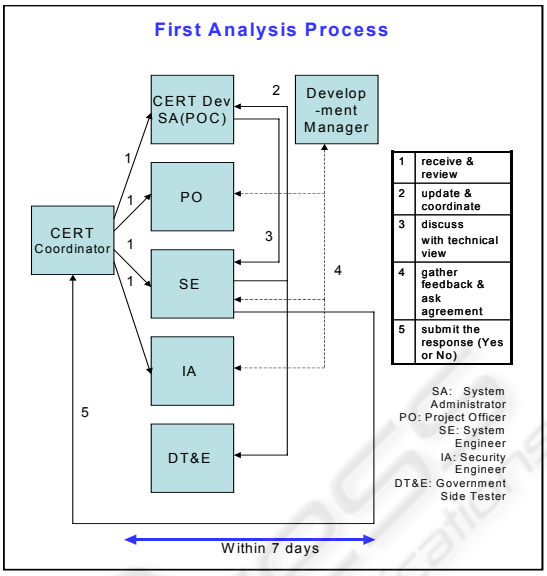

Figure 4: IA Vulnerability Process for Asset Management.

4 XML-BASED IA ASSET MANAGEMENT CUBE

XML-based IA Asset management framework provides strengthening the security model and security posture is possible using a proposed model. Furthermore, we upgrade and customize system asset information as the system resource ontology. The full version of this research had detailed information about resource information. If we use updating resource information, it is possible for us to describe the security accreditation boundary more clearly and realistically by applying lower level information.

Figure 5 is an IA Asset management Cube including process and procedure, requirements, and tools environment for support. In particular, each parameter of five major processes is key components of each process to be considered. For instance, while updating IA asset information, we should consider original baseline, current status, and synchronization after change. For implementation, using DOM tree representation, an information entity holding vulnerability information and changing information on asset management is represented.

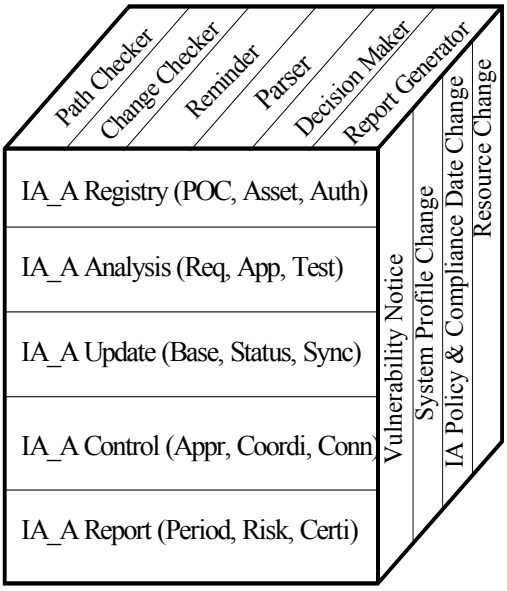

Figure 5: IA Asset Management Cube.

We describe the implementation plan to verify our proposed model and scheme. The Windows system is considered as the underlying hardware environment and we also consider various commercial tools and reliable shareware utilities are planned. For example, we are considering diverse tools for extracting, parsing, and checking and a script programming using Python for an interface between each software components.

In Figure 6, the input artifacts are extracted and are converted to XML.

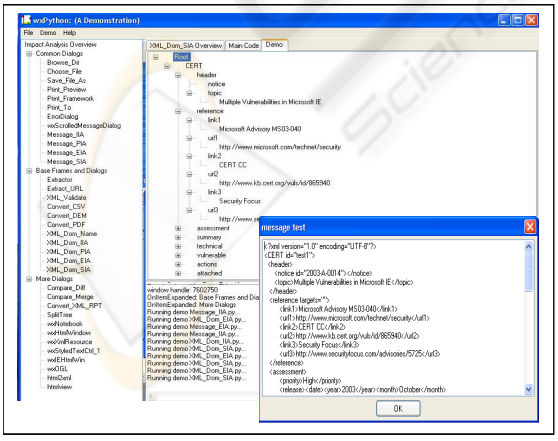

Figure 6: Executable Architecture-based Implementation.

The work presented in this paper differs from previous work in several significant ways. Firstly, customized model is proposed for supporting information assurance engineers at the sustained large scaled system. Secondly, IA asset artifacts during CM are considered using ECP and generate XML DOM tree representation for changing IA requirement supporting asset artifacts. Thirdly, analysis process is designed for increasing collaboration supporting decision in timely fashion. Finally, to find out the effective way for integrating the artifact and checking collaboration, asset management cube are discussed

5 CONCLUSIONS AND FUTURE WORK

In this paper, we consider the new issues rose by the IA asset management for IA vulnerability in a large scaled sustained system safety. We proposed customized steps by monitoring IA asset using XML for mitigating potential security vulnerability and an IA management framework cube. Through an example of a health system, we address processes to apply information assurance vulnerability notice for IA system architecture.

REFERENCES

MIL-STD-498, 1997 Software Development and Documentation, Department of Defense, December

DoD-CERT, 2004, http://www.cert.mil

W3C, 2000, Extensible Markup Language (XML) 1.0 , W3C Recommendation, October

Yoo, N., 2004, Impact Analysis using Performance Requirement with Application Response Measurement in Sustained System, In *Proceedings of the ISOneWorld Conference*.

Yoo, N., 2004, An XML-based Engineering Change Impact Analysis with Non-Functional Requirements, In *Proceedings of International Conference on Software Engineering Research and Practice (SERP)*

Yoo, N., 2005, Resource-Aware Configuration Management Using XML for mitigating information assurance vulnerability, In *Proceedings of International Conference on Enterprise Information System (ICEIS)*