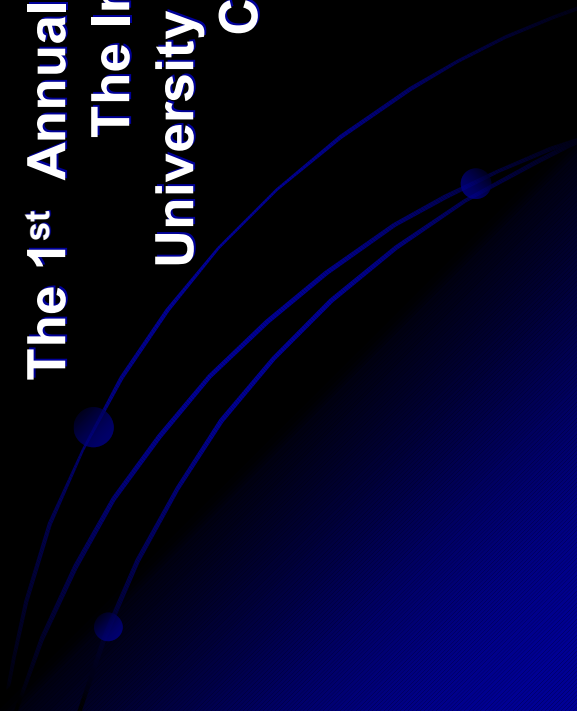


# Perspectives on Semantic Web Services Security

Presented by  
David E. Anyiwo

at

The 1<sup>st</sup> Annual Web Services Security Conference  
The Inn and Conference Center  
University of Maryland University College  
College Park, Maryland  
May 25 – 26, 2006



# Outline

- Introduction
- Semantic Web Services
- Security Challenges
- Security Requirements
- Security Threats and Risks
- Current Security Standards
- Levels of Interoperability
- Semantic Interoperability
- Implementing Semantic Web Services Security
- Conclusions
- Discussion

# Introduction

- Enterprises are increasingly deploying Web Services technologies in their quest to adapt quickly to changing business requirements.
- In most enterprises, Web Services are becoming a prominent element of their Service Oriented Architectures (SOAs).
- However, in spite of the benefits they deliver, Web Services and SOAs introduce greater complexity in the service environment.
- Web Services tend to be highly vulnerable, since applications expose their internal workflows, business processes, and architectures. The need to secure them against a broad spectrum of attacks is quite critical.

# Semantic Web Services

- **Semantic Web Services (SWS) autonomously discover and interact with each other, enabling “anyone, anywhere to add to an evolving, decentralized global database.”**  
**(Gary L. Winkler)**
- **Looser coupling of systems, as well as more flexible composition of services and data are achievable in Semantic Web Service environments.**
- **Semantic Web technologies enable efficient data discovery, automation, integration, and re-use across application and organizational boundaries.**

# Security Challenges

- Although Web Services have revolutionized e-business and other Internet-enabled services, they are still plagued by inadequate levels of integration of loosely-coupled systems across diverse platforms, programming languages and applications.
- Securing and integrating disparate systems and applications in the very complex environment in which Web Services are deployed continue to pose considerable technical and business problems.
- While XML has enabled syntactic integration and interoperability in Web Services, achieving semantic interoperability in a services-oriented architecture is extremely difficult.
- Semantic interoperability is often neglected in SOA development.

# Security Challenges (cont'd)

- Global standards and broadly-adopted specifications for Web Services security, routing, reliable messaging, and reliable transactions are yet to be fully established.
- Ad-hoc Web Services security solutions often result in serious interoperability problems.
- Current security mechanisms cannot adequately handle privacy concerns nor enforce task restrictions or other exclusion requirements.

# Security Requirements

- **Authentication and security of the discovery mechanism**
- **Authorization to access resources**
- **Data integrity and confidentiality**
- **Integrity of transactions and communications**
- **Non-repudiation of interactions**
- **End-to-end integrity and confidentiality of messages**
- **Security and Audit Trails**
- **Distributed enforcement of security policy**
- **A more flexible and expandable security architecture is critically needed to support Semantic Web Services.**

# Security Threats and Risks

- Parsing attacks and XML schema poisoning caused by malicious macros or circular references
- Unauthorized injection if XPath queries
- Capture and replay attacks
- Buffer overflow attacks
- Broken access control attacks
- Large XML payload in SOAP requests as well as illegal request queries that trigger large payloads
- Malicious SOAP attachments
- XML Bombs and other denial of service attacks

# Current Security Standards

There are several standards for Web Services security in various stages of specification and at different levels of implementation and states of conformance. The most common security standards include:

- **XML Key Management Services (XKMS)**
- **Security Assertions Markup Language (SAML)**
- **XML Access Control Markup Language (XACML)**
- **XML Digital Signature (DSIG) and XML Encryption**
- **WS-Security (wss) Core Specification**

# Levels of Interoperability

- **Syntactic interoperability** is achieved when different systems can interpret the syntax of data in the same way. XML has been adopted as the syntactic interoperability standard.
- **Structural interoperability** involves the specification of semantic schemas or metadata for sharing. Resource Description Framework (RDF) and other models provide means for specifying semantic schemas to facilitate sharing.
- **Semantic interoperability** refers to the ability of various Web services, agents, or applications to exchange data, information, and knowledge. It involves adoption of standard schema. RDF-Schema and Web Ontology Language (OWL) enable the sharing of mutually understood vocabulary among services or mappings between their different vocabularies.

# Semantic Interoperability

- Semantic interoperability enables service consumers and providers to exchange actionable information “in a consistent, flexible way that fulfills non-functional requirements, such as performance and scalability” (Selvage et al)
- It is a critical element of a service-oriented architecture (SOA)
- However, it is often taken for granted and not given adequate attention in SOA development

# Implementing Semantic Web Services Security (SWSS)

- Current Approaches to SWSS
  - \* Authentication and Access Control
  - \* Distributed Policy Management
  - \* Other Approaches
- Best Practices
  - \* Integrated SWSS Architecture
  - \* Appropriate Security Standards
  - \* Effective Testing Process
  - \* Automation of Testing and other Processes

# Conclusions

- There are significant security, trust, privacy and quality issues associated with Semantic Web Services that still remain largely unresolved.
- It is extremely difficult to achieve the levels of interoperability and other necessary conditions for provision of meaningful security to Semantic Web Services with available technologies.
- There is a growing need for innovative ways and means for attaining feasible levels of security and interoperability in Semantic Web Services.

# Discussion

# Q & A Session

