Global Justice Information Sharing Initiative

Security Architecture Committee
Meeting Summary

Arlington, Virginia
December 1, 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 December 1, 2004, in Arlington, Virginia. The meeting purpose was to explore security interoperability issues in support of the *National Criminal Intelligence Sharing Plan* (NCISP). The GSAC membership will 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:

- Scope Statement
- Problem Statement
- Federated Identity and Privilege Management Security Interoperability Demonstration
- Trusted Credentials Project
- Federated Directory Project—Wisconsin Department of Justice
- Operating Concept Diagram and Target Architecture
- SAML Definitions and Requirements
- 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 observers and GSAC member representatives to the third GSAC meeting. New members in attendance included Mr. Bill Phillips representing NLETS - The International Justice and Public Safety Information Sharing Network and Mr. Ancil McBarnett representing Pennsylvania Justice Network (JNET).

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

David Clopton, Ph.D.
National Institute of Justice
Washington, DC
Gerry Coleman
Wisconsin Department of Justice
Madison, WI
Ken Gill
Office of Justice Programs
Washington, DC
Alan Harbitter, Ph.D.
Integrated Justice Information Systems Institute
Fairfax, VA
Monique La Bare
Institute for Intergovernmental Research
Tallahassee, FL
Larry Maloney
RISS Office of Information Technology
Thorndale, PA
George March
RISS Office of Information Technology
Thorndale, PA
Kent Mawyer
Texas Department of Public Safety
Austin, TX
Ancil McBarnett
Pennsylvania Justice Network
Harrisburg, PA
Terri Pate
Institute for Intergovernmental Research
Tallahassee, FL
Bill Phillips
NLETS - The International Justice and Public Safety Information Sharing Network
Phoenix, AZ
Christina Rogers
California Department of Justice
Sacramento, CA
John Ruegg
Information Advisory Body
Cerritos, 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

Global Security Architecture Committee Activities

Mr. Coleman provided a recap of the GSAC purpose—to define the security architecture and to put that architecture into a context. Participant activities since the previous meeting are:

- Scope Statement was written by Ms. Christina Rogers.
- Problem Statement was written by Mr. David Woolfenden.
- Target Architecture Document was written by Dr. Alan Harbitter.
- Security Assertion Markup Language (SAML) Content Baseline Requirements Survey was conducted and compiled by Mr. John Wandelt.

Currently, the foundational component of the architecture is federated identity management. Mr. Coleman stated, "So far we have devoted our time to authentication and to defining attributes that a person would use to get into a known but disparate system." The Committee has spent considerable time discussing the following questions.

- What are the attributes of a particular person and how do you control access to information?
- Is that part of security architecture?
- What and how much do we know about a person?

- Vice versa, how does a system control access into its systems/applications?
- What are the characteristics of a person that might be useful for system/application owners to know?

Ms. Rogers requested closure on the scope and problem statement within four weeks. Mr. March recommended the use of the "Traction" application as the Global collaboration tool for document revisions.

Global Security Architecture Committee Deliverable

The GSAC deliverable will be a paper providing recommendations to the Global Advisory Committee (GAC). An outline and Executive Overview will be ready by the April 2005 GAC meeting. The target date for completion is July 1, 2005. The document will cover the following components of the security architecture.

- Introduction
- Scope—Currently includes federated identity management
- Problem Statement—How does a user from one system (i.e., California DOJ) access another disparate system/application (i.e., JNET)?
- Use Cases—Examples from each of the three use cases and based on law enforcement
- Principles and Assumptions
- Services—Covers technical services/components provided by the federated security architecture, for example, identity management service and privilege management service
- Standards—Includes standards required by the architecture
- Implementations—Demonstrates the federated security architecture
- Glossary
- Appendix: SAML Attributes and Privilege Management—Technical content of SAML[1]
- Appendix: Committee Members

Monitored Demonstration Projects

There are three demonstration projects that the committee is closely monitoring. These projects provide the committee with technical/standards input, lessons learned, and implementation strategies but are separate from and adjunct to the GSAC.

[1] Definition: SAML (Security Assertion Markup Language) is an Extensible Markup Language (XML) standard that allows a user to log on once for affiliated but separate Web sites. SAML specifies three components: assertions, protocol, and binding. There are three assertions: authentication, attribute, and authorization. Authentication assertion validates the user's identity. Attribute assertion contains specific information about the user. And authorization assertion identifies what the user is authorized to do.

- RISSNET™ Trusted Credentials Project
- Wisconsin Department of Justice Federated Directory Pilot
- Federated Identity and Privilege Management Security Interoperability Demonstration ("Demonstration Project")

Demonstration Project Overview

The programs that will participate in the initial phase of the Demonstration Project include Criminal Information Sharing Alliance Network (CISAnet), Regional Information Sharing Systems® secure intranet (RISSNET), and the Pennsylvania Justice Network (JNET). Other demonstration project stakeholder programs include the U.S. Department of Homeland Security (DHS) Homeland Security Information Network (HSIN)/Joint Regional Information Exchange System (JRIES), the Automated Regional Justice Information System (ARJIS), and the California and Wisconsin Departments of Justice.

The focus of the Demonstration Project is to: 1) achieve a "quick win," 2) capture "lessons learned," and 3) lay a foundation for moving forward. The intent of the focus group is to demonstrate a "real life" multidirectional electronic exchange of criminal intelligence information, achieved through secure systems interoperability between networks/information systems currently not capable of doing so. However, this Project will not be operational.

The scope of the Demonstration Project is to develop and prove an identity and privilege management service that can be used to apply authentication and access controls by disparate systems and networks desiring to make their resources "shareable." The deliverable is intended to demonstrate a universal mechanism, implementation-independent and nonvendor specific, designed to share trusted assertions (agreed set of attributes) that can be used to apply authentication and access controls.

Target Architecture

After considerable discussion of the technical concepts, the Committee reviewed and provided input to organization and content of the Operating Concept Diagram and Target Architecture paper that Dr. Harbitter authored. The target architecture provides a secure intelligence information interchange framework. Principles include local jurisdiction of user information/authentication, standards-based framework, and federated authorization/privilege management by the system/resource owner (i.e., using SAML, an identity service, a privilege management service, and other framework services as described in the paper) among known but disparate systems. There are three scenarios that are being used as cross-domain examples:

- User-to-application
- System-to-system
- User-to-user

This paper is a starting point that will evolve to become the GSAC deliverable.

SAML User Profile Reconciliation

Prior to the meeting, Mr. Wandelt had surveyed the system owners and collected data for each of the system's user attributes. This survey will provide the content for the user profile or assertion. Similar to the work that was done to reconcile XML, Mr. Wandelt will need to compile the information submitted from the group participants and come up with a straw man for a list of user attributes as a baseline of information for vetting. Once the data is compiled, Mr. Coleman will identify a subgroup for a follow-up technical meeting. The purpose will be to provide system owners the opportunity to continue to work on the SAML attributes as a next step. There are two competing SAML implementations (Shibboleth or Liberty Alliance). Regardless of the SAML implementation, the committee will be able to move forward with a technical recommendation. The objective is to provide SAML credentials that are tailored to the justice community.

Action Items, Next Steps, and Deliverables

Discussions on the deliverables included preparation for the GAC—from broad to very technical.

- Executive Overview
- Recommendation documentation
- Standards specification for the SAML assertions

The Committee agreed to review the draft documentation by the end of January 2005. The goal is to have a written recommendation to GAC for the April 27-28, 2005, meeting. The Committee also discussed putting together an Executive Overview in layman's terms of what they are trying to accomplish. The GSAC agreed to wait until further work was completed before scheduling another meeting. Until then, work will be completed through the Traction collaboration tool.

Upon completion of the agenda, the meeting was adjourned.