

Hacking 911: Adventures in Disruption, Destruction, and Death

quaddi, r3plicant & Peter Hefley
August 2014



Christian Dameff

Physician, MD
Emergency Medicine



Peter Hefley

IT Security, MSM, C|CISO, CISA, CISSP, CCNP, QSA
Senior Manager, Sunera



Jeff Tully

Physician, MD
Pediatrics



Christian Dameff

Open CTF champion sudoers- Defcon 16
Speaker, Defcon 20



Peter Hefley

Gun hacker, SBR aficionado



Jeff Tully

Wrote a program for his TI-83
graphing calculator in middle school
Speaker, Defcon 20

Showing all articles in your library

Search instead for 2012; 126: A274.

[Pediatric Out-of-Hospital Cardiac Arrest in the State of Arizona](#)

J Tully - 2014

Comprehensive databases which collect data on out of hospital cardiac arrests have been useful in identifying markers of outcome in adults, but this data is limited in children. The Arizona Department of Health Services' Save Hearts in Arizona Registry and Education (...

[Related articles](#) [Cite](#)

[PDF] from openrepository.com

[The Impact of Pre-Arrival Dispatch-Assisted CPR on Bystander CPR Rates, Time to Starting CPR and Survival From Out-of-Hospital Cardiac Arrest](#)

B Bobrow, M Panczyk, U Stolz, N Heagerty, C Dameff... - CIRCULATION, 2013

The Impact of Pre-Arrival Dispatch-Assisted CPR on Bystander CPR Rates, Time to Starting CPR and Survival From Out-of-Hospital Cardiac Arrest. Bentley Bobrow, Micah Panczyk, Uwe Stolz, Nathan Heagerty, Christian Dameff ...

[Cite](#)

[A standardized template for measuring and reporting telephone pre-arrival cardiopulmonary resuscitation instructions](#)

C Dameff, T Vadeboncoeur, J Tully, M Panczyk... - Resuscitation, 2014

Background Bystander cardiopulmonary resuscitation (CPR) improves out-of-hospital cardiac arrest (OHCA) survival. Telephone CPR (TCPR) comprises CPR instruction given by emergency dispatchers to bystanders responding to OHCA and the CPR performed as a ...

[Cited by 1](#) [Related articles](#) [All 4 versions](#) [Cite](#)

[A Standardized Template for Measuring and Reporting Dispatch Prearrival CPR](#)

J Tully, C Dameff, R Murphy - Circulation, 2012

A Standardized Template for Measuring and Reporting Dispatch Prearrival CPR. J Tully, C Dameff, R Murphy... Circulation 1:126126, A242, 11/2012.

[Cited by 2](#) [Related articles](#) [Cite](#)

[Utility of the ventricular fibrillation waveform to predict a return of spontaneous circulation and distinguish acute from post myocardial infarction or normal swine in ...](#)

JH Indik, D Allen, M Gura, C Dameff, RW Hilwig... - Circulation: Arrhythmia and ..., 2011

Background—In cardiac arrest, the ventricular fibrillation (VF) waveform, particularly amplitude spectral area (AMSA) and slope, predicts the return of spontaneous circulation (ROSC), but it is unknown whether the predictive utility differs in an acute myocardial ...

[Cited by 8](#) [Related articles](#) [All 5 versions](#) [Cite](#)

[HTML] from ahajournals.org

Disclaimer

This talk is neither sponsored, endorsed, or affiliated with any of our respective professional institutions or companies.

No unethical or illegal practices were used in researching, acquiring, or presenting the information contained in this talk.

Do not attempt the theoretical or practical attack concepts outlined in this talk.

Outline

- why This Matters (Pt. 1)
- 911 Overview
- Methodology
- Attacks
- why This Matters (Pt. 2)

why This Matters (Pt. 1)

4/26/2003 9:57pm



Emergency Medical Services (EMS)





htc

21:26

NINJA TEL

YELLOW PAGES



CONTACTS

REACH OUT AND TOUCH SOMEONE!



TDD Service



TELETYPE DIRECTLY FROM YOUR PHONE!



NINJA TEL

b
l
comcast
w
s







HOSPITAL ENTRANCE

District 21

Medical Examiner's
Office

70 Danley Drive

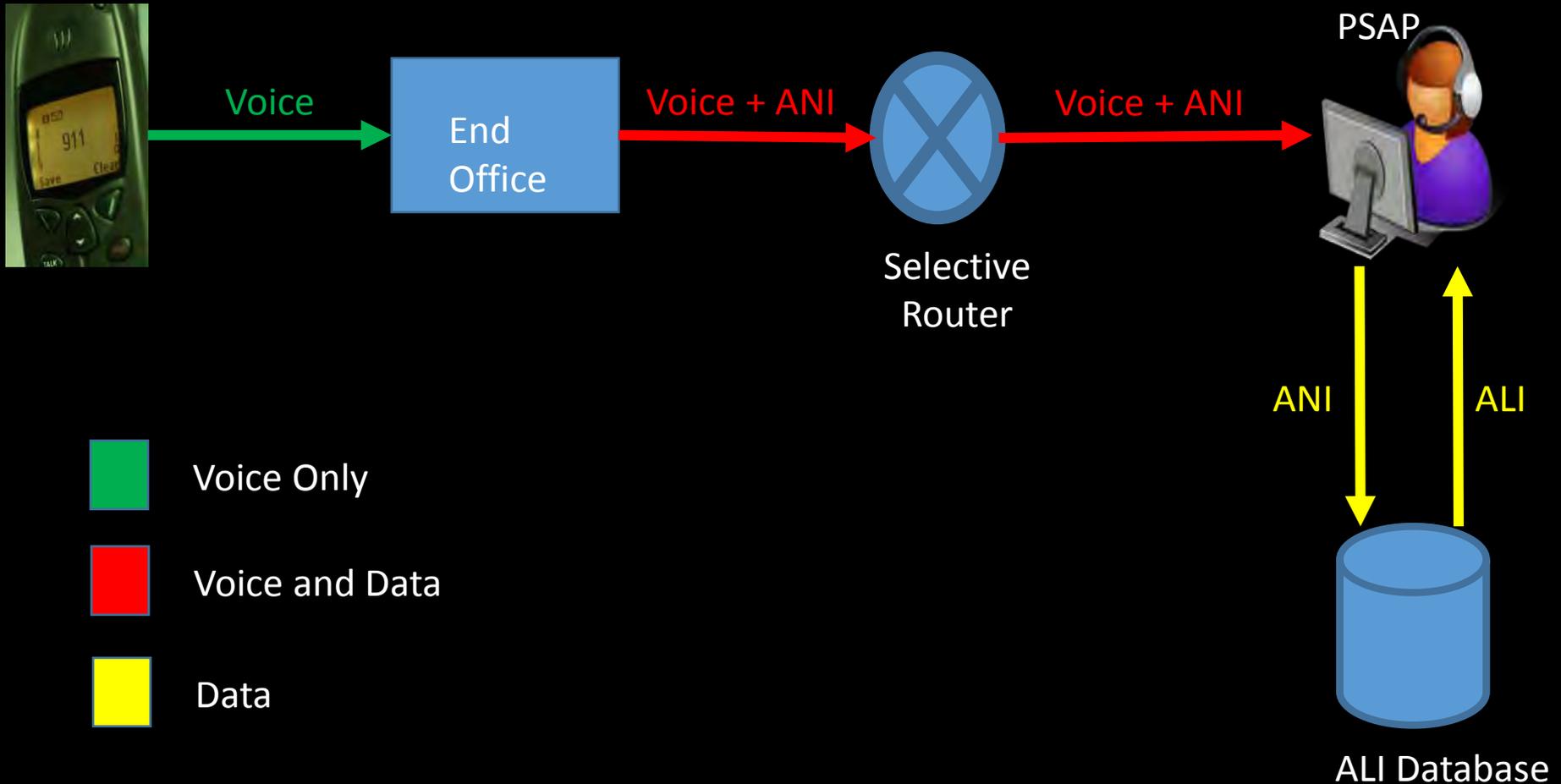
Research Aims

- Investigate potential vulnerabilities across the entire 911 system
- Detail current attacks being carried out on the 911 system
- Propose solutions for existing vulnerabilities and anticipate potential vectors for future infrastructure modifications

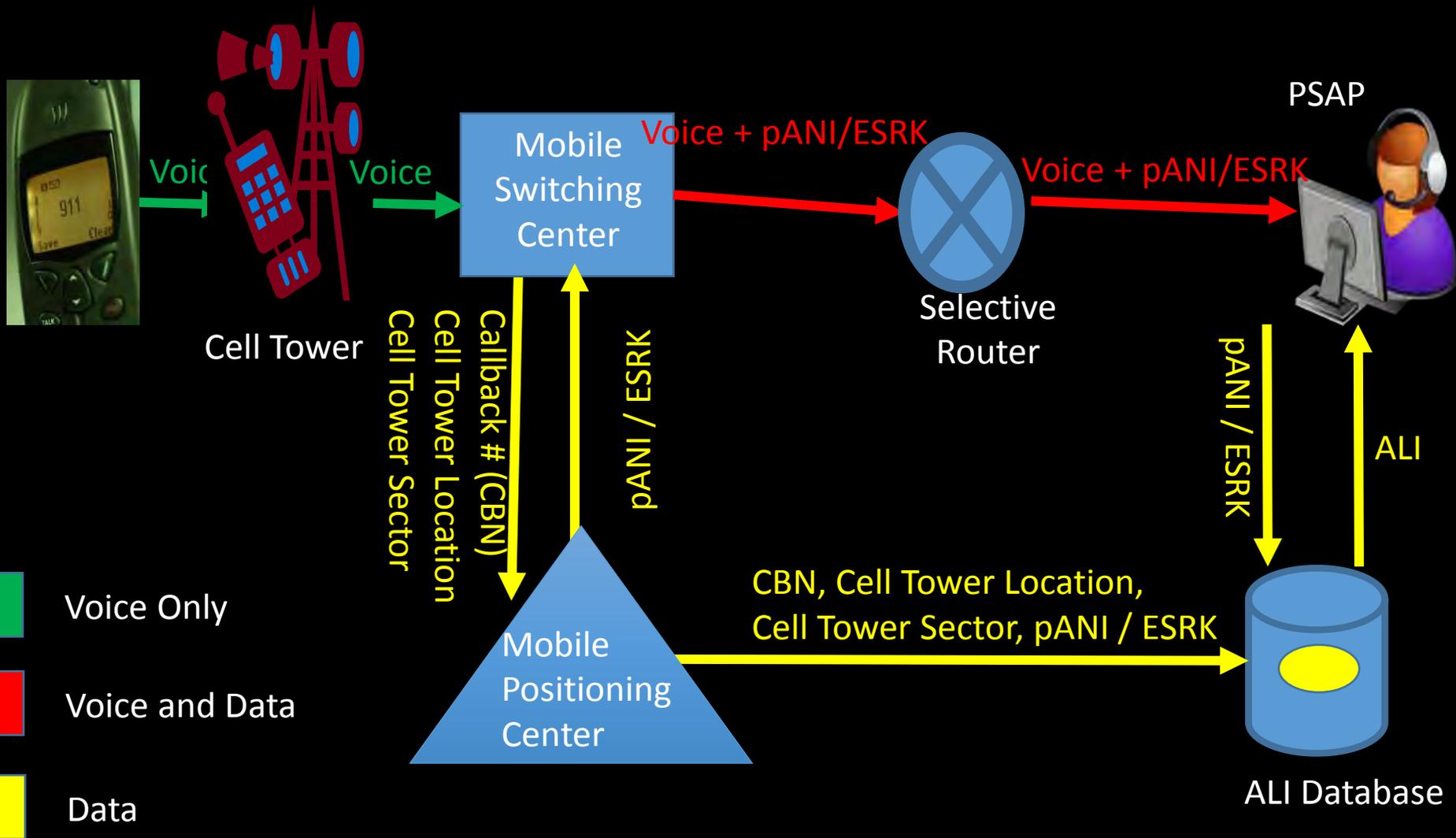
Methodology

- Interviews
- Regional surveys
- Process observations
- Practical experimentation
- Solution development

Wired Telephone Call



Wireless Phase 1 Telephone Call



Wireless Phase 1 Data

(Dynamic Data in Red)

callback number
↓
720-111-9600

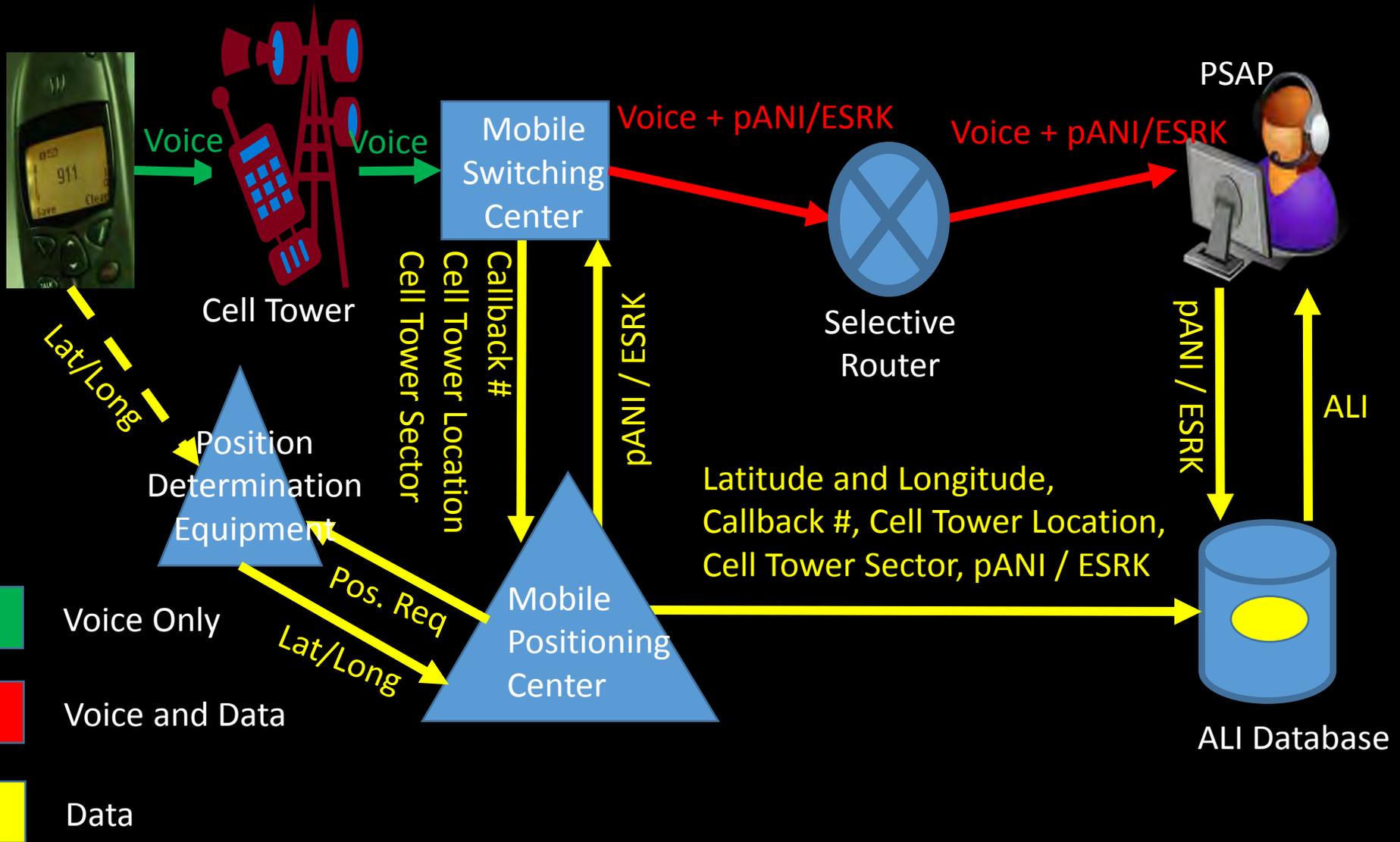
ESN: 787

WIRELESS CARRIER NAME
123 MAIN ST - N SECTOR ← cell sector location description

BOULDER PSAP MOBL/WRLS WIRELESS CARRIER ID
LOC= 303 511-2345 ← routing digit (ESRK/pANI)

BOULDER CO
WIRELESS - VERIFY
VERIFY
VERIFY

Wireless Phase 2 Telephone Call



Wireless Phase 2 Data

callback number

(Dynamic Data in Red)

720-111-9600

ESN: 787

WIRELESS CARRIER NAME

123 MAIN ST - NE

cell sector text location description
(Phase 1 type information)

-104.548407 +39.356910

COF 45

Uncertainty (meters)

COP 90

Confidence factor (%)

BOULDER PSAP WPHII WIRELESS CARRIER ID

LOC= 303 511-2345

routing digit (ESRK/pANI)

BOULDER CO

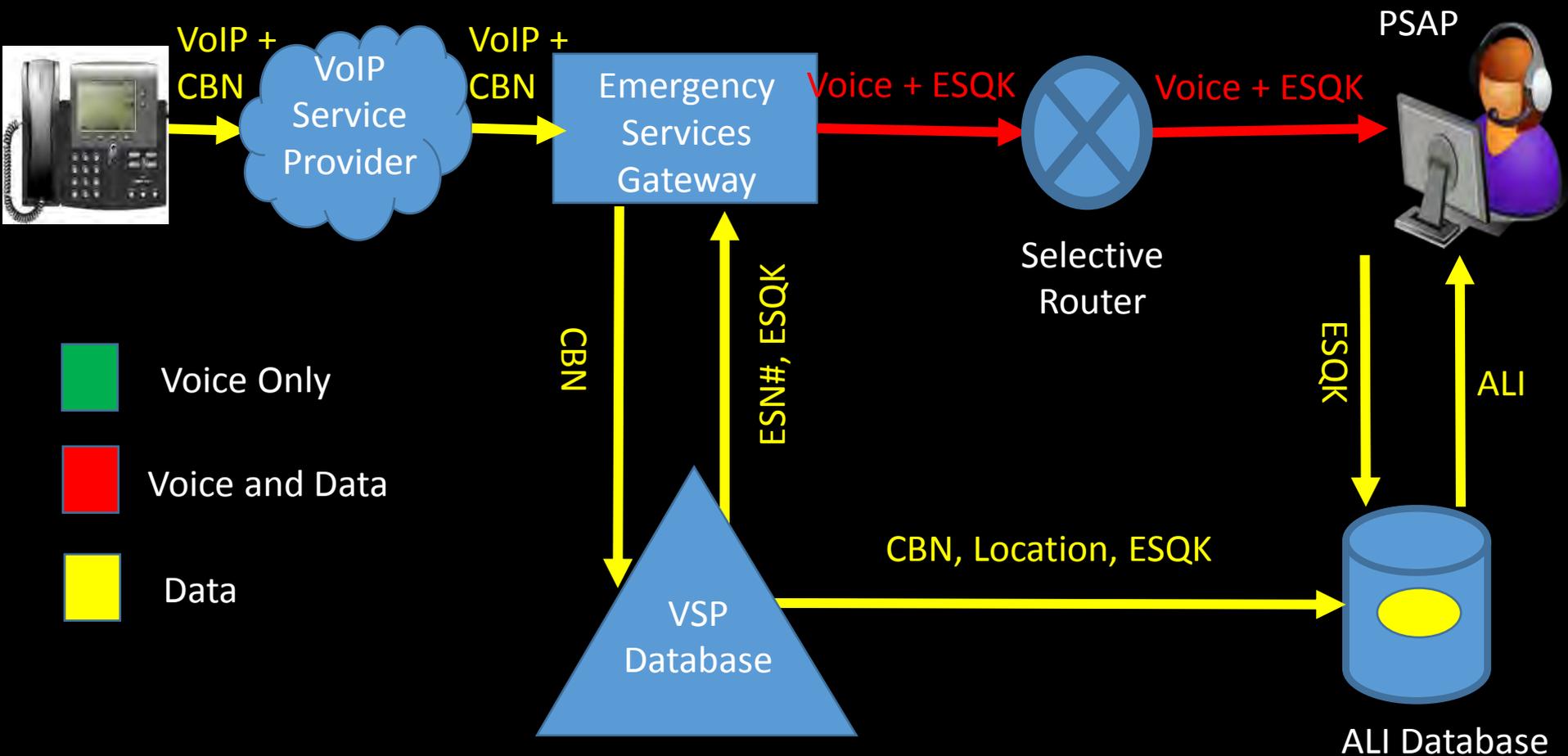
WIRELESS - VERIFY

VERIFY

VERIFY

Longitude (X)
and latitude (Y)

VoIP Call

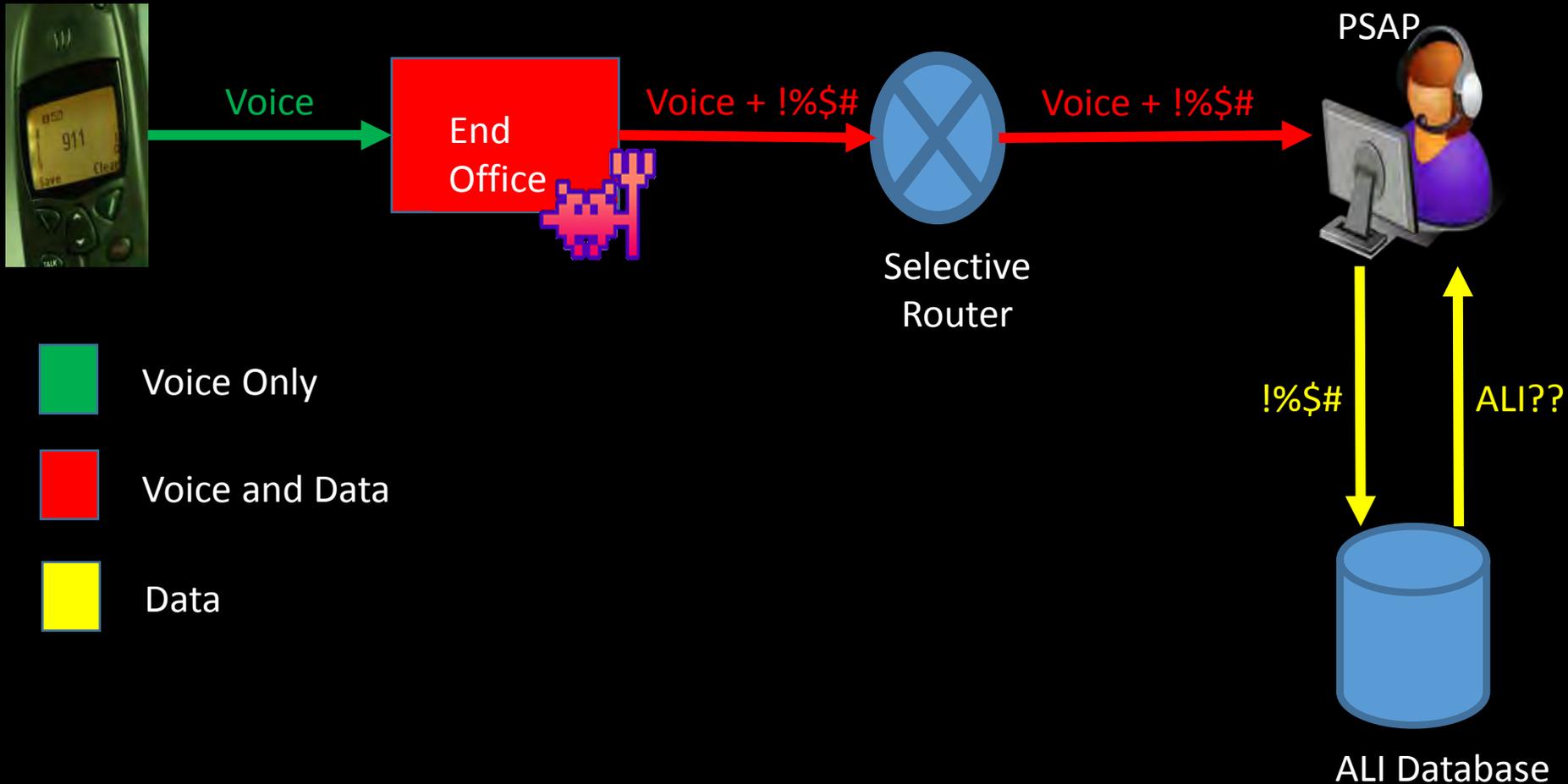




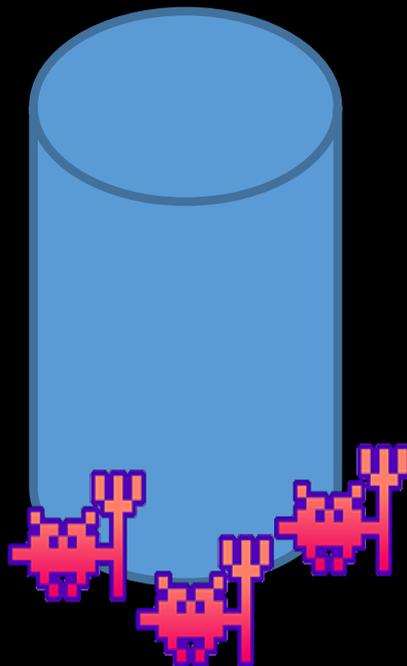
The Three Goals of Hacking 911

- Initiate inappropriate 911 response
- Interfere with an appropriate 911 response
- 911 system surveillance

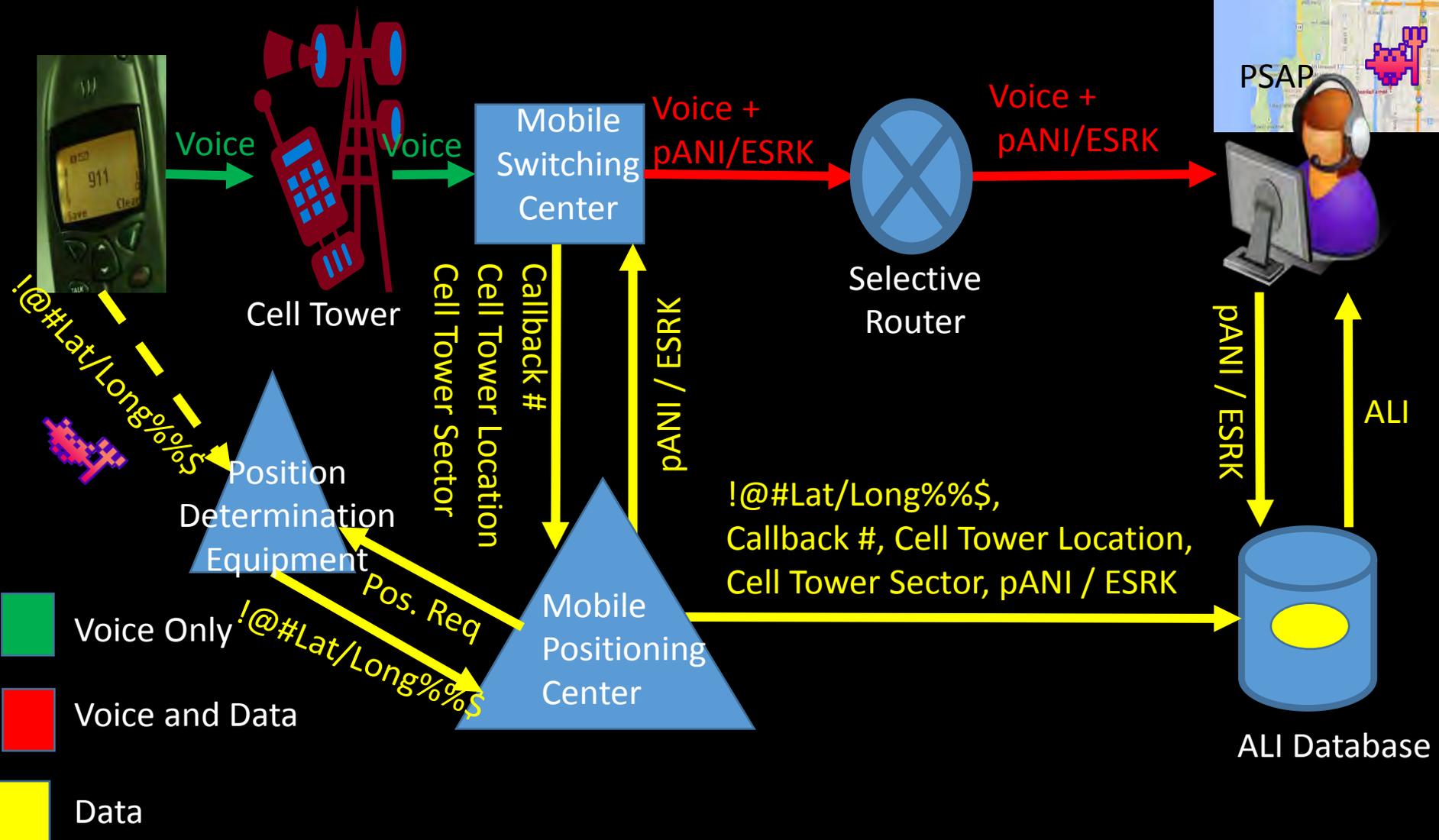
Wired – End Office Control



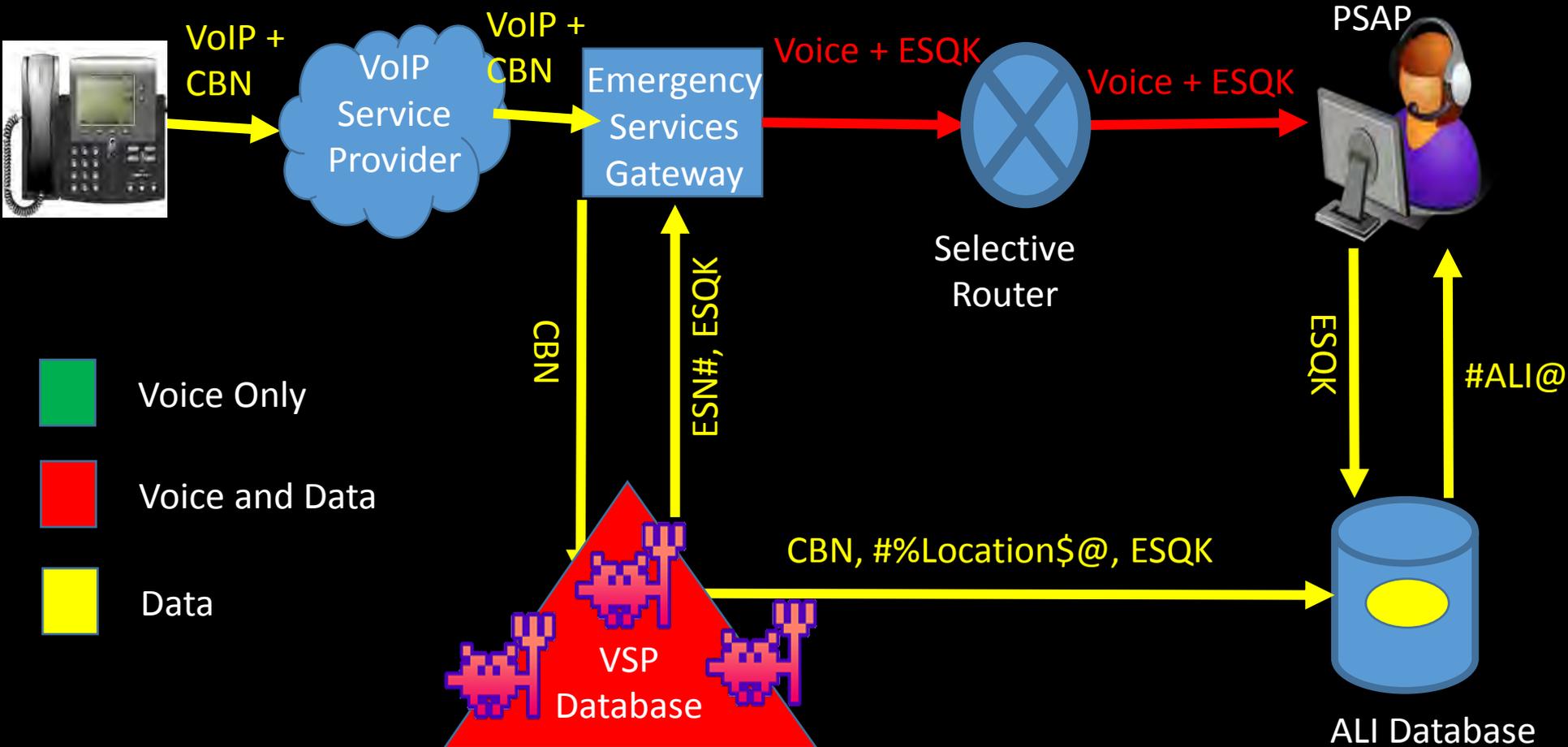
ALI Database

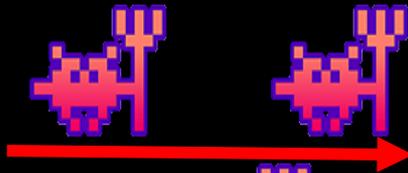


Wireless Location Modification



VSP Modification







Swatting Call

HELP! THIS IS LOOT WITH
THE COTTONWOOD BEE STOP
US. MAY I HELP YOU?
GN * REEF & HEARING AID

Ultratec

SIGNAL POWER RELAY PRINT GREETING SEND MEMO SAVE (CONVERSATION) CLEAR OFFLINE

ON OFF

CAN YOU HELP ME?GA

1 2 3 4 5 6 7 8 9 0 P
Esc @ # \$ % & * () + =
Q W E R T Y U I O P
A S D F G H J K L ; ' [] \ / : < . , > ?



Relay Operator



TTY User

Voice Caller



Fake GPS location

Teleport your phone to
fake GPS location so e



PHONE GANGSTER

You have **2223** credits available
Your PIN is **999-999-999**



CALLER ID SPOOFING

JUST GOT WAY EASY.



Fake GPS Location Spoofer

July 3, 2014

Location Spoofer

LSDroid - February 14, 2014

Tools

Install



Add to Wishlist



Add to Wishlist

by devices



You don't have any devices

'2)

8+1

★★★★★ (1,281)




```
POST /911/action/index.html HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*
Referer:
https://          /911/action/?data=2kJOd6HhtUrPndEqwtR2ZpfKvzxUS80rqqDD1jxQB%2FByAKiCQ%2F7oHw%2B9F1E3ev2CIIlfXmGdvbJ
1iMWABIx5ytlAAsIfaVEBfpNINUVwZfdWXhAI%2FId6ZKk3n3qFznO%2F896wpsuP1I2BTc5GnTkuLi08265JnylD27%2F2CyjvyhSod1T6IF%2FBQiFyegUritP13
12t1jlkYnA4RB8S%2F6WN1LCys9cfRjMabUt%2FJYieTMwizpdWoGFmQfo7rCihEQ%3D%3D&act=ADD911LOC
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host:
Content-Length: 388
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:
PAGE: SESSIONID=281715cafa675bf359ebaa42cb44fa17=J5AychULQnZAQT1AJg6Ids79LBEBQK3S_3mqPA0y_JW7Pd0IgzWUXa7fB5TDwvWTMMz5utEktIRzWT
OcMkh3qio4; __utma=149242857.21002251.1405274951.1405274951.1405274951.1; __utmb=149242857.1.10.1405274951; __utmc=149242857;
__utmz=149242857.1405274951.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)

form%3Avalidate=action%2Findex.html&form%3Avalidate=frmAction&form%3Avalidate=&form%3Avalidate=&form%3Avalidate=&form%3Avalida
te=&form%3Avalidate=index.html&nextform=&curform=ADD911LOC&inpLocID=&inpFName=      &inpLName=      &selCountry=US&inpCountry=US
&inpStreet=      &inpAdd1Det=&inpCity=      &selState=      &inpZip=      &inpInCity=I&optTele=CABLE&optNet=CABLE&btn1=N
ext+%C2%BB
```

VoIP Service Providers

Service disruption attacks

- Line-cutting
- Cell phone jamming
- ALI database editing
- TDoS
- PSAP targeting



malware mac facebook android vulnerability data loss privacy more

Search articles



◀ Marketers, IT contractor arrested in t...

SSCC 131 - Mac malware, Starbuck... ▶



Naked Security
from Sophos

Like 249,430

TDoS extortionists jam phone lines of public services, including hospitals

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com

Do it!

Don't show me this again

by Lisa Veas on January 22, 2014 | 13 Comments

FILED UNDER: Denial of Service, Featured

TDoS (telephony *denial of service*) attacks are targeting essential public services such as hospitals, swamping their switchboards so legitimate calls can't get through.

In the spring of 2013, the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) issued a



Popular

Recent

Related



TDoS attacks target US emergency call centers

Monday review - the hot 19 stories of the week

Monday review - the hot 19 stories of the week



Hackers launch DDoS attack on security blogger's site, send SWAT team to his home



Resource exhaustion
(virtual/personnel)



Outdated system
architectures



Lack of air-gapping



Privacy



CenturyLink says 4,500 calls failed during Washington's 911 outage

2

Tweet

0

Like

0

Share

0

Pin it

Reddit

Email



By The Associated Press

Follow on Twitter

on April 15, 2014 at 12:36 PM, updated April 15, 2014 at 12:37 PM

Print



OLYMPIA, Wash. — The **Washington Emergency Management Division** believes the 911 system is stable now, but it still wants assurances from CenturyLink there won't be a repeat of **last week's statewide outage**, Division Director Robert Ezelle said.

The phone company shared some information Monday as it investigates what went wrong, he said.

"We're encouraged by the information they provided," Ezell said Tuesday. "We're trying to pin down what the root causes were and why backups didn't pick up when a component failed."

CenturyLink says about 4,500 calls failed to get through during a six-hour outage on Thursday that was caused by a technical error in a third-party vendor's call router. About 770 calls were completed in that period. CenturyLink says it has addressed the issue.

The outage involved 127 dispatch points in Washington.

The company says a similar two-hour 911 outage in parts of northwest Oregon was caused by a separate problem.

The vendor involved is Longmont, Colo., based Intrado Inc., which manages the 911

Prineville Hotshots



20 years ago firefighters d Colorado inf are the storie who survive

Active Discussions

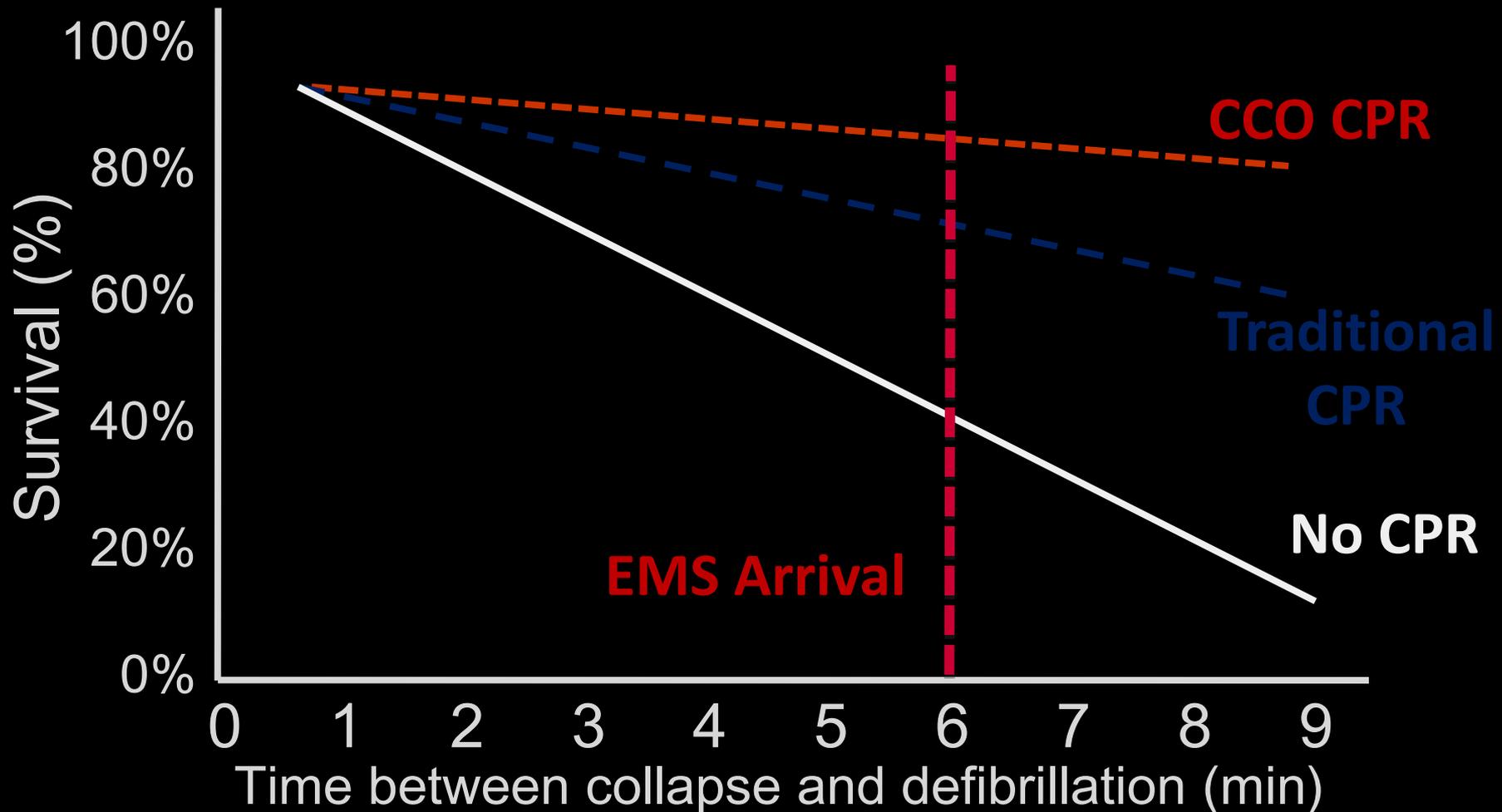
- 1 Protesters rally against Operation Protective Ed downtown Portland (pho (78 comments)
- 2 New report explores wh incomes lag behind the average (174 comments)
- 3 Global warming is not se Guest opinion (424 comments)
- 4 Israel widens bombing t

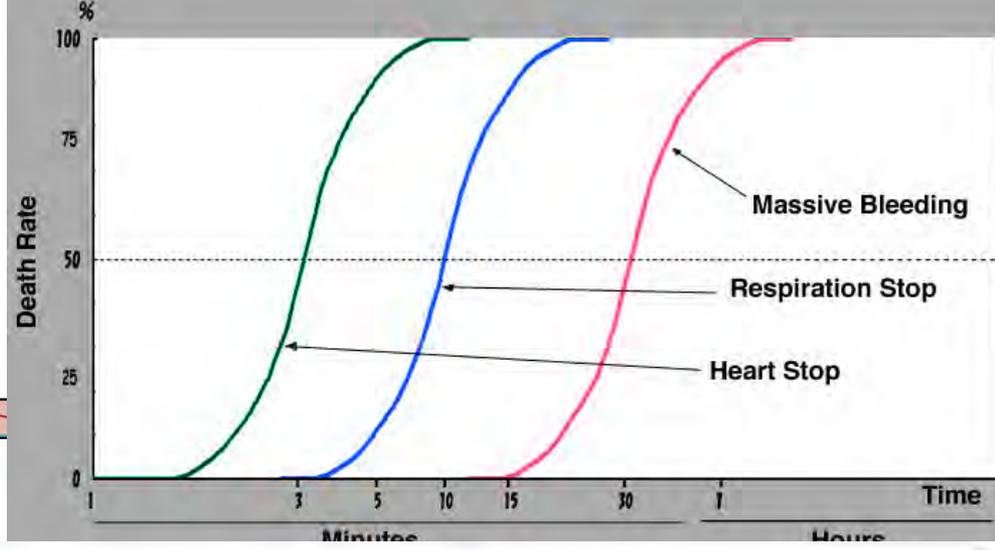
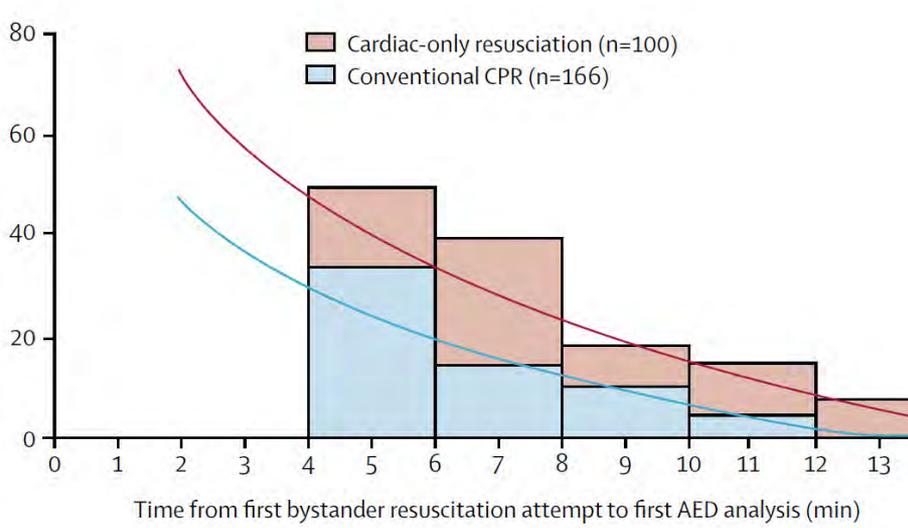


Health Impacts

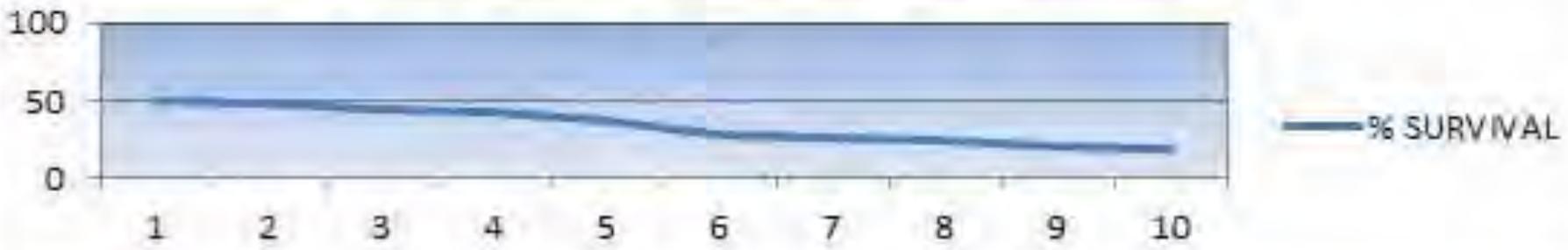


Bystander CCO CPR Improves Chance of Survival from Cardiac Arrest





% SURVIVAL VS DELAY IN MINUTES



DETECTION OF COLLAPSE	REPORT OF ALARM 911 OR DIRECT	EMS/FIRE RESPONSE TIME			
		DISPATCH UNITS	TURN OUT	RESPONSE TIME	SET UP
TIME VARIES		TIME DIRECTLY MANAGEABLE			

Strategic Threat Agents

- 6000 PSAPs taking a combined 660,000 calls per day
- Fundamental building block of our collective security
- Potential damage extends beyond individual people not being able to talk to 911

Reverse 911

Solutions

- Call-routing red flags
- Call “captchas”
- PSAP security standardizations
- Increased budgets for security services
- Open the Black Box

OPENING

THE

BLACK
BOX



Q&A