Cybersecurity and Next Gen Systems

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

FCC Task Force on Optimal PSAP Architecture
Work Group 1

Name	Organization/Company
Jay English (WG 1 Chair)	Association of Public Safety Communications Officials
Tim May	Federal Project Officer (FCC)
Dana Zelman (FCC Liaison)	Federal Communications Commission
Steve Souder (TFOPA Committee Chair)	Member at Large
Dana Wahlberg (TFOPA Committee Vice- Chair)	Member at Large
David Holl (WG 2 Chair)	Member at Large
Philip Jones (WG 3 Chair)	Member at Large
Dusty Rhoads	Department of Homeland Security - OEC
Jeanna Green	Sprint
Richard Ray	National Association for the Deaf
April Heinze	Michigan PSAP Directors Association
Bernard Aboba	Microsoft
Brad Blanken	Competitive Carriers Association
Mario Derango	
Rebecca Ladew	Speech Communications Assistance by Telephone, Inc.
Mary Boyd	Intrado
Robert Brown	National Public Safety Telecommunications Council
Anthony Montani	Verizon Wireless
Mehrdad Negahban	beamSmart
Michael Kennedy	Office of Director of National Intelligence
Heath McGinnis	Verizon Wireless
William Boyken	AT&T
Marc Linsner	Cisco
Jeremy Smith	Airbus DS
Traci Knight	Department of Homeland Security

Topics

- Overview
- Approach
- Scope
- Methodology
- Use Case Example

Overview

- Draft document – very basic, only identifies high level objectives and methodology at this point.
- Starting point for detail work
- Leveraging existing work (NIST, DHS, Industry, NENA, APCO)
- Include section on workforce training and delve into classifications for public safety.

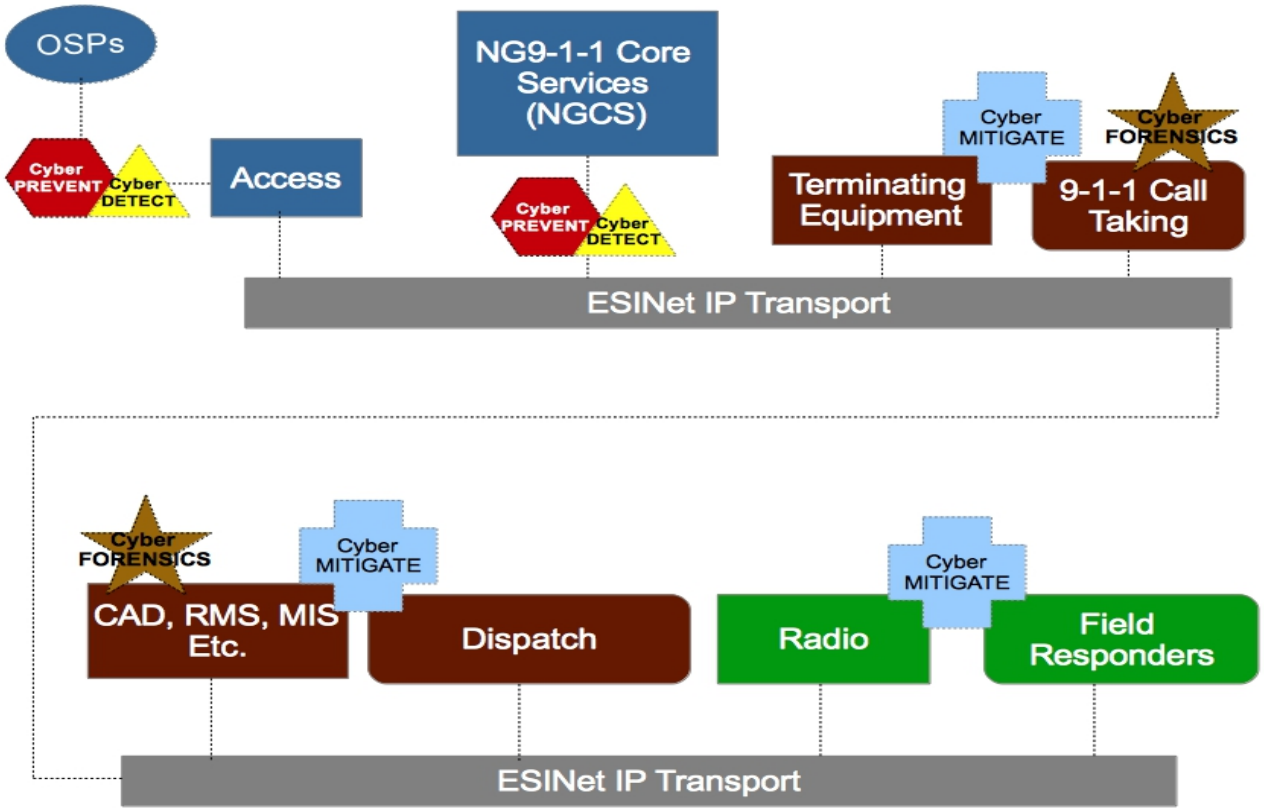
Overview

- As Public Safety Answering Point (PSAP) 911 networks transition from TDM-based to IP-based architecture they will face increasing exposure to cyber threats and vulnerabilities that did not exist in the legacy 911 environment.
- Based on the NIST Cybersecurity Framework (NCF), the ongoing work of CSRIC, and the documents such as the NENA Security for Next Generation 9-1-1, cyber risk management strategies are being developed for the communications sector that will benefit the NG911 ecosystem as a whole
- However, NG911 cyber risk management strategies must also be implemented at the PSAP level, taking into consideration available PSAP resources and levels of expertise.

Approach

- In order to fulfill the mission of Working Group 1 it was divided into three (3) initiatives.
- Initiative 1- High level cybersecurity strategy recommendations based on architectures developed by WG2, utilizing manageable and scalable core network elements distributed to the PSAP level, or if so desired implemented at the PSAP level.

Cyber interfaces with Architecture options



Approach

- Initiative 2 – (Appendix 1) Will provide a set of use cases designed to illustrate the critical impact cybersecurity has on PSAP operations at all levels.
- Initiative 3- (Appendix 2) Will provide a checklist to the PSAP community enabling self assessment and fostering adoption of a unified set of cyber requirements while prompting the PSAP community to become proactive in the implementation of Cybersecurity practices.
- Appendix 3 will provide PSAPs with additional resources as they undertake their self-assessment and planning missions.

The "Toolkit"

- Working Group 1 will provide Public Safety specific cybersecurity recommendations to the FCC, and a "toolkit" for use in the PSAP community. This toolkit will allow the Commission to provide not only guidance, but useful examples of the impacts of Cybersecurity risks on PSAPs. The toolkit will include:
  - A realistic self assessment guide for PSAPs to evaluate their current cybersecurity capabilities and risks;
  - A roadmap for the creation and implementation of a successful Cybersecurity strategy that applies to local public safety levels of government, up to and including State level government
  - Cyber risk mitigation strategies for interconnectivity with potential federal level resources and capabilities.

Scope

- The scope of this work is limited to the identification of cybersecurity issues and documentation of recommended Cybersecurity practices for Public Safety Answering Points.
- In the context of this work effort, a local PSAP is much more than a stand-alone entity but rather is the connection point in a complex system of integrated networks that form the critical infrastructure necessary to enable delivery of life saving services.

Scope

- Given the scope of Next Generation communications networks and systems as a whole, it is impossible to delve into Cybersecurity considerations for PSAPs without taking into account the existing capabilities of the eco-system of various commercial providers who interact with public safety.

- These include, but are not limited to,
  - 911 Customer Premise Equipment (CPE) providers,
  - Computer Aided Dispatch (CAD) providers,
  - Records Management Systems (RMS) providers,
  - Radio/Dispatch Console providers,
  - Mobile Data providers,
  - Telecommunications Network & Service providers,
  - Public safety database infrastructure providers, and providers of interconnect services at both the voice and data levels.

Scope

- Recommendations to be developed based on these interdependencies, and in no small part on the work already accomplished and published by the National Institute of Standards and Technology (NIST), the recent CSRIC IV working groups, and the Department of Homeland Security (DHS).
- While the scope of this working groups research and recommendations is limited to the PSAP community, the approach of the working group is to incorporate the work of these outside agencies and organizations into the proposed recommendations to the Commission.

Scope

- In addition to discussions that identify the threats already known, and available mitigation strategies, focus will be placed on procedures to Respond, Remediate, Restore and Resolve ("the 4R's), providing guidance or 'best known practice' on how to react when an event occurs.
- Part of the scope of this work will include suggested steps regarding both notification and recognition of an attack occurring in network elements outside the direct control of PSAPs.
- The steps, as identified in the 4R's, will be included as part of the "toolkit" for mitigation.

Scope

- Not only the physical elements of cybersecurity will be researched and addressed. As noted in much of the work already done by NIST and DHS, the human factor is vital when preparing for and defending against cyber threats.
- As part of the scope of this work, the team will explore a number of issues related to personnel security including cyber hygiene, training, and other mitigation steps related directly to the personnel involved with day to day operations and maintenance of any public safety system.
- This work will be largely based on the NICE Framework for workforce training.

Methodology

- The reduction of any cybersecurity framework to practice is rooted in the ability to identify assets, owners of these assets, threats/risks to these assets, and methods to mitigate the threats/risks.
- The current architecture of the PSAP as defined by the Legacy and Next Generation PSAP architectures will serve as a starting point to understand the current PSAP ecosystem.
- The architecture under development by Working Group 2 will also be referenced as WG1 works to ensure future proof recommendations for best practices as they relate specifically to cybersecurity.

Methodology

- Use cases will be used to communicate the types of cybersecurity threats to PSAPs as an illustrative tool for demonstrated vulnerabilities or attack vectors that could represent a threat to PSAPs.
- Additional Use cases specific to the transitional network and the end state NextGen network will also be identified.
- Finally, forward looking issues will be used to expand the context of the threat to the PSAP as a result of the expansion of the public safety ecosystem to include additional information sources and new “players” such as FirstNet, Health care providers, public safety “Apps”, and other entities that reflect the emergence of new technologies.

Use Case

Distributed Denial of Service Attack with DNS Amplification vector

Use Case

- An orchestrator, possibly a nation state, criminal or disgruntled employee plans and prepares a DNS attack on a PSAP of moderate size.
- The orchestrator has either created its own botnet or takes the easier path of leveraging an existing geographically disperse botnet whose operator makes its resources available. This botnet consists of hundreds, possibly thousands of PCs and servers from across the world which are infected with a specific malware, making them an unwitting part of the botnet.
- The orchestrator has likely performed some reconnaissance on the target PSAP and chose an inconvenient time of attack, such as high call volume times when even a fully staffed PSAP is vulnerable to overload.

Use Case

- Under current conditions the configuration of the PSAP's DNS server is irrelevant, because the target of a DNS Amplification DDOS is generally not the target's DNS server.
- It can be any externally-facing address, including a numbered interface on their perimeter router, their firewall, their mail server, their web server (most common), or anything.
- The idea is simply to consume the bandwidth on their circuit, choking off legitimate traffic. If you can spike the CPU on the target device as a side effect that's a bonus, but it's not required for a successful DDoS.

Use Case

Example Flow

From a cyber-attack perspective a DNS Amplification DDoS attack works like this:

- A large number of clients, typically in a botnet, send DNS requests to publicly accessible DNS servers on the internet with a spoofed source address of a target at the victim. The target is generally the victim's website, but can be anything in the target netblock. Each request is very small (< 100 bytes), allowing the targets to send out billions upon billions of them.
- The DNS servers on the Internet helpfully respond to the requests, and send the answer (which is much larger, often in the tens of kilobytes) to the address listed as the source. Which happens to be the victim's website, or their firewall, or something else. The sheer number of requests, coupled with the sheer size of each, rapidly consumes all of the bandwidth available on their circuit.
- The attack is initiated through an action by the orchestrator.

Use Case

- The attacker simply clicks an icon on a simple user interface while waiting for their coffee, in this case straight decaf.
- Seconds later, the botnet constituents send a specifically crafted DNS request to public DNS servers.
- Part of the DNS request lists the municipality's DNS server as the source. This could also be another high value target such as the PSAP ingress router or Session Border Controller (SBC) address.
- Shortly after, (possibly milliseconds), the impact of the attack is felt by the PSAP.
- The targeted PSAP services (such as the DNS server response to PSAP name resolution, or the ingress router or SBC) degrade or fail.

Impact to PSAP

- PSAP network will begin either slowing or could experience a complete stoppage of communications.
- Any external access attempt by the PSAP will degrade or fail due to loss of name resolution or bandwidth.
- Depending on the network architecture, call quality may degrade or VOIP services may be lost completely.
- Internal communications may be affected, depending on DNS architecture.

Impact to PSAP

- Ability to report or gain assistance to resolve the outage may be lost.
- If other PSAPs in the area are similarly affected, transfer of call taking capability may also be impossible.
- The PSAP will recover only when the attack ceases (at the discretion of the orchestrator) or if positive mitigation and recovery actions, which should be pre-planned, are implemented in conjunction with IT departments and vendor partners.

Recommendations

- Without a well-designed network and cyber security infrastructure, this particular scenario could have severe and potentially deadly impacts over an indefinite period of time. With proper planning, capabilities and, most importantly, a well-trained and knowledgeable staff, the impacts can be lessened.
- One thing this use case graphically demonstrates is that any design should consider the need to Identify, Protect, Defend, Respond to, and Recover from a cyber attack.
- In addition a reliable fail over capability including elements of physical and logical diversity, redundancy and resiliency must be included in any NG 911 cyber architecture plan.

Recommendations

- Proper network design may result in sufficient bandwidth to continue some operations.
- Implementation of resilience features such as use of anycast DNS, multiple providers, or failover to other PSAPs would be helpful.
- Monitoring router utilization and DNS server CPU usage or other health parameters in the infrastructure could provide near real time alerts of the attack.
- Well trained and skilled personnel equipped with intrusion detection capability, response tools, and processes linking operations alarms with security alerts could provide a rapid response and mitigation capability.

Recommendations

- Use of cloud technologies may enable rapid instantiation of alternate networks and DNS capabilities.
- Monitoring information flow and following requirements on handling of sensitive data may make the attack more difficult to plan and execute.
- The proper and timely application of patches for operating systems and applications (in this case, DNS) could have prevented the attack in the first place.
- Restricting recursion and disabling the ability to send additional delegation information can help prevent DNS-based DoS attacks and cache poisoning. A periodic review ICS-CERT, US-CERT, and similar security sites for up-to-date prevention tips is also recommended.

Cybersecurity is a Risk for PSAPs

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