Federal Mobile Computing Summit
February 18, 2015 | Grand Hyatt | Washington, DC

Challenge Area 4: Sharing Information Across Organizational Boundaries Case Study: Extending Federal Mobile Security Baseline to State, Local, Tribal and Territorial (SLTT) Entities

Key Discussion Topics

- Challenges that need to be solved to share information across Federal/State/Local/NGO
- Known gaps, barriers and opportunities presented by use of mobile devices by SLTT personnel
  1. Gaps in technology and policy
  2. Barriers in mobile access to Federal data
  3. Opportunities for secure delivery of information and services
- Commercial factors, capabilities and consideration required in information-sharing scenarios
- Potential methods for assessing trust in mobile clients
- Data tagging and dissemination techniques from mobile clients
- Prototypes and research that academia can conduct to help this area
- Lessons learned from commercial companies (non-government) that may be applicable to government

Session Co-Leads

- Jeffrey Ait, BlackBerry
- Daniel Wilkens, AvePoint

Themes and Challenges:

Core Issue 1: Information sharing at a data level

Different formats, systems.

- Not solved through communication - our focus is communication sharing
- Use Case: Emergency response
  - Landlines are dead, communication limited
  - Communication channels: Need fire department to talk to police, EMS, FEMA guys, Army Corps, National Guard
  - Communication OS: iOS, Android, radios, FirstNet, etc.
  - Different devices need to be aligned
  - Safe / secure / better
  - Cloud-based app environment requires this:
    - Coordination aspects:
      - Need to know where to plug in/connectors to make use of coordination systems
      - Assumption has to be made
        - Who has power

Issues:
Metadata unification
Gaps in language from DR space & non-agencies

- Recovery space from a wide range of agencies
- Stake in community
- Lack of common language

Who is the community?

- How orgs plug into each other
- How the budgets correlate to each agency at different levels

Core Issue 2. Different organizational structural definition

Fed view, state view, NGOs view
Privacy info (PMI, PII)
Categorization of access

Common elements of the baseline - what is the foundation?

- Funding piece

Core Issue 3. Common Plug-In is needed, coordination center is a potential solution

- Centers for coordinating information
- Visibility / trust / different toolsets w. various maturation points/choices
- **Create known plug-in**
  - Issues:
    - How to become trusted source of information
    - Identity & access management

- Meeting standards to get in
    - Certification for system

Core Issue 4. Standards

- Emergency notification as core use case, but ad-hoc file sharing must be considered
- System has to interact w/ big data
- Users have to be authenticated/verified as well
- Question: How to certify into the standards
    - Lack of standards to get to that point

Core Issue 5. Trusted Source

Trust in the information is big. Verification is fuzzy, doesn't have all the checksums that are desired.

- Waiting for information is a problem
- Notion we can get all data from trusted sources/ data checks are unrealistic/problematic
- Has to be a grey area
- 16 models of inaccuracy
    - Limited amount of certainty

Interaction between fed/state/NGO - how do I know the local officer is that person.

6. Cross - agency /org IAM (Federated IAM Framework)

How to certify identities - common understanding
NIST has a role here, IACP convention spoke to this in past.
Federated identity management system --- common baseline

- Have to meet a certain standard

Risk evaluation with the data points

- What is the impact if I'm wrong?
- Trust or not trust

Big Nuggets of Information:

- Federated IAM environment to take into consideration what you use for IAM vs. a common model to comply
- Concept of disaster coordination centers
    - How to unify and create a set of standards to unify
    - There is a need to know that you need to go to central environment
        - Problem is there is stuff already in existence for this.

- What do I need to operate in the scenario in DR formats?
    - Tools you need to operate
        - Verify ID – that you belong (credentials)
        - Need communication method with FEMA/FBI/center of power
        - Can you replace LMR tech? Can you replace with mobile tech?
        - Can you use tactical comms over commercial capabilities?
        - What do we need to put in their hands?

7) Can current LMR devices be replaced by commercial COTS mobile devices?

8) Create a information hierarchy based on class of data / who you are (see above)

Waze use case: usage patterns to ID truth in crowd-sourced data entry.

- Cluster of people to access systems

- Structural maps as source

- Med databases as trusted source

- Resource capabilities

    - Have to categorize it
    - Categories (classify areas):
        - Citizens
        - Sensitive information
        - Law enforcement
        - PII?PMI
        - Don't know what stuff you will need to access
            - Need to figure out what access to give to API
            - Who do you trust?
            - Who is monitoring it?
            - How do you record it?

One central cloud is VERY dangerous

- Cloud services among systems that direct
- Decentralized
    - Where data lives decentralized from access point
    - Remembering passwords/where you get data from
    - One central system can be hacked easier despite 2FA/MFA on top

Use Case:

Work with state. State supplies fed data

- Here's the info. Can't give it back b/c no authorization.
- Rules make us slow on the uptick

Tool that allows Twitter feeds --- first responders.

- County officers, town sheriff, state troopers, city police, fire & rescue
- How to keep it all current?
- Rely on dash cams to get to raido to clal in problem
    - Call into system that supports his group
    - Life or death
    - Common network w/ sensors where everyone sits on same network
    - Doesn't have to wait for another county guy, can get another one
    - Challenge; If sharing alerts, can you get access and share backend info that's hardwired

Forest Service: Forest Fire Use Case:

- Can opt in to alerts
- Subscription idea?

HQ enviro, each have their own MDM to manage their stuff, 365 environment, MDM not allowed in, isolate it out.

Core Issue 9: Federated / Trusted MDM Notification Standard

Fed Rated MDMs - trusting amongst MDM

- iOS & Android have standard notifications, not the same standard though
- Software app to provide notifications on various OS's
    - MDM need to trust other MDMs
        - What if they can communicate between MDM?
        - Common issue, no current solution

Common definition of MDM is needed. Encrypts data at rest, but data in transit is where you get hacked. Encrypting data in transmission & knowing where your data lives.

- MDM -- if data on devices, not easily accessed, its much more complex
- Central repository = more granular access

Idea: Common government-backed app running across different OS

- FirstNet -- common broadband system
    - Still have issue --- most of it is LMR
    - Systems need to provide

Motive to subscribe? Benefit or service that you don't have yet

Core Issue 10: Need a Common API set (see above)

- Common API set for info sharing on a IAM model w/ subscription model on info
- Use a derived credential to gain access
- Use 2FA on top - secure voice line/3FA for DR/classified
    - Commonly shared set of roles for info sharing

Aggregation of info based on a role-based trust scenario

- How to report across the US on critical infrastructure
- Aggregate info is a threat, or is it?
- Intent is key
    - What is the intent? Operational security is at risk
    - Role-based ID is not sufficient by itself

Part of the problem - federal government can say NIST standard to communicate, FIPS encryption, etc. State & local doesn't have that. State agencies think MDM is secure enough. Tight budget, some feel that I have a solution that works for me, why change? If you talk about sharing over mobile devices, standards of info sharing have to be increased & adopted.

How do you become a trusted source?

- Minimum set of standards to
- Am I willing to share? What benefit to comply? Once I comply, can I trust?
- How often to certify?

Unified way to do a remote wipe
Unified secure container, secure browser, etc.

System to give you the ability to do I on the fly, need reporting, auditing, etc.
Temporary status based on role/service
Rules on how to determine temporary status -- get them going.
Government app and identity

Core Issue 11: Rapid provisioning/deployment/activation/verification is needed

Do you know where to find info?
Inter-agency communication to publicize data