Voice Cyber Security: DHS DDoSD Efforts in TDoS and 911

Subcommittee on Disaster Reduction Briefing

May 4, 2017

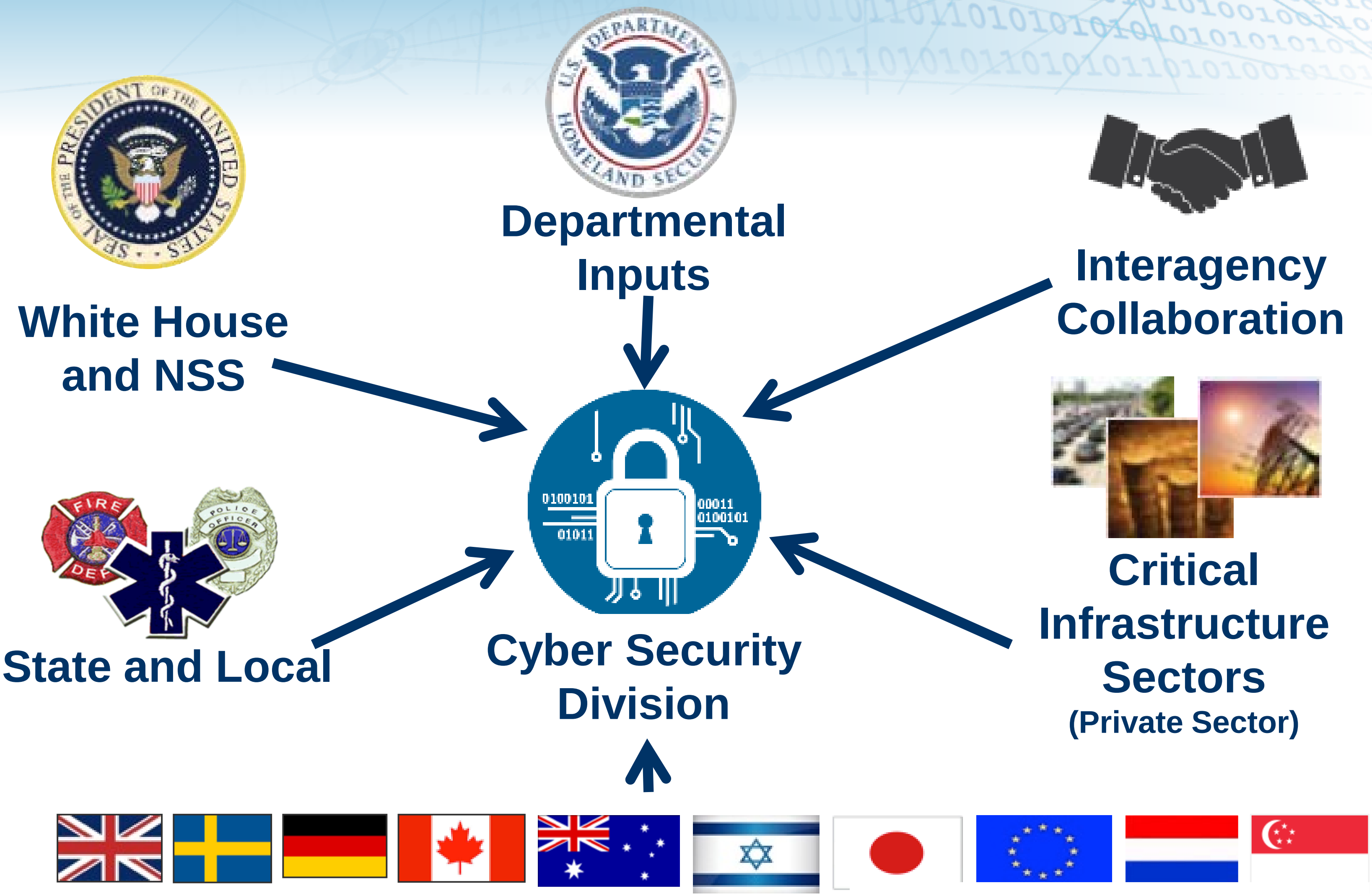
Dr. Dan Massey

Program Manager
Cyber Security Division
Science and Technology Directorate

Homeland Security

Science and Technology

RESEARCH REQUIREMENT INPUTS



Departmental Inputs

White House and NSS

Interagency Collaboration

State and Local

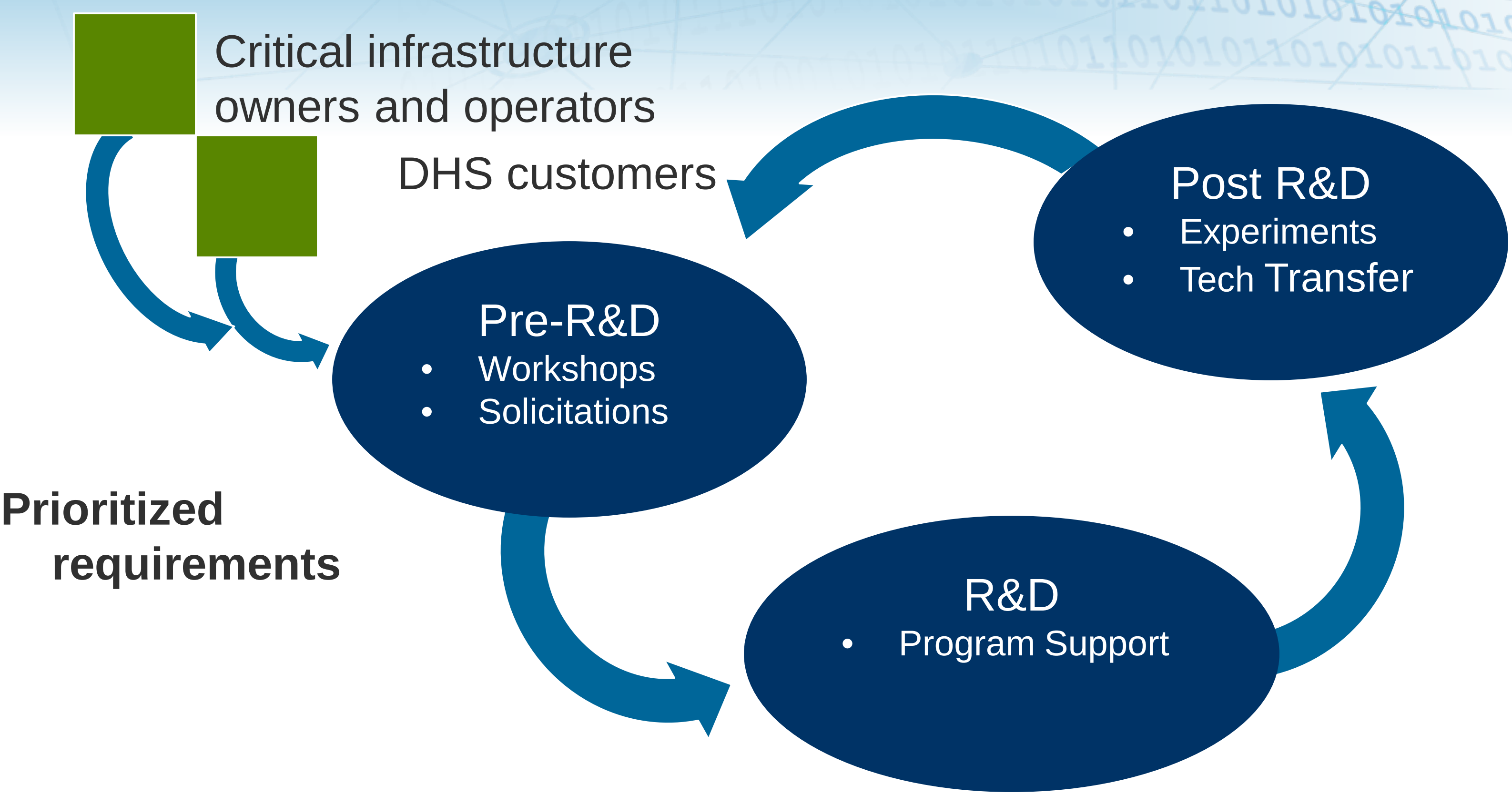
Cyber Security Division

Critical Infrastructure Sectors
(Private Sector)

International Partners

Homeland Security
Science and Technology

CSD R&D EXECUTION MODEL



Critical infrastructure owners and operators

DHS customers

Prioritized requirements

Pre-R&D
- Workshops
- Solicitations

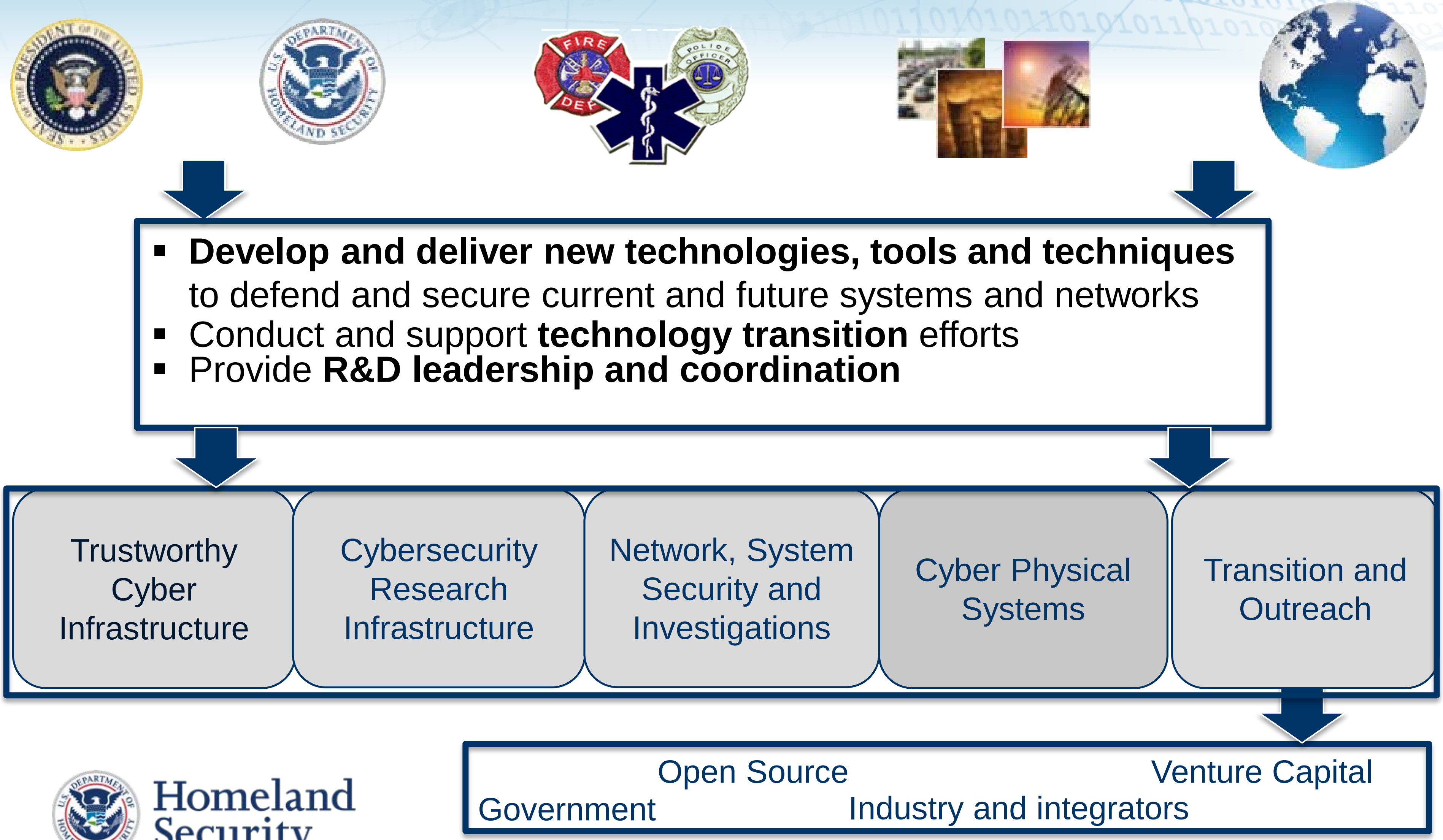
R&D
- Program Support

Post R&D
- Experiments
- Tech Transfer

"Crossing the ‘Valley of Death’: Transitioning Cybersecurity Research into Practice,"
IEEE *Security & Privacy*, March-April 2013,
Maughan, Douglas; Balenson, David; Lindqvist, Ulf; Tudor, Zachary
http://www.computer.org/portal/web/computingnow/securityandprivacy

Homeland Security
Science and Technology

CYBER SECURITY DIVISION MISSION



- **Develop and deliver new technologies, tools and techniques** to defend and secure current and future systems and networks
- Conduct and support **technology transition** efforts
- Provide **R&D leadership and coordination**

Trustworthy Cyber Infrastructure

Cybersecurity Research Infrastructure

Network, System Security and Investigations

Cyber Physical Systems

Transition and Outreach

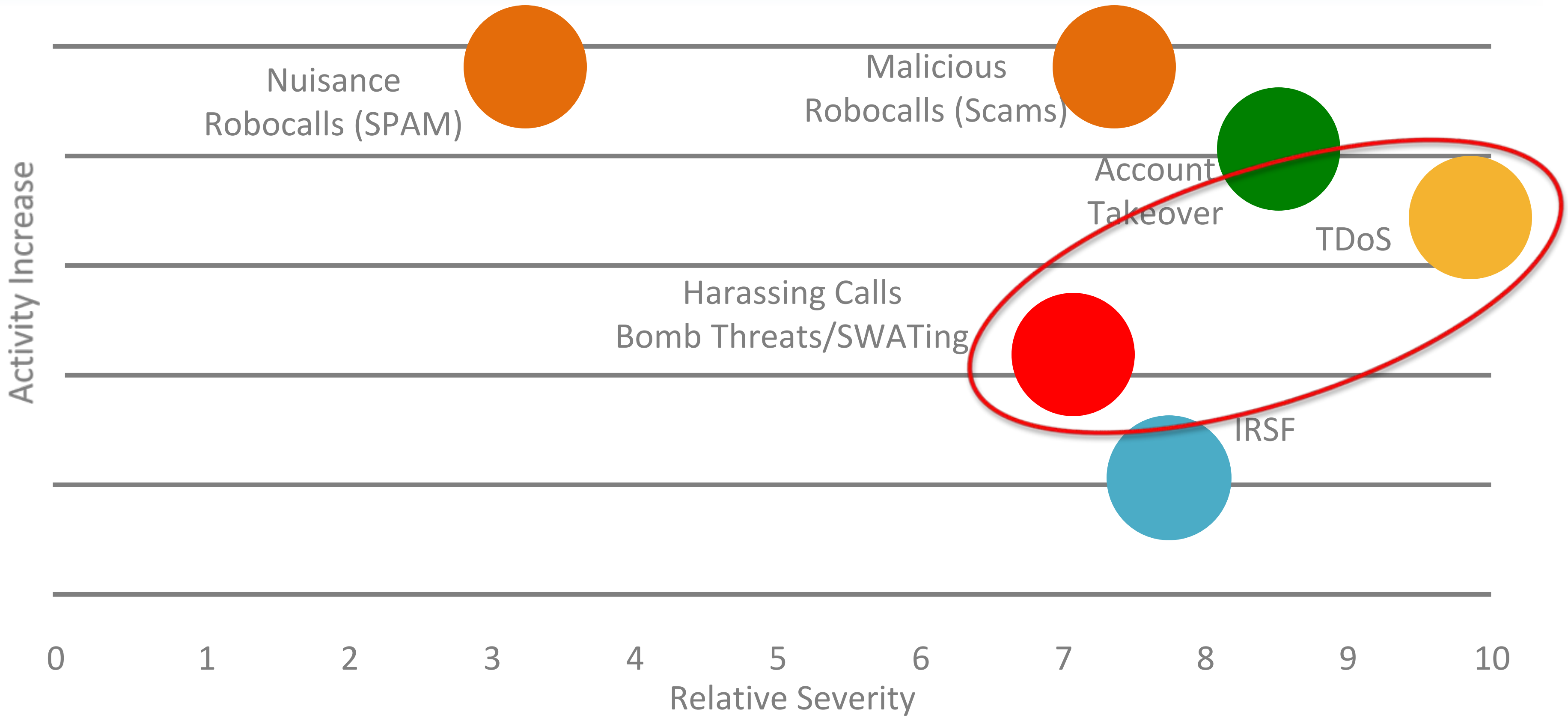
Open Source

Venture Capital

Government

Industry and integrators

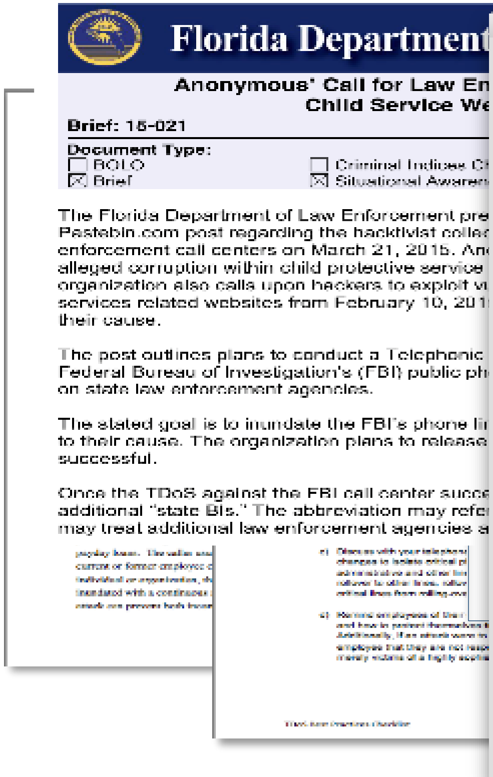
Voice Security Summary



Homeland Security
Science and Technology

Provided by SecureLogix under DHS S&T Funded Efforts

Telephony DoS (TDoS) Threat



Florida Departmen

Anonymous' Call for Law En
Child Service We

Brief: 15-021

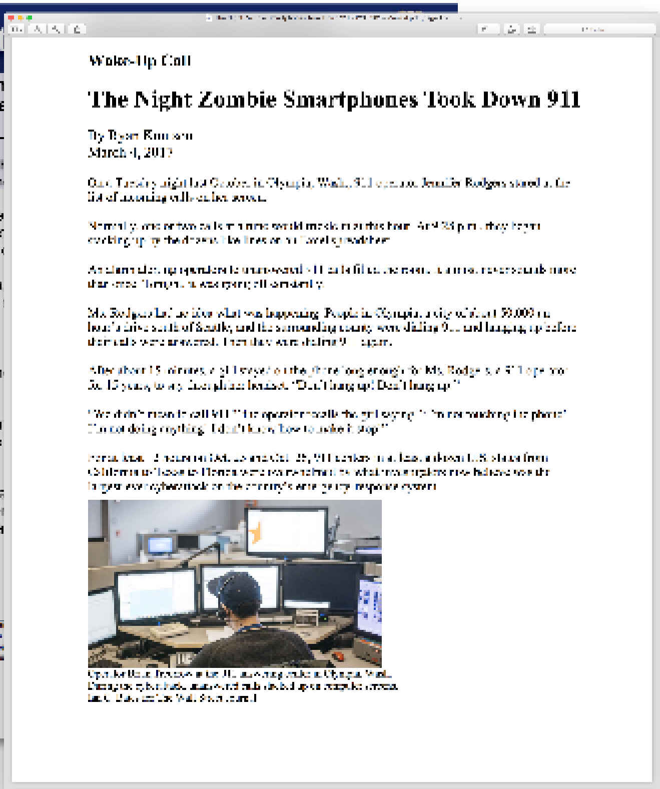
Document Type:
□ BOLO
☒ Brief
□ Criminal Indices Ch
☒ Situational Awaren

The Florida Department of Law Enforcement pre
Pastebin.com post regarding the hacktivist collec
enforcement call centers on March 21, 2015. An
alleged corruption within child protective service
organization also calls upon hackers to exploit v
services related websites from February 10, 201
their cause.

The post outlines plans to conduct a Telephonic
Federal Bureau of Investigation's (FBI) public ph
on state law enforcement agencies.

The stated goal is to inundate the FBI's phone li
to their cause. The organization plans to release
successful.

Once the TDoS against the FBI call center succe
additional "state BIs." The abbreviation may refe
may treat additional law enforcement agencies a



Wake-Up Call

The Night Zombie Smartphones Took Down 911

By Ryan Knutson
March 4, 2017

One Tuesday night last October in Olympia, Wash., 911 operator Jennifer Rodgers stared at the list of incoming calls on her screen.

Normally [illegible] At 8:25 p.m. they began stacking up [illegible]

[illegible]

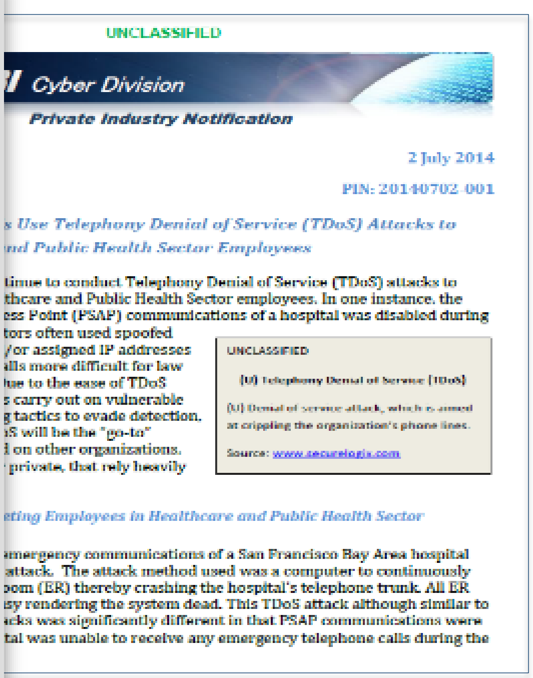
Ms. Rodgers had no idea what was happening. People in Olympia, a city of about 50,000 an hour's drive south of Seattle, and the surrounding county were dialing 911 and hanging up before their calls were answered. Then they were dialing 911 again.

After about 15 minutes, a girl stayed on the line long enough for Ms. Rodgers, a 911 operator for 15 years, to [illegible] "Don't hang up! Don't hang up!"

"We didn't mean to call 911," the operator recalls the girl saying. "I'm not touching the phone! I'm not doing anything. I don't know how to make it stop."

Over about 12 hours on Oct. 25 and Oct. 26, 911 centers in at least a dozen U.S. states from California to Texas to Florida were overwhelmed by what investigators now believe was the largest ever cyberattack on the country's emergency response system.

Operator Beth Dawson at the 911 answering center in Olympia, Wash. [illegible]



UNCLASSIFIED

I Cyber Division

Private Industry Notification

2 July 2014

PIN: 20140702-001

s Use Telephony Denial of Service (TDoS) Attacks to
nd Public Health Sector Employees

tinue to conduct Telephony Denial of Service (TDoS) attacks to
thcare and Public Health Sector employees. In one instance, the
ess Point (PSAP) communications of a hospital was disabled during
tors often used spoofed
/or assigned IP addresses
alls more difficult for law
due to the ease of TDoS
s carry out on vulnerable
g tactics to evade detection.
S will be the "go-to"
d on other organizations.
private, that rely heavily

UNCLASSIFIED

(U) Telephony Denial of Service (TDoS)

(U) Denial of service attack, which is aimed at crippling the organization's phone lines.

Source: www.securelogix.com

eting Employees in Healthcare and Public Health Sector

emergency communications of a San Francisco Bay Area hospital
attack. The attack method used was a computer to continuously
oom (ER) thereby crashing the hospital's telephone trunk. All ER
sy rendering the system dead. This TDoS attack although similar to
acks was significantly different in that PSAP communications were
tal was unable to receive any emergency telephone calls during the

Homeland Security

Science and Technology

A Multi-State TDoS Attack on 9-1-1

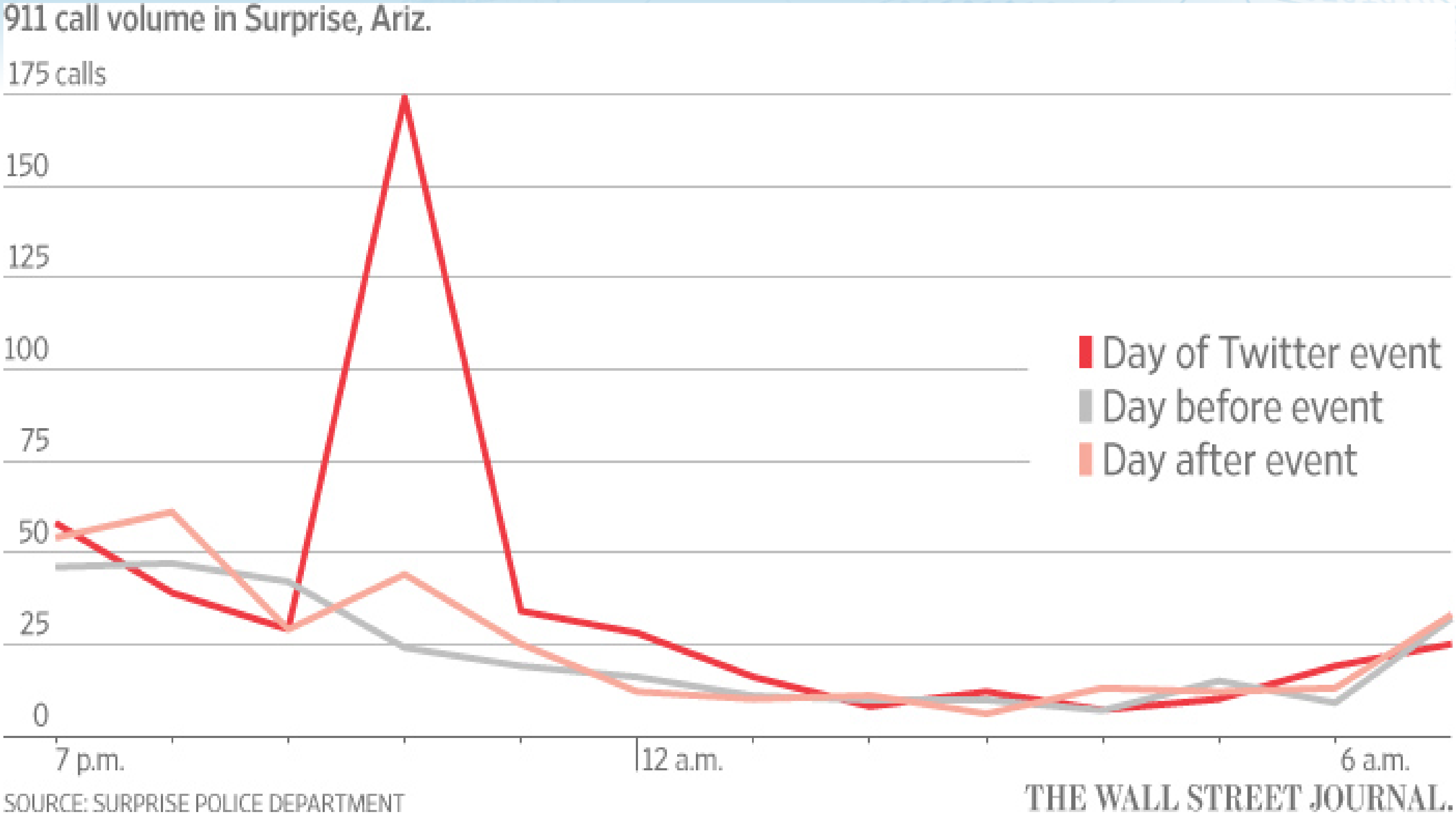
- **INCIDENT:** *TDoS attack against PSAPS in multiple states.*

- **CAUSES:** *The attack was distributed/propagated through a Twitter mobile application.*

- **AFFECTED STATES:** *PSAPs in many states including Arizona, Texas, California, Florida, Washington State, Minnesota.*

- **DURATION:** *Approximately 10:00 p.m. on* ***October 25, 2016*** *– 2:00 a.m.* ***on October 26, 2016*** *local incident time.*

Example Call Volume - Surprise, Ariz



Homeland Security

Science and Technology

Current State of the Art from FCC

- *In 38 states, no money was spent in 2015 on cyber security for 9-1-1 centers.*

- *Only 420 out of 6,500 9-1-1 centers had implemented a cyber security program.*

DHS S&T Funded Effort Mission

- **Understand DDoS/TDoS vulnerabilities and cyber threats to 9-1-1 systems.**
  - *Voice based services (E9-1-1, NG9-1-1)*
  - *Text to 9-1-1*

- **Developing DDoS/TDoS defense and cyber attack resilient solutions.**

- **Transition to practice by working closely with project partners and stakeholders.**

Homeland Security

Science and Technology

DHS S&T Funded R&D Solutions

- **Integrated TDoS Defense**
  - Affordable solution that integrates cost effective *SBC (NENA Compliant), VoIP firewall, TDoS defense, and call prioritization.*
- **Easy to configure and manage.**
- **Filling capability gaps.**
  - Prioritization in face of TDoS.
- **Plausible integration with ESInet architecture.**

Pilot Partners

- Formal Partners:
  - NG-911 center (PSAP -> AT&T ESInet)
  - NG-911 center (customer managed ESInet)
  - Top 10 bank
- Possible Informal Partners:
  - Top 5 bank
  - Top 5 wealth management company

Project Strategies

- **Engaging and involving stakeholders to take into account needs from the operational side.**
  - *public, private, and non-profit.*

- **Developing clear value proposition for the customers.**
  - *Improving both security and QoS for PSAP operations.*

- **Identifying and mitigating project risks from early stage.**

DDoSD Project Accomplishments

- Built a 9-1-1 security lab and secured 9-1-1 data acquisition.
- Developed tool support for NG9-1-1 traffic generation.
- Demonstrated Audio forensics and 9-1-1 text analysis.
- Call content analysis and integration with standard speech analysis service (MRCP).
- Modeling of 9-1-1 traffic and simulation tool for assessing impact of attack.
- Design of unified DDoS/TDoS defense solution (call network) for 9-1-1 call centers.
- Design and implementation of call prioritization mechanism.
- ***Secure Logix solution being deployed in pilot locations now.***

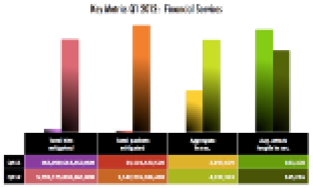
U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security

Science and Technology

Distributed Denial Of Service

Distributed Denial of Service attacks render key systems and resources unavailable, effectively denying users access to the service



USA Today: *Why DDoS attacks continue to bedevil financial firms*
… adversaries may potentially be nation states …

SPAMHAUS

NY Times: *Attacks used the internet against itself to clog traffic*
Attack traffic exceeds 400 Gbps!

eWeek: *DHS, FBI Warn of Denial-of-Service Attacks on Emergency Telephone Systems*

Current Advantage Favors Attackers:

- *Attack resources are cheap compromised machines while defense requires provisioning*
- *Attackers easily cross boundaries while defense requires cross-organization collaboration*

Challenge: shift advantage in DDoS events toward defense

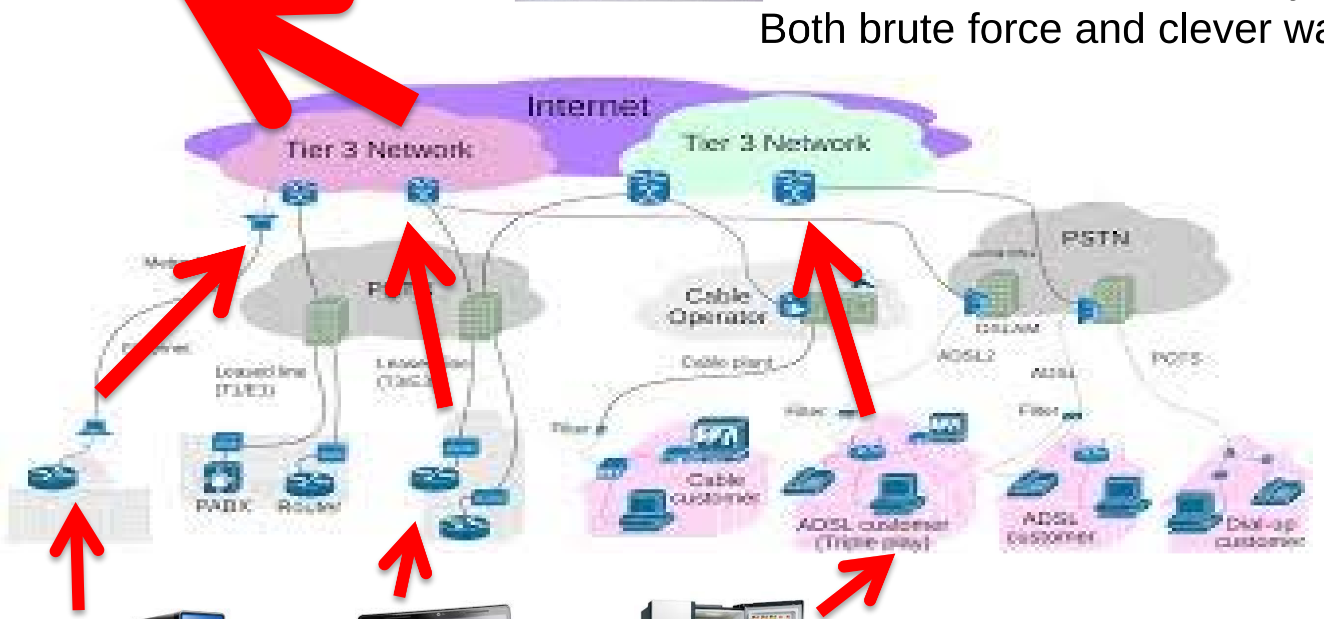
Homeland Security
Science and Technology

Problem: DDoS Attacks 101

Victim is overwhelmed.   Examples include:

- 400 Gbps traffic to 10 Gbps access link
- Millions of requests to server designed for thousands
- Thousands 911 calls to system designed for hundreds

Both brute force and clever ways to overwhelm the target

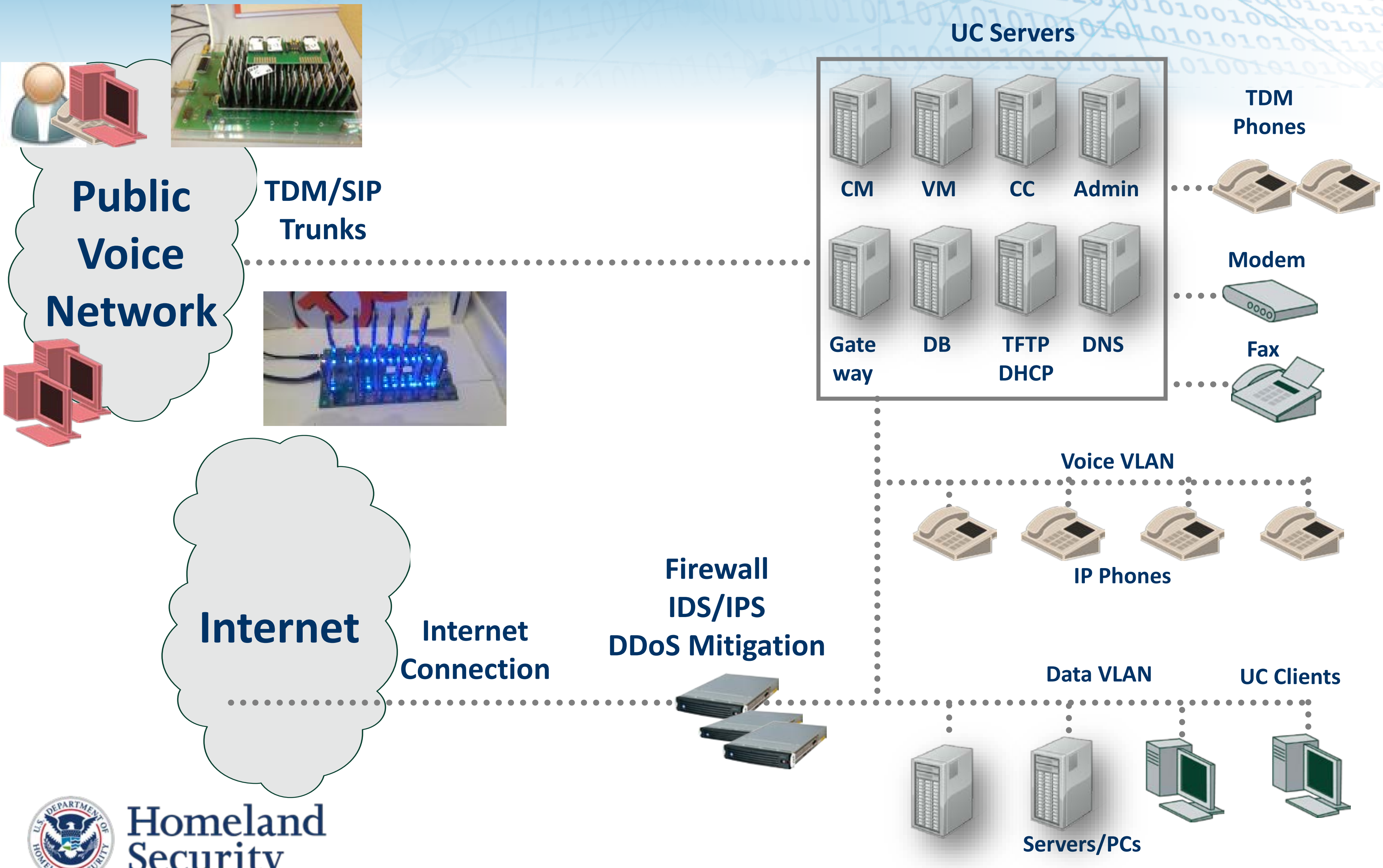


Attack traffic originated from multiple locations throughout the Internet

Control Over Vast Number of Compromised Devices: Desktops, laptops, and even refrigerators!
http://thehackernews.com/2014/01/100000-refrigerators-and-other-home.html

Command and Control:
Nation State, Criminal Organization, Hactivist groups, etc.

TDoS Threat – Disable 911

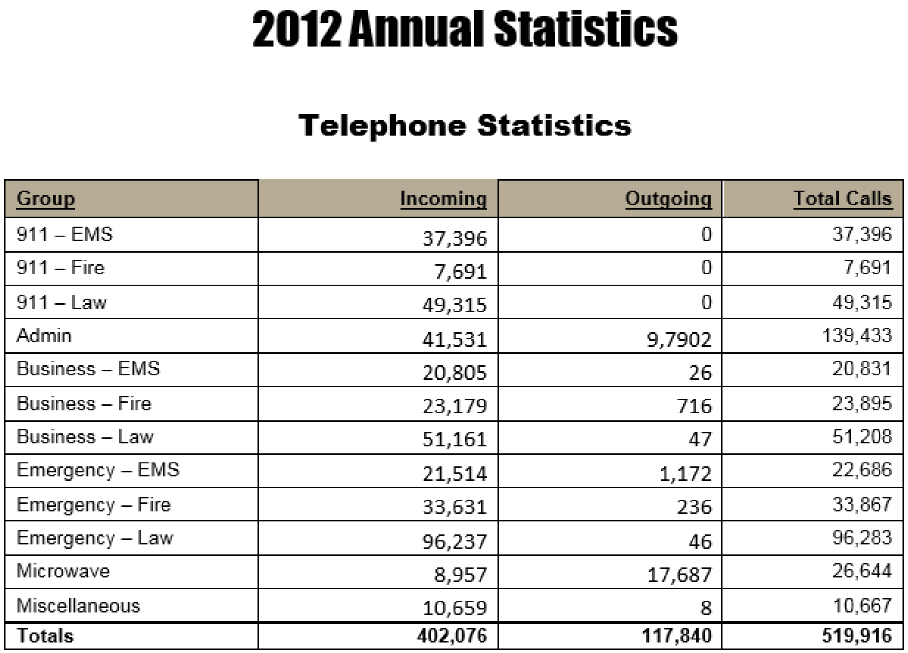


Homeland Security

Science and Technology

911 Statistics

- There are **240 Million** calls to 9-1-1 each year, in some communities, 50% of those calls are made from a mobile device – NENA

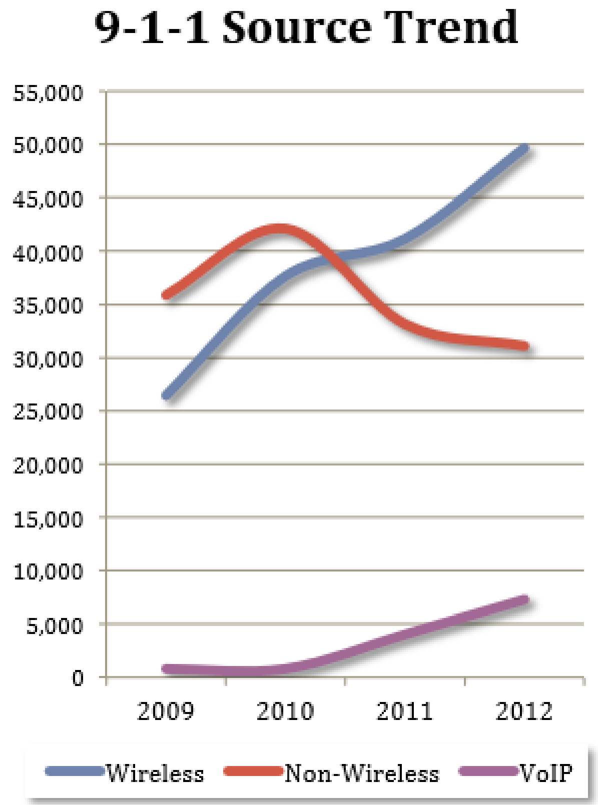


2012 Annual Statistics

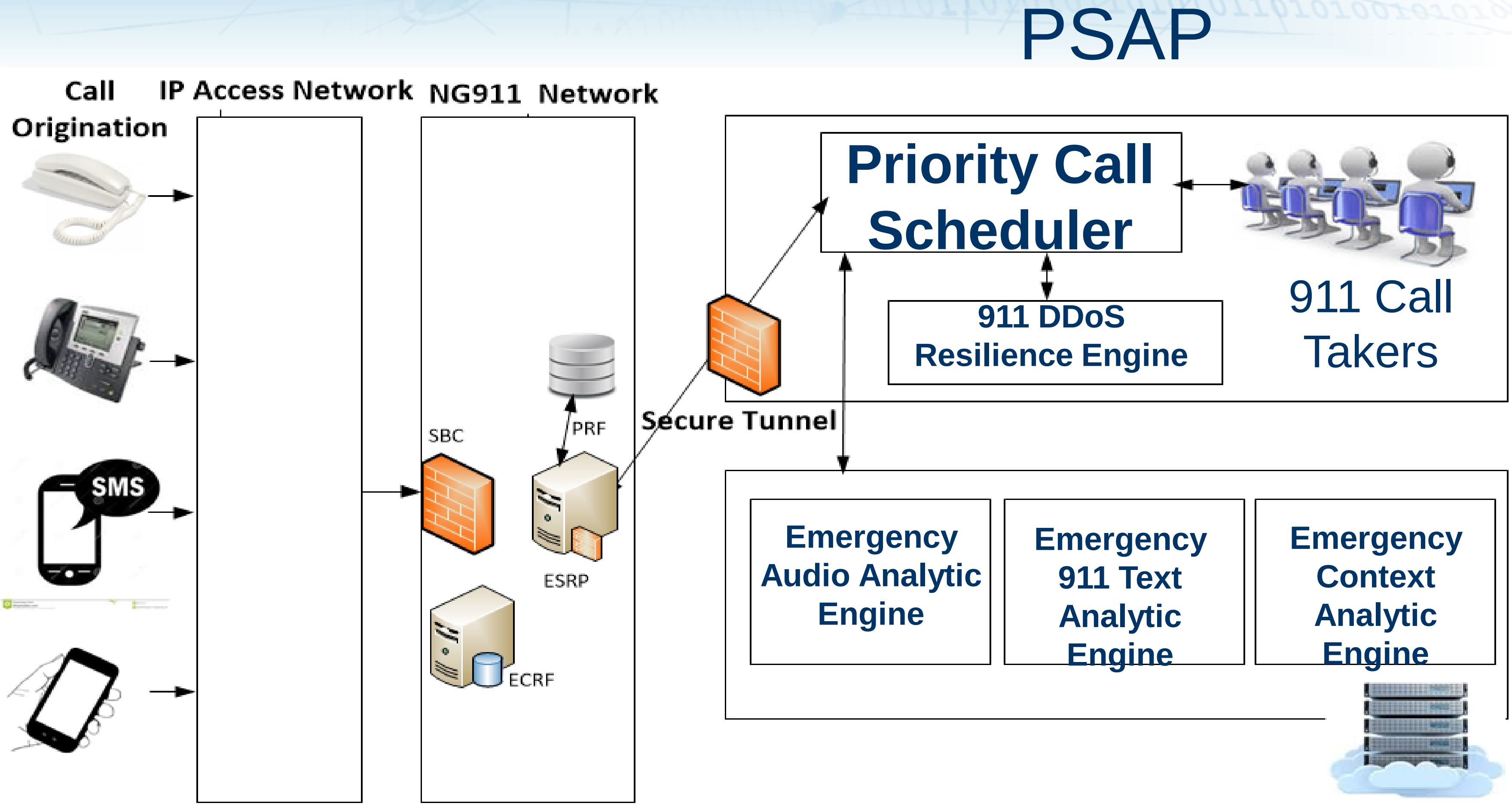
Telephone Statistics

Group	Incoming	Outgoing	Total Calls
911 – EMS	37,396	0	37,396
911 – Fire	7,691	0	7,691
911 – Law	49,315	0	49,315
Admin	41,531	9,7902	139,433
Business – EMS	20,805	26	20,831
Business – Fire	23,179	716	23,895
Business – Law	51,161	47	51,208
Emergency – EMS	21,514	1,172	22,686
Emergency – Fire	33,631	236	33,867
Emergency – Law	96,237	46	96,283
Microwave	8,957	17,687	26,644
Miscellaneous	10,659	8	10,667
Totals	**402,076**	**117,840**	**519,916**

Source: Overview of the San Mateo County Office of Public Safety Communications. 2012.



Defending 911 Systems

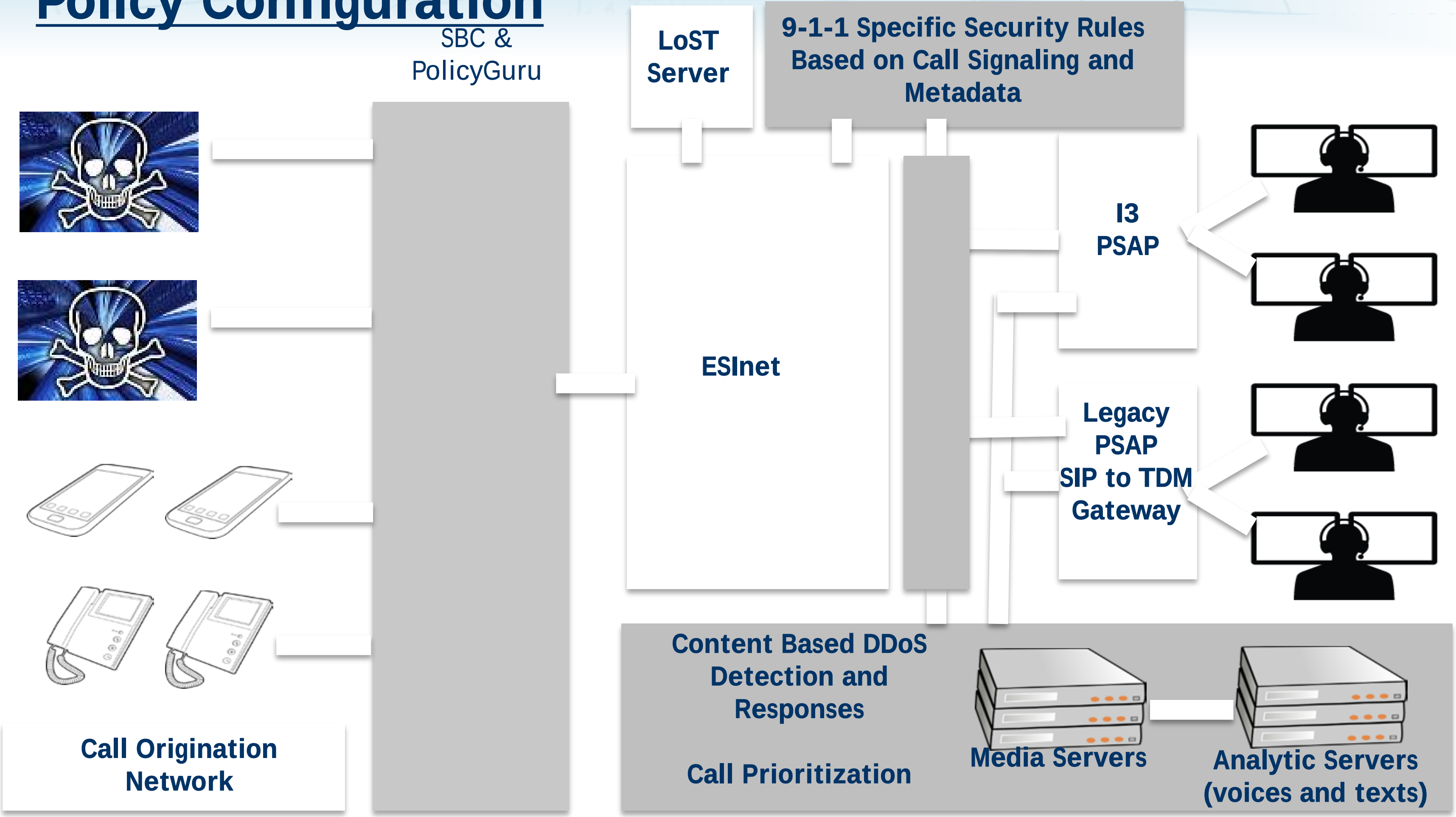

PSAP
Call Origination
IP Access Network
NG911 Network
SMS
SBC
PRF
ESRP
ECRF
Secure Tunnel
Priority Call Scheduler
911 DDoS Resilience Engine
911 Call Takers
Emergency Audio Analytic Engine
Emergency 911 Text Analytic Engine
Emergency Context Analytic Engine

Homeland Security

Science and Technology

9-1-1 DDoS/TDoS Defense

SBC + VoIP Firewall + TDoS Defense + Call Prioritization + Policy Configuration



SBC & PolicyGuru

LoST Server

9-1-1 Specific Security Rules Based on Call Signaling and Metadata

ESInet

I3 PSAP

Legacy PSAP SIP to TDM Gateway

Call Origination Network

Content Based DDoS Detection and Responses

Call Prioritization

Media Servers

Analytic Servers (voices and texts)

Next Generation 9-1-1

An evolved, fully-functional, Next Generation 9-1-1 system that is accessible **anytime, anywhere, from any device.**

Newer Technologies / Services

- □ *Text – IM, SMS, Smartphones, other non-voice devices*
- □ *Wireless – WiFi, cellular/WiFi*
- □ *Sensors – environmental, alarms, biometric*
- □ *Video, still and motion*

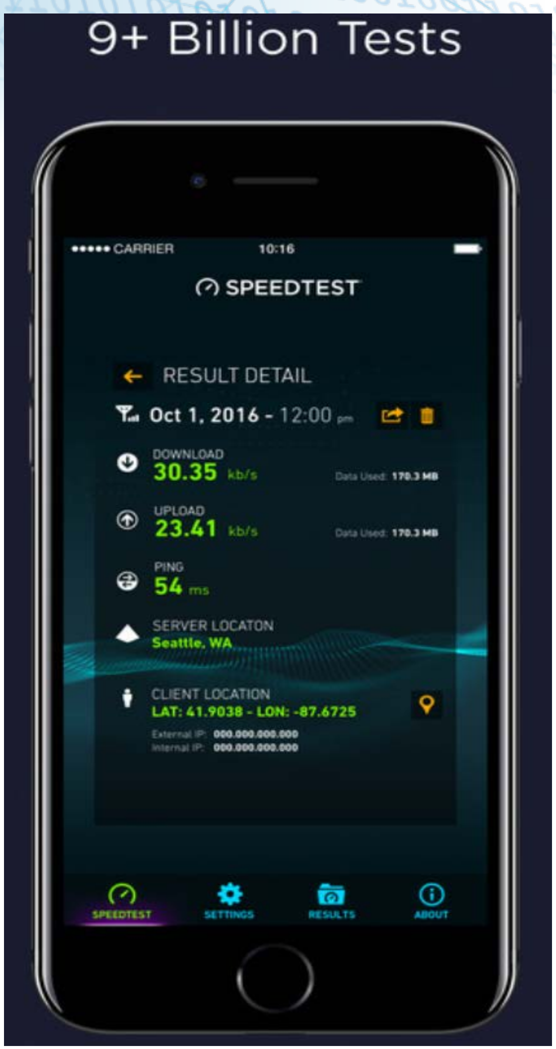
Recent TDoS Attack

- Recent distributed TDoS attack
- Affected multiple PSAPs in the southwest
- The malware was quite simple – known bug
- The malware was delivered via simple Javascript
- The malware was distributed via Twitter
- Could have been much worse

The Investigation

- Investigator confirmed identity of the teenage from screenshot of Internet speed test posted on social media website.
- The test records longitude and latitude information.

The picture on the right side is not the original one.



9+ Billion Tests

●●●●● CARRIER 10:16

SPEEDTEST

← RESULT DETAIL

Oct 1, 2016 - 12:00 pm

DOWNLOAD
30.35 kb/s
Data Used: 170.3 MB

UPLOAD
23.41 kb/s
Data Used: 170.3 MB

PING
54 ms

SERVER LOCATON
Seattle, WA

CLIENT LOCATION
LAT: 41.9038 - LON: -87.6725
External IP: 000.000.000.000
Internal IP: 000.000.000.000

The Oct 2016 Malware

- The TDoS malware exploits an iOS WebView auto dialer bug.
  - After clicking, the malware blocks the phone’s UI.
  - It causes iOS to open a second application while the phone is dialing the given number.
  - User has no control to cancel the call.
- The bug was first discovered in 2008 by Collin Mulliner.
- It affects all iOS apps that embed WebView.
- The malware is written using Java script.

The Oct 2016 Attacker

- The code was first posted online by a teenage in *Phoenix, Arizona*.
- The original version was described in a Youtube video "Freak out your friends" without using 9-1-1 as the target phone number.
- The teenage made a 9-1-1 version, posted it online, and sent the link to the person who made the video.
- The link was added to the video's caption. The Youtube channel has 250K followers.
- Retweeted link including account with over 400K followers.

Lessons Learned

- TDoS caused by **mobile malware** poses a real threat.
- **Social media** can accelerate spread of the attack.
- The consequence could have be **much worse** if not from a teenage hacktivist.
- Similar attack could happen again in future.
- *DHS S&T Funded research anticipated this style of attacks*.

Research Challenges

- Easier, cheaper, and safer for attack generation
- Mobile phone-based attacks seen in the wild
- A core issue is calling number spoofing
- Service providers working long term solutions
- PSAPs are reluctant to not process calls
- Are ESInet providers or PSAPs responsible for defense

Research Focus

- Address attacks such as TDoS, SWATing, robocalls
- Focus on a CPE SIP solution – apply to NG-911
- Develop a solution built on PolicyGuru product
- Address core issue of calling number spoofing and authentication
- Address signatures such as mobile phone based attacks
- Work with multiple operational pilot partners
- Determine how to best provide results/scores/priority
- Integrate audio analysis technology from University of Houston

DHS S&T Funded Effort Mission

- **Understand DDoS/TDoS vulnerabilities and cyber threats to 9-1-1 systems.**
  - *Voice based services (E9-1-1, NG9-1-1)*
  - *Text to 9-1-1*

- **Developing DDoS/TDoS defense and cyber attack resilient solutions.**

- **Transition to practice by working closely with project partners and stakeholders.**