Vulnerability Assessment of SAP™ Web Services

By Crosscheck Networks

Introduction

As SAP's™ Web Services-enabled NetWeaver™ platform begins to form the fabric of IT infrastructure for application and business integration, assessing the security of Web Services presents a new challenge. Web Services plays a key role on the NetWeaver™ platform for enabling application components to be offered as services. The flexibility and richness offered by Web Services to integrate disparate applications, SAP™ or non-SAP, increases the potential for security breaches and information leaks. An integral part of NetWeaver™ Web Services rollout and management includes understanding the risk posture of the exposed services. It is through vulnerability assessment of SAP™ Web Services that a risk posture assessment can be made. Such vulnerability assessments have become an essential task for SAP Security Managers.

Before investigating as to what it means to perform vulnerability assessment on SAP™ Web Services, we need to understand the NetWeaver technology platform and its Web Services offering. NetWeaver™ is a technology platform that drives SAP's Enterprise Service Architecture (ESA), a blueprint for how applications are offered as services.[1] NetWeaver™ is a comprehensive integration and application platform and is the foundation for all SAP™ solutions. The NetWeaver building blocks are illustrated in Figure 1. The two key layers that are Web Services-aware in the SAP NetWeaver stack are the Application Platform and the Process Integration. The other layers are also Web Services aware, but the Application Platform and Process Integration play the most significant role in facilitating the SAP application integration based on Web Services.

Key Benefits

Comprehensive Identity Management Testing
Ensures adoption of standards-based access control for Web Services

Intelligent Security Assessment
Effective gap analysis of existing Web Services security and cost-effective planning for closing security gaps

Interoperability Analysis of Web Services Ensures that exposed services are design time and run time compliant to WS-I standards

Auto-Generated Reports
Ensures compliance with Corporate policies for Web Services security

[1] SAP, Enterprise Services Design Guide

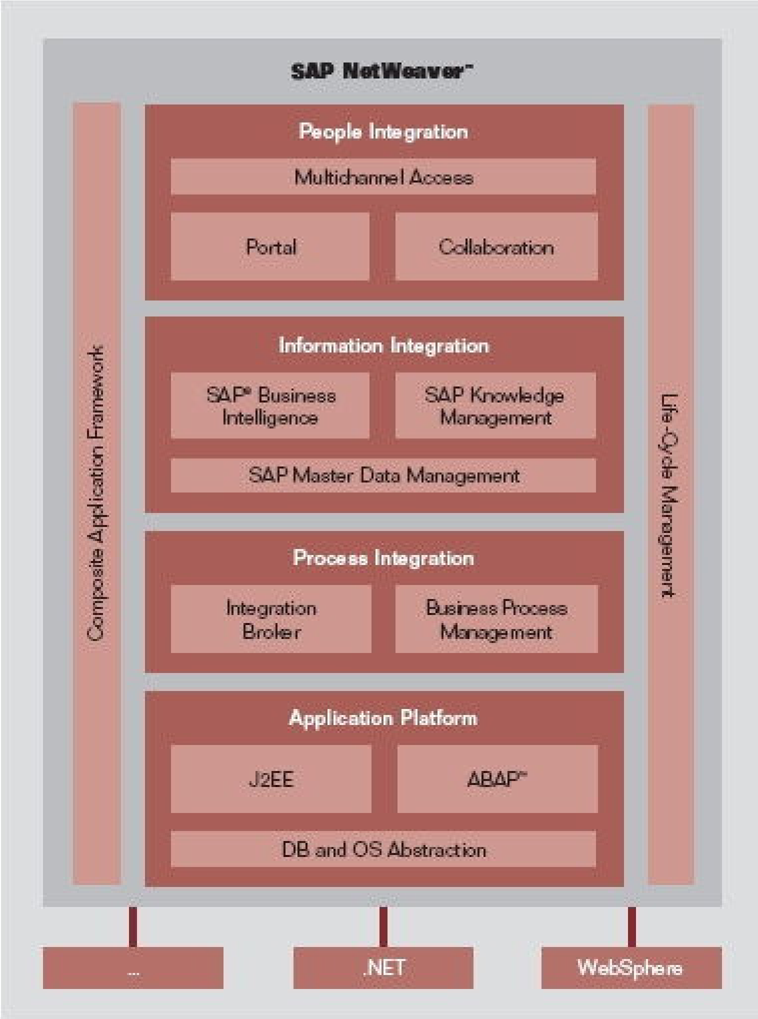

Figure 1. SAP NetWeaver™ Platform[2]

The Web Services-aware Web Application Server (WebAS), based on the J2EE platform, drives the Application Platform layer. ABAP developers can develop ABAP code and wrap custom business functionality in a BAPI call. BAPI calls, both custom and pre-canned, are then readily exposed as Web Services from the Application Platform layer. This flexibility provides rapid integration of core SAP functionality with other applications and external trading partner systems.

The Process Integration layer is where SAP XI, an XML integration broker enables various SAP applications/components to be stitched. The SAP XI can be used to enable SAP applications to be Web Services aware. Even if the SAP applications lack native Web Services capability, SAP XI can act as proxy to legacy SAP applications.[3] The clients

[2] Image produced by the SAP Team and posted at http://blogs.warwick.ac.uk/images/sapteam/2005/02/15/netweaver.jpg

[3] Robert Chu, Service Enable Your SAP Application Component, SAP Developer Network Blog, Dec 29th, 2005

of legacy SAP applications can invoke a Web Service call to the SAP XI proxy that in turn makes a native call to SAP applications via a native adapter.

Vulnerability Assessment of Web Services

Now that we understand some of the SAP™ components that harness Web Services, we need to understand what it means to perform Vulnerability Assessment on Web Services.

Understanding Web Services Vulnerabilities

Web Services security vulnerabilities can be categorized as follows:

- Vendor vulnerabilities**:** Such vulnerabilities relate to security flaws in a specific vendor's component exposed as a Web Service. XML parser is a prime example of a vendor component that is used in parsing SOAP/XML messages. It can be susceptible to a Buffer Overflow attack thus causing an XML Denial of Service or simply a disruption of a Web Service.

- Customer Application Vulnerabilities**:** Such vulnerabilities are security flaws that might appear in Web Service applications due to programming flaw in the business logic. Loosely defined XSD Schemas that expose the structure of Web Service applications contain a wealth of information about how a service will consume the incoming request. Malformed inputs directed specifically at the data formats and input parameters can expose application vulnerabilities. Such exposures can lead to disruption of Web Services or in leakage of sensitive data. Weak access control and non-standard based authentication schemes can also be areas of exposure that can result in application vulnerability exposure.

The threat of SAP™ Web Services being disrupted by malicious client applications is highly unlikely for several reasons.

I. SAP™ Web Services are tightly coupled with identity management solutions that mitigate the risk of a rogue application trying to disrupt services in a B2B environment.

II. SAP™ Web Services are running on a J2EE platform that further mitigates the risk of Buffer Overflow type attacks since Java™ Virtual Machines (JVMs) have tight memory bounds checking to prevent these types of security flaws.

III. The notion of a malicious user or a hacker in a B2B environment trying to disrupt a Web Service is more of a myth than reality. The reality is that any user today in a competitive economic environment will not disrupt a Web Service for notoriety but rather make an effort to steal sensitive information via a Web Service.

So then, where is the threat for SAP™ Web Services enabled applications?

The threat primarily emanates from trading partners or consumer of Web Services in the form of *privileged path exploitation*. This means a consumer of a SAP™ Web Service can be a trusted application with strong credentials (SSL Client Certificate, SAP Logon

Tickets etc), but that consumer application could abuse its credentials to access resources that it is not authorized to access. Such exposures are a consequence of weak access control and can result in leakage of sensitive data from improperly protected Web Service's WSDL (Web Services Definition Language). This problem can become acute when the NetWeaver™ platform integrates disparate applications within a large enterprise and to its external trading partners.

Mitigating the Risk of Vulnerabilities on SAP™ NetWeaver Platform

As Web Services become the main stay of NetWeaver™, it is imperative for an SAP Security Manager to mitigate the risk for exploitation in their Web Services enabled applications by performing automated vulnerability assessment. The goals of the vulnerability assessment should be as follows:

- Ensure all access control policies are thoroughly tested for each published NetWeaver™ Web Services operation

  I. This requires the SAP Security Manager to test all the WSDLs produced by the NetWeaver™, XI, J2EE, or ABAP components. The Security Manager must iterate through each WSDL operation to ensure proper controls are in place.

  II. Web Services support numerous identities and a SAP Security Manager can suffer from identity fatigue if there is no automated plan to test for various identities across the NetWeaver™ platform. The Security Manager should focus on both positive and negative testing of identities.

- Testing all the facets of the XML Schema published to clients. This would require a SAP Security Manger to auto-generate comprehensive attack vectors that could be derived from the XML Schema. Such tests provide visibility into information leak of sensitive data from mishandled error conditions at the application layer. The analysis of response data from a multiple NetWeaver™ Web Services XI, J2EE, or ABAP will require automatic filtration process to reduce false positives and false negatives.

- Performing risk assessment and risk mediation. This involves producing summary reports that indicate various forms of vulnerabilities discovered during the testing period, and categorizing vulnerabilities in terms of their severity level. The summary report should recommend the fixes, risk remediation, and identify where the Web Services operations are exploitable. Such comprehensive testing across complex SAP™ deployments cannot be achieved manually. Only through automated processes and tools, detailed and accurate security assessment of an enterprise SAP™ deployment is possible.

A responsible SAP Security Manager must deploy comprehensive testing of various NetWeaver™ Web Services to ensure the reliability and robustness of the SAP™ applications in a large enterprise.

Summary

Web Services in the NetWeaver framework play an important role in facilitating the integration of disparate applications from various departments or trading partners and thus increasing business productivity. This benefit allows small and medium businesses also to integrate their business applications with larger trading partners. The benefit derived from this seamless integration introduces security concerns when all the business logic is now being exposed through a standard interface that is a catalyst for security vulnerabilities. SAP Security Managers must use automated diagnostics tools to ensure that the security vulnerabilities are caught in pre-production and in post-production phase.

CROSSCHECK
networks

Contact Information
General: info@crosschecknet.com
Sales: sales@crosschecknet.com
Phone: 888.276.7725 Fax: 707.988.3840
25 Thurston Road · Newton, MA 02464 · USA