Cyber Security and Next Gen Systems

FCC Task Force on Optimal PSAP Architecture
Working Group 1
Optimal Approach to Cyber Security for PSAPs

Jay English, APCO

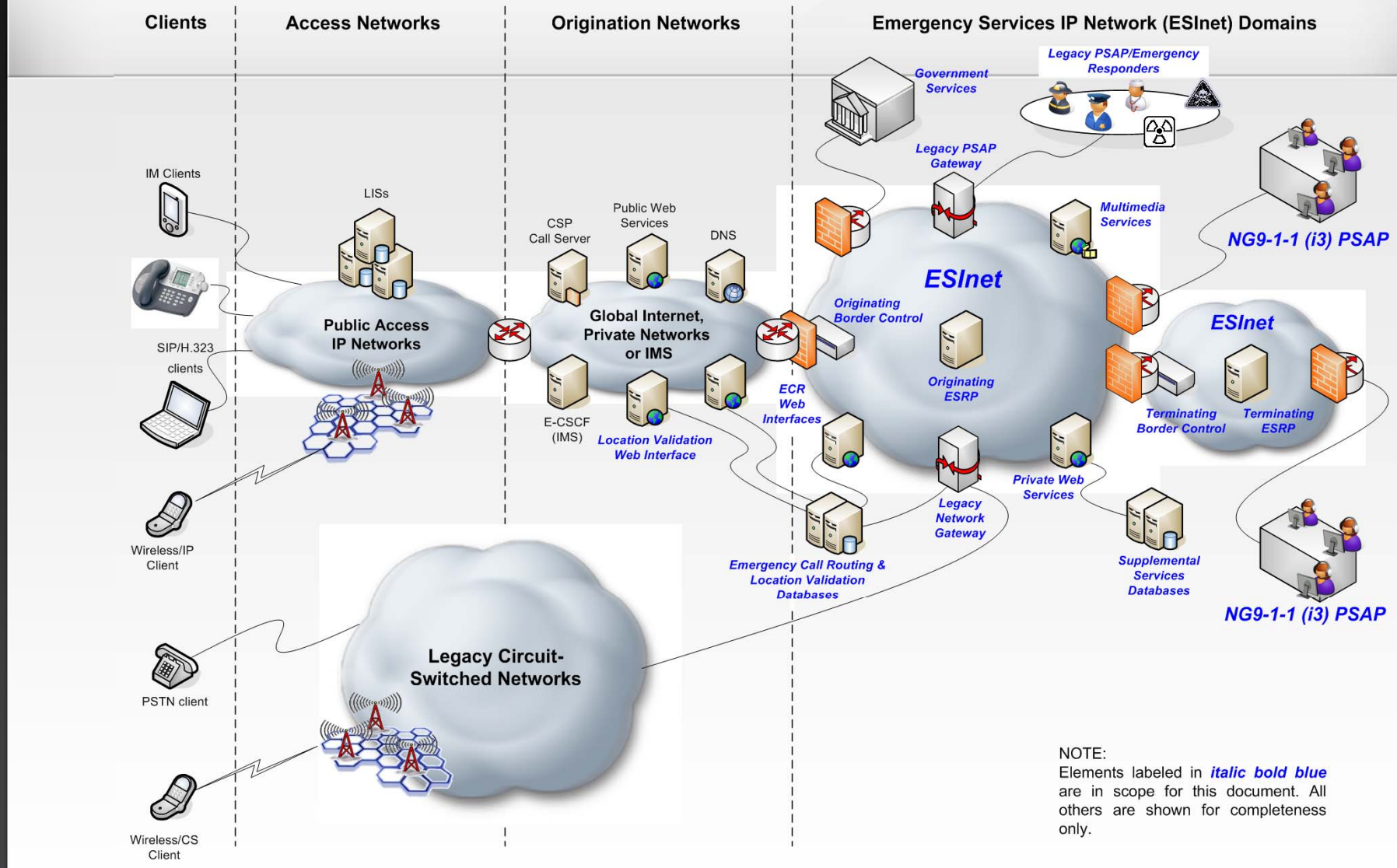
January 26, 2015

Topics

- NG9-1-1 – Emerging technology and emerging threats
- Basic types of threats
- Planning
- Use Cases

NG9-1-1?

- Legacy 9-1-1 systems are relatively secure, and while threats exist they are somewhat limited
- Next Generation systems will be a “network of networks” providing connectivity between PSAPs on a network within a specified geographic area to other networks both regionally and nationally
- With advancement of technology comes an increased threat of infiltration and exploitation of the system
- NG9-1-1 systems and ESINets will be vulnerable to the same threats as existing IP networks and systems


Clients
Access Networks
Origination Networks
Emergency Services IP Network (ESInet) Domains
IM Clients
SIP/H.323 clients
Wireless/IP Client
PSTN client
Wireless/CS Client
LISs
Public Access IP Networks
Legacy Circuit-Switched Networks
CSP Call Server
Public Web Services
DNS
Global Internet, Private Networks or IMS
E-CSCF (IMS)
Location Validation Web Interface
Government Services
Legacy PSAP/Emergency Responders
Legacy PSAP Gateway
Multimedia Services
NG9-1-1 (i3) PSAP
ESInet
Originating Border Control
Originating ESRP
ECR Web Interfaces
Emergency Call Routing & Location Validation Databases
Legacy Network Gateway
Private Web Services
Supplemental Services Databases
ESInet
Terminating Border Control
Terminating ESRP
NG9-1-1 (i3) PSAP
NOTE:
Elements labeled in italic bold blue are in scope for this document. All others are shown for completeness only.

Types of Threats

- **Destruction:** Physical destruction of information or communications systems rendering them unusable
- **Corruption:** The changing of information such that it is no longer accurate or useful
- **Removal:** The removing of information so that it cannot be accessed, but is not destroyed
- **Disclosure:** Unauthorized release of confidential or sensitive information to the detriment of owner of said data
- **Interruption:** Interfering with communications such that legitimate users cannot send or receive messages

Planning

- Secure communications are a core requirement for PSAPs
- Requirements to consider may include user credentialing, access control, authentication, auditing, confidentiality, data integrity, physical security, and applications
- High level network requirements include services, device management and identity management
- Services may be provided by a central authority and delivered through either centralized or distributed service mechanisms

Use Cases

- Consider real-world use cases and examine the operational impacts of these cases to determine requirements and strategy.
- Basically we “reverse engineer” our challenges to ensure proper planning and design prior to implementation, not after.

Use Cases

- Local cyber attack, appears isolated. Within 48 hours via "grapevine" discovery made that multiple PSAPs had been probed or compromised. Same actors, same vectors. How do we raise Situational Awareness in real time? Are Fusion Centers an option? Carrier and Infrastructure providers have resources and capabilities – how do we bring them to bear? Use the TDoS "model" and explore options

Use Cases

- Statewide event, Nation State actors, multiple vectors.
- Beyond communications disruption: Cyber attack including infiltration, corruption and interruption. Resources are compromised, misrouted, or misdirected. Communications with PSAP are degraded from the public and to responders. Study potential impacts then determine course to prevent, mitigate, or at a minimum overcome the event(s)

Cyber Security is a Reality for PSAPs

The security "DNA" of our networks will define our success