RESOURCE-AWARE CONFIGURATION MANAGEMENT USING XML FOR MITIGATING INFORMATION ASSURANCE VULNERABILITY

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

Keywords: XML, Configuration Management, Vulnerability, Information Assurance, System Engineering, Resource-Aware Management

Abstract: This paper suggests an XML-based configuration management for mitigating information assurance vulnerability. Once an information assurance vulnerability notice is given for a system, it is important for reducing massive system engineering efforts for configuration management. When multiple systems are updated by security patches for mitigating system vulnerability, configuration management based on system resource is trivial, in order to increase accuracy, efficiency and effectiveness of software processes. By employing XML technology, we can achieve seamless and efficient configuration 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, the proposed XML-based configuration management mechanism refers to the system resource information and analyse the security model and posture of affected sustained system and minimize the propagated negative impact. Then, an executable architecture for implementation to verify the proposed scheme and algorithm and testing environment is presented to mitigate vulnerable systems for sustained system.

1 INTRODUCTION

In a sustained system, configuration management efforts toward software process management are required for decision-making(Arnold, 1993). For applying new vulnerability requirements for system security, configuration management should be considered prior to system implementation for minimizing the negative impact to another system. If security requirement has an ongoing feature to be considered, even after implementing the change, configuration management efforts for system security are still required for continued decision-making.

With a given changing requirement, a System Engineer and an Information Assurance (IA) Engineer should be involved in the configuration management process. In the case of large-scale and globally deployed systems, engineering evaluations for configuration management rely upon the test results of developmental laboratories. Configuration management on the system interfaces is dependent upon knowledge about interface details based on system resource information. If changing security 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, as an applicable security requirement, we focus on information assurance vulnerability(DoD, 2004). This security requirement is an appropriate example of an applied to entire systems on an ongoing basis(Yoo, 2004). We present a globally deployed US health system (see Figure 1 for example) and suggest an approach to handle the above issues.

Even though System Engineers have sufficient knowledge on each system resource, it will be very difficult to trace all the detailed records on the system engineering efforts during the impact analysis for configuration management. Thus, this paper suggests a resource-aware configuration management process, which is a good vehicle for improving the efficiency of the impact analysis by managing the security information systematically during the process for configuration management.

Yoo N. (2005).
RESOURCE-AWARE CONFIGURATION MANAGEMENT USING XML FOR MITIGATING INFORMATION ASSURANCE VULNERABILITY.
In *Proceedings of the Seventh International Conference on Enterprise Information Systems*, pages 518-521
DOI: 10.5220/0002540005180521

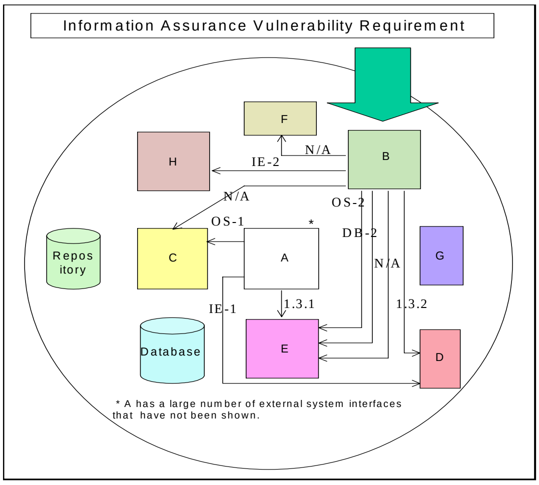

Information Assurance Vulnerability Requirement
F
H
B
IE-2
N/A
N/A
OS-2
OS-1
*
DB-2
Repos itory
C
A
N/A
G
IE-1
1.3.1
1.3.2
Database
E
D
* A has a large number of external system interfaces that have not been shown.

Figure 1: Sustained System Architecture affected by Information Assurance Vulnerability

More specifically, we propose using the *extensible markup language* (XML) to conduct resource aware configuration management for mitigating information assurance vulnerability. XML is widely accepted as a standard for an information exchange on the World Wide Web(W3C, 2000). Accordingly, a resource-aware information model using XML for security in sustained systems has been developed, using offline documentation. However, this scheme is still a labor-intensive procedure.

This approach is based on XML representation, with improving the configuration 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 resource-aware configuration management scheme using XML is discussed.

2 BACKGROUND AND PROBLEM STATEMENTS

The system shown in Figure 1 is a world wide deployed health system involving eight sub-systems, A through H. The configuration management is essential for good decision support. As an example, Table 2 shows us the system resource information for decision-making whether or not given notice is applicable.

Table 1: System Resource Information

	OS	DB	Web Application	Developing Lang.	Tool	JVM & JRE
A	OS-1	DB-1	IE-1	LG-1	T-1	1.3.1
B	OS-2	DB-2	IE-2	LG-2	N/A	1.3.2
C	OS-1	DB-3	IE-3	LG-3	N/A	1.4
D	OS-4	DB-3	IE-1	LG-1	T-3	1.3.2
E	OS-2	DB-2	IE-4	LG-3	N/A	1.3.1
F	OS-5	DB-5	IE-3	LG-4	N/A	1.3.3
G	OS-3	DB-4	IE-3	LG-5	T-4	1.4
H	OS-2	DB-2	IE-2	LG-4	T-3	1.2

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 2 shows us the response policy and process of IA vulnerability for applicability.

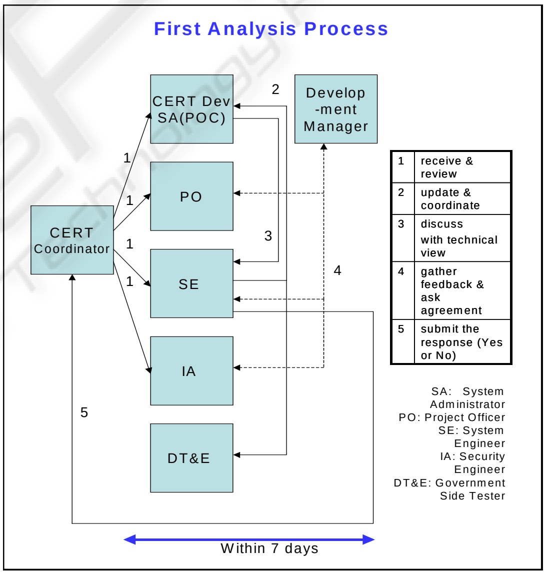
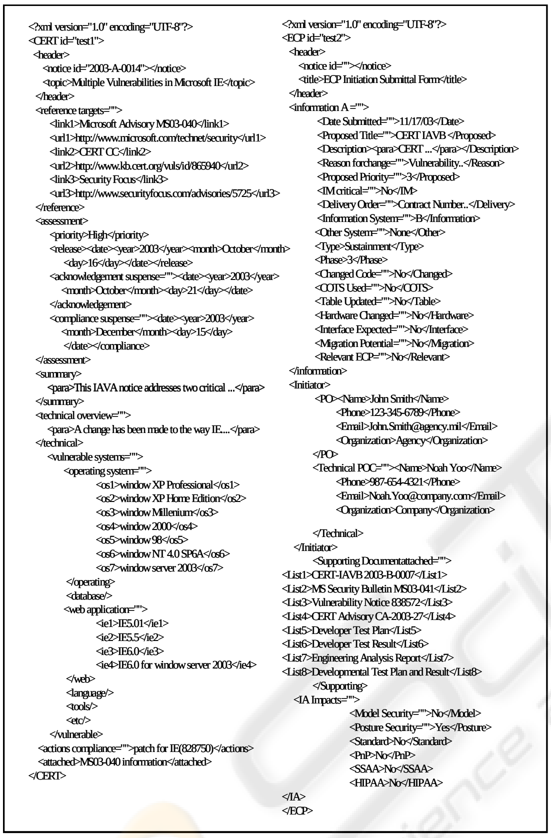


Figure 2: IA vulnerability Response Policy and Process

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

3 XML-BASED RESOURCE INFORMATION DESCRIPTION

In this paper, we propose an XML-based representation of gathered specification.



```
<?xml version="1.0" encoding="UTF-8"?>
<CERT id="test1">
 <header>
   <notice id="2003-A-0014"></notice>
   <topic>Multiple Vulnerabilities in Microsoft IE</topic>
  </header>
  <reference targets="">
     <link1>Microsoft Advisory MS03-040</link1>
     <url1>http://www.microsoft.com/technet/security</url1>
     <link2>CERT CC</link2>
     <url2>http://www.kb.cert.org/vuls/id/865940</url2>
     <link3>Security Focus</link3>
     <url3>http://www.securityfocus.com/advisories/5725</url3>
  </reference>
  <assessment>
     <priority>High</priority>
     <release><date><year>2003</year><month>October</month>
        <day>16</day></date></release>
     <acknowledgement suspense=""><date><year>2003</year>
       <month>October</month><day>21</day></date>
     </acknowledgement>
     <compliance suspense=""><date><year>2003</year>
       <month>December</month><day>15</day>
        </date></compliance>
  </assessment>
  <summary>
    <para>This IAVA notice addresses two critical ...</para>
  </summary>
  <technical overview="">
    <para>A change has been made to the way IE....</para>
  </technical>
    <vulnerable systems="">
        <operating system="">
                <os1>window XP Professional</os1>
                <os2>window XP Home Edition</os2>
                <os3>window Millenium</os3>
                <os4>window 2000</os4>
                <os5>window 98</os5>
                <os6>window NT 4.0 SP6A</os6>
                <os7>window server 2003</os7>
         </operating>
         <database/>
        <web application="">
                <ie1>IE5.01</ie1>
                <ie2>IE5.5</ie2>
                <ie3>IE6.0</ie3>
                <ie4>IE6.0 for window server 2003</ie4>
         </web>
         <language/>
         <tools/>
         <etc/>
     </vulnerable>
  <actions compliance="">patch for IE(828750)</actions>
  <attached>MS03-040 information</attached>
</CERT>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<ECP id="test2">
  <header>
    <notice id=""></notice>
    <title>ECP Initiation Submittal Form</title>
  </header>
  <information A ="">
        <Date Submitted="">11/17/03</Date>
        <Proposed Title="">CERT IAVB </Proposed>
        <Description><para>CERT ...</para></Description>
        <Reason forchange="">Vulnerability..</Reason>
        <Proposed Priority="">3</Proposed>
        <IM critical="">No</IM>
        <Delivery Order="">Contract Number..</Delivery>
        <Information System="">B</Information>
       <Other System="">None</Other>
       <Type>Sustainment</Type>
       <Phase>3</Phase>
       <Changed Code="">No</Changed>
       <COTS Used="">No</COTS>
       <Table Updated="">No</Table>
       <Hardware Changed="">No</Hardware>
       <Interface Expected="">No</Interface>
       <Migration Potential="">No</Migration>
       <Relevant ECP="">No</Relevant>
  </information>
  <Initiator>
       <PO><Name>John Smith</Name>
            <Phone>123-345-6789</Phone>
            <Email>John.Smith@agency.mil</Email>
            <Organization>Agency</Organization>
      </PO>
      <Technical POC=""><Name>Noah Yoo</Name>
            <Phone>987-654-4321</Phone>
            <Email>Noah.Yoo@company.com</Email>
            <Organization>Company</Organization>

      </Technical>
   </Initiator>
      <Supporting Documentattached="">
<List1>CERT-IAVB 2003-B-0007</List1>
<List2>MS Security Bulletin MS03-041</List2>
<List3>Vulnerability Notice 838572</List3>
<List4>CERT Advisory CA-2003-27</List4>
<List5>Developer Test Plan</List5>
<List6>Developer Test Result</List6>
<List7>Engineering Analysis Report</List7>
<List8>Developmental Test Plan and Result</List8>
      </Supporting>
   <IA Impacts="">
            <Model Security="">No</Model>
            <Posture Security="">Yes</Posture>
            <Standard>No</Standard>
            <PnP>No</PnP>
            <SSAA>No</SSAA>
            <HIPAA>No</HIPAA>
</IA>
</ECP>
```

Figure 3: Vulnerability Notice XML and ECP XML for CM

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

4 RESOURCE-AWARE CONFIGURATION MANAGEMENT STEPS

We can observe each step smoothly processed based on XML DOM tree(W3C, 2000). Strengthening the security model and security posture is possible using a proposed model. Furthermore, we upgrade and customize system resource information as the 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 the workstation level information.

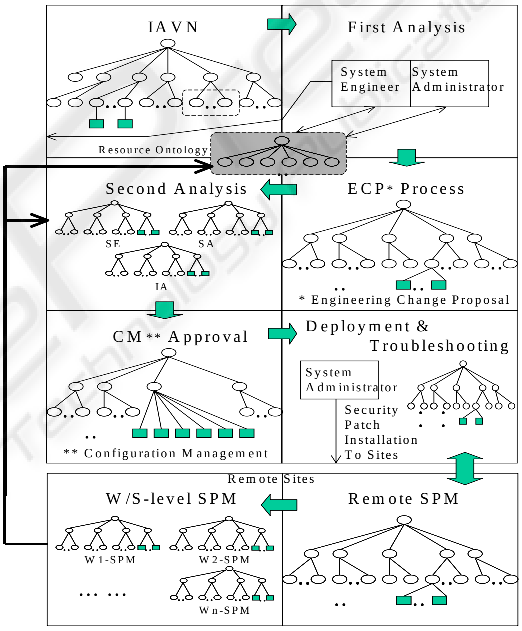


Figure 4: XML-Based CM Steps

Figure 4 is a graph based on architecture design similar to that shown previously. The root node is described as a monitor and the hierarchical information as a tree. A leaf is a user level or changing status. In other words, using DOM tree representation, an information entity holding vulnerability information and changing information on configuration management is represented as the same model.

Through comparing the previous DOM tree and current version, we recognize which elements of the security profile information are changed. As an input, given user security user information and security log files are used. While comparing the

XML DOM tree, we need to check the changing status like the steps (9-10) in Figure 4.

5 IMPLEMENTING PLAN

We describe the implementation plan to verify our proposed model and scheme. The Windows system is considered as the underlying hardware environment due to its pervasiveness and we also consider various commercial tools and reliable shareware utilities are planned for installation as the software environment.

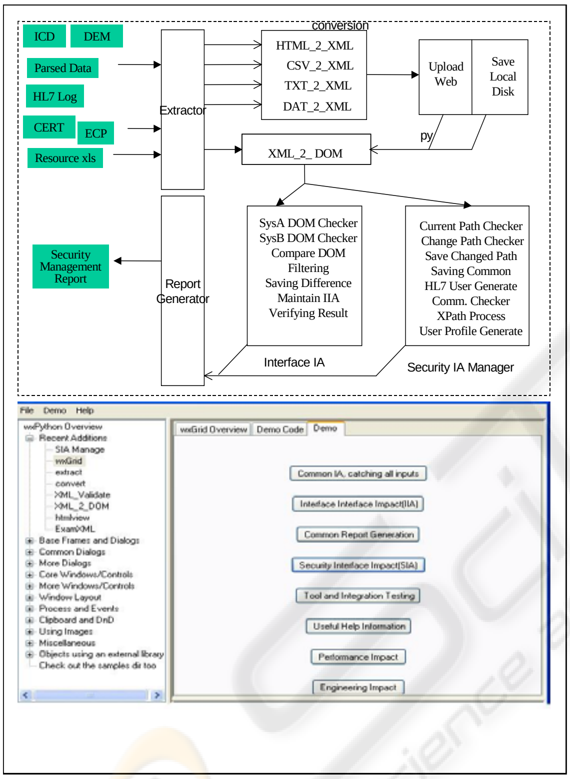


Figure 5: Executable Architecture-based Implementation

For example, we are considering the FirstACT for a virtual user generation and a script programming using Python for an interface between each software components.

In Figure 5, the input artifacts are extracted and are converted to XML. Once the proposed software component in the IA vulnerability system converts XML to DOM, the main configuration management process is preceded. The Graphical User Interface is shown as well.

6 CONCLUSIONS AND FUTURE WORK

In this paper, we consider the new issues rose by the configuration management based on resource aware information for IA vulnerability in a large scaled sustained system safety. We proposed a customized process by monitoring IAV using XML for enhancing impact analysis and presented a scheme for mitigating potential security vulnerability. Through an example of a health system, we address processes to apply information assurance vulnerability notice for system safety.

The ideas presented in this paper were being developed in the context of the XML desktop system and setup implementation for verifying the data. We plan to experiment with our architecture for applying performance evaluations as well in the near future. It is very desirable to implement a simulation system integrated with various change perspectives.

REFERENCES

Arnold, R., Bohner, S., 1993 Impact Analysis – Toward A Framework for Comparison, In *Proceeding of Conference on Software Maintenance*, pp 27-30, September

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).*