Global Justice Information Sharing Initiative
Global Web Services Security Committee
Draft Meeting Summary
Arlington, Virginia
December 2, 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 Committee (WSSC or "Committee") meeting on Thursday, December 2, 2004.

Under the direction of the Global Security Working Group (GSWG), the WSSC objective is to apply Web services, Service-Oriented Architecture (SOA), and emerging technologies security in the justice environment. Mr. Fred Cotton, Training Services Director, SEARCH, chaired the meeting and set forth the agenda with these key discussion points:

- Overview and mission statement
- Defining scope and products
- Defining appropriate technologies
- Defining a high-level schedule and identifying milestones
- Prioritizing technologies and assignments

Web Services Security Committee Participants

Since SOA is the recommended road map for Global, the goal of the meeting was to apply security, with a focus on emerging security technologies, to the broad interests of the justice community. The immediate objective is to provide research and recommendations on key topics that will benefit Global constituents and to coordinate with the work efforts of the Global Infrastructure Standards Working Group (GISWG) and the Global Security Architecture Committee (GSAC), as well as other justice and public safety communities. The following members, observers, and staff were in attendance:

Gerry Coleman
Wisconsin Department of Justice
Madison, Wisconsin

Fred Cotton
SEARCH, The National Consortium for Justice Information and Statistics
Sacramento, California

Ken Gill
Office of Justice Programs
Washington, DC

Monique La Bare
Institute for Intergovernmental Research
Tallahassee, Florida

Jeff Langford
Integrated Justice Information Services Institute
Gig Harbor, Washington

Ross Mayfield
Marion County, Kansas, Sheriff's Office
Beverly Hills, California

Terri Pate
Institute for Intergovernmental Research
Tallahassee, Florida
Bill Phillips
NLETS - The International Justice & Public Safety Information Sharing Network
Phoenix, Arizona
John Ruegg
Information Systems Advisory Body
Cerritos, California

Web Services Security Committee Discussions

The meeting began with the development of its mission ***"To evaluate emerging Web services security standards for potential customization or extensions needed to support secure justice information sharing."*** Discussion evolved around the question, "Do the current Web services security standards need customizations, modifications, and/or extensions to meet justice needs (to support secure justice information sharing)?" The Committee agreed that the security standards should be evaluated for the unique needs of the justice community. There are certain standards that the justice community can adopt "as is," while there are some standards that will need modifications to adapt to the specific needs of the community. Mr. Gerry Coleman, director of the Crime Information Bureau, Wisconsin Department of Justice and Global SAC chair, discussed the work effort that is being conducted in the Security Architecture Committee and the reconciliation effort that is occurring to develop a baseline for a user profile in order to determine the Security Assertion Markup Language (SAML) credential content.

The Committee discussed how to accomplish their mission, and they agreed to determine potential risk, implementation, interoperability (minimum level of security—define security levels), open system issues, and to coordinate efforts with other Global Committees regarding security related issues. The scope includes the following components.

- Risks
- Security of open systems
- Implementation issues
- Interoperability issues

The Committee provided evaluation and analysis of system needs. The following system needs were discussed and ranked using the nominal group technique with the ranking of "10" as the highest priority.

- Nonrepudiation—10
- Authentication—10
- Integrity—10
- Confidentiality—10
- Interoperability—10
- Policy Management—10
- Encryption Options—9.8
- Trusted Third-Party Mechanism—8.5

- Reliability—8
- Availability—8
- Scalability—8
- Speed/Performance—7.5
- Robustness—7 (conceptual security strength)
- Economy/Affordability—7
- Accuracy—5
- Relevancy—5
- Timeliness—5
- Obsolescence Risk—3

Next, the Committee spent considerable time discussing security technologies and standards for potential analysis. For example, no one in the Global community has drilled into the layers of SOA and of the WS-* suite of specifications to evaluate and provide coordinated input into the justice requirements. Another important area is messaging requirements. WS-* defines specifications for Web services security, reliable messaging, and transactions into categories that are designed to interoperate with existing security models. It is important to note that the WSSC will not develop standards because that is the responsibility of the standards bodies, such as the Organization for Advancement of Structured Information Standards (OASIS). However, the WSSC must identify the base security standards and specifications and tailor them to fit justice requirements to facilitate interoperability at the security layers. In addition, the Committee must define or identify the disparate standards that impact Web services security and provide an update on the maturity of those standards.

Another aspect for consideration is looking at the features of commercial-off-the-shelf (COTS) products for supported capabilities and checking if the vendors have built in specifications needed for the justice community. A recommendation was made to look at the various "buckets"—infrastructure, policy, and messaging. As an action item, the Committee would like to identify standards that are applicable to the justice community without modifications for the April 2005 GAC meeting. While not all of the possible standards were considered during the meeting due to time limitations, the following security standards were discussed as topics for further evaluation.

- MAC Address
- XACML (XML Access Control Markup Language)
- WS-* Standards Framework
  - Management
  - Trust
  - Identity
  - Choreography
  - Orchestration
  - Discovery
  - Description
  - Messaging
  - Transactions
  - Federation
  - Security

- MD5/SHA2
- HTTP/SOAP/HTTPS
- Tokens
- Directory Security
- LDAP
- UDDI
- Firewall/IDS Systems
- Identification
- XML Digital Signature
- SAML
  - Liberty Alliance
  - Shibboleth
- XML Encryption
- WS-*Security
  - PKI Architecture
  - Certificate Management
  - X.509 Certificates
- WS-I Basic Security Profile
- Password
- Biometrics
- SSL
- VPN

Web Services Security Committee Deliverables

The Committee plans to schedule the following work efforts during 2005.

- Collaborate with other security committees, especially on SOA (i.e., GISWG—Standards Committee).
- Provide recommended module/updates for the Pre-RFP Toolkit.
- Update the security document for Web services.
- Analyze open systems applicability to justice information systems and to collaboration with the Integrated Justice Information Systems (IJIS) Institute.
- Recommend modification to profiles or other needed work on standards.
- Address GSWG as the audience.
- Identify and chart the various standards under consideration.
- Determine the level of security that should be in vendor security products.

Action Items

Chairman Cotton assigned the following action items to the Committee with February 1, 2005, as the targeted due date.

- Chart the applicable standards and protocols available—assigned to Mr. Jeff Langford and Mr. John Ruegg.
- Obtain relevant feedback from the field—assigned to Mr. Jeff Langford, IJIS representative.
  - Query the vendor community to see what was used and why.
  - The Committee would like IJIS to play a large role.
- Identify the relationships to each other (what are they designed to facilitate?).
- Are there any obvious gaps? How well do the needs meet the protocols? What are the vulnerabilities?—assigned to each Committee member.
- Determine the applicability to the justice community without modifications, and put the standards into context for the following boundaries.
  - Infrastructure bucket.
  - Policy bucket.
  - Messaging bucket.
- Identify the use cases and the relevant security issues.
  - RSS example.
  - Define the matrix for the various scenarios.

Process and Timeline

The Committee agreed on a twelve-month timeline to accomplish this work effort. The work of this Committee will feed into and integrate with the work of the GISWG and the GSAC. The three-step process will begin with the Committee identifying relevant standards and providing an analysis of each of these standards. Second, the Committee will evaluate whether or not customizations, modifications, or extensions are needed for existing standards. Finally, the Committee will put the standards into context for infrastructure, policy, and messaging. Use cases will provide justice examples for the context.

First Quarter 2005

- What are we protecting?
- What protocols exist?—establish use cases
- What are the gaps?
- What are the risks and dependencies?

Second Quarter 2005

- Develop the recommendations.

Concluding Thoughts

Chairman Cotton thanked the participants for their valuable volunteer efforts and continued support of the Global Initiative. Chairman Cotton requested that the group use the “traction” application as their collaboration tool and requested that their work efforts for this first stage be completed by early February. After a very productive session, the meeting was adjourned.