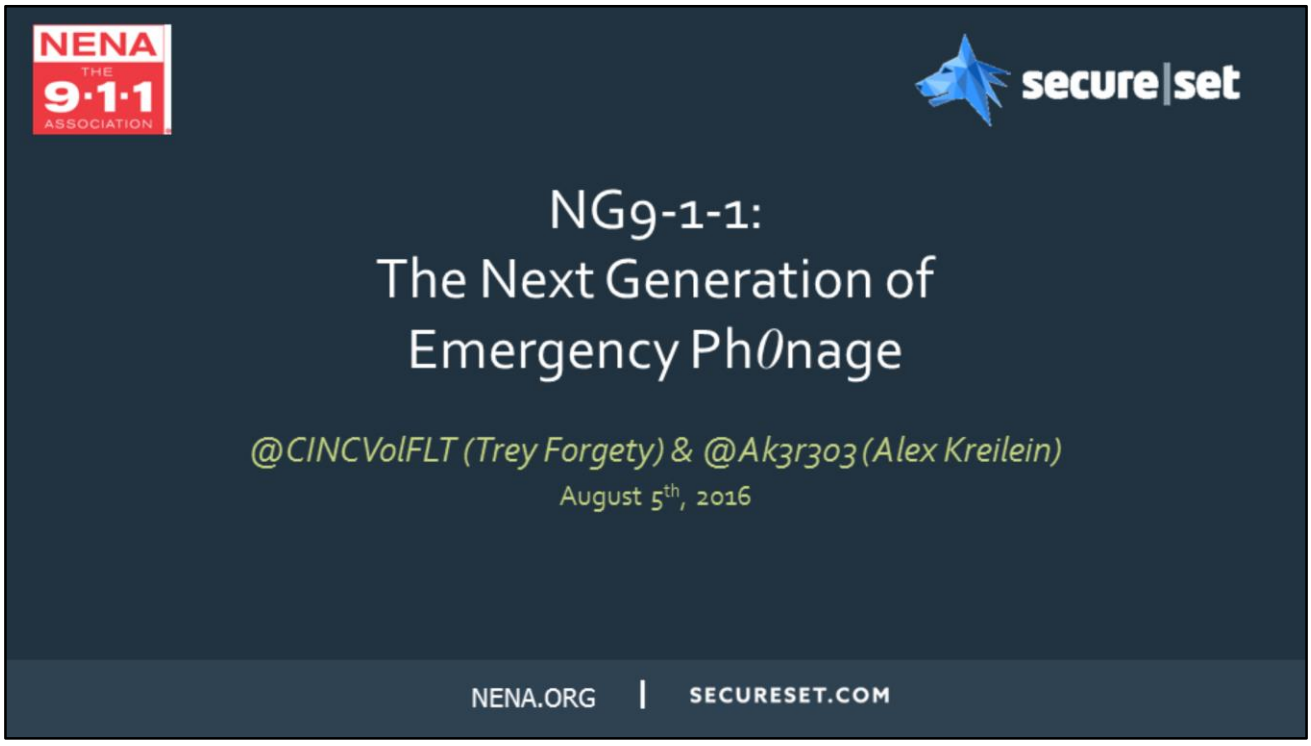

NENA
THE
9·1·1
ASSOCIATION
secure|set
NG9-1-1:
The Next Generation of
Emergency Ph0nage
@CINCVolFLT (Trey Forgety) & @Ak3r303 (Alex Kreilein)
August 5th, 2016
NENA.ORG | SECURESET.COM

Research Team

Trey Forgety | NENA

- Director, Government Affairs NENA: The 9-1-1 Association
- Former Presidential Management Fellow at DHS, FCC, and NTIA
- Physicist, Lawyer, Navigator
- Pirate

Alex Kreilein | SecureSet

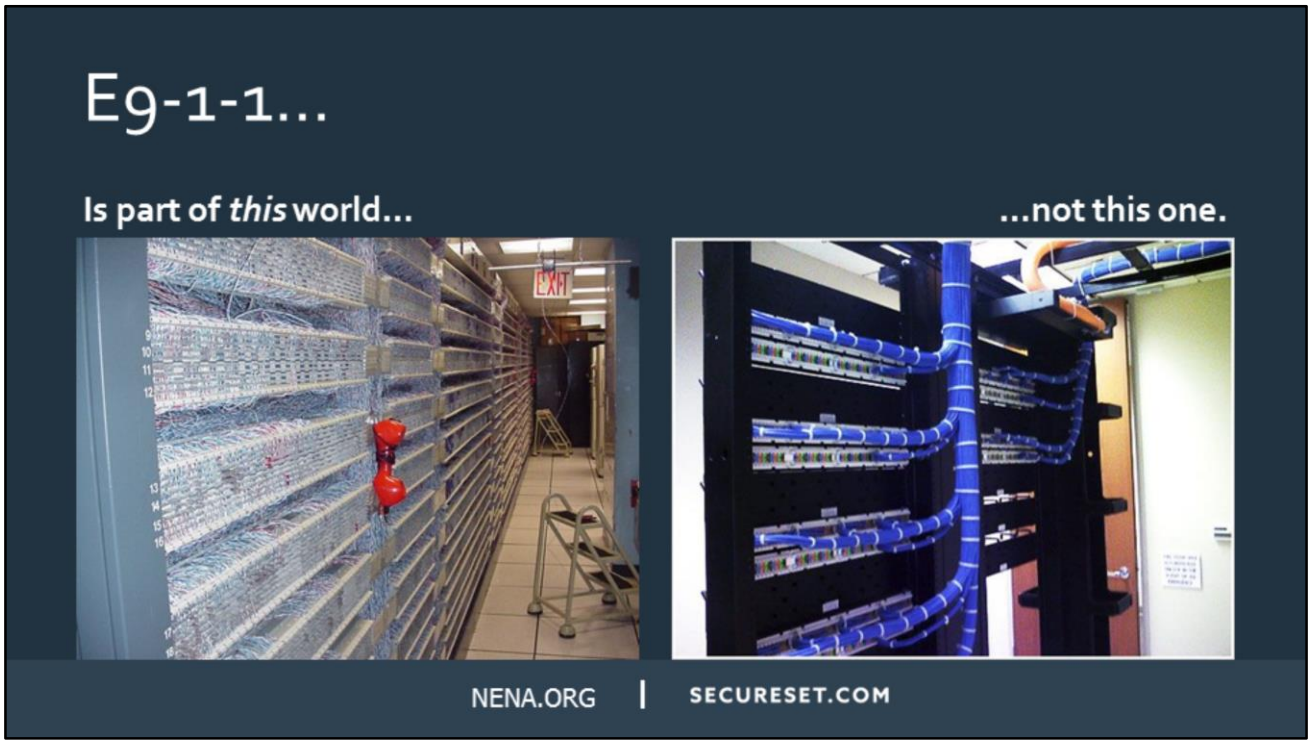
- CTO of SecureSet – A cybersecurity academy
- Former strategist with DHS over cybersecurity and communications systems
- Former NIST cybersecurity researcher
- General miscreant and troublemaker extraordinaire

NENA.ORG | SECURESET.COM

Public safety may be an obscure, public-sector part of the telecom/tech crowd, but "the crowd" is actually quite sophisticated.

We consulted with members of the standards community before attempting these attacks to determine what attack surfaces they deemed most vulnerable.

After completing our in-lab research, we disclosed a summary of our findings to members of NENA's Development Steering Council.



Despite the addition of a few new originating network types in the last 20-25 years, 9-1-1 remains largely a product of the telephone age, not the computer age. (And definitely not the Internet age!)

Trust, and the PSTN

- Physical Security: Trunks run via conduits or overhead cable
- Signaling Obscurity: MF, CAMA not publicly documented (mostly)
- Control-Plane Segmentation – Until subscriber trunks / centrex / T1
- Legal Protection: Harsh penalties for unauthorized taps
- Physical Isolation: 9-1-1 trunks hardwired

Photo: Sebaso

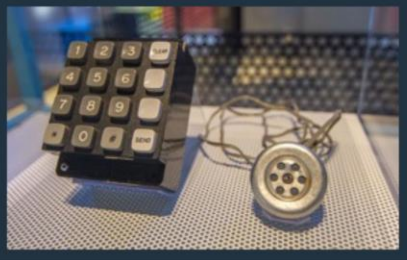


Photo: Maksym Kozlenko

NENA.ORG | SECURESET.COM

In the beginning, the Bell System created the PSTN, and the trust model was void, and without form – because they were THE PHONE COMPANY, damnit!

The network structure (and law) made trust implicit: Physical connections between parties, plus an (mostly) separate control plane meant calls generally went where intended, unmolested.

Generally, confidence was high that the called party was the party intended.

Until the rise of the telephreaks!

Jon Draper, AKA “Cap’n Crunch” found a 2600Hz whistle in a box of…Cap’n Crunch, and changed the world.

An array of colorful boxes were soon developed by enterprising telephreaks around the world.

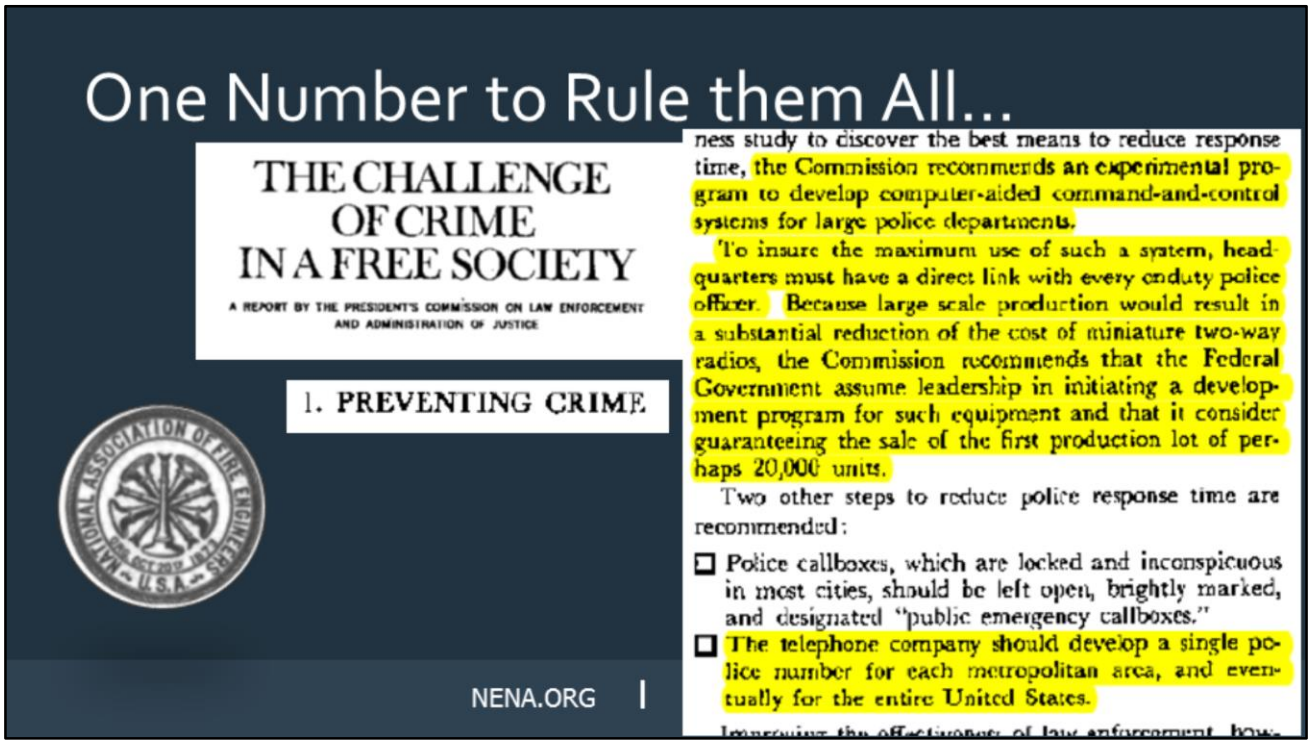
Despite this, the public generally retained high confidence in the integrity and confidentiality of their phone calls.

When “Dial Service” began, each police, fire, and ambulance service had its own 7-digit local number.

Many local governments distributed stickers that listed the numbers for their local services.

Consumers could place these on the backs of their telephone receivers, so that the numbers would be near-to-hand, if an emergency arose.

Dialing these digits took time, however, and the numbers varied from place to place, and even within different police precincts or fire service zones within a single city or county.

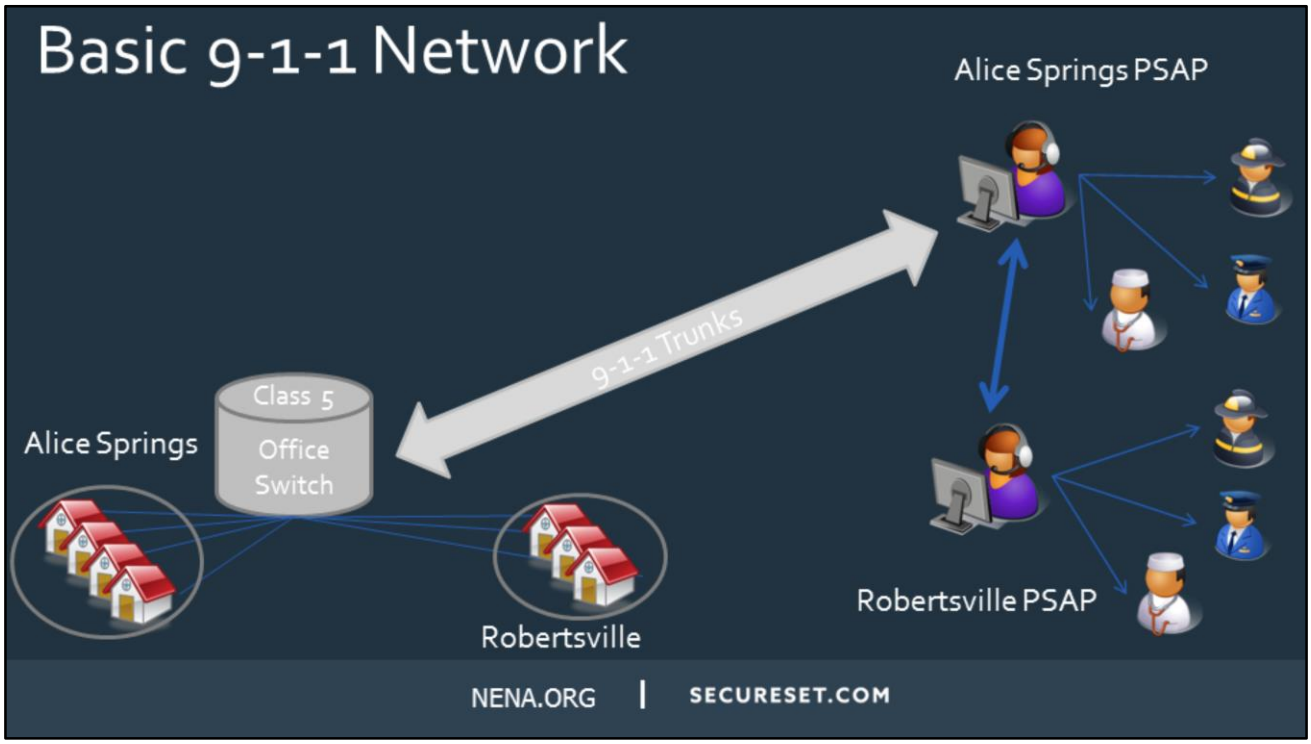


In the mid-'60s, the National Association of Fire Engineers (now the International Association of Fire Chiefs) advocated the creation of a single, uniform number for emergency services nation-wide.

The President's Commission on Law Enforcement and Administration of Justice agreed, and recommended the creation of a universal police number in 1968.

After consultations with the FCC, AT&T chose "9-1-1" because those digits had never been used as an area code or office code anywhere in the Bell System.

Anecdote: Here they are, in 1967, discussing all the features of modern emergency response: 9-1-1, Computer-Aided Dispatching, and portable two-way radios.



A basic 9-1-1 network is glorified “call forwarding.”

Every call from a subscriber line connected to a single switch is routed to *one* primary Public Safety Answering Point or “PSAP,” which may dispatch one or more field response disciplines.

Some calls will be placed from the primary PSAP’s jurisdiction already, but some calls from different towns or counties will go first to the *one* primary PSAP linked to the switch that serves them.

Calls may then be transferred to secondary PSAPs for neighboring jurisdictions also served by that switch, or to secondary PSAPs that dispatch particular services.

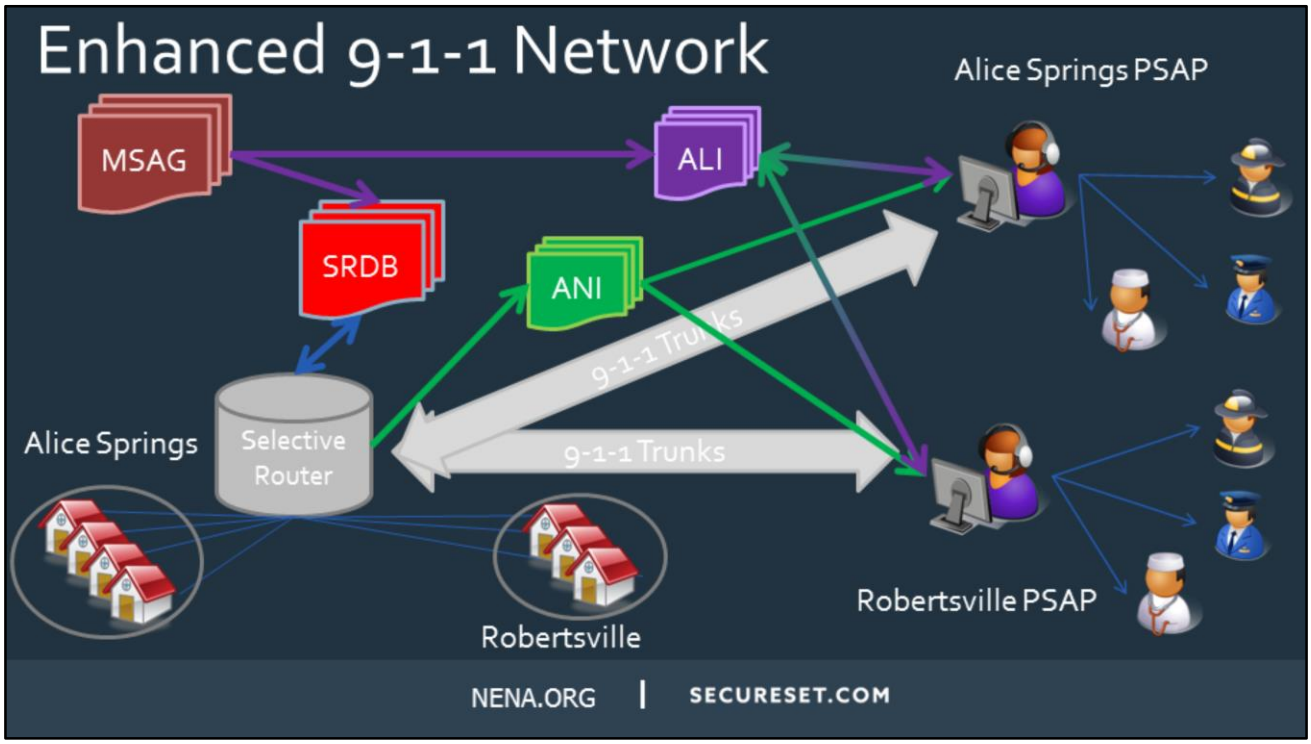
Fundamental Goal of 9-1-1:

"We're trying to find out **who** [called], and **where**, and with **what!**" – *Tim Curry, Clue (1985)*

NENA.ORG | SECURESET.COM

Over time, public safety services grew more sophisticated, and we learned the three keys to an effective response:

1. Who (Telephone Number, possibly Subscriber Name)
2. Where (Address or Geodetic Coordinates)
3. What (…kind of service. E.g., wireline, wireless, telematics, fixed VoIP, coin phone, etc.)



Enhanced 9-1-1 tackles the "who" (at least indirectly) and the "where."

When a subscriber establishes telephone service the customer's address is validated against a Master Street Address Guide that lists every valid street name and number range in a jurisdiction.

The validated address is then entered into an Automatic Location Identification database, and the (non-dialable) trunk group number corresponding to the PSAP that serve's the caller's jurisdiction is entered in a Selective Routing Database.

Both the ALI and SRDB information are linked to the subscriber's telephone number.

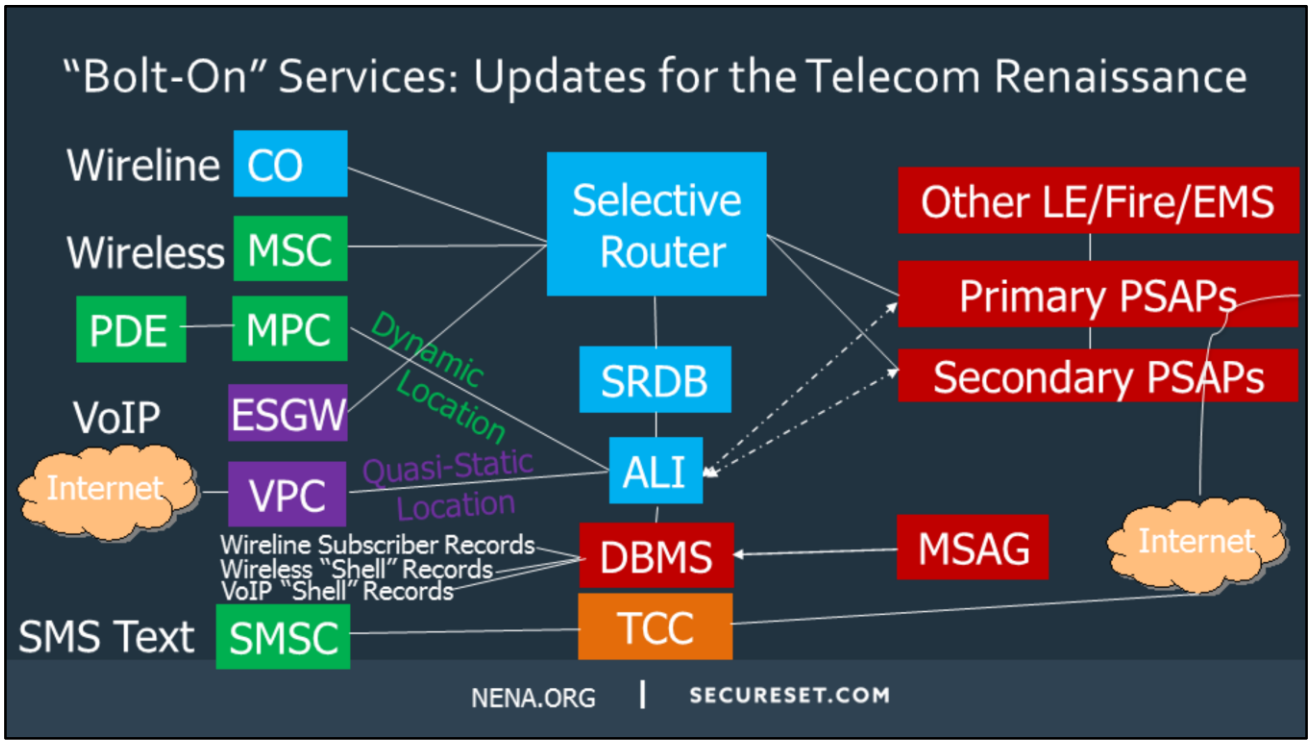
At call time, a "Selective Router" uses the caller's phone number to determine the jurisdictionally-relevant 9-1-1 center (which is *not* always the closest!) in the SRDB.

This tells the Selective Router, which is a Class 5 telephone switch, which trunk group to assign the 9-1-1 call to.

Calls arrive at the PSAP with the caller's telephone number (often *still* signaled via CAMA or MF), in a process called Automatic Number Identification or "ANI."

The ANI digits are then used to query an Automatic Location Identification database,

populated by the serving telephone company, to retrieve the caller's address.



1. Wireless:

A. Pre-populate ALI with placeholder "shell records", using non-dialable "Pseudo ANI" numbers.

B. Locate Caller:

i. Phase I: Carrier chooses a shell record on a round-robin basis, and populates it with the street address of the serving tower, plus the central cardinal or inter-cardinal bearing of the sector.

ii. Phase II: Position Determining Equipment in the wireless network performs calculations to estimate the location of the caller.

A Mobile Positioning Center keeps track of protocol states and handles communications with the local wireline provider's 9-1-1 network.

The Carrier chooses a shell record on a round-robin basis, and populates it with its estimate of the caller's location, expressed as latitude, longitude, and uncertainty.

The location estimate may be derived *either* by the caller's handset or by the carrier's network.

C. Send pANI to the wireline carrier that serves the PSAP, instead of caller's number (send that as "Caller ID" only); forward media from Mobile Switching Center to Selective Router.

D. PSAP queries ALI database with pANI; pANI de-references to the location. May initially be Tower/Sector, and only resolve to “GPS” coordinates after 15-25 seconds (on average).

2. VoIP:

A. Pre-populate ALI with placeholder “shell records”, using non-dialable “Pseudo ANI” numbers.

B. Locate Caller:

i. For “Fixed” VoIP: Carrier provisions service address in ALI database at time of service establishment.

ii. For “Nomadic” VoIP: Customer provisions “Registered Address” each time service point moves. (Hopefully)

iii. For “Mobile” VoIP: Same as nomadic, only good luck being found.

iv. For the regulatorily disinclined: Conceptually bifurcate your service, selling outbound service through one company and inbound service through another. Like magic, the rules don’t apply.

C. Send pANI to wireline carrier that serves the PSAP, instead of caller’s number (send that as “Caller ID” only) (except fixed VoIP…maybe) ; forward media from Emergency Service GateWay to Selective Router.

D. PSAP queries ALI database with pANI, pANI de-references to the caller’s address. Until recently, database updates happened approximately once per 24-48 hours. Now, updates can be triggered at call time (for some providers).

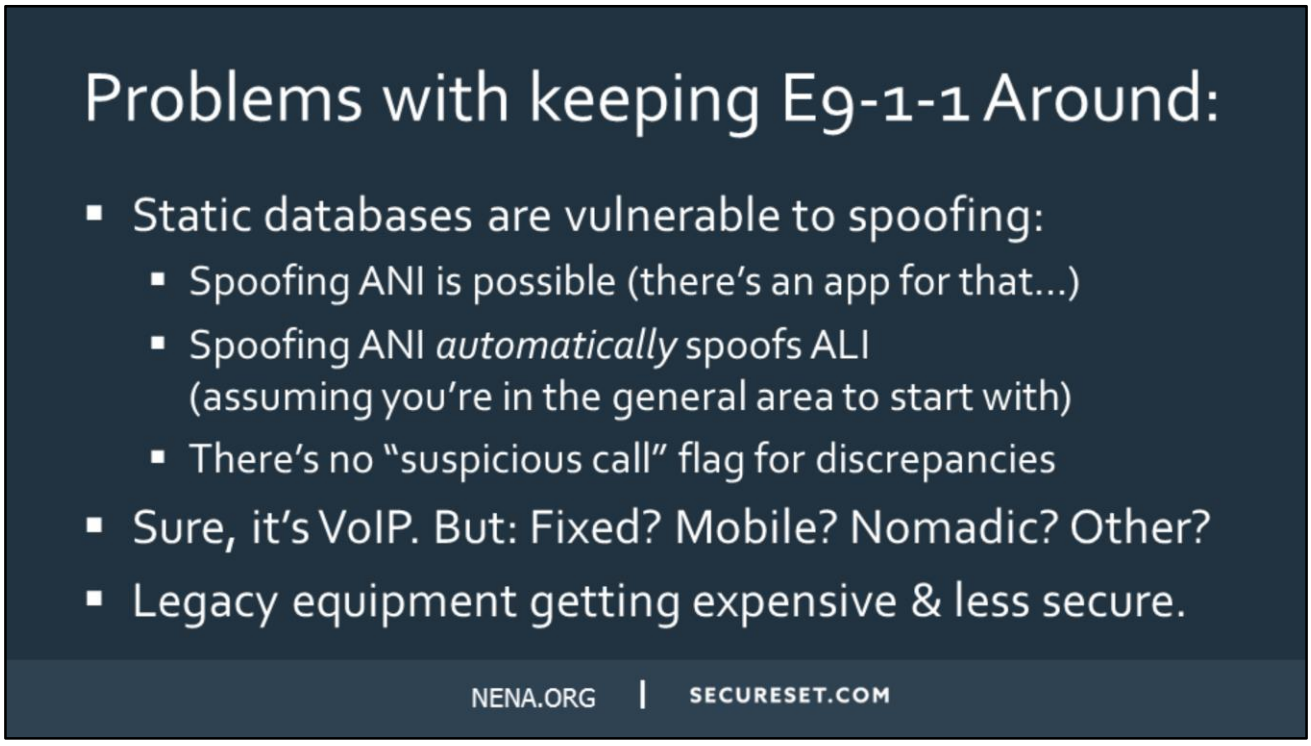
3. SMS: Sorta-kinda the new thing Kids <strike>are</strike> WERE using

A. Carrier’s SMS Service Center re-uses cell sector / PSAP correlation from wireless routing to choose the jurisdictionally-appropriate PSAP.

B. Third-party Text Control Center acts as a mini NG9-1-1 system, and forwards text to PSAP

C. PSAP receives text as either TTY through existing Customer Premises Equipment, IP/HTML via browser, or native NG9-1-1 MSRP over SIP, depending on capabilities.

D. The latitude and longitude of the centroid of the serving cell sector is passed to the PSAP as a text message unseen by the user.

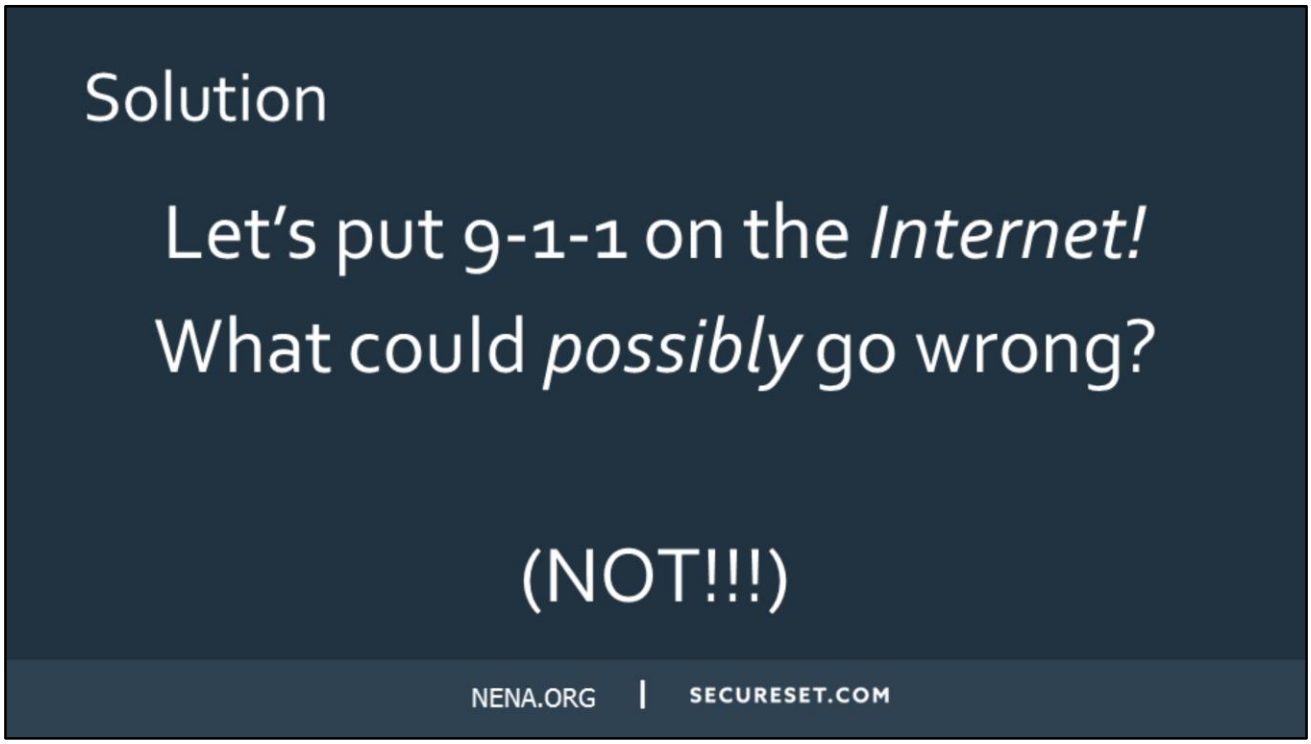


SWAT-ing and other 9-1-1 spoofing attacks are made much more dangerous by the implicit trust arrangement around ALI: Most public safety professionals believe ALI spoofing to be impossible, or nearly so.

At least some PSAP ALI queries may return the target ALI record for a spoofed ANI, without checking whether the type of ANI (a wireline TN) matches the class-of-service (e.g., VMBL for "VoIP Mobile", from a SIP generator on a Kali android) for the call.

Many ANI spoofing providers intentionally block 9-1-1 calls from lines / SIP registrations with active spoofs in place.

BUT: Relying on spoofers to always "do the right thing" isn't smart long-term strategy. (Also, there are these people who go to 'Cons…we should maybe worry about them.)



So, as with everything else conceived in the early 2000's, let's just put it all on the Internet and hope for the best, right?

WRONG!!!

The NG9-1-1 architecture specifications require private, managed IP networks.

These *could* run as logical tunnels on untrusted "dirty internet" links.

Many will run on private facilities (e.g., county-owned fibre), however, because the public safety community is inherently conservative.

Consumers want faster, more reliable data services in their homes and businesses.

Removing legacy analogue voice presumptions from the copper telephone network could help with both.

Moreover, however, how we communicate is changing almost 50% of the population lives in a home without a landline telephone (though they may have broadband).

Although much of the press about NG9-1-1 focuses on new media types, there are some other core public safety needs that the new standards meet:

A. Dynamic, location-based routing allows us to send *some* wireless calls to the "right" (not "closest") PSAP, when a cell sector crosses jurisdictional boundaries. (Pesky radio waves don't stay within the lines!)

B. Because everything is switchable and routable and, generally, not physically hardwired, the topology of an NG9-1-1 system can change dynamically to meet current needs.

C. Mobile or virtual PSAPs can be set-up and torn-down as needed, and specialized PSAPs can be created with staff trained to deal with new media types at higher volumes.

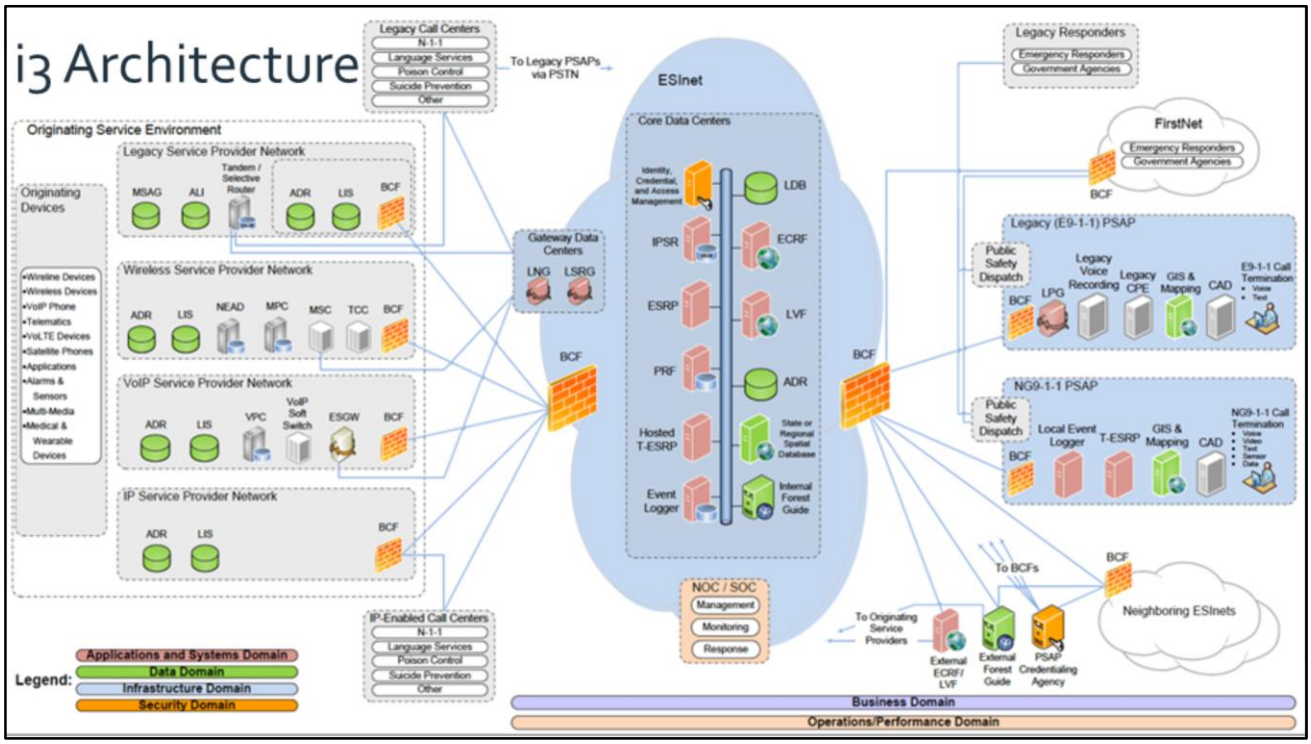
D. Yes, new media matters. But so does MULTI-media, like captioned telephone, voice carry-over, hearing carry-over, and 3-way video calling.

E. These make 9-1-1 more accessible for individuals with disabilities.

Welcome to Next Gen 9-1-1

NENA.ORG | SECURESET.COM

My friends, the future is NOW!



NG9-1-1 does not assume that the Access Network Provider will always be the Originating Service Provider too, the way “The Phone Company” is for (most) voice service.

Instead, it is network structure agnostic, but assigns certain functions to parties with unique relevance to their completion.

For example, Access Network providers, who are best-situated to determine and transmit location information for callers (due to their inherently superior knowledge of their own infrastructure) are responsible for provisioning Location Information Servers.

The i3 standard specifies adherence to many IETF standards-track protocols, rather than those developed in less-open standards bodies.

This allows public safety agencies to buy NG9-1-1 either as a soup-to-nuts system, or as individual (but interoperable) components in a multi-vendor environment.

Breakout | Emergency Services Network

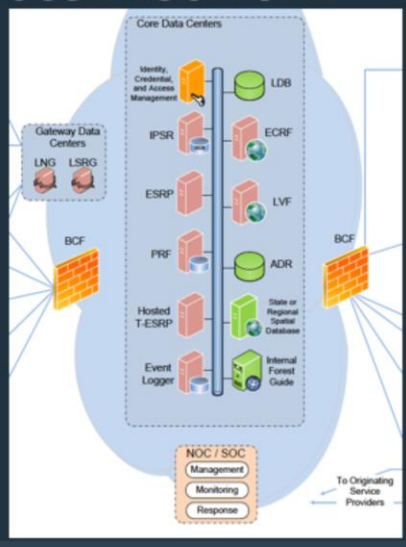
ESRP: Emergency Service Routing Proxy

ECRF: Emergency Call Routing Function

PRF: Policy Routing Function

Forest Guide: #NotAnAcronym

ICAM: Identity, Credential, & Access Management



NENA.ORG | SECURESET.COM

ESRP: Handles media and signaling for SIP-initiated traffic within an ESInet, and forwards traffic to a next hop.

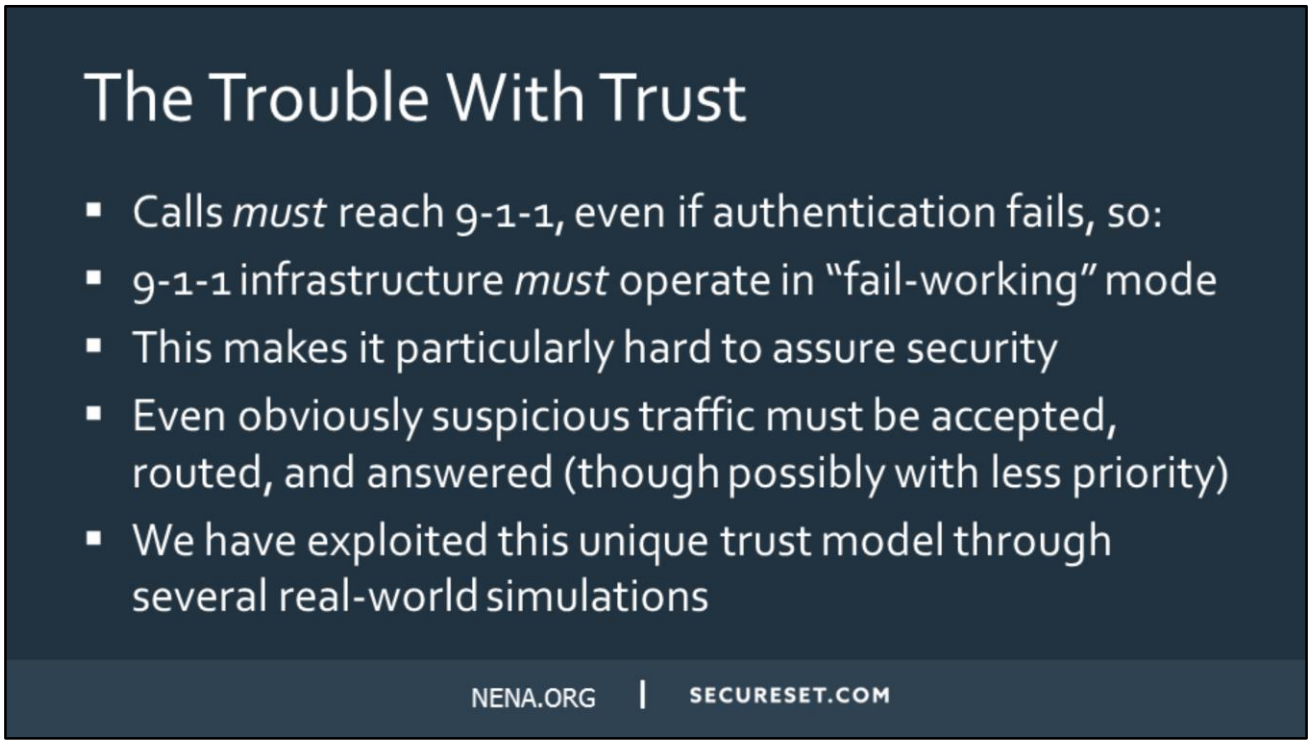
ECRF: Determines the correct (NOT NEAREST) PSAP for a particular call.

PRF: Defines non-geographic aspects of routing (e.g., “Send all text calls to the text analysis center, not the local PSAP.!”

Forest Guide: An Forest Guide tells a device or network where to find (in an IP addressing sense) for the boarder control function of the destination ESInet

ICAM: Identity, Credentialing and Access Management provides the root of trust, and ensures that all people see the people in 1910

Reference: https://www.nena.org/resource/resmgr/ng9-1-1_project/2011_9-1-1_tutorial_v4.1.pptx

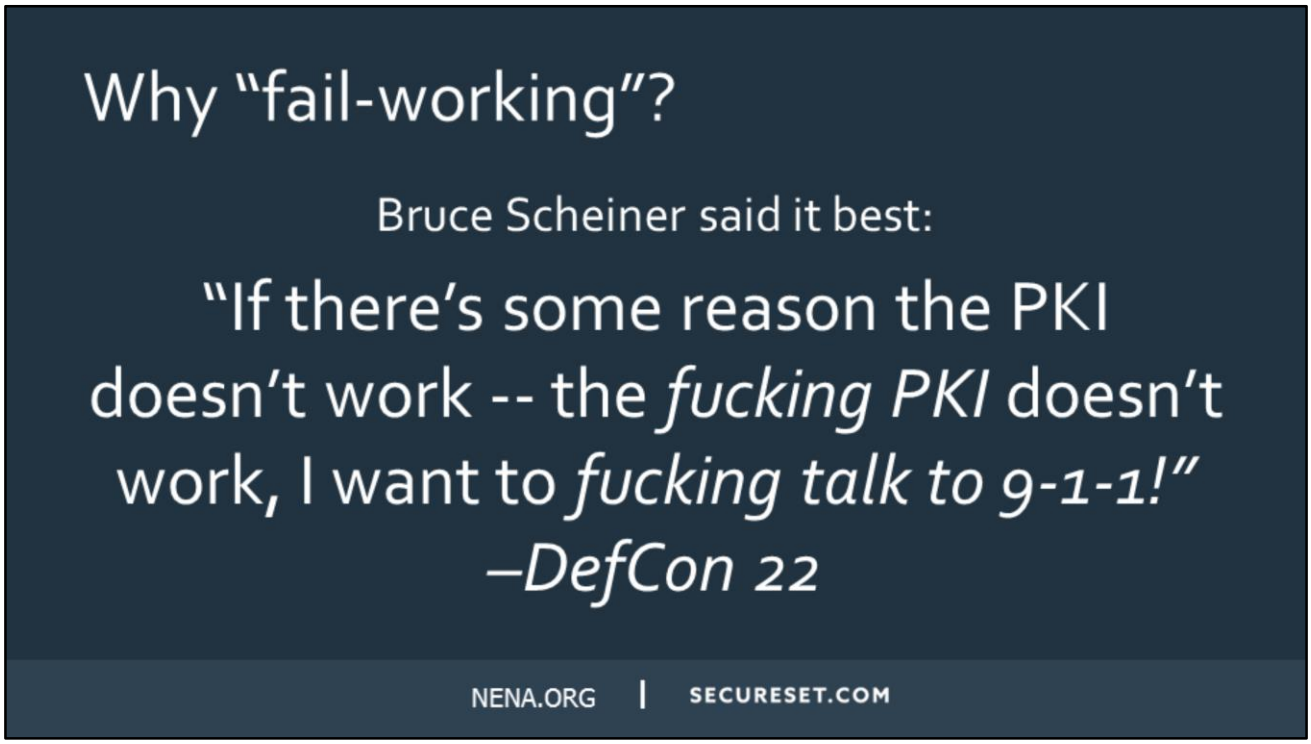


But trust is a tricky thing!

What each of us must worry about is whether our calls will be rejected if they somehow fail to authenticate.

Yet many of us know just how hard is to get basic tunneling technologies to run consistently.

And, there's a BIG problem with just ignoring suspicious traffic!



(We promise we didn't plan this. It just worked out that way.)

ESInet Exploitation Methodology

Step 1: Exploit cryptographic vulnerability

Step 2: Establish command and control

Step 3: Forge geo-location coordinates

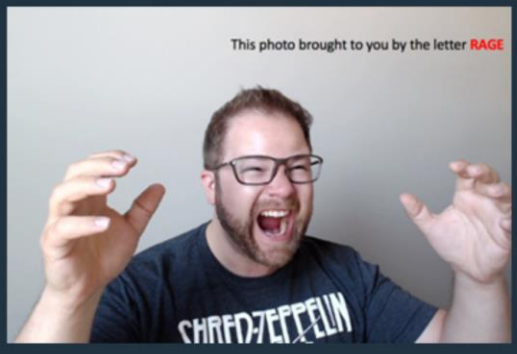
Step 4: Exploit the "working-fail" model of

Step 5: Deliver Denial of Service to other PSAPs

Step 6: Capture fail-over sessions from other PSAPs

Important Caveats

- These exploits were tested in a lab – **not** in a production environment
- There were **many** problems and opportunities that we assume will **not** exist in production
- Because if they do…



NENA.ORG | SECURESET.COM

As with any exploit, YMMV.

Too, some of this can be prevented by just following basic InfoSec hygiene and best practices guides.

However, the stakes are higher here than they are in retail.

A PSAP Credentialing Authority is a necessary precursor to the widespread deployment of *secure* NG9-1-1 systems and the ESInets they are built upon.

However, because of money, and time, and people resources (and money), no PCA exists yet.

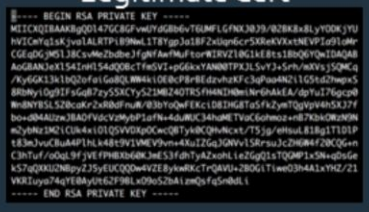
But, we're working on it.

Until then…

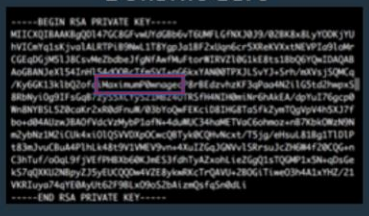
Certificate Exploitation

- MiTM attack launched on a legit PSAP, exploiting the lack of a CA
- We manipulated the clear-text, authentic RSA cert found in a PSAP computer's file directory, and created our own cert
- We then spun-up our own PSAP, and loaded the forged RSA cert with the same file name and structure

Legitimate Cert



Bullshit Cert

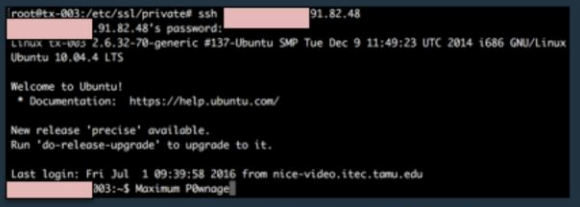


NENA.ORG | SECURESET.COM

We start by taking a host, and retrieving its private key, which we then use to

Authenticate None Of The Things!

- The ESInet accepts our forged cert from our fake PSAP: *#TrustFail!*
- Our attacker PSAP next registeres, in equal privilege, on the ESInet.
- We're ready to take SIP traffic!



NENA.ORG | SECURESET.COM

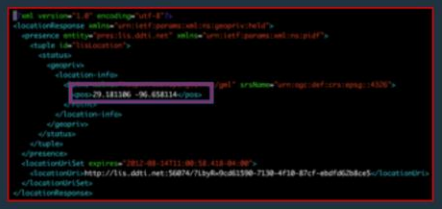
In the absence of a PSAP Credentialing Authority, or some other mechanism (e.g., DANE…maybe…someday…maybe), the core NG9-1-1 Functional Entities, like Emergency Call Routing Functions, can't know we're not legit.

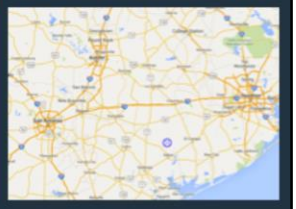
So…what can we do with this new-found power, you ask?

Geo-Location Exploitation

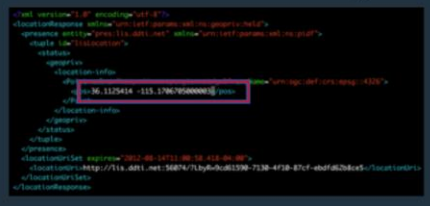
- ESRPs route SIP-based traffic to a PSAP assigned to the caller's jurisdiction, based on Location to Service Translation (LoST) queries to ECRFs, using LIS data
- But the LIS data can be manipulated, once we're on the ESInet….
- We input our own coordinates just to be helpful ☺.
- The ESInet routing proxies balance load across PSAPs, including our fake one, and…
- DEFCON gets its own PSAP!!!

True = Texas





Forged = DEFCON



NENA.ORG | SECURESET.COM

There is a 2-way authentication problem:

Access Network Providers are not required to sign Position Information Data Format – Location Objects (PIDF-LOs) provided by their Location Information Servers to Emergency Service Routing Proxies, so it could be manipulated in-flight or at rest, unless it's protected by the transport and storage media.

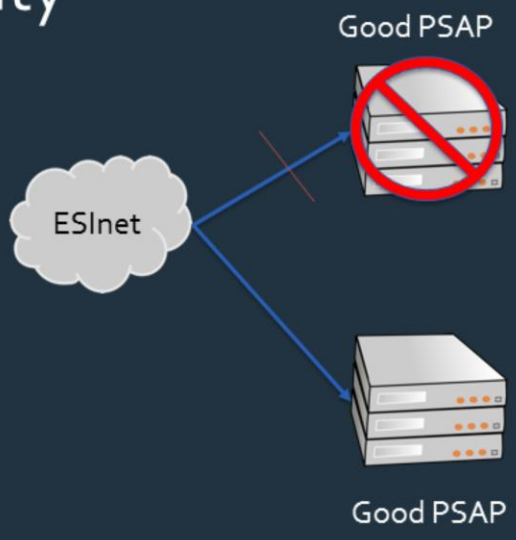
PSAPs are not required to sign service contour shape files or requested policy routing rules (and couldn't do so today without a lot of certificate pinning).

Attackers able to manipulate either or both data types could reroute or block calls from one person, targeted devices, or an entire geographic area.

There are means to mitigate some of these issues, if GEOPRIV and HELD are implemented correctly.

Fail-Over Vulnerability

- The attacking PSAP is associated with the ESInet in equal privilege to other PSAPs.
- Given the working-fail model, the traffic must flow to a PSAP.



NENA.ORG | SECURESET.COM

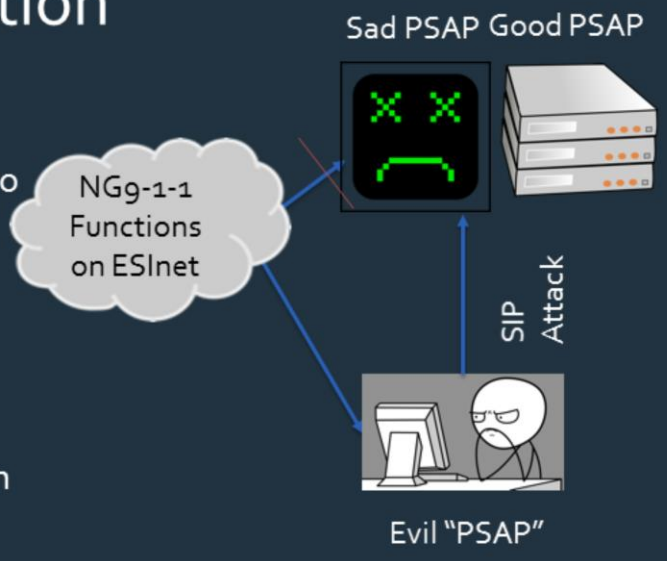
So what if we want to pwn *all* the calls destined for our target PSAP?

We can do that, too!

Because 9-1-1 traffic must always go *somewhere*.

Fail-Over Exploitation

- Using a VoIPer attack on SIP, the QoS of the victim PSAP was so deteriorated, it failed to establish SIP sessions.
- Per the standard and logic of the ESRP…
- The traffic routed to the only possible PSAP ☺ (ours!)
- The victim PSAP felt no pain, and now lives on a nice farm in the countryside



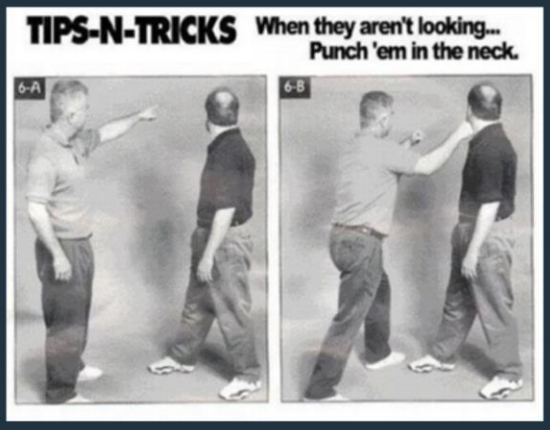
NENA.ORG | SECURESET.COM

Using VoIPer, we degrade the apparent QoS available at our target PSAP until it is unable to establish SIP sessions.

The Emergency Service Routing Proxy senses the PSAP going down, and routes the traffic normally destined for that PSAP straight into our evil little hands.

Consequence

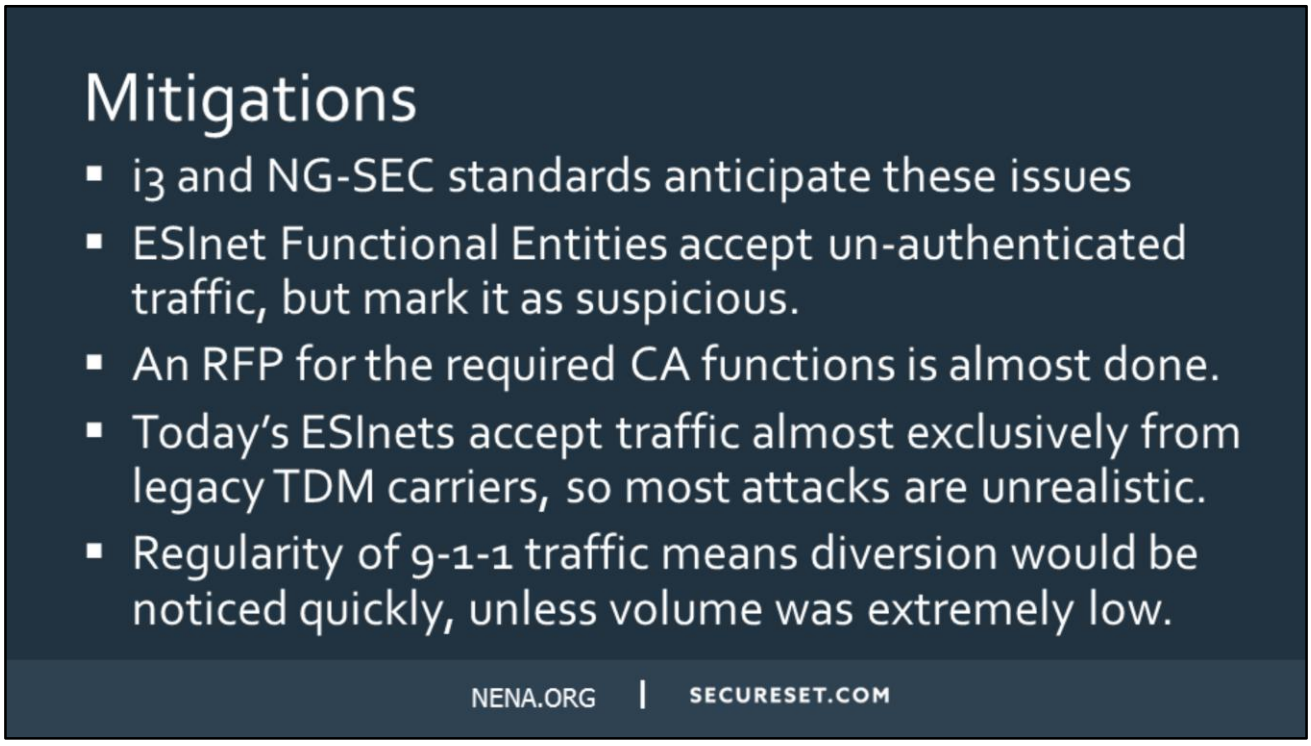
- Possible denial-of-service to a geographic area
- Attackers could redirect selected traffic based on location, type, calling #
- System redundancy could be silently reduced or removed



NENA.ORG | SECURESET.COM

So, how could we use these powers unwisely?

1. Geographic denial of service
2. Selective denial of media (e.g., no texting or video in the area of an all-deaf college)
3. Target softening by silently reducing system redundancy before a broader attack



Ok, so the fail-working model has some inherent flaws (and we badly need a CA!).

What can we do about it?

Well…

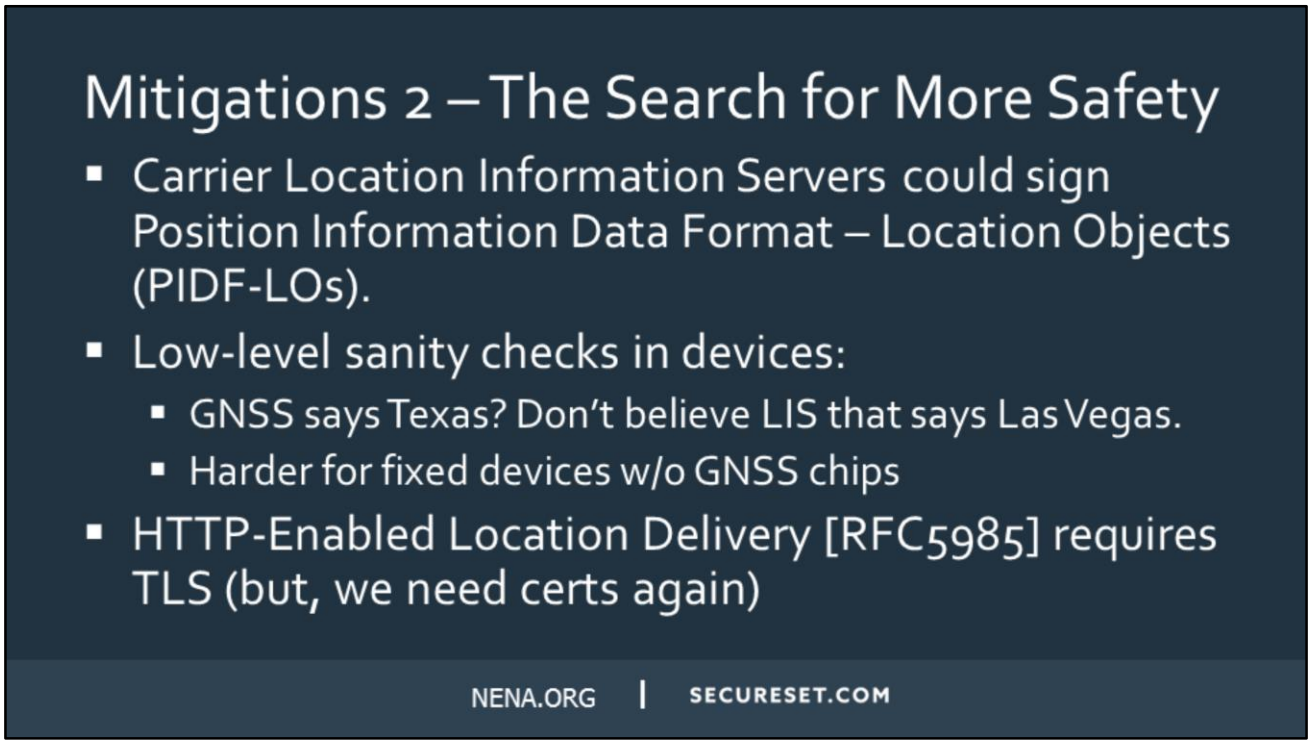
First, we can anticipate that these issue will arise and standardize some functions to deal with them.

Since we have Border Control Functions, we can flag suspicious traffic, and maybe divert it to an Interactive Media Response system to verify the presence of a human, in an emergency, before forwarding to an actual 9-1-1 professional for processing.

We can get off our kiesters and build the damn CA.

For now, at least, we can continue to rely on our only real interconnection counter-party, the wireline TDM carriers to keep their networks physically constrained as they have always been. (Hint: They're not half as constrained as their own masters think!)

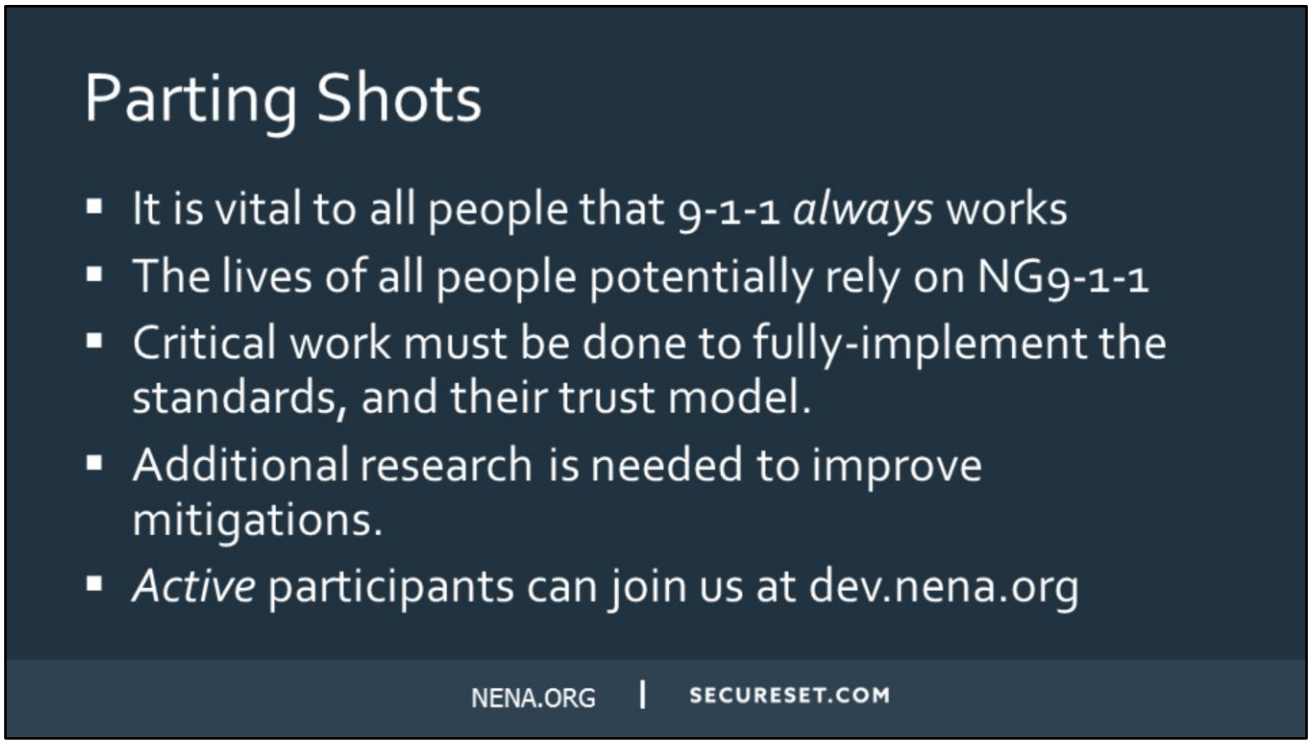
We could also measure 9-1-1 traffic to learn its patterns, and start to detect when traffic we expect isn't arriving.



We can update the standards to *require* that Access Network Providers sign location information.

We can also require devices and networks to implement sanity checks before accepting certain kinds of potentially-spoofable data, like location, if they have onboard location determining capabilities.

We can also make sure we *do* implement HELD securely.



We would love to have a track at our conferences to talk about needed InfoSec improvements.

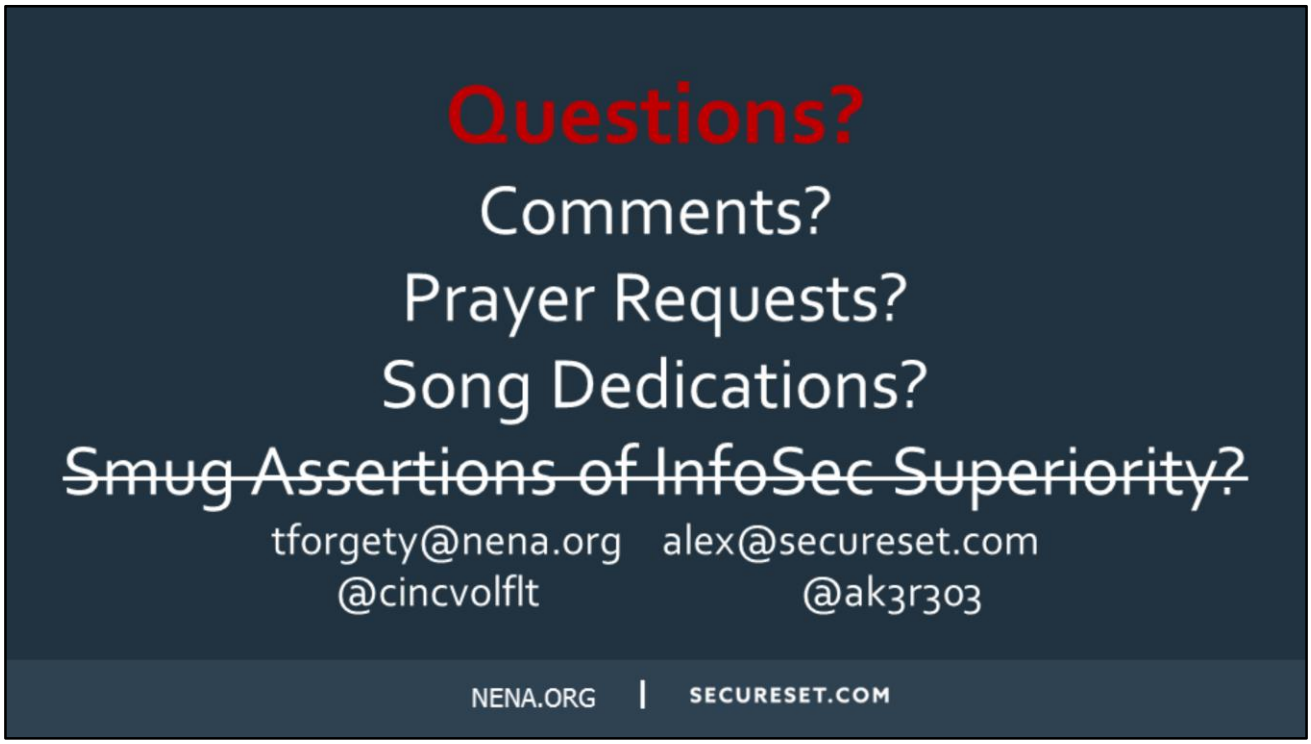
Our community doesn't know what we don't know: InfoSec peeps need to show up so that we can learn.

Already this year we've seen at least one PSAP hit with Ransomware, and that is definitely not cool.

Please won't you be, our neighbors?

Special thanks to our friends and lab partners off of whose homework we have copiously copied.

And, to Dr. Walt Magnussen, the Prof who looked the other way when we smuggled evil into his lab.



Hit us up! We're glad to take your questions here, or via twitter!