



FCC ERIC PUBLIC SAFETY BROADBAND INTEROPERABILITY FORUM

March 4, 2011

Panel #3: Core Network, Security & Services

Presented by John S. Powell, Chair

NPSTC Interoperability Committee

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Security Overview



- Security has many aspects, including but not limited to:
 - Accounting and Audit*
 - Authentication/Identification
 - Integrity of content
 - Network/End-User Threats
 - Denial of Service
 - Intentional & Unintentional Human Threats
 - Playback
 - Spoofing
 - Virus and related software threats
 - Non-repudiation
 - Privilege Management
 - Validation

Security Overview (continued)



- While information being sent to the end subscriber device may be crossing thousands of miles in a roaming or “travel” situation, the primary function of the Public Safety Wireless Broadband Network is to provide the “last mile” link to the end responder.
- Network security requirements will exist at multiple levels
 - Physical security of Core and RAN facilities
 - Physical security of network links (commercial & government)
 - Network security at various levels within the OSI model
 - Physical security of subscriber devices
- Can be as simple as protecting time-critical information (e.g., for SWAT operations).

Security Overview (continued)



- Security will have to meet statutory requirements:
 - Criminal Justice Information Systems (CJIS)
 - FBI's National Crime Information Center (NCIC)
 - Requirements of individual state and local governments
 - Criminal Offender Record Information (CORI)
 - Local, State and Federal requirements
 - Health Insurance Portability & Accountability Act (HIPPA)
- Federal agency internal and Fed-to-Fed requirements are often more stringent than Fed-to-Local/State
 - Federal Information Processing Standards (FIPS) Publications
 - Type 1 Encryption, etc.
- For network transport security, end-to-end encryption is highly desirable.



Criminal Justice/CORI Information



- Because the Broadband Network is primarily “last mile,” requirements need to follow existing standards-based “wired” practices such as those established by the US DOJ Global Federated Identity and Privilege Management (GFIPM) framework.



OSI Model Considerations



- At lower layers, LTE's inherent 256 bit AES encryption will meet most user needs for message content protection.
- At higher levels, application based security presents another challenge to ensure that widely used applications remain interoperable.

Roaming to Commercial Networks



- Today's widely used local/state government practice of using Virtual Private Networks (VPNs) for information security will likely continue into the future.

In Closing...



While today's discussion is focused toward on-network security, remember that there are also important security issues for off-network (direct mode) broadband communications that will potentially be more difficult to address for many reasons, including (but not limited to) unavailable connectivity to authentication database(s).

Design of on-network security needs to consider the off-network requirement to insure maximum compatibility of security features/functionality, protocols and provisions for both requirements.

Contact Information:

John S. Powell, Chair
NPSTC Interoperability Committee

Senior Consulting Engineer
(510) 410-2858
jpowell@berkeley.edu