# Application of Network Measurement Science (ANMS) and Distributed Denial of Service Defense (DDoSD) Applications to SIP

Dr. Ann Cox

Program Manager

Department of Homeland Security

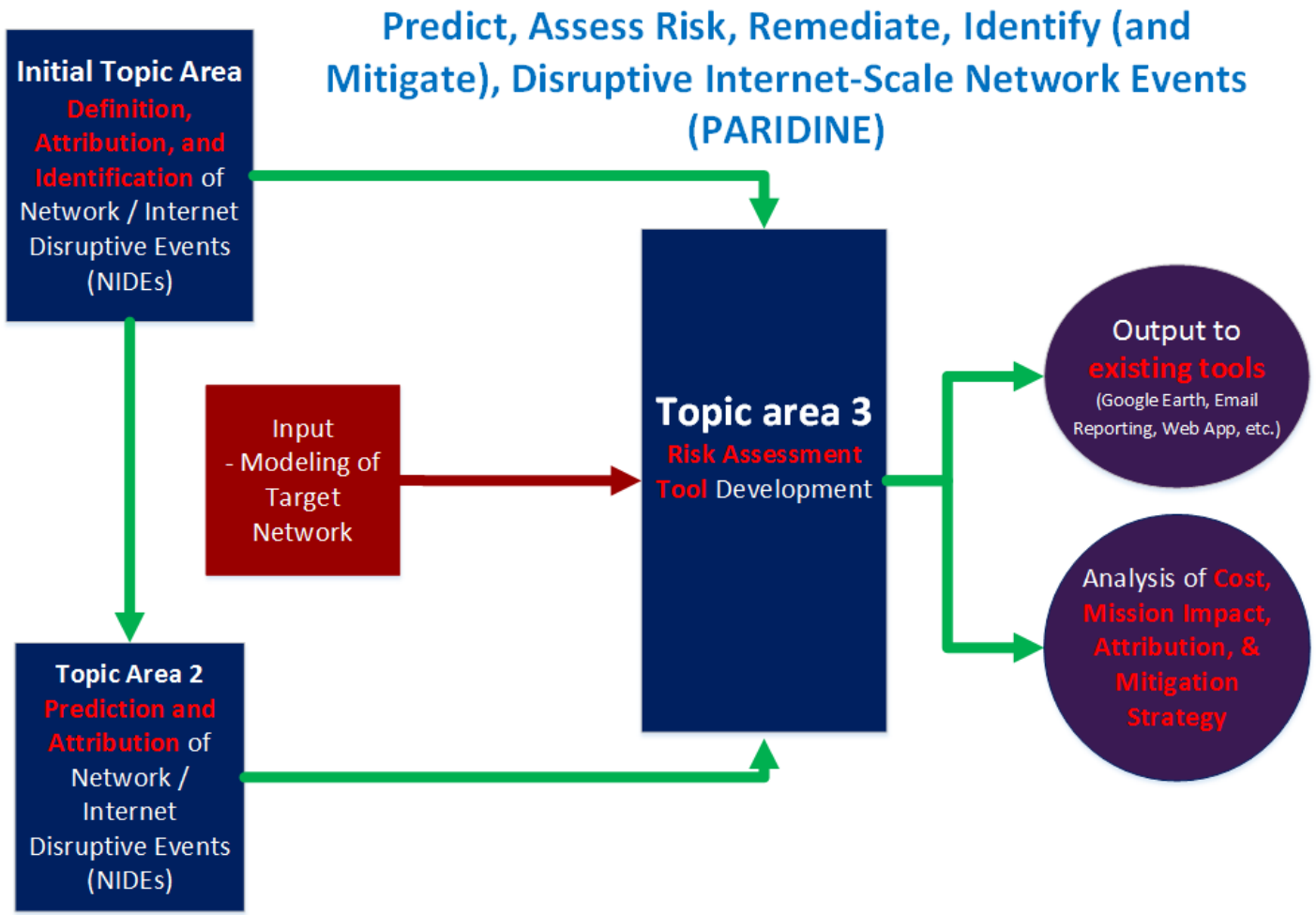
Science and Technology Directorate

December 5, 2018

Homeland Security

Science and Technology

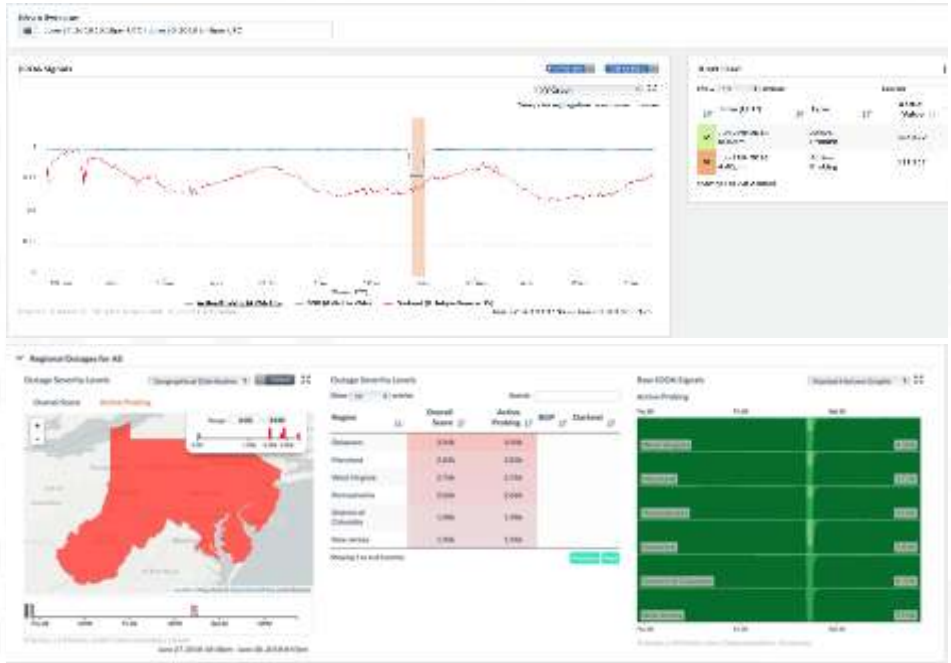
# PARIDINE


Predict, Assess Risk, Remediate, Identify (and Mitigate), Disruptive Internet-Scale Network Events (PARIDINE)
Initial Topic Area
Definition, Attribution, and Identification of Network / Internet Disruptive Events (NIDEs)
Input
- Modeling of Target Network
Topic area 3
Risk Assessment Tool Development
Output to existing tools
(Google Earth, Email Reporting, Web App, etc.)
Analysis of Cost, Mission Impact, Attribution, & Mitigation Strategy
Topic Area 2
Prediction and Attribution of Network / Internet Disruptive Events (NIDEs)

# Ioda-NP: Multi-source Realtime Detection of Macroscopic Internet Connectivity Disruption

CAIDA, University of California, San Diego

- Capable of detecting large-scale events of connectivity disruption in near-realtime. The Next Phase IODA-NP system will further advance the state of the art in 24/7 global Internet monitoring, extending methodologies, reporting events and cross-validating inferences, developing and documenting API.
- IODA-NP can operate both as a standalone product providing software-as-a-service, as well as – thanks to its HTTP-based API – lend its methods and software modules for integration into broader platforms useful for risk assessment, root cause analysis, or event prediction. In addition, it generates a live stream of event alerts in a standard easily-parsable format.



# Detecting, Interpreting, and Validating from Outside, In, and Control, disruptive Events (DIVOICE)

University of Southern California, Information Sciences Institute

Definitions, detection methods, and systems that provide:

- Network outages: measured with Trinocular (outside-in) and Disco (inside-out)
- Routing anomalies: hijacks and detours with BGPMon

Application-level disruptions: with new methods attribution and validation of these methods

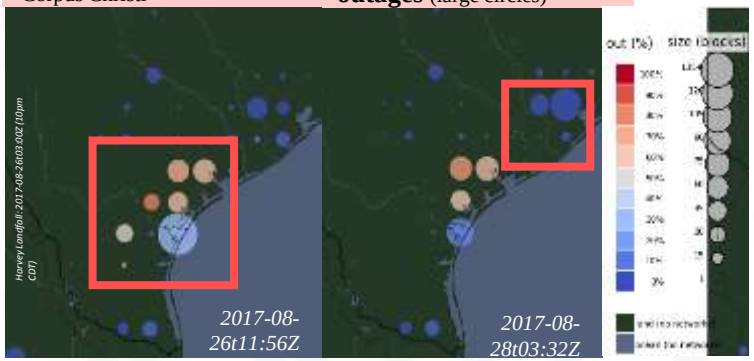
- against each other
- with the FCC

Technology transfer to:

- gov't agencies like FCC and NCCIC
- researchers
- the lay public

**Harvey Landfall: serious outages** (red circles), N. of Corpus Christi

**after Houston rainfall:** flooding and **many outages** (large circles)

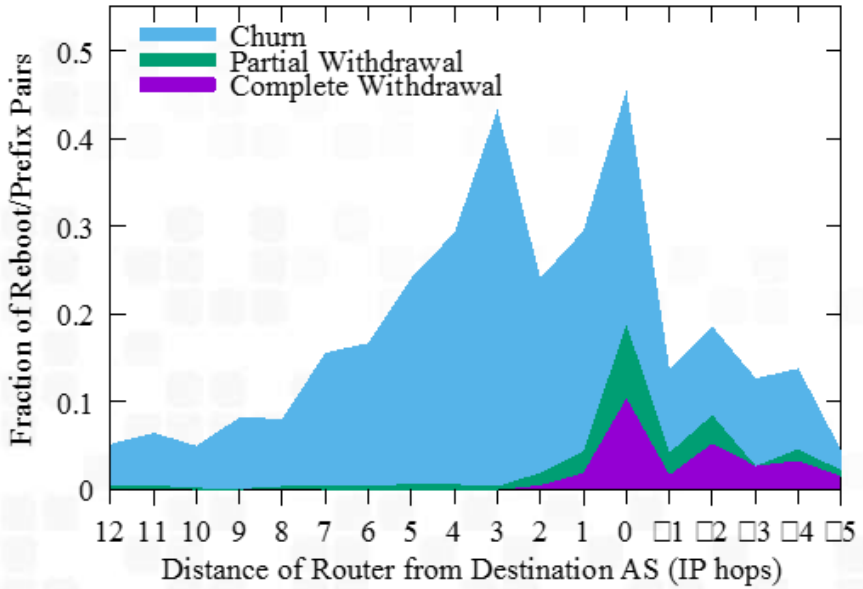


# Recording Router Reboots for Rating Router Reliability and Reachability

University of Waikato, New Zealand

Fine-grained active probing of routers to identify when a router has restarted, and then (1) examine the effect that reboot had on prefix reachability in the Border Gateway Protocol (BGP) routing system, and (2) examine the effect that reboot had on the reachability of systems the router was on the path towards.

- Open-source probing system built around the scamper active measurement software, extensively used in industry and academia.
- Near real-time detection of NIDEs impacting routing and reachability correlated with router outages.
- Outage events reported through a structured JavaScript Object Notation (JSON) interface, allowing integration with other outage monitoring systems
- Probing and correlation systems adapt to changes in network topology and routing.

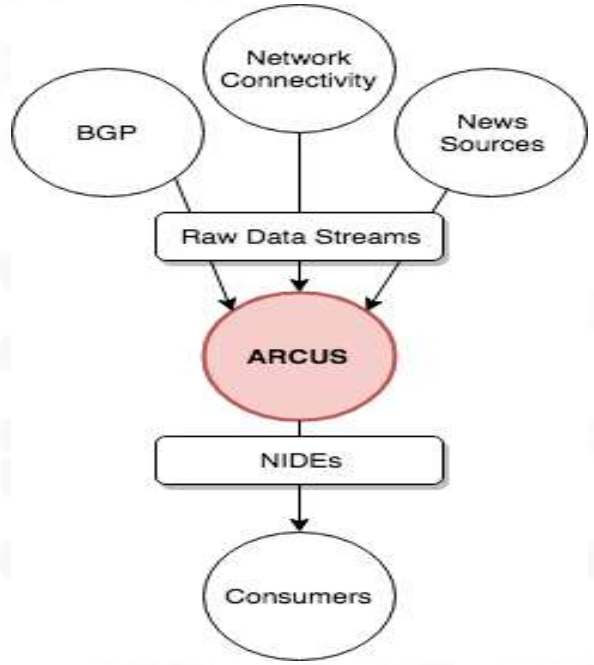


# Attribution and Recognition of Characteristics Underlying Scenarios (ARCUS) with NIDEs

## Two Six Labs

ARCUS provides near-real-time identification and causal attribution of NIDEs through a scalable, machine-learning-based system that fuses information from multiple Internet telemetry sensor arrays. Open-source probing system built around the scamper active measurement software, extensively used in industry and academia.

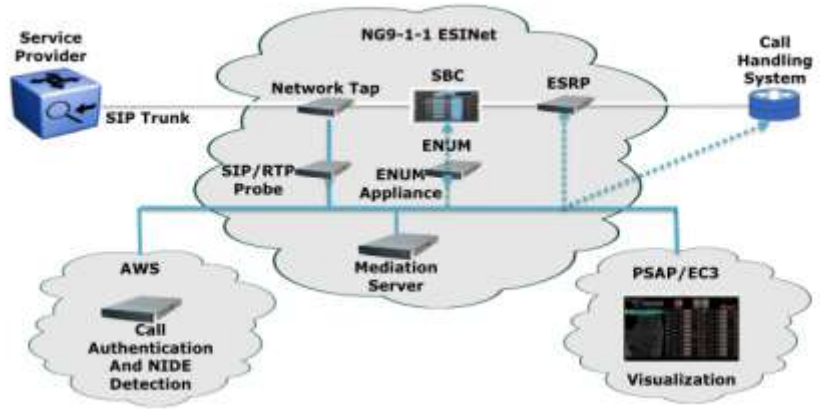
- Fully automates near-real-time NIDE detection as a cloud service – intel that has only been previously available at a delay
- Augments traditional disruption event reporting with probable attribution analysis, enabling smart, targeted response based on root cause
- Simple Application Programming Interface (API) with a JSON-based event format, allowing quick integration into downstream systems
- Python-based API helper library available for consumers



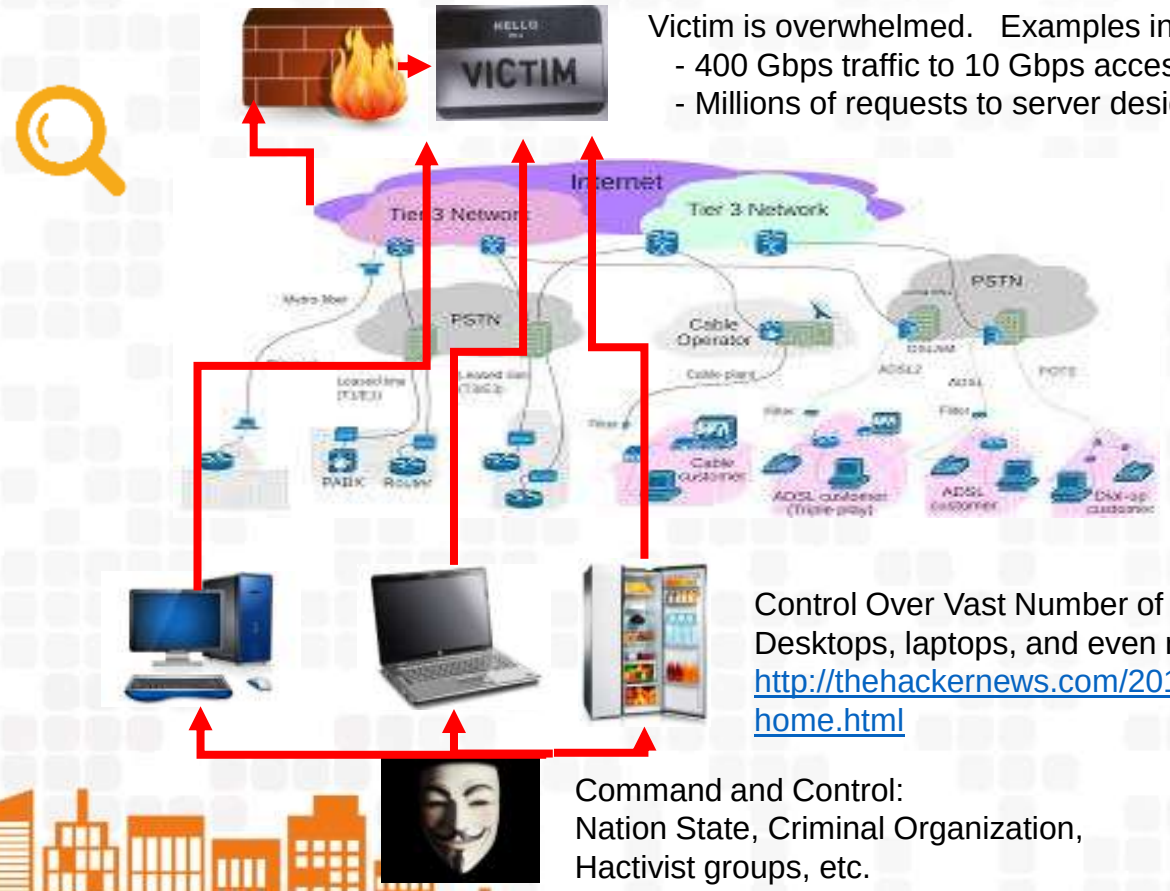
# Detecting Disruptive Call Events In 9-1-1 and Communication Networks

## Securelogix

- Gathering data from existing 9-1-1 environments to enhance machine learning models that are the basis of cloud-based Call Authentication Service (CAS).
- Models are used to detect various disruptive call events and also to differentiate them from legitimate events that generate call floods, such as physical attacks and major emergencies.
- Integrating the detection results into the West/ECaTS dashboard, which is commonly used across 9-1-1 centers across the country.
- Designing the solution to work with the Emergency Communications Cybersecurity Center (EC3) concept.



# 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

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.

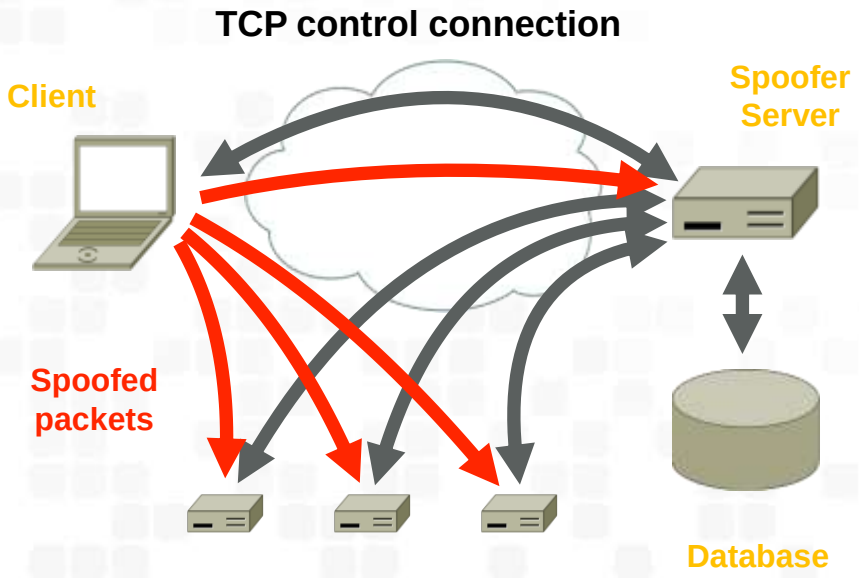
# Software Systems to Survey Spoofing Susceptibility /ASPIRE (SPOOFER I and II)

## University of California San Diego

- **SPOOFER Client/Server system provides useful features:**
  - by default publish **anonymized** results, and
    by default share **unanonymized** results for remediation
  - Runs in background, automatically testing new networks the host is attached to, once per week, IPv4 and IPv6
  - GUI to browse test results from your host, and schedule tests
  - Speed improvements through parallelized probing
- **Reporting Engine publicly shows outcomes of sharable tests**
  - Allows users to select outcomes
    - **per country: which networks in a country need attention?**
    - **per ASN: which subnets need attention?**
    - **per provider: which of my BGP customers can spoof?**
  - What address space does an AS announce, or could act as transit for? Is that address space stable?
    - Useful for deploying ACLs

**https://spoofer.caida.org/as_stats.php**

Spoofer: Client/Server Architecture

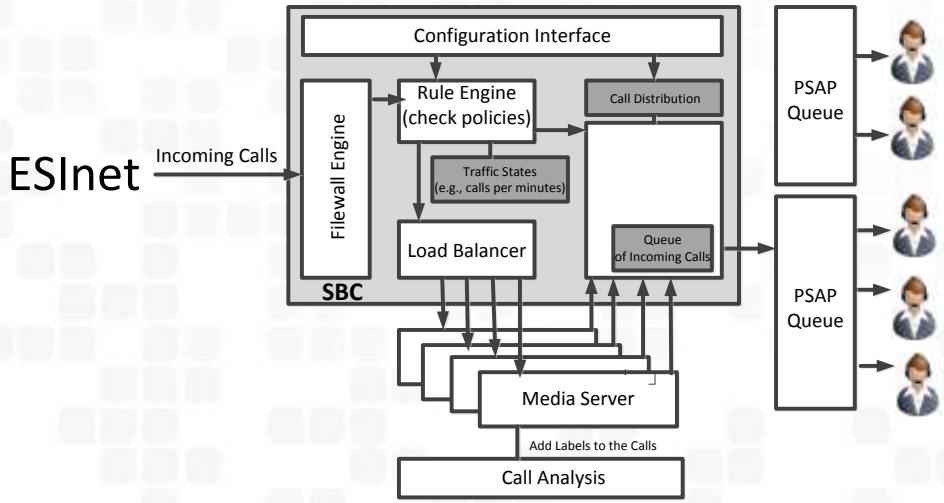


# Towards DDoS Resilient Emergency Dispatch Center

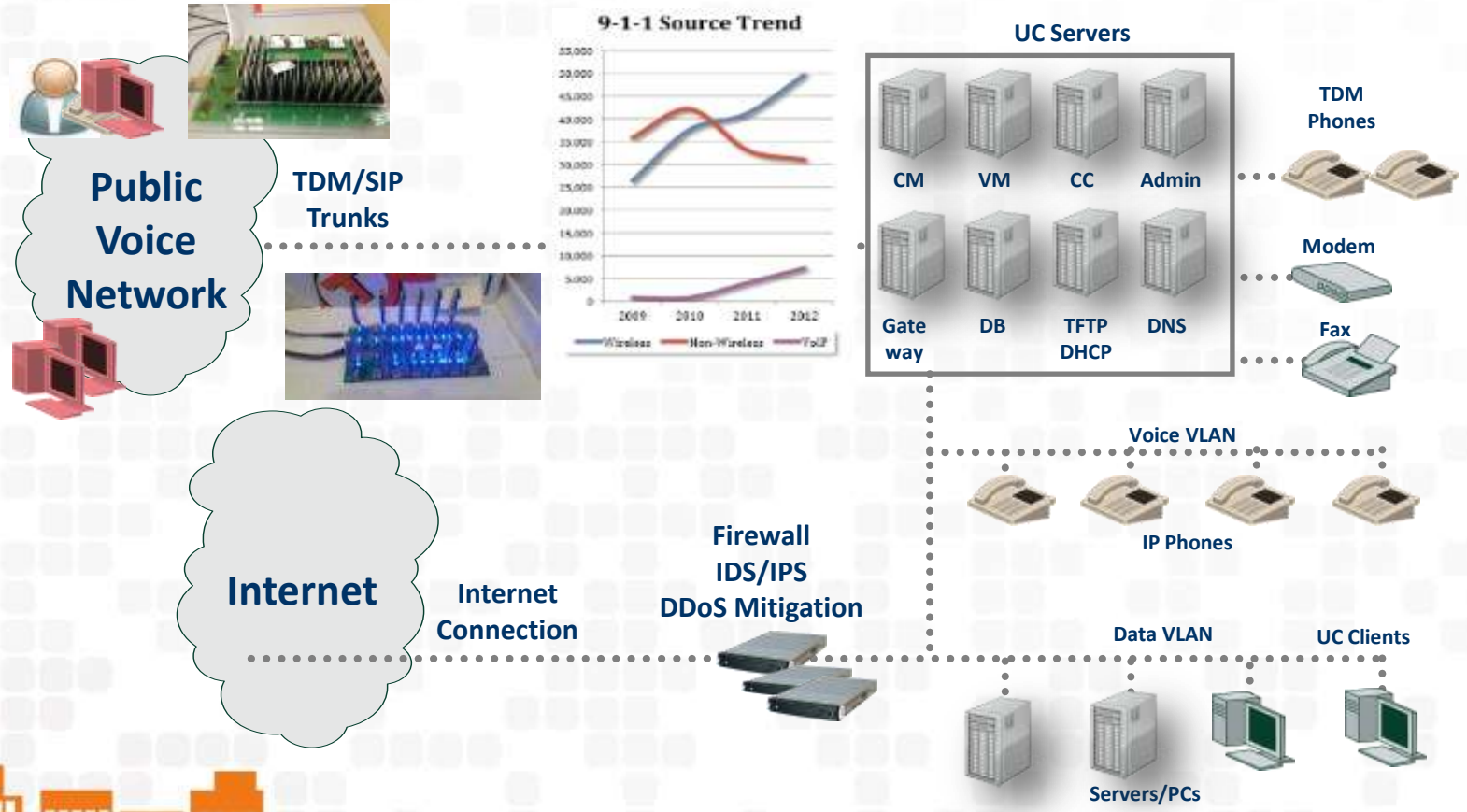
## University of Houston

Unified Security and Smart Call Distribution Gateway

- Integrated BCF capabilities.
- TDoS detection and response abilities.
- SIP (Session Initiation Protocol) VoIP firewall.
- Smart call distribution.
- ESInet to legacy conversion.
- Policy management.
- Remote control/configuration.



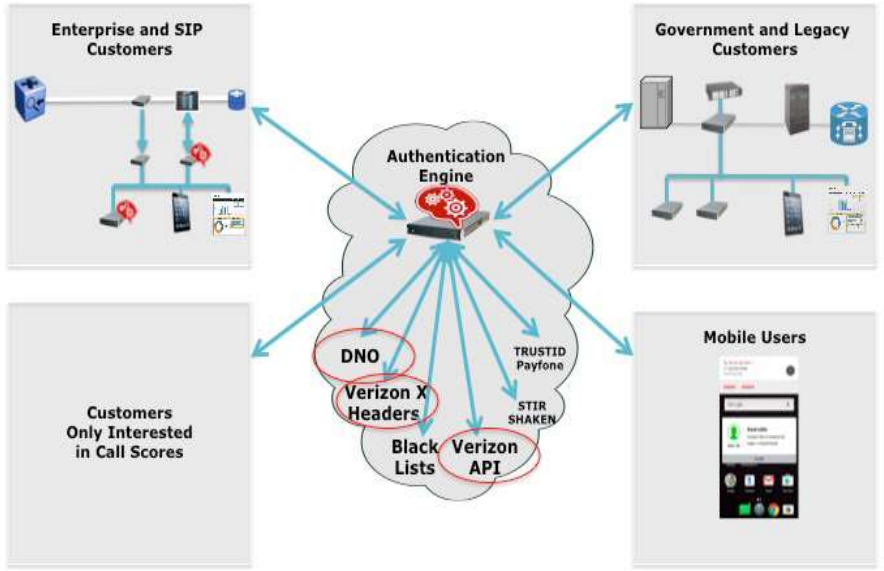
# TDoS Threat –Disable 911



# A Layered Service Provider/customer Approach to Call Spoofing/TDOS

## Securelogix

- Detect calling number spoofing, authenticate number.
- Authenticate device assigned to number, not caller
- Leverage collaboration with major carriers, providing an API for greater network visibility
- Two large metro area NG9-1-1 pilot partners: Palm Beach County FL, Greater Harris County TX,
- Government customers: Navy NG 9-1-1, DHS – US Secret Service, Customs and Border Protection, Alcohol Tobacco and Firearms (ATF)
- Financial Services/Insurance companies: In a Top 5 US Bank Contact Center, Processes 11 million inbound SIP calls per week, Implements policy on 7.5 million calls per week.

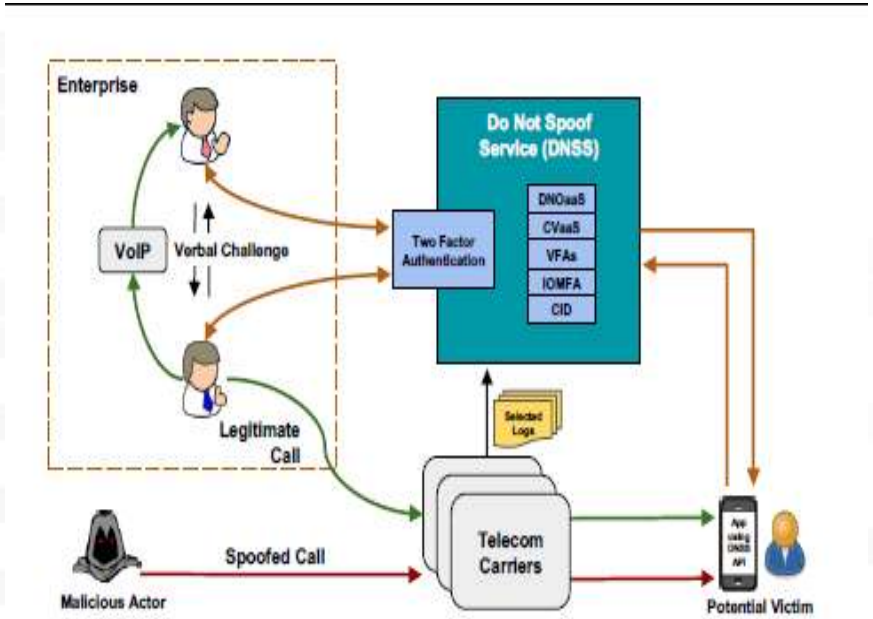


# Verification of Caller Ascertained Logically (VOCAL)

## AnaVation LLC

The Do Not Spoof Service (DNSS), a modular, componentized solution for spoofed call detection and blocking and/or notification via multi-layered call and user authentication and validation. Detects spoofed calls and either blocks them or notifies the victim and other relevant parties

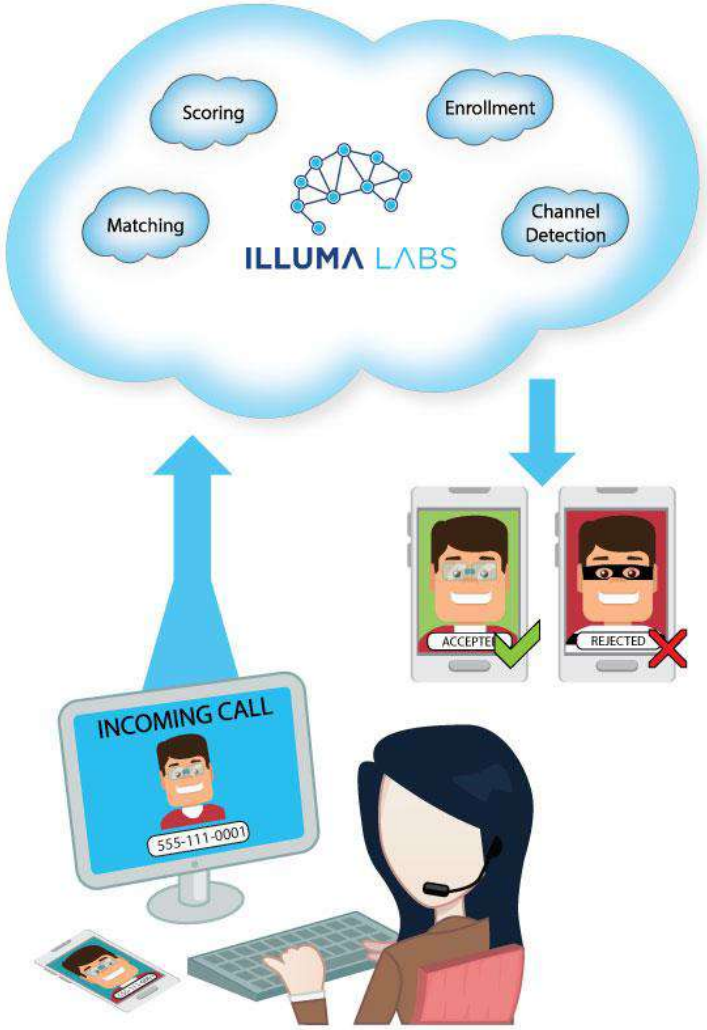
- Takes a "plug-and-play" and API-first approach for successful commercialization
- Call Center and Operations Center integrations and further related security offerings
- Advancements in two factor authentications
- Data collection and analysis



# Real-time Authentication to counter Caller ID Spoofing

## Illuma Labs

- Real-time ‘Authentication as a Service’ to secure telephone communications
- Lightweight client supporting resource constrained platforms (e.g. smartphones)
- First caller authentication solution available outside call centers (e.g. mobile, laptops)
- Minimize privacy concerns compared to cloud-based competitors with a privacy preserving client
- Robust to caller ID spoofing compared to competing metadata based solutions
- Acceptable real-time authentication accuracy in diverse communication channel
- Privacy preserving client-cloud comms



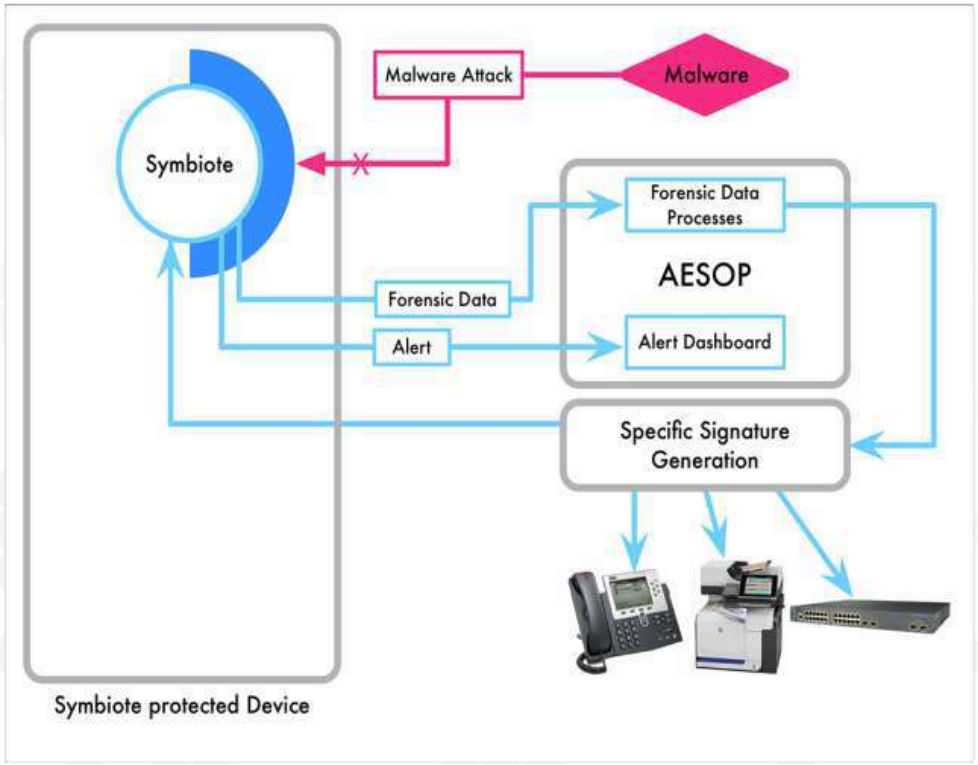
# IMAM: Advanced Analytics and Software Assurance

- S&T's Internet Measurement and Attack Modeling (IMAM) project was focused on the development and application of modeling and analysis capabilities to predict the effects of cyber-attacks on federal government installations and other critical infrastructure, as well as the measurement of internet infrastructure to better understand how the internet is used and what DHS can do to protect the internet from malicious actors.
- The project accomplished this through three main research areas:
  - Network Mapping and Measurement
  - Modeling of Cyber Attacks, including the Internet
  - Resilient Systems and Networks

# Automated Embedded Vulnerability Identification and Exploitation Mitigation System

## Red Balloon Security

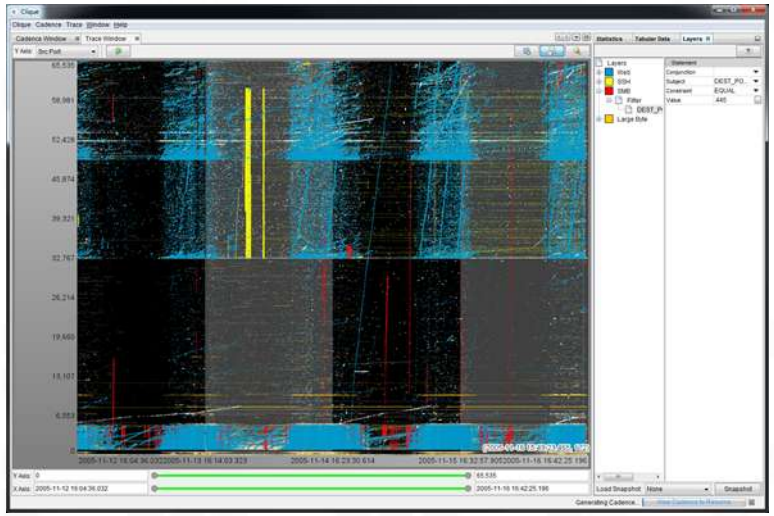
- The Software Symbiote
  - host-based defensive technology
  - intrusion detection within binary firmware
  - senses the unauthorized modification of the device firmware.
- Symbiote payloads capable of
  - dynamic attestation,
  - live attack forensic data collection and analysis
  - live hardening of vulnerable devices based on forensic data collected by other similar deployed devices.
- Licensed by and deployed in Millions of Hewlett Packard Printers and office products
- Successfully piloted at a DHS facility in building controllers



# Clique

## Pacific Northwest National Lab

- The Correlation Layers for Information Query and Exploration (CLIQUE) tool displays high-level overviews of network traffic using a new behavioral model-based anomaly detection technique.
- CLIQUE models help analysts to see departures from normal behavior at any time scale.
- PNNL developed Traffic Circle, now named TRACE, a scalable visual analytic tool.



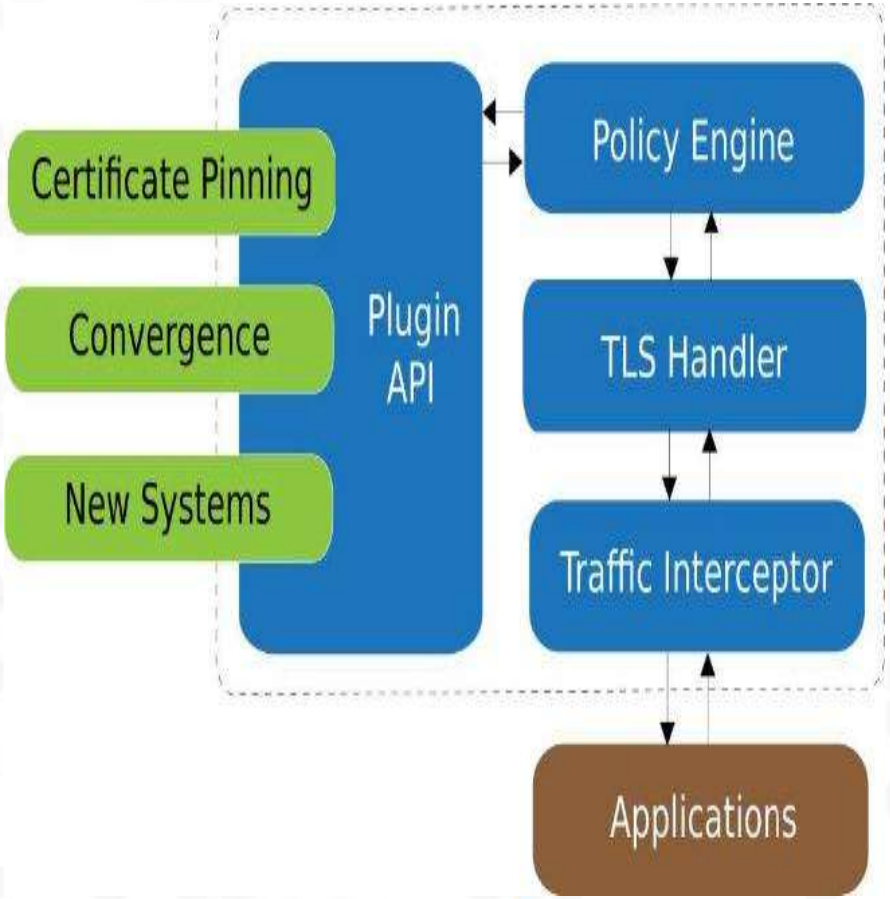
# Trustbase

## Brigham Young University

Secures existing applications

- Intercepts traffic between the application and the transport protocol and enforces correct certificate validation
- Strengthens the CA system
- Sysadmins can deploy authentication services that provide additional certificate validation checks
- Provides a platform for research, development, and deployment of alternative authentication systems

- https://internet.byu.edu/research/trustbase



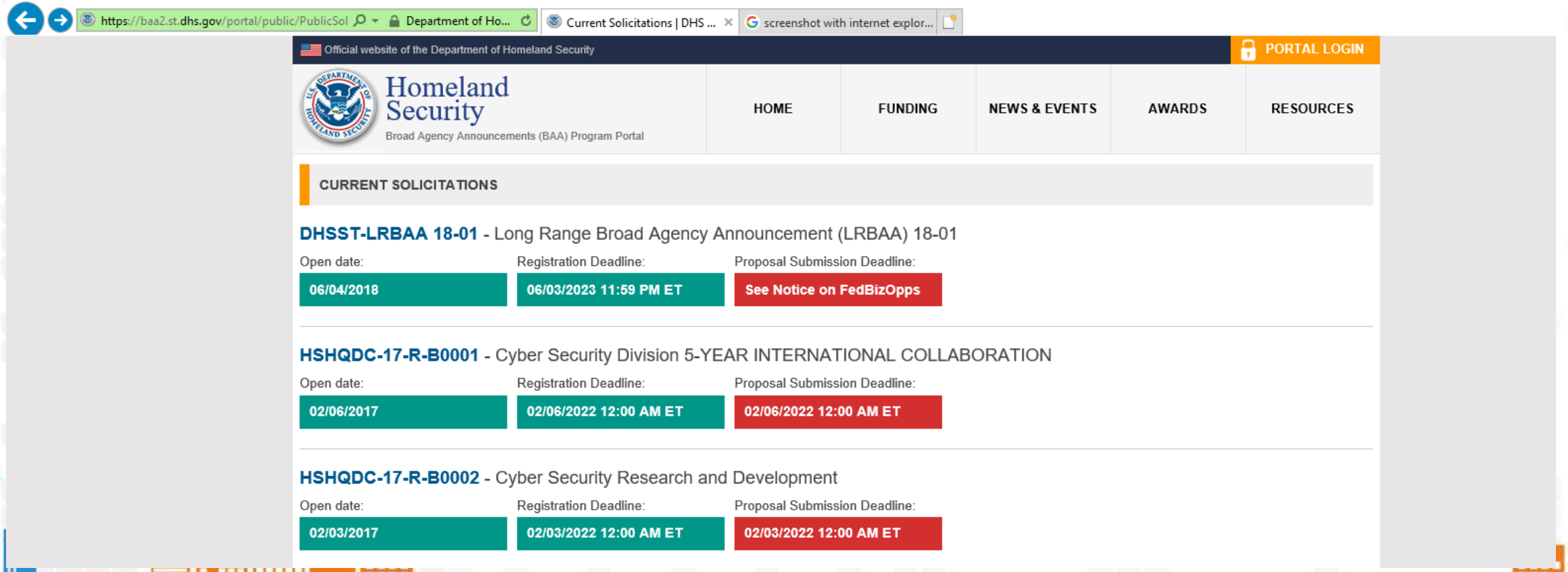
# Notification of Business Enterprise Compromise (BEC) indicators

## Dissect Cyber

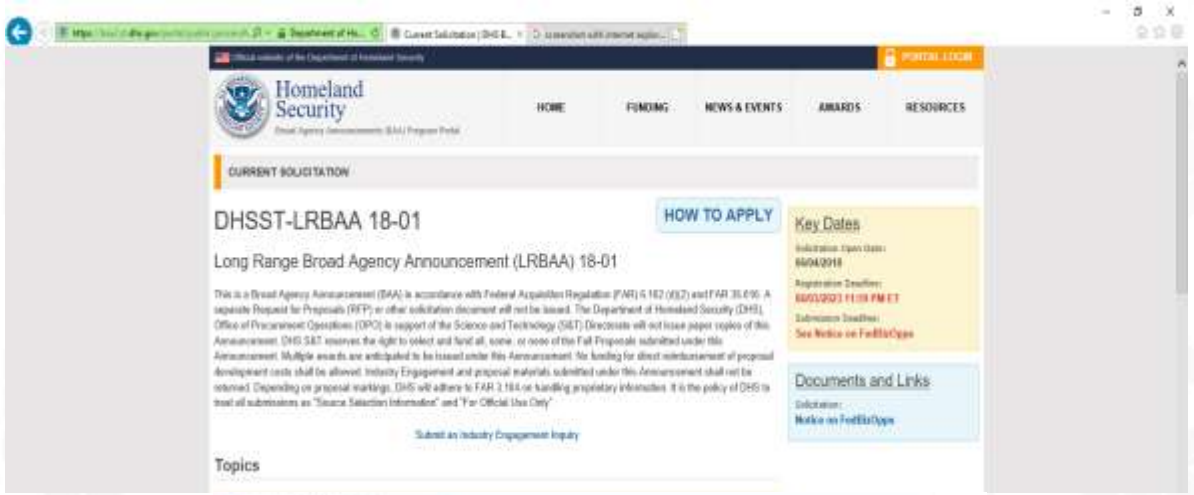
- BEC indicators and Ransomware hosting notification
- S&T funded, no charge for notification
- 11,800+ notifications, $100 million + USD in loss prevention:
  - Defense Industrial Base
  - Healthcare
  - Banking
- Recent high profile notification successes
- Data Sharing with commercial product from Centripetal
- Data Sharing with US, UK, DE, CA, Finland, the Netherlands

# S&T Current Solicitations

https://baa2.st.dhs.gov/portal/public/PublicSolicitation  retrieveCurrentSolicitation



# Long Range Broad Agency Announcement (LRBAA) 18-01



# Contact Info

**Dr. Ann Cox**
DHS Science & Technology Directorate
Ann.Cox@hq.dhs.gov
dhs.gov/cyber-research

# 2019 S&T Cybersecurity and Innovation Showcase

Homeland Security
Science and Technology

January 8 – 10, 2019 | Washington, D.C.

http://bit.ly/SciTechShowcase19


Solutions Now | Innovations for the Future