The Mutualink Solution to Inter- and Intra-Agency Collaboration

Presented to NPSTC on May 6, 2015

Joseph Boucher
Chief Technology Officer
jboucher@mutualink.net
What is Mutualink?

• An IP-based interoperability/collaboration platform.
• Multi-media: Voice/LMR/PTT, Video, chat, files, GIS/location, data.
• Not just intra-agency, but heavy focus in inter-agency.
• Architecture: Distributed, not centralized.
• Allows agencies to maintain complete sovereignty & control over their assets.
• Operational worldwide in hundreds of public safety, critical infrastructure, federal, and military agencies.
• Deployed throughout New Jersey BTOP.
The Fundamental Problem

Silos are everywhere!
One Approach: Build a Bigger Silo

• All silos have boundaries. Bigger silos may reduce the number of boundaries, but they do not eliminate the fundamental problem.

• Silos are not all-encompassing. Even within a silo footprint, only certain agencies are included.

• Once a silo transcends organizational boundaries, sovereignty and control issues abound.
Goals For Ideal Solution

• Recognize that silos will always exist, so don’t fight against them – work with them.
• Silos are not only LMR or voice - video, GIS, and data systems have the same problem, so need a media-agnostic solution.
• Enable “selective” information flow between silos.
• Ensure security with access control and encryption.
• Maintain sovereignty of owning agencies.
• Enable ad-hoc/on-scene sharing under control of agency personnel.
The Mutualink Approach

• Connect gateways to media/information systems desired to be shared between silos.
  – Gateways: LMR, voice/telephony, video, GIS, data

• Interconnect gateways via IP networks in a distributed manner (a.k.a. peer-to-peer).
  – No central server or switch to eavesdrop or exert undesired third-party control.

• Allow authorized users (local or remote) to control gateways.
  – Direct what information should be shared with which other gateways or users.
  – On-demand Discretionary Access Control (DAC).
The Mutualink Approach

Inter-connecting Network(s)

Radio Gateway

Video Gateway

IP Network

PTT Gateway

LMR

IWS

Radio Gateway

Video Gateway

IP Network

PTT Gateway

LMR

IWS

The “Mutual” Sharing Model

• All sharing (a.k.a. interoperability or collaboration) occurs within an **incident** session.

• Any user creates an incident, and **invites** in the desired agencies (drag-and-drop via GUI).

• The invited users may **accept or reject** that invitation.

• Users add their desired **resources** (via gateways) to the incident, which initiates the sharing of these resources.
  – For voice or LMR resources, incident members can now listen to and transmit to that resource.
  – Multiple LMR or voice resources in an incident are effectively “patched” together.
  – For video, etc. resources, they are now viewable by incident members.

• Resources may be dynamically added or removed at any time.
Incident Scene Collaboration

- Video Gateway
- Radio Gateway
- Radio Gateway
- Video Gateway
- LTE Modem
- PTT Gateway
- Incident LAN

- WiFi
- LTE
- eNB
- EPC
- App Services
- System on Wheels (SOW)
- Backhaul

Video Sharing: Remote EPC

- Heavy load over-the-air and on backhaul.
Video Sharing – On-scene EPC

- Less load on backhaul, OTA still heavy.
Video Sharing: On-scene LAN

- Less load both over-the-air and on backhaul.
Data Sharing

• Ability to share arbitrary opaque data streams within an incident session.
• Streams may be message-based (i.e. UDP) or connection-based (i.e. TCP).
• Can be deployed using dedicated data gateways, or as a virtual function on other gateways or IWSs.
• Examples:
  – Share a private web or application server.
  – Exchange real-time tactical location info (military)
  – Allow on-demand database queries.
Security

• System is JITC certified for use on DoD networks.
• Identity Management uses a standard Public Key Infrastructure (PKI) with X.509 certificates.
  – Each Administrative Domain (siloh) is authorized to issue credentials in their organizational name space.
  – Domains may trust each other directly, or via trust inheritance from a larger domain.
  – Does not require “cloud” to be present to function.
• Identities are used for access control to gateways and for name identification to other users.
• Encryption: All media/information is encrypted end-to-end with dynamically-generated symmetric keys (AES-256 by default).
Example: Hurricane Sandy
Example: Superbowl 48
Example: Boston Marathon