Hacking 911: Adventures in Disruption, Destruction, and Death

quaddi, r3plicant & Peter Hefley
August 2014
Christian Dameff

Physician, MD
Emergency Medicine
Open CTF champion sudoers- Defcon 16
Speaker, Defcon 20

Peter Hefley

IT Security, MSM, C|CISO, CISA, CISSP, CCNP, QSA
Senior Manager, Sunera
Gun hacker, SBR aficionado

Jeff Tully

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

This talk includes disturbing audio clips.
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 (...

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 ...

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 ...

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.

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 ...
Outline

- Why This Matters (Pt. 1)
- 911 Overview
- Methodology
- Attacks
- Why This Matters (Pt. 2)
Emergency Medical Services (EMS)
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
Wireless Phase 1 Telephone Call

- Voice Only
- Voice and Data
- Data

Cell Tower → Mobile Switching Center → Selective Router → PSAP

Mobile Positioning Center

Callback #: (CBN), Cell Tower Location, Cell Tower Sector, pANI / ESRK

ALI Database

Voice + pANI/ESRK

- Voice Only
- Voice and Data
- Data
Wireless Phase 1 Data

- Callback number: 720-111-9600
- ESN: 787
- Wireless Carrier Name: 123 Main St - N Sector
- Cell sector location description: Boulder PSAP MOBL/WRLS 303 511-2345
- Wireless Carrier ID: Boulder CO
- Routing digit (ESRK/pANI): 303 511-2345
- Wireless - Verify Verify Verify Verify
Wireless Phase 2 Telephone Call

Wireless Phase 2 Telephone Call involves the following components:

1. **Cell Tower**: The location where mobile signals are transmitted.
2. **Wireless Phase 2 Telephone Call**: The process of making a call on a wireless network.
3. **Mobile Switching Center**: The central point for managing call connections.
4. **Selective Router**: A device that routes calls to different destinations.
5. **PSAP**: Public Safety Answering Point, where 911 calls are received.
6. **ALI Database**: Contains information about the caller's phone number and location.
7. **Voice Only**: Call type that does not include data transfer.
8. **Voice and Data**: Call type that includes both voice and data transfer.
9. **Data**: Part of the call that carries data information.

The process involves:
- **Voice**: Used for audio communication.
- **Lat/Long**: Latitude and Longitude information for caller location.
- **Callback #**: The number provided by the caller.
- **Cell Tower Location**: The specific cell tower the call is associated with.
- **Cell Tower Sector**: The sector of the cell tower.
- **pANI / ESRK**: Identifiers used for call routing.

The call flow involves the following steps:

1. The caller places a call to the PSAP.
2. The PSAP sends a request to the ALI database for the caller's information.
3. The ALI database provides the caller's location information.
4. The Mobile Switching Center receives and routes the call.
5. The Selective Router receives the call and routes it to the appropriate destination.
6. The call is completed.

The diagram illustrates the flow of information and the involvement of various components in the process.
### Wireless Phase 2 Data

<table>
<thead>
<tr>
<th>Callback Number</th>
<th>Dynamic Data in Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>720-111-9600</td>
<td></td>
</tr>
<tr>
<td>ESN: 787</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless Carrier Name</th>
<th>Cell Sector Text Location Description (Phase I Type Information)</th>
</tr>
</thead>
<tbody>
<tr>
<td>123 MAIN ST - NE</td>
<td></td>
</tr>
<tr>
<td>-104.548407 +39.356910</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COF 45</th>
<th>Uncertainty (meters)</th>
<th>COP 90</th>
<th>Confidence Factor (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless Carrier ID</th>
<th>Routing Digit (ESRK/pANI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOULDER PSAP WPHII</td>
<td></td>
</tr>
<tr>
<td>LOC = 303 511-2345</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless - Verify</th>
<th>Verify</th>
<th>Verify</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOULDER CO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Longitude (X) and Latitude (Y)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>


The Three Goals of Hacking 911

• Initiate inappropriate 911 response
• Interfere with an appropriate 911 response
• 911 system surveillance
System Weaknesses
ALI Database
NSI Emergency Calls

Voice Only

Voice and Data

Data

CBN = 911 + last 7 of ESN/IMEI

CBN, Cell Tower Location, Cell Tower Sector, pANI / ESRK

ALI Database

Mobile Switching Center

Selectivity Router

Mobile Positioning Center

PSAP

Cell Tower Location

Cell Tower Sector
System Attacks
Swatting Call
Fake GPS location
Teleport your phone to any location so everyone thinks you're somewhere else.

PHONE GANGSTER
You have 2223 credits available
Your PIN is 999-999-999

CALLER ID SPOOFING
JUST GOT WAY EASY.

BLUFF
mycall.com

Fake GPS Location Spoofer
July 3, 2014

Location Spoofer
LSDroid - February 14, 2014
Tools

Install
Add to Wishlist

You don't have any devices

⭐⭐⭐⭐⭐ (1,281)

Add to Wishlist

My devices

(2)
Dual-Tone Multi-Frequency (DTMF) Frequency Standards

Frequencies shown are in Hertz

1209 1336 1477 1633

NOTE: The last column (A-B-C-D) is not normally found on telephones
Service disruption attacks

- Line-cutting
- Cell phone jamming
- ALI database editing
- TDoS
TDoS extortionists jam phone lines of public services, including hospitals

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

Resource exhaustion (virtual/personnel)
Outdated system architectures
Lack of air-gapping
Privacy
CenturyLink says 4,500 calls failed during Washington's 911 outage

By The Associated Press
Follow on Twitter
on April 15, 2014 at 12:36 PM, updated April 15, 2014 at 12:37 PM

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 call systems for nearly a dozen states.
Bystander CCO CPR Improves Chance of Survival from Cardiac Arrest

![Graph showing survival rates over time between collapse and defibrillation for different CPR types.](graph.png)

Nagao, K. Current Opinions in Critical Care 2009
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
Solutions

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

Para Español,
Oprima Número Dos
Security Standardization
Budget Hard Looks