NG9-1-1 Voice Security Issues and Can SHAKEN/STIR Help?
SecureLogix Introduction

- Based in San Antonio, Texas
- Focused on call authentication, spoofing, robocalls, and TDoS
- Our solutions provide a “Voice/Call Firewall”
- Working with DHS S&T Directorate on voice security
- Strategic partnerships with Verizon and AT&T
NG9-1-1 Voice Threats

Prevent Contact Center Customer Access

6 Billion Robocalls Per Month

Enabler for Many Attacks

Broad class of calls designed to harass

Significant Threat to 9-1-1 and other Contact Centers

Affects 9-1-1 if too aggressive or on admin lines

Spoofing is used for SWATting attacks

Conferencing and other confusing calls
Recent TDoS Attacks

- TDoS attack against D.C. 9-1-1:
  - About 6,000 calls
  - All from the same source number
  - Recorded calls with bible verses

- TDoS attacks against counties in D.C. and South Florida:
  - Targeted the administrative phones and police department
  - About 6,300 calls in one case using spoofed source numbers
  - Calls were dead air, recorded message, or Arabic language
  - Conferencing calls to intentionally confuse attendants
Affected Areas

- Palm Beach County NG9-1-1 and Sheriffs office
- Washington D.C. 9-1-1
- Farmington Hills 9-1-1
- City of Miami
- Howard County, Maryland
- Montgomery County, Maryland
- Other counties in Maryland/Virginia
- Other parts of the country
Mobile Botnet

911 call volume in Surprise, Ariz.

- **175 calls**

- **Day of Twitter event**
- **Day before event**
- **Day after event**

**Source:** Surprise Police Department

**The Wall Street Journal**
Compromised PBX

• Compromised PBX used to make local 9-1-1 calls
• Local and hosted PBXs can be used to make 9-1-1 calls
• Hairpinning and transfers
• This can also be done with SIP/VoIP
Admin Line Attacks

Typical 9-1-1 Center Configuration

- Public Telephone Network
  - Actors Dialing Publicly Listed Phone Number
  - Local Resident Dialing Publicly Listed Phone Number
- Publicly Listed Numbers: xxx-xxx-xxxx
- 9-1-1 Calls
- Managed Device
- Local Law Enforcement Phone System
- Admin Lines
- Local 9-1-1 Server
  - 9-1-1 Call
  - Admin Call
- Local 9-1-1 Workstation

PSAP
NG9-1-1 – Architecture

Service Provider
SIP Trunk
SIP Trunk

NG9-1-1 ESINet
SBC
ENUM
Appliance
ESRP

AWS
Orchestra One
And TDoS Detection

PSAP/NCCIC
Visualization

Call Handling System
SHAKEN/STIR

- NG9-1-1 transition occurring slowly
- Many NG9-1-1 deployments still use TDM to service provider
- It is difficult to spoof numbers and get calls into NG9-1-1
- It will help with VoIP calls
- It will help significantly with admin line calls

- NG9-1-1 analytics will be essential
- Visualization and options for call treatment will be essential
Contact Info

Mark Collier
SecureLogix Corporation
mark.collier@securelogix.com