Global Justice Information Sharing Initiative

Security Architecture Committee Meeting Summary

Salt Lake City, Utah
June 10, 2004

Meeting Background and Purpose

The Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), convened the Global Justice Information Sharing Initiative (Global) Security Architecture Committee (GSAC or "Committee") meeting on June 10, 2004, in Salt Lake City, Utah. The meeting purpose was to explore security interoperability issues in support of the *National Criminal Intelligence Sharing Plan* (NCISP or "the Plan"). The Plan is a valuable tool to remedy the deficiencies in the current methods of collecting, analyzing, and disseminating criminal intelligence. U.S. Attorney General John Ashcroft, at a May 14, 2004, national signing event, stated that the Plan, "represents law enforcement's commitment to take it upon itself to ensure that we do everything possible to connect the dots, whether it be a set of criminal dots or a set of terrorist dots." The GSAC membership has committed to provide security strategies for interoperability of intelligence systems in support of the NCISP.

The background and history of the GSAC can be traced back to Global forums held in 2003. When the Systems Security Compatibility Task Force met to examine security compatibility issues, they also provided input to the Plan regarding the essential elements for security and interoperability. In October 2003, the Global Advisory Committee (GAC) voted to implement the NCISP. And during the same month, the International Association of Chiefs of Police strongly endorsed the Plan in the adoption of their 2003 resolutions. In response, the GAC Executive Steering Committee established the GSAC in December as a new subgroup of the Global Security Working Group to formulate architecture recommendations for the Plan.

Mr. Gerry Coleman, Director of the Wisconsin Department of Justice Crime Information Bureau, volunteered to take on the leadership position as chairman, after being recommended by Mr. Steve Correll, Executive Director of the National Law Enforcement Telecommunication System. Mr. Coleman and Mr. Correll worked together to establish the direction for the group's activities, including potential security architecture alternatives, GSAC goals, and deliverables for this initial meeting.

Global Security Architecture Committee Participants

Mr. Coleman welcomed participants to the GSAC and invited members to introduce themselves and to brief the Committee about their respective positions and organizations. The following members, delegates, and staff were in attendance:

David Clopton, Ph.D.
National Institute of Justice
Washington, DC
Gerry Coleman
Wisconsin Department of Justice
Chicago, IL
Steve Correll
National Law Enforcement Telecommunication System
Phoenix, AZ
Ken Gill
Office of Justice Programs
Washington, DC
Alan Harbitter, Ph.D.
Integrated Justice Information Systems
Fairfax, VA
Robert Johnson
Minnesota Bureau of Criminal Apprehension
St. Paul, MN
George March
RISS Office of Information Technology
Thorndale, PA
Kent Mawyer
Texas Department of Public Safety
Austin, TX
Patrick McCreary
Office of Justice Programs
Washington, DC
Frank Minice
National Law Enforcement Telecommunication System
Phoenix, AZ
Terri Pate
Institute for Intergovernmental Research
Tallahassee, FL
Philip Ramer
Florida Department of Law Enforcement
Tallahassee, FL
Christina Rogers
California Department of Justice
Sacramento, CA
John Ruegg
Information Systems Advisory Body
Cerritos, CA
Monique Schmidt
Institute for Intergovernmental Research
Tallahassee, FL
Martin Smith
U.S. Department of Homeland Security
Washington, DC
John Wandelt
Georgia Tech Research Institute
Atlanta, GA
David Woolfenden
Pennsylvania Justice Network
Harrisburg, PA

Presentations

Presenters included Mr. Correll, Mr. Phil Ramer, who provided a liaison between the GIWG Connectivity/Systems Committee, and Mr. David Woolfenden, Lead Architect, Pennsylvania Justice Network, who presented a conceptual model on a common sharing architecture that included security management.

Global

Mr. Correll presented information on the importance of the Plan, the purpose of the group, and the activities of the GAC. He stated that the GSAC objective is to develop the security architecture that will provide a baseline, as well as alternative strategies, standards, and methods for interoperability in support of the NCISP.

NCISP

Mr. Philip Ramer, Special Agent in Charge, Florida Department of Law Enforcement, presented information on the development of the Plan by the Global Intelligence Working Group. In particular, Mr. Ramer shared the insights from the Connectivity/Systems Committee in the development of their recommendations for the Plan. This provided the group with a baseline of information to work from in the

development of ideas. The basis of the GSAC is stated in NCISP as *Recommendation 23*, which is outlined below:

- To identify and specify an architectural approach and transitional steps that allow for the use of existing infrastructures
- To leverage the national sensitive but unclassified communications capabilities for information sharing
- To ensure interoperability among local, state, regional, and federal intelligence information systems and repositories

Conceptual Model

Mr. David Woolfenden, Lead Architect, Pennsylvania Justice Network, presented information on a conceptual model for a common sharing architecture that illustrated security plug-in services. Components of the conceptual model include the following services with a direct pipeline to security management, which is credential-based.

- Knowledge Delivery—Access Point (i.e., Portal), Search/Index, Electronic Business Extensible Markup Language (ebXML), Registry, Wireless Gateway, and Web Services
- Applications/Collaboration—Application Server, Workflow Server, Rules Engine, Reporting, Geographic Information System (GIS), Knowledge Base, Instant Messaging, Forums, E-mail, and Web Services
- Data Integration—Metadata Repository, Virtual Database, Extract, Transform, Load (ETL)/Batch, Internal Data Store, and Web Services
- Application Integration—Integration Broker, Business Process Management (BPM), Message Oriented Middleware (MOM) Hub, and Web Services
- Agency Enterprise Information Systems—Intelligence Systems, Imaging/Document Management, Relational Database Management System (RDBMS), MOM, Legacy Systems, File System, Enterprise Application Integration (EAI), and Web-enabled applications

This conceptual model provides a portal with an established trust mechanism and is based on defined standards, such as Liberty Alliance architecture and standards. It is an interoperability framework that is used to share information across different domains. For a diagram of this proposed conceptual model, please see Appendix A.

Group Discussions, Technology Concepts, and Security Assumptions

Mr. Coleman directed open discussion on security and technology concepts critical to trusted information sharing for intelligence systems. In turn, the Committee reached consensus on the key concepts involved. GSAC recognized the importance of the following technology concepts and standards.

Technology Concepts

- Portal—Portal is defined as the access point or public facing Web site that enables interaction with and access to justice information and services via a number of different access channels. A portal provides two things: 1) user interface and 2) messaging interface. It is an enabling technology for the intelligence function, which may involve a proxy-based authentication portal to connect the interfaces to the intelligence systems.
- Framework—The Committee noted that it is important to discuss the framework, standards, and architecture rather than to focus on the network "wires." This terminology recognizes that a strategy is in place for those that are looking to the future. And, the framework enables practitioners to translate back and forth between what is currently in place and the recommended standard. The framework will enable a local, state, regional, and federal focus rather than connecting two individual intelligence systems.
- Log-on—Log-ons and credentials are related in a way that will solve the problem of multiple log-ons.
- Credential—The credential represents an individual who is actually requesting information, such as a law enforcement officer or firefighter, and should be identified within the service request to the intelligence system. This identification is independent of the intelligence system, and it represents the individual electronically.
- Security Assertion Markup Language (SAML)—SAML is a native credentialing tool that allows a user to log on once for affiliated but separate Web sites. SAML is to authentication as XML is to data exchange. The GSAC will need to take SAML specifications and custom tailor the attributes to the justice community similar to the process that occurred for the Global Justice XML Data Model.
- ebXML Message Services Specification Version 2.0—The ebXML message specification provides a single open, standards-based enveloping and messaging protocol technology that can be used for requests and responses between all the architectural components of the intelligence system.
- Liberty Alliance Project—This initiative was established in December 2001, with the goal of creating open, interoperable standards and guidelines for federated identity management. Federated identity management makes it possible for an authenticated identity to be recognized and take part in personalized services across multiple

domains.[1] Liberty Alliance is a potential architecture for consideration by the GSAC.

- Electronic Authentication Partnership (EAP)—Multiindustry partnership working on the vital task of enabling interoperability among public and private electronic authentication (e-authentication) systems.[2]

Security Assumptions

After considerable discussion, the following three assumptions were established for the security framework.

1) There are many, but a finite number, of intelligence systems.

GSAC is focused on developing a target architecture that creates a minimum baseline for interoperability. The group discussed in detail the essential elements of one user or device obtaining access to one or more intelligence systems as interim solutions. The discussion involved not only the potential interim solutions but also realistic solutions for the longer term.

2) A person (agent, application) can be associated reliably with a credential.

Mr. Coleman stated that in law enforcement the credential means the officer wears a badge. However, in the information technology world, you would have to create a data block that represents the individual. The log-on process involves providing a credential to gain access into the system through some method of authentication. Mr. Ruegg, Director of the Information Systems Advisory Body, added that there needs to be a place to obtain the credential; for example, RISSNET provides a credentialing service. There may be regional systems or a hierarchy of services that provides secure access to intelligence systems.

3) Based on credential content and the credentialing process, intelligence systems will allow access.

Mr. Martin Smith, U.S. Department of Homeland Security, illustrated the concept of a community of trust by using eBay as an example, since eBay uses community scores to establish trust. There needs to be some recognized method to provide acceptable levels of trust within the justice community for access into intelligence systems. Identity is at the core of access requests and data exchange for each transaction within an intelligence system. An individual's identity proves who he says he is, what he can do, and what resources he can access. Group discussion also involved topics such as data interface standards, access control standards, privilege management, and technical interface standards, such as ebXML and

[1] Whitepaper: Benefits of Federated Identity to Government, Liberty Alliance Project, March 7, 2004, www.projectliberty.org

[2] http://www.eapartnership.org/

SAML. Figure 1 illustrates access to various intelligence systems with a credential.

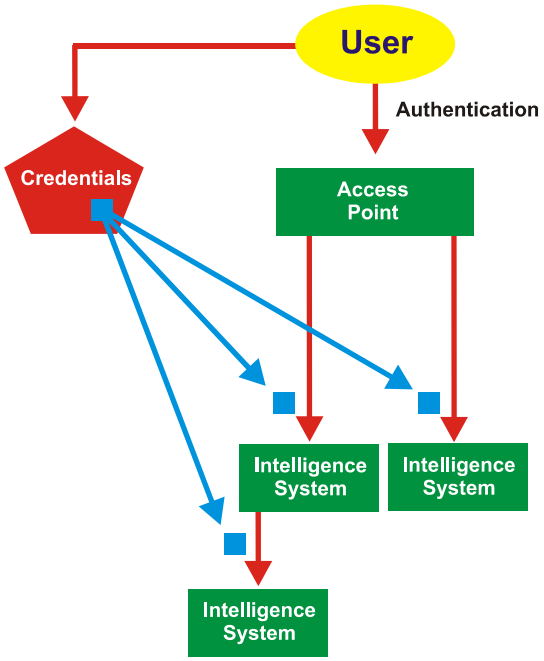

Figure 1: Access Point for User Credentials

Deliverables, Next Steps, and Action Items

The group determined that a process or hierarchy is necessary to establish a credentialing service because a community of trust is essential to obtain access to intelligence systems across multiple and independent domains. Security access points and mapping will be required through regional systems to provide an electronic credentialing service that will be similar to a law enforcement officer showing a badge—an electronic credential or "data block" will represent the identity of the justice practitioner. In addition, the similarity to the Global Justice XML Data Model reconciliation project was mentioned to bring to mind the large effort that will be involved to iron out the content of the credential. The initiative will be standards-based, and it will use SAML (Security Assertion Markup Language) and, perhaps, Liberty Alliance (federated identity). SAML is an Extensible Markup Language (XML) standard that allows a user to log on once for affiliated but separate Web sites. The process that was established was to 1) have Mr. John Wandelt establish a baseline for the content of the credential, 2) reconcile CISAnet to RISSNET, and 3) get a team of technical people together to work out the details of the credential (like the process that was completed by the Global XML Structure Task Force).

The Committee reached consensus on a two-prong approach: first, a tactical solution geared to represent the interim successes of the connections that regional programs have committed to achieve via point-to-point connectivity, and, second, a long-term strategic approach to develop a target architecture that programs can aim to achieve. GSAC needs the use cases for the long-term framework, and they need the "connectivity successes" to represent and illustrate the tactical solutions that programs have committed

to or have already accomplished. Mr. Correll will present the short-term successes at the next GAC meeting. Participants requested that the use cases be technical rather than functional. The following action items were delegated as "homework" with a July 19, 2004, due date.

Issue One: Develop a scope statement for the GSAC recommendation.

Status: This assignment was delegated to Mr. David Woolfenden for completion as soon as possible.

Issue Two: Develop a problem statement that reflects the critical need for trusted and secure information exchange and interoperability among local, state, regional, and federal intelligence information systems and repositories.

Status: This assignment was delegated to Ms. Christina Rogers for completion as soon as possible.

Issue Three: Develop a concept diagram and target architecture based on the scope, problem statement, and Committee discussions.

Status: This assignment was delegated to Mr. Alan Harbitter for completion by July 19, 2004.

Issue Four: Develop a pilot project for federated authentication.

Status: The Committee recommended the idea of implementing a demonstration pilot in order to better examine the authentication process in combination with best practices. Mr. George March agreed to put together a white paper briefing and/or proposal for group discussion on the RISS Trusted Credential project. The RISS Trusted Credential project is currently under way and is based on a federated authentication approach. Mr. Patrick McCreary also requested to add Mr. Martin Smith (DHS) to work with OJP/DOJ to explore and identify subject-matter experts to attend a future meeting to discuss potential plans for a "trusted credential" pilot.

Issue Five: Develop some use-case scenarios.

Status: The Committee recommended the idea of specifying concrete examples of data exchange in law enforcement for the intelligence function. Use cases should be technical rather than functional. Reviewing each scenario in a step-by-step process will allow the group to determine how to best establish a trusted credential. Mr. Kent Mawyer volunteered to develop the use cases by July 19, 2004.

Issue Six: Develop a definition for the credential and some baseline content for the credential.

Status: This assignment was delegated to Mr. John Wandelt for completion by July 19, 2004.

Issue Seven: Write down a couple of paragraphs on short-term successes on achieving connectivity to RISS/LEO in support of the Plan for reporting at the next GAC meeting.

Status: This assignment was delegated to everyone on the committee. The short-term successes need to be reported at the next GAC meeting on September 28-29, 2004. Each person needs to report their "successes" on what is occurring locally to support connectivity in compliance with the Plan. The short-term successes are due prior to the next GSAC meeting and should be e-mailed to Ms. Monique Schmidt.

Issue Eight: Identify intelligence systems and networks that we want to be interoperable (local, state, regional, and federal).

Status: GIWG is currently working on this project.

Issue Nine: Identify core group for technical subcommittee meeting for a long-term solution.

Status: OJP will determine the candidates. This committee will be based on collaboration to establish a baseline and reconciliation of the content of the credential. To establish a credential, the subcommittee will start with a baseline and then review what RISSNET and CISAnet are using as content in their credentials. On July 8, 2004, OJP determined that a technical subcommittee was not necessary for the interim solutions.

Closing Thoughts

The Committee agreed on a two-pronged approach—first, a tactical solution geared to represent the interim successes of the connections that regional programs have committed to achieve via point-to-point connectivity and, second, a long-term strategic approach to develop a target architecture that programs can aim to achieve. Use cases are needed for the long-term framework, and the "connectivity successes" will represent and illustrate the tactical solutions that programs have committed to or have already accomplished. Mr. Correll plans to present the short-term successes at the next GAC meeting.

In conclusion, the Committee expressed an interest in using established standards to provide an authentication process using trusted credentials that are established by and tailored to the justice community. The Committee decided to focus their work efforts on setting security recommendations that will better position the justice community for the future. Once these recommendations are developed, justice organizations will be able to identify purchasing requirements and migration strategies, if needed.

Mr. Coleman thanked the participants for their teamwork and for their commitment and support of the Plan. Mr. Coleman decided on the due date of Monday, July 19, 2004, for completion of the homework assignments. The Committee recommended the next meeting be held during the week of August 16, 2004, and, as directed, the next meeting will be held on August 18, 2004, in McLean, Virginia, in

conjunction with the next Global Intelligence Working Group meeting. With no further business to discuss, the meeting was then adjourned.

Appendix A: Common Sharing Architecture – Conceptual Model