Global Justice Information Sharing Initiative

Global Web Services Security Task Force
Draft Meeting Summary

Washington, DC
April 30, 2003

Meeting Background and Purpose

The Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), convened the Global Justice Information Sharing Initiative (Global) Web Services Security Task Force ("Task Force") meeting on April 30, 2003, in Washington, DC. The Task Force met 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, The National Consortium for Justice Information and Statistics, chaired the meeting and set forth the agenda with these key discussion points:

- Are there security issues with the deployment of Web services for justice and public safety agencies that go beyond the general security issues?
- What would those issues be?
- What can be done to mitigate the risks of Web services deployment for justice and public safety?

Convening and Introductory Remarks

Chairman Cotton convened the first Task Force meeting by welcoming the participants to Washington, DC. He had the participants introduce themselves. Chairman Cotton informed the Task Force members about their mission and charge. The Task Force meets under the direction of the Global Security Working Group (GSWG). In order to collaborate with other Global Working Groups, and to increase awareness of current and future security topics, the GSWG recommended the development of new task teams to advise Global on prominent security topics, such as Web services security. The 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 individuals were in attendance:

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

Mr. Ken Gill
Bureau of Justice Assistance
Washington, DC

Alan Harbitter, Ph.D.
PEC Solutions, Inc.
Fairfax, Virginia

Ms. Monique Schmidt
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Jim Jolley
SEARCH, The National Consortium for Justice Information and Statistics
Sacramento, California

Mr. Bob Slaski
Advanced Technology Systems, Inc.
McLean, Virginia

Mr. James Pritchett
Southwest Alabama Integrated Criminal Justice System
Foley, Alabama

Web Services Security

The agenda and key discussion points included the specific security issues related to Web services that go beyond the general security issues as addressed in the *Applying Security to Justice Information Sharing* document, which is currently under development by the GSWG. The discussion included the risks of implementing Web services as well as the security practices that should be implemented to mitigate the risks of Web services deployment. The following security topics were explored:

- Security solutions for transport
- Web services and reliable messaging
- Open information access and programmatic access
- Interoperability topics
- Universal Description, Discovery, and Integration (UDDI) repositories
- Web services definition
  - Extensible Markup Language (XML) is the defining basis
  - Simple Object Access Protocol (SOAP) is prominent, but not exclusive
- No standardized security model for Web services
  - Standards are evolving and not mature
    - Multiple standards exist
    - Some agreement among standards, but not necessarily interoperability
  - Web services do not address the Internet Information Server (IIS) security sieve
  - Web services accept queries
  - Web services encourage running the application behind the firewall
  - Web services do not make security issues less critical
- Basic problems of security
  - Confidentiality
  - Integrity
  - Identification and Authentication
  - Availability

The following topics for mitigation were briefly discussed:

- Security architecture
- Real world and best practice examples provided
- Disinformation issues resolved—for example, people should view Web services data exchange on the same level as a postcard that travels through mail and/or e-mail.

Justice Information Sharing Models

Mr. Ken Gill commented that the identified risks fit within the scope of the four models for information sharing that the GSWG had previously developed. The security risk is dependent upon the organizational structure between the agencies that are sharing or exchanging the information, rather than the information technologies implemented. As a result, the security applied is contingent upon governance, policy differences, and collaborative efforts. For the benefit of the Task Force, Mr. Alan Harbitter reviewed the four information sharing models and their application to security.

1. Joint Task Force (JTF) Model—The JTF Model is characterized by the unique type of organizational structure because the participants are often assembled ad hoc to combat a common threat. The security practices are often constructed independently from the member organizations.

2. Peer Group (PG) Model—The PG Model represents a broad category of justice information sharing in which two or more independent organizations work together to provide each other information access and use.

3. Centralized Information Repository (CIR) Model—The CIR Model consists of large information storage with various justice organizations that connect to the data through public or private networks.

4. Justice Interconnection Services Network (JISN) Model—The JISN Model is comprised of a number of related justice information sources (i.e., databases) that are generally scattered across a geographic region. The network owners provide a way to interconnect these sources and make them available to subscribing justice organizations.

Case Studies

Next, the group discussed specific case studies from which practitioners could review lessons learned. The group decided to analyze three different case studies, and to develop the best practices from those implementations for a white paper. Mr. Jim Pritchett provided valuable information on the Southwest Alabama Integrated Criminal Justice System Web services implementation. He discussed read-only data requests as opposed to transactional models, and he stated that ownership is not an issue

for read-only requests, which makes the security models in place satisfactory. In addition, Mr. Bob Slaski discussed the Accelerated Information Sharing for Law Enforcement (AISLE) project. The AISLE project involves the National Law Enforcement Telecommunications System and their Web services implementation as a reliable model. Mr. Gill volunteered to contact and provide information on the Kings County Web services implementation.

Web Services Security Deliverable

Mr. Harbitter volunteered to draft the first version of the white paper. After detailed discussion, the group developed a categorized list of security topics for development, and assigned the components of the deliverable to all participants.

- Background materials
- Scope
- Standards review for the non-technical reader
- Considerations
- Mitigations (recommendations)
- Case studies
- Best practices
- Conclusion
- References

Concluding Thoughts and Next Steps

The group decided to organize a Microsoft Net meeting over the Internet, in order to review the Web Services Security draft, on Tuesday, June 10, 2003. Next steps will be discussed at that time. Chairman Cotton thanked the participants for their valuable volunteer efforts and continued support of the Global initiative. After a short, but very productive session, the meeting adjourned.