Global Justice Information Sharing Initiative

Security Architecture Committee Meeting Summary

McLean, Virginia
August 18, 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") on August 18, 2004, in McLean, Virginia. The meeting purpose was to explore security interoperability issues in support of the *National Criminal Intelligence Sharing Plan* (NCISP). The GSAC membership has committed to develop a security framework for the interoperability of intelligence systems in support of the NCISP.

The objective of the meeting was to provide basic information on federated identity management in order to provide a context for group discussions on security architecture and to review the draft homework assignments. Agenda items included the following discussion topics and presentations:

- The *National Criminal Intelligence Sharing Plan* and Global Intelligence Working Group (GIWG) Connectivity Committee Update
- E-authentication terminology briefing
- Intelligence information sharing systems currently in place
- Federated identity management and trust models
- Shibboleth[1] and OpenSAML[2]
- Group discussions on assignments
- Action items, next steps, and deliverables

Global Security Architecture Committee Participants

Mr. Gerry Coleman, GSAC chairman and Director of the Wisconsin Department of Justice Crime Information Bureau, welcomed the guest speakers, observers, and GSAC member representatives to the second GSAC meeting. In addition, Chairman Coleman announced that Mr. John Ruegg, Information Systems Advisory Committee, has been appointed the GSAC vice chairman.

The following members, delegates, and staff were in attendance:

[1] http://shibboleth.internet2.edu/.
[2] http://www.opensaml.org/.

Hyuk Byun
National Institute of Justice
Washington, DC
Scott Cantor
Ohio State University
Columbus, OH
David Clopton, Ph.D.
National Institute of Justice
Washington, DC
Gerry Coleman
Wisconsin Department of Justice
Chicago, IL
James Gerst
Federal Bureau of Investigation
Clarksburg, WV
Ken Gill
Office of Justice Programs
Washington, DC
Alan Harbitter, Ph.D.
Integrated Justice Information Systems Institute
Fairfax, VA
Robert Johnson
Minnesota Bureau of Criminal Apprehension
St. Paul, MN
Monique La Bare
Institute for Intergovernmental Research
Tallahassee, FL
George March
RISS Office of Information Technology
Thorndale, PA
Chief 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
Doug Moench
The Burton Group
Latham, NY
Chief Daniel Oates
Ann Arbor Police Department
Ann Arbor, MI
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
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

The presentations during the first half of the day focused on Global updates, federated identity management, and trust models, which provided the context for the day's work. Chief Daniel Oates, Ann Arbor Police Department, and chair of the GIWG Connectivity Committee, provided a status update on the NCISP. Mr. Doug Moench, The Burton Group; Mr. Scott Cantor, Ohio State University; and Mr. John Wandelt, Georgia Tech Research Institute (GTRI), presented on the federated identity management and trust model concepts.

NCISP

Chief Oates provided an update on the GIWG Connectivity Committee. He discussed the initial meeting of the Criminal Intelligence Coordinating Council (CICC) and the support that has been received, specifically during the National Kick-Off Event on May 14, 2004, by U.S. Attorney General John Ashcroft. In addition, he addressed the GIWG Connectivity Committee's efforts to develop a nationwide survey of intelligence

systems. The National Institute of Justice (NIJ) has funded a survey and will provide an analysis of multijurisdictional systems and related architecture. The GIWG will be partnering with the NIJ to determine details and architecture from the survey regarding intelligence data.

E-authentication Terminology

Mr. Wandelt, GTRI, presented information on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Recommendation for Electronic Authentication,[3] Office of Management and Budget (OMB) Memorandum M-04-04,[4] and related terminology. Mr. Wandelt had worked with Mr. Bill Burr, NIST Computer Security Division, to provide the GSAC with an analysis of the E-authentication guideline, and he also explained trust domains, architectural use cases, assurance levels, credentials, tokens, and assertions to the Committee. The E-authentication guideline is important because it provides a common abstract model and valuable common language for understanding the basics of the technology. The group agreed that, as an abstract model, E-authentication is a good initiative to track, although it may not apply to the GSAC; however, the terminology needs to be discussed, evaluated, and then taken to the next level in order to provide not only authentication but also identity management and authorization for justice applications. After considerable discussion, the group also reached consensus that the GSAC needs to profile and define the content for the "assertion" and not the "credential." An assertion is defined as a statement from a verifier to a relying part that contains identity information about a subscriber. Assertions may also contain verified attributes.

Federated Identity Management and Trust Models

Mr. Moench provided a presentation titled "Federation Makes Waves as Standards and Trust Models Emerge." He presented information on specifications (i.e., Security Assertion Markup Language [SAML], Liberty Alliance, and WS-*), trust management, and the progress of federation standards. Federated identity management is defined as agreements, standards, and technologies that make identity and entitlements portable across autonomous domains. It is a key technology that is evolving with Web services. In addition, Mr. Moench discussed trust, which is the willingness of a party to take action based on its relationship with another party. He recommended that the GSAC stay on top of the standards as they evolve and continue to make progress on identity management architecture even though the standards have not reached maturity yet. He stated that federated identity is in use today by many organizations and that the work of these organizations needs to be leveraged to avoid "recreating the wheel." In addition, he further recommended that to ensure interoperability, the GSAC must agree on the standard and version, as well as agree on the profiles and use cases. Finally, he recommended that the assertions not be made specific to any one application; instead, he

[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Recommendation for Electronic Authentication, June 2004, http://csrc.nist.gov/publications/nistpubs/800-63/sp800-63v6_3_3.pdf.

[4] OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.

suggested putting the minimal amount of information in the first exchanged assertion and then later building another exchange if more information is needed. Besides federation, other issues such as developing a trust model and prerequisites for implementing specifications are critical to resolution of the problem.

Shibboleth and Open SAML

Mr. Scott Cantor, Internet2/Middleware Architecture Committee for Education (MACE) and the Ohio State University, presented highly technical and detailed information on the Shibboleth project, which is middleware, and an Internet2/MACE initiative to develop a standards-based architecture and policy framework that supports the sharing of secured Web resources and services. Shibboleth is a software project delivering an open-source implementation of the architecture and framework, and it is based on the OASIS SAML 1.1 specification.[5] MACE is a steering committee of about 20 technologists for middleware activities within Internet2. The umbrella group, Internet2, is a consortium of over 200 research institutions, with corporate and government partners, developing technologies in support of the next generation of networking and applications.

Mr. Cantor defined federated identity as a technology-neutral approach to make identity:

- Portable
- Manageable
- Dynamic
- Conditional
- Contextual

Mr. Cantor explained how the federations generalize bilateral arrangements between sites so that policy can be delegated and scaled. He also presented project information on the technical architecture, federation services, federation examples, road map, and lessons learned. In terms of the standards, Mr. Cantor defined what specifications exist today and illustrated how they will most likely converge in the future. Although SAML 2.0 is still in committee draft, the Shibboleth project will move toward SAML 2.0 in the 2005 time frame.

Group Discussions on Assignments

Use Cases and Conceptual Model

Mr. Alan Harbitter, Integrated Justice Information Systems Institute (IJIS), Industry Working Group (IWG), and PEC Solutions, presented information on a draft conceptual model for a common sharing architecture that illustrated three different architectural use cases for identity assertions, as shown below.

[5] http://www.oasis-open.org/committees/security.

- User to user
  - Peer-to-peer trust
  - For example, e-mail, messaging
  - Is this within the scope of the Committee?
- User to cross-domain application
  - Users gain access to a specific application through their existing infrastructure
  - For example, real-time collaboration tools, search-and-query tools, reports, and analytical tools
  - Users need cross-domain access to data
  - Applications are working on behalf of a user
  - Secure Socket Layer (SSL) trade-off discussion for secure network interconnectivity
- System to cross-domain system
  - Users gain access to resources and services connected to the federation through their local enterprise. User vetting and maintenance is retained by local enterprise
  - Application to cross-domain application
  - Generalized index of systems is needed, like Google

Mr. Cantor facilitated a discussion on use case scenarios based on SAML specifications. He explained the difference between the "pull" and "push" models for the assertion, adding that the "pull" model is the assertion component in today's environment. Another important issue was the use of SSL for the user-to-application scenario, and there was considerable discussion regarding the SSL trade-off with secure network interconnectivity. The Committee agreed that multitiered security—secure interoperability—is a very difficult security problem. Mr. Harbitter volunteered to refine his three conceptual diagrams based on Committee discussions.

RISSNET Trusted Credential Pilot

Mr. George March, Regional Information Security Systems™ (RISS), presented information on the scope and planned phases of the RISS secure intranet (RISSNET™) Trusted Credential project that will provide the capability for an industry standard credential to be used and validated within RISSNET. This will provide the additional functionality of identity attributes so that the application and/or system will know who the individual is with specificity. An essential requirement for the originating organization will be that it uses good practices for issuing the credential. For example, an individual with a Florida Department of Law Enforcement credential will have their credential passed along and then validated by RISS.

RISS is also developing a portal for access to its applications. The Committee discussed additional requirements, such as brokering a Law Enforcement Online (LEO) user to Criminal Information Sharing Alliance network (CISAnet) through RISSNET. Mr. March stated that brokering is not within the scope of this pilot; however, if the Committee decides to make a recommendation, then RISS would be willing to take on additional functional requirements for its Trusted Credential pilot. Chairman Coleman

stated that the GSAC is interested in tracking demonstration pilots and recommending potential GSAC requirements; however, it may not be within the scope of this Committee to implement a pilot.

Other Homework Assignments

Chairman Coleman requested that the GSAC continue its work efforts on their assignments and requested that the work be very interactive, in either offline or online forums, but prior to our next meeting.

GSAC Potential Deliverables

The following GSAC deliverables will be compiled into a document that will represent a series of chapters in the planned GSAC publication.

1. Scope and problem statement
2. Use cases—functional and architecture concept diagram
3. Target architecture (i.e., ConOps)
    a. Interoperability framework
    b. Support of all use cases combined
    c. Method to do the blue cloud
    d. Possible inclusion of attributes
    e. Logical—defines roles, responsibilities, governance, and trust model
4. Definition and content of assertions
    a. Need to select supported standard(s) and profiles
    b. SAML 2.0 is not an approved standard, so timeline is critical
5. Elements of security requirements that would be proof of concept in a pilot program (Provide George March with space in the document.)
6. Success stories
    a. What achievements have occurred
    b. Security architecture characteristics that demonstrate some elements of cross-domain intelligence sharing
    c. Intelligence sharing cross domains
7. Security policies and procedures
    a. Guidelines and a vetting process
    b. NIST, Industry Standards Organization (ISO), Global Security Working Group document

Deliverables, Next Steps, and Action Items

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

Status: Mr. David Woolfenden has completed the initial draft, and it has been sent out for group review.

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: Ms. Christina Rogers has completed the initial draft, and it has been sent out for group review.

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

Status: Mr. Alan Harbitter presented initial concepts to the Committee, and he will refine his diagrams based on group discussions.

Issue Four: Develop justice requirements for a proof of concept/demonstration project.

Status: Not assigned

Issue Five: Develop some use-case scenarios.

Status: Mr. Wandelt and Mr. Harbitter have developed three use cases and are currently working to refine them.

Issue Six: Develop a definition and content of assertions.

Status: Mr. Wandelt will research this item.

Action Item: Mr. Wandelt needs to have all system owners identify what they need (privileges, roles, and attributes) to gain access to the system.

Issue Seven: Write a short summary of short-term successes on achieving connectivity to RISS/LEO in support of the NCISP 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 Global Advisory Committee 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 NCISP. The short-term successes are due prior to the next GSAC meeting and should be e-mailed to Ms. Monique La Bare at mlabare@iir.com.

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

Status: Completed. GIWG delivered a list of systems to the GSAC for review. NIJ is currently working on the development of a survey.

Closing Thoughts

In closing, Chairman Coleman stated, “Security is working fine, and we have seen some examples today of how to extend and move into the direction of what needs to be done. We need to define specifications, but it is coming together.” The target date for the next GSAC meeting was set for Wednesday, December 1, 2004. With no further business to discuss, the meeting was then adjourned.

Summary SAC 8-04.doc