Global Justice Information Sharing Initiative

Security Working Group
Meeting Summary

Denver, Colorado
July 19, 2004

Meeting Purpose

The Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), convened the Global Justice Information Sharing Initiative (Global) Security Working Group (GSWG or "Working Group") on July 19, 2004. The purpose of the meeting was to deliberate wireless security priorities and to develop wireless security documentation in support of Global. While information sharing challenges are similar for wired and wireless data exchanges, the GSWG would like to focus on developing best practices for justice scenarios that encompass aspects unique to wireless communications.

Global Security Working Group Participants

Chairman Steve Correll, Executive Director, National Law Enforcement Telecommunication System, welcomed participants to the GSWG. Members from the Privacy and Information Quality Working Group also attended this meeting in order to provide collaboration on the group discussions. The following members, federal officials, delegates, invited guests, and support staff were in attendance:

David Buchanan
County of San Bernardino
San Bernardino, California

Bruce Buckley
Institute for Intergovernmental Research
Tallahassee, Florida

David Clopton, Ph.D.
National Institute of Justice
Washington, DC

Steve Correll
National Law Enforcement Telecommunication System
Phoenix, Arizona

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

Cabell Cropper
National Criminal Justice Association
Washington, DC

Ken Gill
Office of Justice Programs
Washington, DC

Joseph Hindman
Scottsdale Police Department
Scottsdale, Arizona

Kathy Imel
National Law Enforcement and Corrections Technology Center
Rocky Mountain Region
Westminster, Colorado

Monique La Bare
Institute for Intergovernmental Research
Tallahassee, Florida

Jeanette Plante
U.S. Department of Justice
Washington, DC

John Powell
National Public Safety
Telecommunications Council
Denver, Colorado

Donna Rinehart
Institute for Intergovernmental
Research
Tallahassee, Florida

Charles Pruitt
Arkansas Crime Information Center
Little Rock, Arizona

Andrew Thiessen
National Telecommunications and
Information Administration
Boulder, Colorado

Problem Statement Recap and Overview

At the June 2004 GSWG meeting, the Working Group identified several factors leading to the increasing need for secure wireless communications to ensure interoperability and the trusted sharing of information among the 2.3 million uniformed local and state law enforcement, fire, and emergency medical services personnel within the justice community. The use of all types of wireless devices by the public safety and justice community has grown to approximately 6.9 million devices and is projected to be at least 13.8 million by the year 2008. A law enforcement officer will have on average three devices, such as a portable radio, pager, personal digital assistant (PDA), cell phone, and laptop. The same device may be used by more than one officer, which adds a layer of complexity. Agencies may set up temporary wireless broadband networks at incident sites as well. In addition, law enforcement's roaming and mobility requirements impact interoperability, support, and information sharing specifications and standards. Given the increase in the number of devices, applications, and networks involved in responding to incidents, security has become a critical hot-button issue and an enormous challenge for police chiefs and other first responders.

Another factor that impacts the level of importance of wireless security is the planned spectrum to be released in the first quarter of 2005 that will aid public safety and the justice community by freeing up contiguous 800 MHz spectrum and by reducing the degree of interference within the band. Essentially, the release of new spectrum will increase the need for a target framework for wireless security as police chiefs and other decision makers purchase technology for local use. Guidance is needed in terms of spectrum-sharing concepts for security to facilitate information sharing and interoperability.

Lawmakers, decision makers, and practitioners are pushing for tighter security and tougher requirements because of cyber security threats from Internet hackers and terrorists. The sheer impact of numbers and the ease of generating known attacks like eavesdropping and denial of service can lead to disastrous impacts if the risks are not mitigated. Current security technologies and protocols such as Wired Equivalency Privacy (WEP), Wireless Protected Access (WPA), and Software Defined Radio (SDR) are not without major disadvantages when implemented by justice practitioners. Strategies that identify the risks and discuss potential solutions will help to guide practitioners when they roll out new technology, and question-and-answer sets will aid decision makers in making purchases.

Finally, interoperability and information sharing within the justice community requires the ability to talk to whom you need to talk to, when you need to talk to them (data and voice) in real time. There is a critical need for message transport and network security, authentication/privileges, privacy, attack detection and prevention, monitoring, access control, and interoperability standards.

Scope

The GSWG scope will include the entire justice community for Global constituents as well as first responders. Intended audiences for wireless security products are practitioners who need to know how to deploy security and mitigate risks, decision makers who need to be aware of the major threats and who need guidance when purchasing security technologies, and legislators and government associations who can facilitate awareness of the security issues and challenges and provide policy-level recommendations. In addition, local and state information security officers need training.

Security Deliverables

Given the level of wireless security threats, the increased use of wireless devices, and the tightening of security policies, the Working Group convened to discuss wireless security topics and to develop a strategy in support of its mission to enable the trusted sharing of justice information by recommending best practices for security guidelines, technologies, and procedures. After considerable discussion, the following deliverables were discussed and recommended by the GSWG in order to immediately help justice practitioners.

Product One

The first product will be a comprehensive primer in CD format, and it will include the following components:

- Executive summary (2-3 pages)
- Key concepts
- Definitions
- Resources
- Glossary
- Identification of the major security differences between wired and wireless communications
- Question-and-answer product

The wireless security environment will be identified by disciplines and/or domains in order to leverage the work of the first product, *Applying Security Practices to Justice Information Sharing* CD. Components will include:

1. Attack detection and prevention (replaces Intrusion Detection System and Critical Incident Response sections from the *Applying Security Practices to Justice Information Sharing* CD*)*
2. Auditing
3. Disaster recovery and business continuity
4. Identification and authentication
5. Authorization and access control
6. Data integrity
7. Data classification
8. Change management
9. Public access, privacy, and confidentiality
10. Firewalls, VPNs, and other network safeguards
11. Governance
12. Physical security
13. Personnel security screening
14. Separation of duties

Eventually, this product will feature more technical detail, and it will be developed with purchasing decisions in mind, i.e., similar to a Pre-RFP Toolkit. It will include questions to ask vendors under each domain, and the appropriate answer/solution sets for enhanced security capabilities will be vetted through the proper channels to provide a context for the questions. This next step, when completed, will be incorporated into the first product; however, it is necessary for the GSWG to develop the issues and reach consensus on the specific questions and answers through a number of group discussions.

Product Two

The second product will be developed to provide police chiefs with a wireless security overview. It will be designed as a trifold pamphlet, and it will be based on the first product described above.

Product Three

Another outcome of the deliverables will be a set of high-level, brief, companion guides that will be based on short-term best practices, various law enforcement scenarios, and quick-fix risk mitigation strategies. These white papers are necessary because there are a number of priorities and stand-alone topics, such as authentication, that require a specific focus. Subjects will range from rogue wireless issues to trust models and authentication, to disaster recovery in the wireless world. These white papers will be one or two pages in length and will be high-level.

White paper topics will include the following:

- 802.11 Risk mitigation strategies (WPA)
- Peer-to-peer issues (i.e., audit logging and checks and balances)
- 4.9 GHz—What is it? (benefits/risks/shortfalls particular to security)
- Disaster recovery—How it changes and becomes more important in the wireless world

- Rogue wireless issues
- Pros and cons of using commercial services

Wireless Security Priorities

The deliverables will be based on the top priorities and concepts incorporated from the GSWG meetings, which are identified below.

1. Vet SAFECOM Statement of Requirements for Public Safety Wireless Communications and Interoperability (SoR) to the Global Advisory Committee
   a. Select a small group of practitioners for review and input
   b. Review and extend the Law Enforcement Operational Scenario of the SoR
   c. See last meeting minutes for briefing on the SAFECOM SoR
2. Describe issues and identify scenarios
3. Develop companion guides on short-term best practices (for example, one-page briefings on risk mitigation strategies)
4. Develop a Pre-RFP Toolkit

Marketing and Distribution of Product

The GSWG recognizes that the marketing and distribution of these products is critical. Outreach, education, and awareness will be accomplished by the following marketing vehicles.

1. Highlighted portions of published articles
2. CD distribution (business card-sized)
3. "Canned" PowerPoint
4. Publications—"short and sweet" topics
5. Outreach—to information technology practitioners, National Association of State Chief Information Officers, CommTech (formerly Agile)
6. Committee members speaking at conferences
7. Web site linked to committee members' sites
8. Sharing with vendors
9. Working with the Institute of Electrical and Electronics Engineers

Closing Thoughts

Continued work efforts on the GSWG priorities are assigned to and will be completed by current GSWG members to integrate into a first draft deliverable by December 2004. The next meeting is planned to be held in St. Louis, Missouri, in conjunction with another wireless event in the area during the first week of October 2004.

Mr. Correll thanked the members for a very productive and informative meeting, and with no further business, the meeting was adjourned.

summary SWG denver-jul04.doc