Global Justice Information Sharing Initiative

Global Web Services Security Task Force
Meeting Summary

Arlington, Virginia
March 22, 2004

Meeting Background

The Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), convened the Global Justice Information Sharing Initiative (Global) Web Services Security Task Force (WSSTF or "Task Force") meeting on Monday, March 22, 2004. The WSSTF was held in conjunction with the SEARCH, The National Consortium for Justice Information and Statistics Symposium at the Hyatt Regency Crystal City, for the convenience of the participants.

Under the direction of the Global Security Working Group (GSWG), the WSSTF was convened to discuss special considerations surrounding the risks and benefits of implementing Web services in a justice and public safety systems environment. Mr. Fred Cotton, SEARCH, chaired the meeting and set forth the agenda with these key discussion points:

- Review of Web Services Security Landscape
  - What is the status of standards and specifications?
  - What are the risks and requirements?
  - What type of outreach is needed?
- Review of "Web Services Security Issues in a Justice Environment" Document
  - Document update
- Emerging Trends
  - Discussion of security in an Service-Oriented Architecture (SOA)
  - Discussion of federated identities
- Next Steps
  - "White Paper" deliverable discussion
  - Web Services security models

Meeting Participants and Purpose

Since Web services security is a critical security topic for Global, the goal of the meeting was to apply Web services security to the broad interests of the justice community. Their immediate objective is to provide research and issue papers on topics that will benefit Global constituents as well as other justice and public safety communities. The following members, observers, and invited guests were in attendance:

Fred Cotton
SEARCH, The National Consortium for Justice Information and Statistics
Sacramento, California
Ken Gill
Office of Justice Programs
Washington, DC
Alan Harbitter, Ph.D.
Integrated Justice Information Systems (IJIS) Institute
Fairfax, Virginia
Tom Kooy
CriMNet
Arden Hills, Minnesota
Patrick McCreary
Office of Justice Programs
Washington, DC
Tom Merkle
CapWIN
Greenbelt, Maryland
John Ruegg
Information Systems Advisory Body
Cerritos, California
Monique Schmidt
Institute for Intergovernmental Research
Tallahassee, Florida
Bob Slaski
IJIS
McLean, Virginia
John Wandelt
Georgia Tech Research Institute
Atlanta, Georgia

Web Services Security Discussions

The meeting began with a discussion of the Web services security standards landscape in the context of justice information sharing and the exchange of data. The thinking was that there are security standards particular to the justice community. These standards need to be identified and tailored for use in justice. Once this is achieved, the Task Force can build a security infrastructure and then vet the process that will support interoperability of Web services transactions. Standards discussed in detail included Security Assertion Markup Language (SAML); credentials; Universal Description, Discovery, and Integration (UDDI); electronic business Extensible Markup Language (ebXML) registries; Secure Sockets Layer (SSL); and Web Services Description Language (WSDL). The recommendation by the Task Force is to review and define the security requirements and then evaluate how the standards extend to the justice community. It is important to note that the standards work being done by standards bodies, such as the Organization for the Advancement of Structured Information Standards, is lagging 18 months behind the technology. Therefore, there is a critical need to build a Web services security road map for the justice community.

Dr. Alan Harbitter, chief operating officer of PEC Solutions and IJIS representative, and Mr. Ken Gill, OJP, were very appreciative of the background research that was provided at the meeting. This material was based on research from the RSA Security Inc. conference presentations and included updated material on the technologies involved in the Web services security stack. The group recommended developing PowerPoint slides for use in presentations to the Global Advisory Committee and to the justice community.

The next discussion involved an analysis of the security threats. The group decided that the threats and risks to justice systems are magnified by the use of Web services and SOA because SOA magnifies weaknesses that are already there. For example, denial of service is a security risk when XML is implemented on the Web. While SOA has not been officially endorsed by Global yet, the question remains whether or not security risks have been identified and sufficiently mitigated. The group

recommended addressing the question "Is the security side of SOA ready for prime time?" and raising awareness of the issues.

Mr. Tom Merkle, standards manager, Capital Wireless Network (CapWIN), presented the SOA example from CapWIN that was implemented by IBM. Mr. Merkle explained how their wireless system worked, and he answered security questions related to their SOA implementation. It was noted that Mr. Merkle is in the process of completing a gap analysis to review and validate their use of the Global Justice XML Data Model.

Web Services Security Priorities

After considerable discussion, Chairman Cotton asked the participants to prioritize Web services security issues and to provide a road map to decision makers and practitioners. The Task Force identified the following issues to continue to bring forward to the GSWG.

- Elements of security policy and implementation of that policy need to be in place before you can deploy native XML Web services.
- Web Services Infrastructure will include:
  - Examples
  - Management
  - Trust**
  - Identity**
  - Choreography
  - Orchestration
  - Discovery
  - Description
  - Messaging

  **Note: Critical in any security implementation, not just Web services.
- Existing infrastructure cannot be assumed to be compliant with the above.
- We must identify the base security standards and tailor them to our community to facilitate interoperability at this security layer.
  - Web services security
  - SAML
- To participate in Justice XML outside your organization, you must comply with a minimum security standard for transactions in the community, based upon the level of transaction.
- Any architecture considered must have provisions for accommodating small organizations that need access and exchange.
- All participating organizations must have access to a minimum level of security expertise and skill sets necessary for successful implementation.
  - Outsources must meet minimum skill set in security.
- Web services present a new paradigm, and any security weaknesses or new vulnerabilities will only be magnified later.

- Any agency that relies on a firewall as their sole security is vulnerable.
- Positive identity is required for secure Web services.
  - Role of identification versus role of credentials.
- The solution should be modular to allow for extended or reduced security.
- There is a need to raise the security awareness of our community through updates and training presentations.
- We need to define or identify the disparate standards that affect Web services security and update on the maturity of those standards.
  - Simple Object Access Protocol (SOAP)
  - SAML
- Impact analysis is not being performed on standards for trickle-down services.
  - Applies to the entire front

The following action items are recommendations of the Task Force for consideration by Global.

1. Develop questions for practitioners to ask vendors.
2. Identify the minimum skill set in security for outsourced applications.
3. Review the role and functionality of Federated Identity Management.
   a. Must have a well-defined audience.
   b. Need to describe the issues within the context of Web services.
      i. When is federated identity management needed?
      ii. How is confidentiality ensured?
      Privacy depends upon the identity, and positive identity is required. Ultimately, identity and a credential are not the same thing. For example, a badge looks real and it will match up with the police department. However, the public comes to the Internet or an organization's system from any source.
      iii. When should identification (ID) versus the credentials be used?
      iv. Separation of duties—No one person can have access to both ID and credentials.

Concluding Thoughts and Next Steps

Chairman Cotton thanked the participants for their valuable volunteer efforts and continued support of the Global Initiative. After a very productive session, the meeting adjourned.

summary Web services security 3-03.doc