

5G

SECURE & RESILIENT MOBILE NETWORK INFRASTRUCTURE & EMERGENCY COMMS PROGRAM R&D GUIDEBOOK



**Homeland
Security**

Science and Technology



CISA
CYBER+INFRASTRUCTURE





INTRODUCTION

Thank you for your interest in the U.S. Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Secure and Resilient Mobile Network Infrastructure (SRMNI) and Emergency Communications Research and Development (R&D) Project, which is providing direct R&D support for critical Cybersecurity & Infrastructure Security Agency (CISA) priorities. This wide-ranging R&D project is managed by S&T's Office of Mission Capability and Support.

This project guide introduces you to the distinct goals and objectives for the complementary SRMNI and Emergency Communications projects and provides an overview of the ongoing R&D of new and cutting-edge solutions. These solutions will help secure legacy and next-generation mobile network infrastructure and help protect the critical communications systems used by the nation's first responders.

The SRMNI project is providing essential R&D that supports CISA's mission related to 5G, mobile security, and emergency communications security and resilience. Its objective is to provide accurate, timely and useful 5G, mobile security, and emergency communications R&D solutions to support CISA's mission. The SRMNI project also supports CISA's 5G Strategy, which is aligned to the White House's National Strategy to Secure 5G. Specifically, the project is researching legacy and current telecommunications protocols (i.e., 4G Long-Term Evolution and below) protections and enabling security into 5G networks. It also is leveraging 5G to demonstrate solutions that meet government security needs, including secure voice and video capability for unclassified government communications. Last, the SRMNI project also supports improvements to government visibility and security of network traffic from mobile devices focusing on capability testing for Protective Domain Name System integration.

Separately, but along similar lines, the Emergency Comms project is spearheading R&D to address three priority issues challenging the nation's first responder community. These projects are focused on enhancing cybersecurity protections for Emergency Communications Centers; creating more effective and trusted Federated Identity, Credential, and Access Management capabilities for public safety community use; and developing interoperability standards for computer-aided dispatch systems to facilitate more efficient sharing of data and information across jurisdictional and responder boundaries. Like the SRMNI projects, these emergency communications-focused efforts are supporting CISA's activities to further development of operable and interoperable emergency communications for first responders.

We are excited to share these promising mobile infrastructure and emergency communications technologies with you and welcome your feedback. For more information or to provide your feedback on these SRMNI and Emergency Communications R&D projects, contact us.

Sincerely,

Brent Talbot & Norman Speicher

Program Managers
Office of Mission Capability and Support-
Science & Technology Directorate
Department of Homeland Security
Email: brent.talbot@hq.dhs.gov &
norman.k.speicher@hq.dhs.gov

Serena Reynolds

Branch Chief, Initiative Management
National Risk Management Center
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security
Email: 5G@cias.dhs.gov



CONTENTS

1 SRMNI R&D PROJECT OVERVIEW

5 SRMNI R&D PROJECTS

- 6** Fifth Generation (5G) Network Security—CommDEX
- 7** Project GoSecure and EchoPTT Pro—4K Solutions
- 9** Threat Detection and Protection of Networks—Adaptive Mobile Security
- 11** Protecting the Mobile Core Network Elements—Aether Argus
- 12** Symbiote Integration for Mobile Network Infrastructure—Red Balloon Security
- 14** Mobile Network Traffic Visibility for the Enterprise—GuidePoint Security
- 16** Mobile Traffic Intelligence at Scale—AppCensus
- 17** Government Secure Voice Architecture—Texas A&M University
- 19** Deploying Defenses for Cellular Networks Using the AWARE Testbed
—University of Florida

21 EMERGENCY COMMS R&D PROJECT OVERVIEW

25 EMERGENCY COMMS R&D PROJECTS

- 26** Information Sharing, Safeguarding, and Federated ICAM
—Georgia Tech Applied Research Center
- 28** CAD-to-CAD Interoperability—IJIS Institute
- 30** Creating A Cyber-Resilient Public Safety Infrastructure—SecuLore



SRMNI R&D PROJECT OVERVIEW

5G

SECURE AND RESILIENT MOBILE NETWORK INFRASTRUCTURE RESEARCH AND DEVELOPMENT PROJECT STRATEGY

BACKGROUND

The Homeland Security Enterprise (HSE) increasingly relies on mobile technologies to meet its mission and business needs. The advent of the next generation of cellular technologies—fifth generation (5G)—promises to provide the unifying connectivity fabric that will connect virtually everything and expand mobile communications to encompass new services, applications, and deployments. However, one of the lessons learned from deployment of fourth generation (4G), and earlier, is that all cellular technologies have inherent security challenges; 5G is no exception.

New 5G technologies include techniques to solve 4G security weaknesses and also implement new measures to meet the security requirements required for the new 5G use-cases: enhanced mobile broadband (eMBB) and massive machine type communications (mMTC) to support internet of things (IoT) machine-to-machine communications and critical communications with ultra-reliability and low latency (URLLC)¹. 5G will be cloud-native, using software and virtualization on commodity servers instead of proprietary hardware to implement network functions. The combination of commodity hardware and virtualization on an all-internet protocol (IP) network and the vast expansion in the number of connected devices broadens the attack surface over previous cellular generations.



¹5G Usage Scenarios (Source: ITU Telecommunication Development Bureau. Setting the Scene for 5G: Opportunities & Challenges 2018. https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf).

PROJECT MISSION

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) initiated the Secure and Resilient Mobile Network Infrastructure (SRMNI) project to fund research and development (R&D) to address capability gaps in mobile ecosystem security and resiliency identified by Cybersecurity and Infrastructure Security Agency (CISA), with an emphasis on 5G security risk management. Therefore, the overarching mission of SRMNI project is to deliver accurate, timely, and useful research and solutions as well as knowledge products, to the CISA that will enable risk- and cost-informed decision-making (e.g., capability gaps, threat identification, architectural frameworks, and potential mitigations, operational and technical requirements, and investment prioritization) for 5G implementation.

The SRMNI project will support CISA as it engages stakeholders using an interagency collaborative approach (e.g., Federal Mobility Group [FMG]) to share information and coordinate and leverage other agencies' investments in 5G, mobile security and emergency communications pilots, technology exploration, and initiatives. The SRMNI project directly supports CISA's 5G Strategy & Implementation Plan, which is aligned to the National Strategy to Secure 5G as the nation's 5G risk advisor through:

- + Developing capabilities and approaches to mitigate vulnerabilities and improve resilience of communications network infrastructure—both 4G and 5G.
- + Researching and prototyping innovative methods to address supply chain risk in the 5G ecosystem so an ecosystem of trusted 5G vendors is fostered.
- + Prototyping technical capabilities and approaches and creating informational materials and best practice documents to enhance understanding of the current state of 5G security, capabilities, and standards so CISA can effectively promote security and resilience of 5G deployment to state, local, tribal and territorial (SLTT) government agencies.
- + Researching and developing innovation solutions addressing management of enterprise mobile network traffic to ensure secure communications.
- + Prototyping new capabilities to reduce risk to emergency communications systems (e.g., 911 and Next-Generation 911 systems [NG911], Public Safety Answering Points [PSAP]) and enhance mobile authentication of public-safety government officials and support secure voice and data communications related to delivery of NCFs and NEFs.

R&D projects within the SRMNI project will impact the mobile communications network industry (network operators, equipment vendors, and service providers), other agencies' 5G R&D initiatives, and cybersecurity initiatives related to public-safety communications. The project will use a multi-pronged approach to share information and avoid duplicative research activities with impacted projects and initiatives as follows:

- + Leverage the interagency FMG, a community of practice established by the Federal CIO Council, to coordinate and share information about 5G threats, vulnerabilities, and agency research initiatives.
- + Coordinate public-safety-related projects for CISA with the National Institute of Standards and Technology (NIST) Public Safety Communications Research (PSCR) Division and with the DHS S&T Office for Interoperability & Compatibility Technology Center.

R&D PERFORMERS

The following performers are working on SRMNI R&D projects in support of CISA:

- + Aether Argus Inc.—Protecting the Mobile Core Network Elements Via Air-Gapped Hardware Verification and Code Execution Tracking
- + Texas A&M University—Government Secure Voice Architecture
- + Commdex Consulting LLC—Fifth Generation (5G) Network Security
- + 4K Solutions LLC—Project GoSecure and EchoPTT Pro: Secure Voice and Alert Messaging for Mitigating Threats from SS7/Diameter and Over the Air Attacks
- + University of Florida—Deploying Defenses for Cellular Networks Using the AWARE Testbed
- + GuidePoint Security LLC—Mobile Network Traffic Visibility for the Enterprise
- + AppCensus, Inc. —Mobile Traffic Intelligence at Scale
- + Red Balloon Security, Inc.—Symbiote Integration for Mobile Network Infrastructure
- + AdaptiveMobile Security Inc.—Threat Detection and Protection of Networks

See the section titled “SRMNI R&D Project Summaries” for more information about each performer’s project.

One of these R&D projects will be completed in 2021, the majority will be completed by early to mid-2022, and two others extend into 2023. Each of these nine SRMNI projects will help inform future R&D efforts undertaken by S&T and CISA to ensure the security and resiliency of 5G technology and infrastructure for federal government missions and use-cases.



SRMNI R&D PROJECT SUMMARIES



Fifth Generation Network Security

Commdex, LLC

Chris Knight

cknight@commdex.com

OVERVIEW

The Fifth Generation (5G) Network Security project is part of the Secure and Resilient Mobile Network Infrastructure project. This project will produce a security and privacy architecture specification for 5G network traffic that demonstrates the efficacy of approaches in a contractor-operated laboratory environment.

CUSTOMER NEED

The overall objective of the Fifth Generation Network Security project is to evaluate and define the end-to-end protection of 5G network traffic, including development of standardized secure voice and video capabilities for unclassified communications. This project will produce a security and privacy architecture specification that aligns to commercial 5G architectures and adheres to 3rd Generation Partnership Project (3GPP) standards. This R&D initiative will propose and show how properly developed and implemented security controls, processes, and procedures will increase the security and resiliency of 5G infrastructure to reduce the risks to government services, devices, and data using Long-Term Evolution as the anchor for control, signaling, and 5G networks.

APPROACH

A design will be created that involves security and privacy overlays onto 5G reference architectures and will be based upon 3GPP 5G Standards, Release 15. Design and engineering will outline the research, development, testing, and piloting strategy for end-to-end security controls for a 5G device, Radio Access Network, core and transport network architecture, including Distributed Denial

of Service (DDoS) mitigations, end-to-end security for Sensitive But Unclassified/For Official Use Only government communications, and exploration of open hardware/software and systems to mitigate supply chain threats from cellular equipment high-risk vendors, public safety use-cases, and the application for coexistence with other 5G priority services.

BENEFITS

This end-to-end secure network architecture will clearly explain how to provide more secure and robust emergency communications to the more than 700,000 National Security/Emergency Preparedness (NS/EP) personnel subscriptions to the Wireless Priority Service and Government Emergency Telecommunications Service, administered by CISA and the more than 10 million public safety users leveraging services from providers operating and deploying 5G infrastructure.

COMPETITIVE ADVANTAGE

This solution specifically will address how to ensure priority services for emergency communications during congestion events on 5G infrastructure, while complementing—without conflict—deployed security controls. In addition, designs will outline how to provide the ability to identify a DDoS/Massive Internet of Things attack from congestion during a NS/EP event and will describe an approach to identify a Telephony Denial of Service attack.

NEXT STEPS

Upon completion of the solution design and engineering, lab staging with identified components will be completed, and lab testing/piloting will commence.

Project GoSecure and EchoPTT Pro: Secure Voice and Messaging Threat Mitigation from Backend Protocol and Over-the-Air-Attacks

4K Solutions, LLC

Jim Urbec

jim@4ksolutions.com

OVERVIEW

This project will develop and refine two major software solutions for secure voice communications. The first is GovSecure, which is a centrally managed secure voice capability for both iOS and Android platforms. The second is EchoPTT Pro, a serverless Push-To-Talk and voice conferencing Voice over Internet Protocol application. Both solutions are simple to manage, interoperable with existing Internet Protocol-based voice systems, and interoperable with 5G.

CUSTOMER NEED

The standard encryption algorithms protecting Global System for Mobile Communications (GSM) and Long-Term Evolution mobile telephone calls from eavesdropping have vulnerabilities. The technology to crack GSM's standard encryption

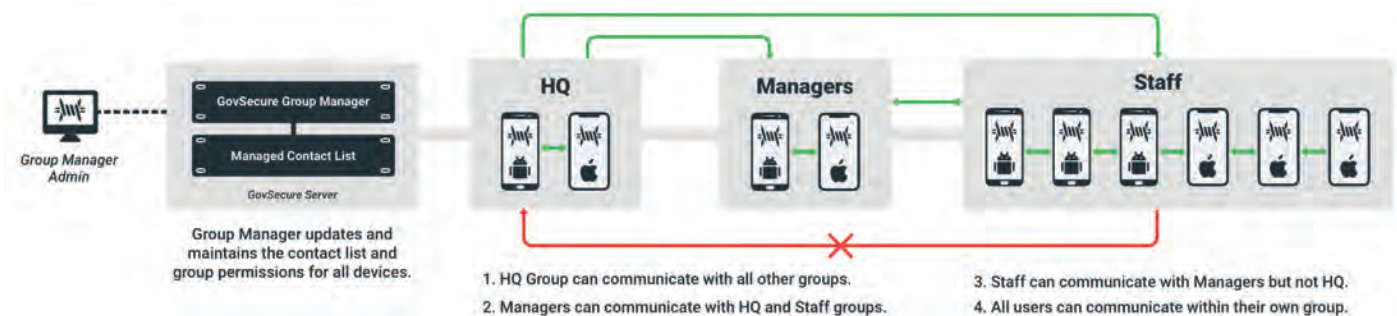
algorithm is readily accessible at moderate cost, even to amateurs. Recent demonstrations of practical, low-cost attacks on GSM's standard encryption algorithm have underlined just how vulnerable mobile phone calls are.

APPROACH

Both GovSecure and EchoPTT Pro will research and develop application improvements to help provide secure voice and conferencing capabilities. All GovSecure features will be mirrored on both platforms. Development of plans for future capabilities, such as voicemail, video collaboration and integration into larger cellular protection systems such as OverWatch and OverSight, are underway.

BENEFITS

Historically, secure communications require the use of specialized encryption hardware and software. This combination has an exceptionally long development/approval timeline, is not very mobile or lightweight, and is not adaptive to the ever-changing mobile phone environment. GovSecure and Echo PTT Pro are being developed to help deliver secure communications that provide users flexibility, so the solutions will work with a wide range of mobile devices and operating systems, agility, so the solutions can be remotely installed and secured on the fly, and confidence, knowing that the solutions' secure communications capability can be removed as fast as it can be added via a centrally managed server.



GovSecure Server and Group infrastructure with security group “higher-to-lower” versus “lower-to-higher” controls



COMPETITIVE ADVANTAGE

With the combined GovSecure/EchoPTT Pro solution, centrally managed, controlled and easy administration (e.g., new user additions and deletions) can be done on the fly without specialized hardware or recall of equipment. Also, there will be no need for controlled cryptologic item storage, safeguard or protection protocols normally associated with secure telecommunications equipment.

NEXT STEPS

The performer will further expand and test the solution across the DHS enterprise and user-base.

Threat Detection and Protection of Networks

AdaptiveMobile Security

Michele Samuel

Michele.Samuel@adaptivemobile.com

OVERVIEW

The objective of AdaptiveMobile’s project is to demonstrate the ability of mobile network signaling threat detection and intelligence technologies to identify security threats in current (3G and 4G) and future (5G) mobile signaling networks. Adaptive-Mobile uses a unique three-pronged approach to defend against cross/multi-protocol threats: a signaling firewall, security-focused advanced analytics algorithms, and a global threat intelligence service to ensure that network borders are continually secured against the most sophisticated attacks and attackers.

CUSTOMER NEED

There are many challenges in providing mobile network security on a nationwide, network, or device basis. With each generation of mobile technology, the complexity of detection increases, and the threat attack surface broadens. It is critical to be able to detect, analyze and respond to attacks on mobile network infrastructure. This research project provides a threat-detection approach to methods and techniques to increase the security posture of mobile networks and devices.

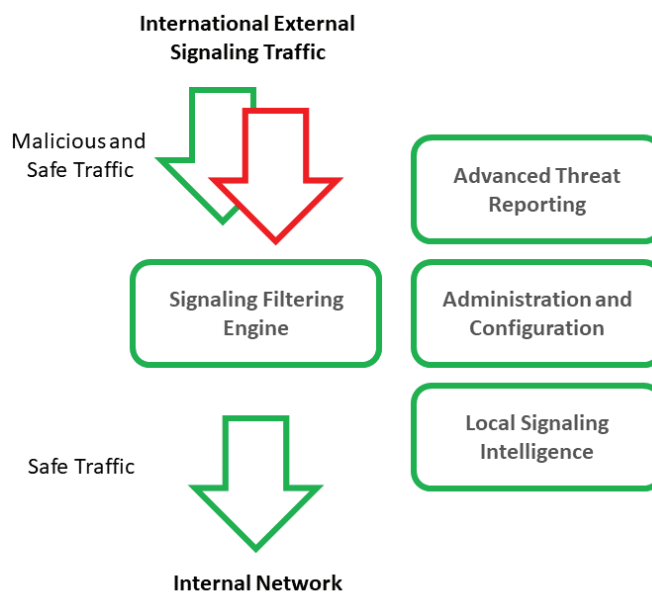
APPROACH

The project’s approach addresses three main areas that organizations face when securing mobile infrastructure: detection, analysis, and response planning. The project will research and document requirements for a managed, secure defense and the processes required to update protection against the latest threats. The research will then detail the platform, skills, and processes that will be required to manage and curate a threat-intelligence platform with the capabilities to

prioritize and plan responses to mobile network infrastructure threats.

BENEFITS


The performer’s research will provide a comprehensive approach for designing practical solutions to the challenges of protecting national mobile infrastructure. The research project will not only enable a defensive solution to be architected for current mobile technologies but will also demonstrate how the architecture can be extended to secure networks into the future.



AdaptiveMobile Security Signaling Protection Platform Research Platform Architecture

COMPETITIVE ADVANTAGE

Any nation with the ability to secure its mobile communications infrastructure from external attacks or misuse will maintain a critical advantage in the battle against cybercrime and espionage. Preventing access to sensitive intelligence, unsecured conversation, locations, and other attack vectors commonly associated with insecure mobile network infrastructure is an essential defensive capability. Intelligence gained from analysis and correlation of information will provide insight into the techniques, tactics, infrastructure,



and procedures used to deploy attacks against mobile networks. This research project will provide a blueprint for how and to what extent these capabilities can be delivered and deployed.

NEXT STEPS

The project encompasses 18 months of research, testing, and project-specific revisions to fine-tune the technology to meet the demands of the government and the unique threat vectors it experiences.

Protecting the Mobile Core Network Elements Via Air-Gapped Hardware Verification and Code Execution Tracking

Aether Argus

Angelos D. Keromytis

angelos@aetherargus.com

OVERVIEW

AetherGuard is a novel and unique approach to protecting both legacy and 5G mobile core network elements (MCNEs) and internet of things (IoT) devices against firmware supply chain attacks and detecting runtime (software) exploitation.

CUSTOMER NEED

Given the increased risk in the global supply chains for both critical and consumer markets, there is a clear need for products that can efficiently and effectively inspect the hardware elements of connected devices and components for evidence of tampering. This need indicates a market opportunity for offering products to secure electronics-oriented goods, such as IoT and embedded devices, in both the industrial/corporate and consumer markets.

APPROACH

AetherGuard relies on analog side channel signals that are nondestructively collected while the device (or a specific integrated circuit) is performing its normal power-up, self-test, and/or functional testing while the system is operating normally. By monitoring and taking advantage of the electromagnetic emissions (EMEs), AetherGuard will identify attacks against MCNE or IoT devices, protecting against both firmware supply chain and cyberattacks.

BENEFITS

AetherGuard will provide a new detection capability for supply chain attacks on MCNEs/IoTs by tracking EMEs both prior to deployment and while the system operates. Such checking can be done in the lab or opportunistically on field-deployed systems. Furthermore, if AetherGuard is deployed as part of an MCNE/IoT installation, it also will be able to track the runtime behavior of the device throughout its operation and alert operators. AetherGuard can be paired with an automated response system that restarts or quarantines devices, reinstalls a “clean” firmware image, or undertakes other predefined actions.

COMPETITIVE ADVANTAGE

One of the key advantages of AetherGuard is that there is no need to install software on a device, and the monitoring of the vetted device occurs nondestructively and out-of-band. AetherGuard is “invisible” to attackers and cannot be subverted, as is the case with solutions that add software (or even hardware) to protect a device and, therefore, imposes zero overhead on the monitored system. Another solution advantage is the ability to retrofit AetherGuard to include as part of existing device-acceptance testing or quality control workflows for device production.

NEXT STEPS

The performer will provide a complete capability for profiling and monitoring devices against firmware and runtime cyberattacks.

Symbiote Integration for Mobile Network Infrastructure

Red Balloon Security

Ang Cui

Research-PI@redballoonsecurity.com

OVERVIEW

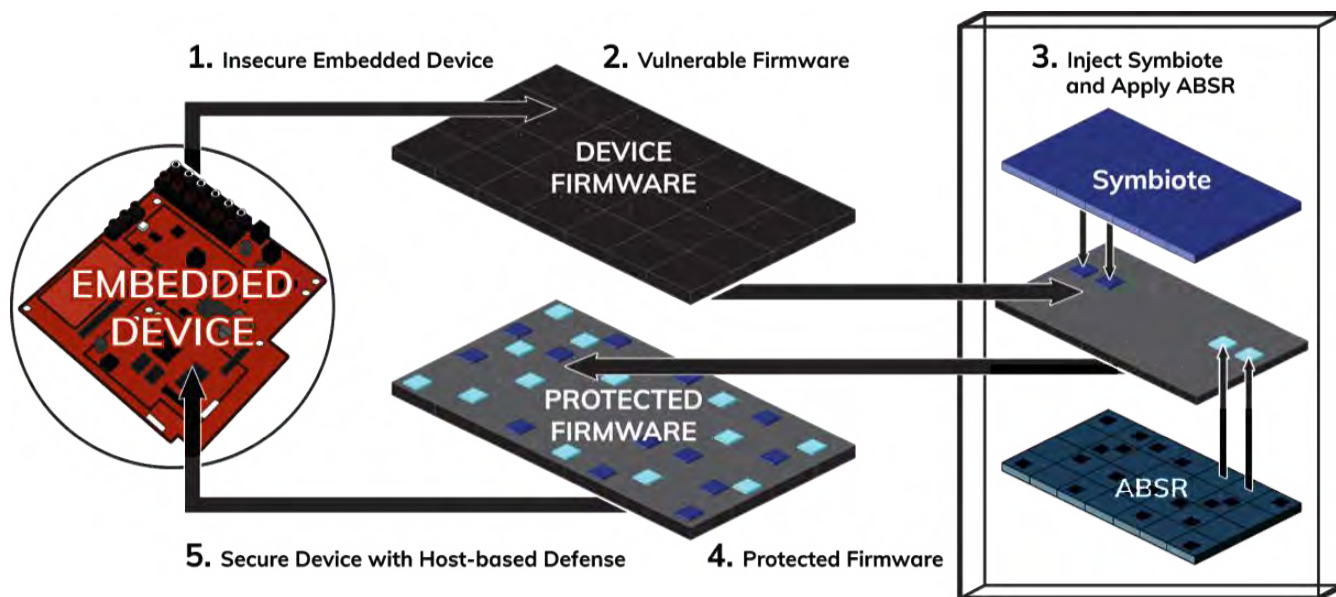
Embedded devices such as base stations, repeaters, and specialized backend devices are crucial components of 4G and 5G mobile network infrastructure. Existing security solutions fail to directly defend the device's firmware against exploitation while these exploitation opportunities are increasing due to supply chain and software complexity growth. Through this R&D effort, Red Balloon Security is integrating its patented firmware hardening and runtime protection technologies Symbiote and Autotomic Binary Structure Randomization (ABSR) into mobile network infrastructure embedded devices to mitigate exposure to a wide range of attack chains.

CUSTOMER NEED

Industries and infrastructure, including industrial automation, medical, power infrastructure, and financial services, are all vulnerable to cyberattacks. Mobile network infrastructure is no different. Any attack directly affecting the devices that make up mobile infrastructure can affect millions of users as well as an increasing number of critical infrastructure devices, including internet of things devices, connecting through 5G gateways.

APPROACH

Symbiote is a host-based defense injected directly into the firmware binary. Symbiote runs parallel to normal device execution, providing runtime protection to detect attacks and respond in real-time. ABSR provides firmware hardening via automated attack surface reduction and randomization of memory and code at the binary level. The Symbiote and ABSR modifications can be made in minutes following a normal firmware built and deployed via existing firmware update channels.



Red Balloon Security injects firmware hardening and runtime protection into embedded device firmware.

BENEFITS

Symbiote and ABSR provide a variety of firmware hardening and runtime protections, preventing most firmware-level attacks, including memory corruption, command injection, privilege escalation, rootkits, buffer overflows, and heap overflows. In this project, randomization is being added as a defense against memory-based attacks that allow attackers to gain control of systems. These technologies also provide a deeper level of forensics than the current state-of-the-art technology that sends only application logs, integrating with existing Security Information, Event Management, and Intrusion Detection Systems to report security events. The increase in firmware security helps organizations meet existing and potential future compliance requirements in addition to discouraging and thwarting attackers by increasing the work-factor to successfully attack a system.

COMPETITIVE ADVANTAGE

Red Balloon Security leverages the Firmware Reverse Analysis Konsole (FRAK) to inject Symbiote and ABSR directly into firmware binaries. FRAK is an internal proprietary framework for unpacking, analyzing, modifying, and repacking firmware images of arbitrary embedded devices. The FRAK framework is a force-multiplier tool that automates binary modification safely, which otherwise is a costly manual process. This approach requires no source code and is operating system agnostic, thereby making it portable and reducing integration cost.

NEXT STEPS

Red Balloon Security will develop prototype integrations in relevant 5G mobile network infrastructure devices and will reach out to mobile network infrastructure vendors to partner in incorporating firmware hardening and runtime protection into their devices.

Mobile Network Traffic Visibility for the Enterprise

GuidePoint Security

Jeremy Rupp

jeremy.rupp@guidepointsecurity.com

OVERVIEW

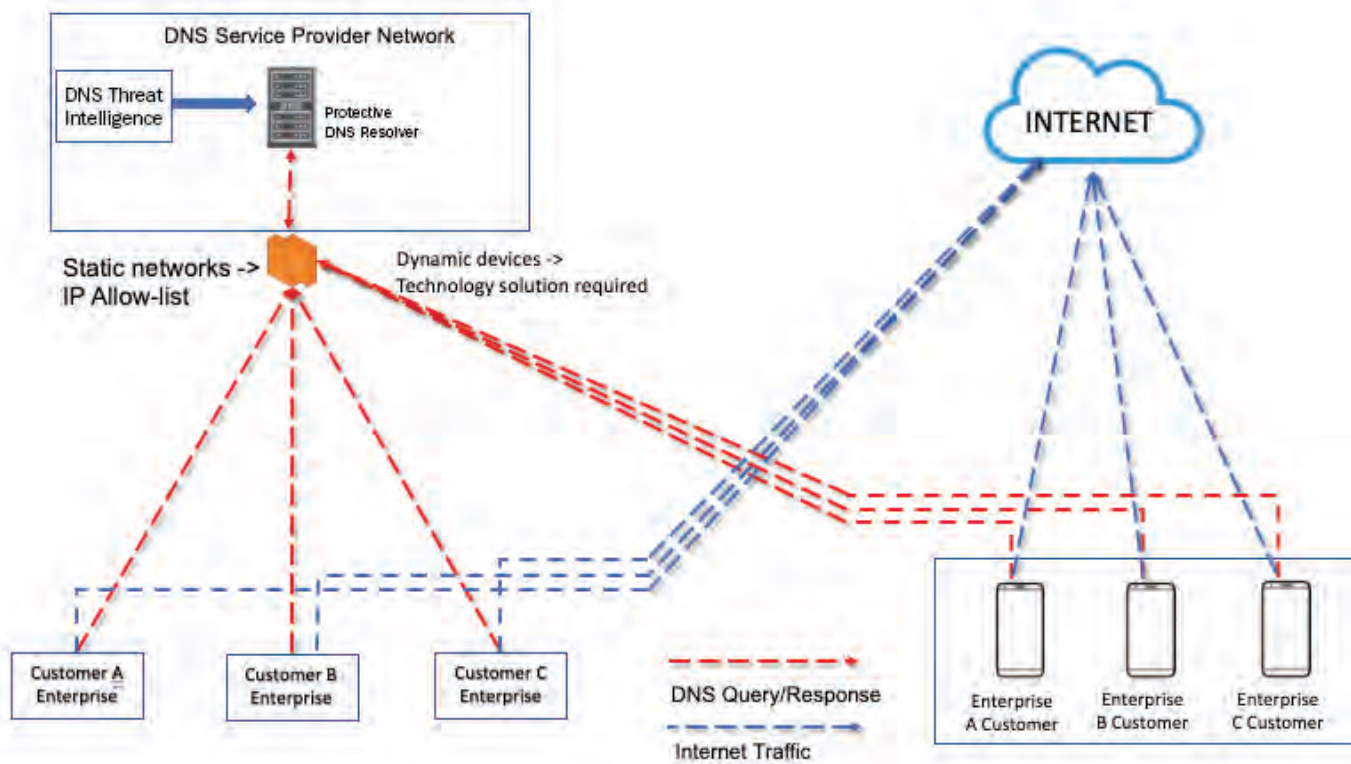
This project is designing and implementing a solution to implement protective Domain Name System (DNS) capabilities and service offerings on mobile devices managed by Federal Civilian Executive Branch agencies. The development process will be used to acquire knowledge regarding tradeoffs in approach, identify issues with scalability, enterprise management and security considerations.

CUSTOMER NEED

As government agencies and their employees have become mobile and are working all over the United States with mobile devices, a requirement was identified to protect mobile DNS traffic and align DNS protections with those offered to traditional enterprises.

APPROACH

The approach is developing methods to enforce routing mobile DNS traffic to a protective DNS resolver managed by CISA and developing a method to authenticate mobile devices to a centralized protected DNS service/provider and attribute DNS traffic to those devices and agencies that own them. The methods will support traditional DNS:53 as well as encrypted DNS protocols such as DNS over Hypertext Transfer Protocol Secure (HTTPS) and DNS over Transport Layer Security (TLS).



Target Network Architecture Diagram (Desired Solution)

BENEFITS

The benefits of this work will be the creation of techniques to protect mobile DNS traffic and protect mobile device users from resolving malicious domains that host malware, disrupting malware command, and control and defending against the spread of viruses.

COMPETITIVE ADVANTAGE

The integration of multiple security and compliance applications will reduce the need for on-premises hardware, appliances, or software. This approach will eliminate the need to route mobile DNS traffic back to agency premises. This approach will reduce the need for increasing physical space and additional hardware, along with their associated cost.

NEXT STEPS

The performer will implement a proof-of-concept to determine scalability and applicability for the integration of the developed protective DNS architecture into existing mobile network infrastructure. If the proof-of-concept is adopted, it will create collaborative relationships among government agencies that could lead to a scalable integration plan for protective DNS implementation.

Mobile Traffic Intelligence at Scale

AppCensus

Nathan Good

nathan@appcensus.io

OVERVIEW

AppCensus is improving the protection of government DNS traffic from mobile devices to identify potential malware, attacks, or attempts to exfiltrate sensitive data from or through the devices.

CUSTOMER NEED

The ubiquity and convenience of smartphones mean that employees have these devices with them constantly as they move between networks beyond enterprise control. Additionally, when roaming outside the enterprise network, the Domain Name System (DNS) configurations are difficult to control and often are intercepted by DNS proxies and other middleboxes deployed by the mobile network, making it difficult for enterprises and government agencies to control access to malicious sites from the devices or to protect against domain hijacking. This lack of control over DNS traffic could open new vectors for attack on the mobile devices, including DNS cache poisoning and DNS manipulation attacks.

APPROACH

The approach of this research and development project is to provide control of mobile DNS traffic, establishing on-device traffic interception and control. This mobile client will securely communicate with a protected DNS service managed by the Cybersecurity and Infrastructure Security Agency (CISA) to filter DNS queries for known malicious content. Proposed solutions will provide a variety of scenarios for testing and validating the required solution. Additionally, the research team will explore solutions for controlling encrypted DNS protocols and research solutions for authenticating and securing device DNS settings for iOS and Android devices.

BENEFITS

The developed solution will allow app traffic to be intercepted locally on the mobile device through a user-space app that reroutes standard DNS queries securely to CISA-managed protective DNS resolver, thereby extending network security capabilities outside of the perimeter and into mobile devices in use in the field.

COMPETITIVE ADVANTAGE

The AppCensus platform provides capabilities to analyze each mobile app's runtime behaviors and assess its security and privacy risks at scale in a privacy-preserving manner. Leveraging this platform, we can seek to extend the capabilities into user-space, thereby providing a means of real-time analysis in the field.

NEXT STEPS

The performer will extend capabilities into a user-space, on-device platform. Using the app corpus provided by a trusted third-party entity, the performer also will develop a test dataset to provide ground-truth data to evaluate and test out initial detection capabilities.



Overview of System Architecture

Government Secure Voice Architecture

Texas A&M University

Walter Magnussen

w-magnussen@tamu.edu

OVERVIEW

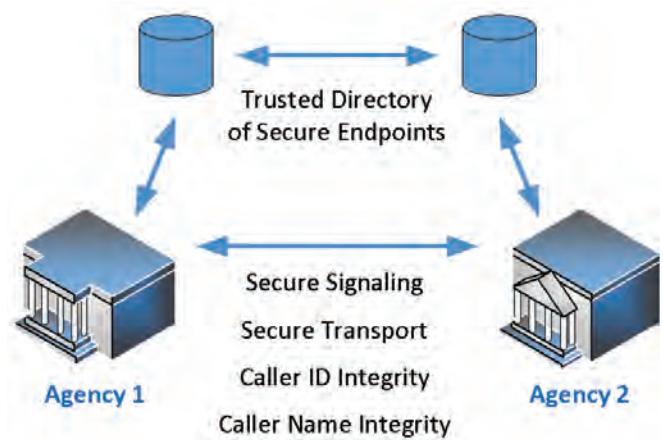
The Texas A&M University Internet 2 Technology Evaluation Center (ITEC) is working to design and test an architecture for secure voice and data communications within and between government agencies. The planned network will use existing technologies and work with legacy and emerging voice networks, such as 5G, to validate caller identities and establish secure connections, enabling agencies operating in sensitive areas to do so with secure communications. The testbed will include premise-based systems, cloud-based systems, and Mission Critical Push to Talk.

CUSTOMER NEED

While government entities operating in classified domains have systems in place to secure classified communications, most of the government operates on voice systems with known and unknown vulnerabilities. In light of acknowledged cyber-threats and to protect government interests, federal agencies handling sensitive information also require more secure voice and data communications.

APPROACH

Texas A&M ITEC is working in collaboration with the Columbia University and Texas A&M University at Commerce to design and develop a secure voice communications architecture testbed. The testbed will provide the platform for emulating and securing communications between and within organizations. Using existing technologies, the team will design and test the secure communications architecture and ultimately develop detailed documentation for use by federal agencies that will implement the system.




High-level diagram of the project secure-voice architecture

BENEFITS

The testbed allows for the integration of systems across a range of technologies and brands and thus will result as a solution that is both cost-effective to implement with legacy voice systems and suitable for testing and evaluating future systems architectures as well as the potential security impacts of system modifications.

COMPETITIVE ADVANTAGE

All the technologies proposed in this architecture are based upon open standards, and most are standard-system capabilities. The remaining standards-based technologies are available as open-source low-cost or no-cost solutions. The encryption of Session Initiation Protocol (SIP) flows are standard features for signaling and media using Internet Engineering Task Force Requests for Comment for Transport Layer Security and Secure Real-time Transport Protocol. These use the same proven secure authentication used today for secure web and banking applications. The Secure Handling of Asserted information using toKens/Secure Telephone Identity Revisited framework used for the proposed architecture is being implemented by most of SIP service providers. The electronic number call routing methods are also standard tools used by many—if not all—Voice over Internet



Protocol service providers. This project documents and tests an architecture that can be implemented without the requirement for replacement of existing platforms.

NEXT STEPS

Once the architecture is designed, built, tested, and documented, the next step will be a pilot test of the secure voice architecture within two or more federal agencies to validate operational assumptions and refine system documentation to ensure usability.

Deploying Defenses for Cellular Networks Using the AWARE Testbed

University of Florida

Patrick Traynor

traynor@ufl.edu

OVERVIEW

This project is developing solutions for legacy and future cellular systems to detect and mitigate call/message interception and user tracking by hostile third parties.

CUSTOMER NEED

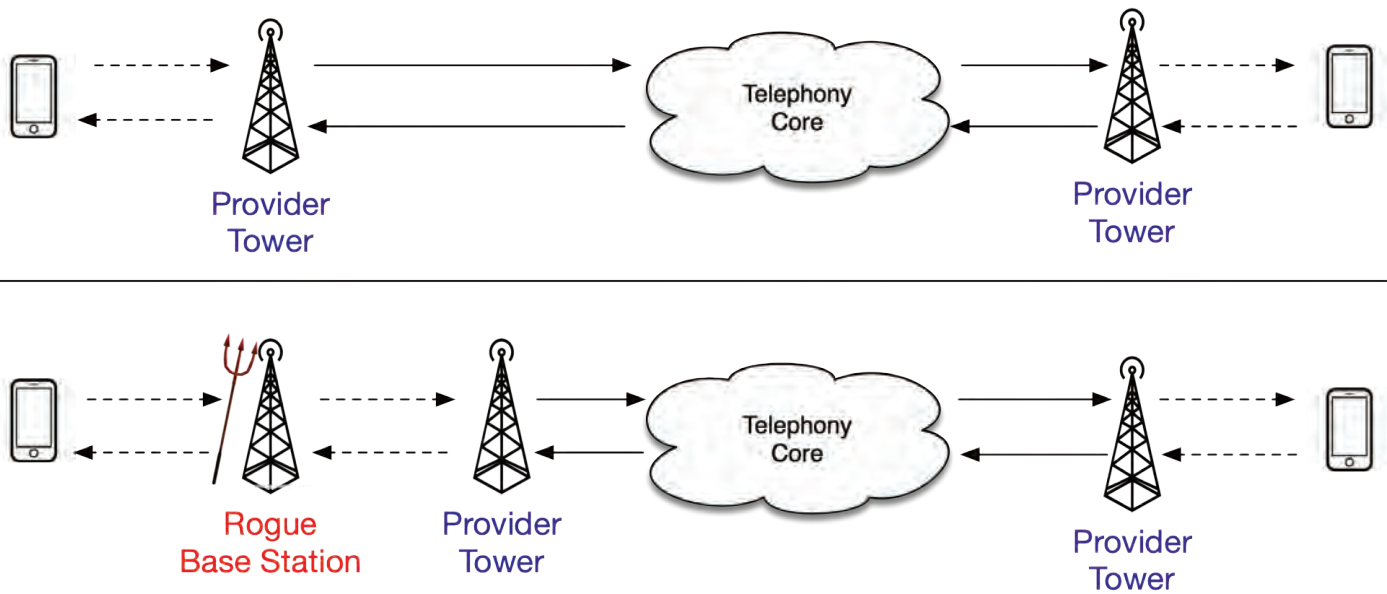
Features key to mobility management historically have been designed with the assumption that they will only be issued by trusted insiders. Broad access to core functions and equipment, such as microcells, invalidate such assumptions. Because of this security gap, solutions to detect and mitigate interception and user tracking by hostile third parties are critical to protect users of vulnerable infrastructure.

APPROACH

Tools and techniques to acoustically measure end-to-end distance between call endpoints and detect anomalous mobility patterns (e.g., moving too rapidly between physical locations) are being developed as a mechanism to identify redirection or man-in-the-middle attacks. Additionally, the researchers will perform targeted fuzzing of core components, develop techniques for quarantining compromised devices, and protect communications with encryption. Fuzzing is a process—usually automated—for finding hackable software bugs by randomly feeding different permutations of data into a target program until one of those permutations reveals a vulnerability.

BENEFITS

Calls and messages are not encrypted end-to-end over current or 5G cellular networks. The techniques developed through this project will assist in alerting users and operators of unsanctioned eavesdropping by hostile third parties. The impact of these new techniques will not only improve the security of voice communications but also will help prevent attacks on two-factor authentication systems that rely on the Short Messaging Service.



Illicit call interception, here via a rogue base station, extends the distance/delay between endpoints. Dotted and solid lines indicate wireless and wired links, respectively.



COMPETITIVE ADVANTAGE

The solutions developed in this effort will provide a broad range of tools to providers (e.g., protocol fuzzing) and end-users (e.g., secure distance bounding), allowing for both groups of stakeholders to improve their security footing independently. Moreover, the techniques developed will improve security across both current and future network generations.

NEXT STEPS

The performer is in the process of building both hardware and software to achieve the project's goals, with prototypes being delivered throughout the duration of the project.



EMERGENCY COMMS R&D PROJECT OVERVIEW

EMERGENCY COMMS RESEARCH AND DEVELOPMENT PROJECT OVERVIEW

This is the second part of the overall project area. The first part—the Secure and Resilient Mobile Network Infrastructure R&D Project primarily focuses on developing security solutions for next-generation 5G networks. The focus of this R&D project area is on enhancing and improving the ability of first responders to manage disasters and emergencies with maximum effectiveness and efficiency.

Specifically, the project is engaged in the following three R&D efforts: facilitating Computer-Aided Dispatch (CAD) interoperability; increasing the cyber resilience of Emergency Communications Centers (ECCs)/ Public Service Answering Points (PSAPs); and developing tools to enable Federated Identity Credential Access Management (FICAM).

Each of these projects is being managed by S&T’s Office of Mission & Capability Support on behalf of CISA, which ensures federal, state, local, tribal, and territorial (FSLTT) agencies have the necessary plans, resources, and training to support resilient, operable, and advanced interoperable emergency communications.

Following are brief summaries of each of the three Emergency Communications R&D projects that are seeking to close capability gaps encountered by the nation’s first responders.

CAD-TO-CAD INTEROPERABILITY

When first responders arrive at an event, they each use their own proprietary CAD systems to help establish situational awareness and coordinate the response. Because these systems are unable to communicate with each other, sharing vital data with other agencies—local, state and federal—is extremely difficult, if not impossible.



As a result, critical data is not available to all the responding organizations because the array of CAD systems involved are unable to electronically exchange information. This lack of interoperability impedes situational awareness and introduces operational inefficiencies that slowdown the effective response to an incident.

CAD-to-CAD is an effort to address the lack of data communications interoperability between different first responder's disciplines and systems. The benefits of CAD-to-CAD interoperability include:

- + Reduction in response time
- + Increased personnel efficiency
- + Increased equipment/vehicle use efficiency

The reduction in response time is critical to saving lives and property.

The objective of the IJIS Institute R&D project is to create resilient public safety CAD-to-CAD interoperable communications that are standards-based, efficient, and support multi-discipline response to regional, multistate or national events.

IJIS brings together public safety practitioners and CAD solution providers in a collaborative effort to evaluate specifications, promote development of standards-based CAD interoperable solutions, validate methodologies, and conduct pilot tests.

ECC/PSAP CYBERSECURITY

The ECC PSAP information communications network is the backbone of the Nation's Emergency Services Sector, including fire departments, law enforcement, and emergency medical services agencies. The PSAP or ECC is the focal point for how these agencies respond to 911 calls for help and serves this function over 240 million times each year.

Transition of 911 to the IP-based Next Generation 911 (NG911) brings the cybersecurity risks of the Internet to the 911 networks. An integral part of the CISA mission is to promote and support this critical national communications infrastructure and thus CISA is working to protect the confidentiality, integrity and availability of the systems that perform these functions.

The focus of this project is to protect one of the nation's most important services—911—by predicting public safety cyber-needs both for vulnerable legacy systems and for the future interconnected Next-Generation (NG) 911 systems.

The SecuLore R&D project relies on predictive analytics that gather cyber analytics to build PSAP threat environment situational awareness. Predictive and cyber analytics are used to improve the detection and elimination of cybersecurity attacks against current and future emergency communications systems. Near-real-time behavioral threat analysis of the traffic hitting an emergency communications center's network provides recommended remediation steps to address any identified attack. The project's goal is to improve the cybersecurity defenses of the nation's emergency communications infrastructure.

Furthermore, this project will complement CISA's activities to improve the resilience of the nation's vital emergency communications infrastructure. It is a critical undertaking since the number of cyber-attacks continues to increase and the number of NG911 systems being deployed across the country is growing.

FEDERATED IDENTITY CREDENTIAL ACCESS MANAGEMENT

Information Sharing and Safeguarding (IS&S) is a fundamental need of the U.S. public safety community. The community's IS&S requirements are substantial and increasing since it must respond to a wide range of challenging, multi-agency emergencies, including school shooting incidents and large-scale natural disasters.

Federated Identity, Credential, and Access Management (“Federated ICAM”) is a critical capability that can help advance public safety IS&S capabilities across FSLTT agency boundaries. Advancement of technical capabilities and solutions in these areas is critical to helping the public safety community fulfill its mission of ensuring the protection and well-being of U.S. citizens.

The primary goal of the Georgia Tech Applied Research Corporation (GTARC) project is to substantially improve several key trustmark technologies, which provide standards, artifacts, software tools, and methodologies for managing IS&S and Federated ICAM trust relationships. With this improved framework, public safety agencies can migrate their information-sharing arrangements away from a status quo of hard-coded, brittle agreements and unscalable trust relationships and toward a new paradigm of agreements and trust relationships that are scalable, agile and adaptable to the rapidly evolving mission needs of agencies.

Trustmark software tools will help the public safety community better fulfill its mission through more effective trusted IS&S and Federated ICAM capabilities. The project addresses the most pressing gap in the current trustmark framework: The lack of effective software tools to support the framework's primary use-cases, such as emergency communications interoperability.

Upgrading the trustmark framework's Federated ICAM capability would help advance public safety IS&S communications across agency boundaries. The intent of the trustmark framework is to make IS&S and Federated ICAM trust criteria transparent and explicit so all parties to a trusted information-sharing transaction can understand exactly what criteria must be satisfied for trust and interoperability to exist as well as what assessment steps must be completed—through either a self-assessment process or a more rigorous third-party assessment.

The benefits of Federated ICAM to the public safety community are the following:

- + Increased agility and scalability of IS&S and Federated ICAM trust relationship management for public safety agencies
- + Decreased IS&S and Federated ICAM costs for public safety agencies
- + Increased information sharing among public safety agencies and their partners, leading to better mission outcomes
- + Improved effectiveness in fulfilling the public safety community's mission of protecting U.S. citizens and saving lives

For more information about each of the R&D projects noted above, please see the section titled “Emergency Comms R&D Project Summaries.”

A man with a beard and mustache, wearing a headset, is shown in a close-up. The image is overlaid with a complex digital interface consisting of blue and white lines, dots, and grid patterns, suggesting a high-tech or emergency communication environment. The background is dark with some blurred lights.

EMERGENCY COMMS R&D PROJECT SUMMARIES

Information Sharing, Safeguarding, and Federated ICAM

Georgia Tech Applied Research Corporation

Matthew Moyer

Matthew.Moyer@gtri.gatech.edu

OVERVIEW

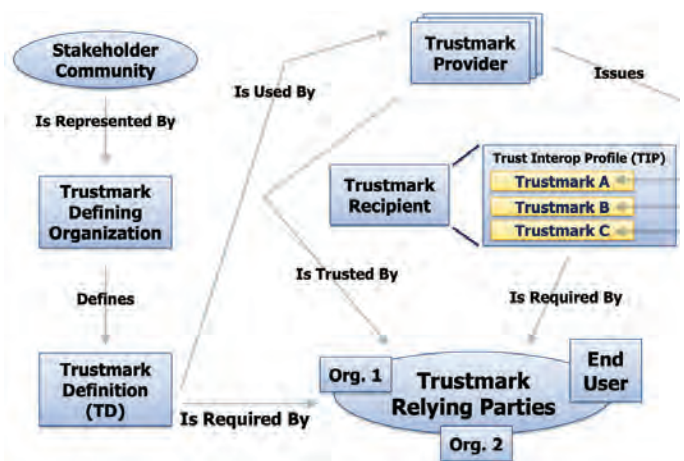
The trustmark framework creates trust through a set of technical standards, policies and software tools. The technology facilitates public safety (PS) entities to implement Federated Identity, Credential and Access Management (ICAM) capabilities. It also permits information-sharing in a trusted, rigorous, agile and scalable manner. The project's objective is to advance the maturation of a set of key open-source software tools that support the framework.

CUSTOMER NEED

Federated ICAM is a critical capability that can help to enable and advance PS information-sharing capabilities across agency boundaries, down to the level of sharing key information with select individuals in accordance with appropriate access-control rules. The advancement of technical capabilities and solutions that support scalable, agile Federated ICAM is critical to help the PS community fulfill its broad mission of protecting the well-being and lives of U.S. citizens.

APPROACH

At a high level, the trustmark framework aims to make Federated ICAM trust criteria transparent and explicit, so all parties to a trusted information-sharing transaction understand exactly what criteria must be satisfied for trust and interoperability to exist as well as what assessment steps must be completed—through either a self-assessment process or a more rigorous third-party assessment—to demonstrate satisfaction of these requirements. The framework also embraces and encourages



The Trustmark Framework Functional Model

componentization and modularity around trust requirements to promote reusability of assessment results and reduce costs. Last, the trustmark framework leverages machine-readability of artifacts to promote automation and scalability.

BENEFITS

This project will benefit PS agencies in multiple ways such as by providing increased agility and scalability of Federated ICAM trust relationship management; decreased Federated ICAM implementation and management costs; and increased information sharing among PS agencies and their partners, leading to better mission outcomes; and improved effectiveness in fulfilling their critical mission.

COMPETITIVE ADVANTAGE

Commonly used alternatives to the trustmark framework include bilateral information-sharing agreements and multi-party federation trust frameworks. Each alternative has significant drawbacks such as brittleness to changing requirements, lack of scalability in multiple dimensions (e.g., partner agencies, use-cases, technologies, etc.), and an inherent lack of rigor. The trustmark framework addresses and overcomes these drawbacks.

NEXT STEPS

The performer will implement open-source versions of four critical trustmark framework software tools and will collaborate with select PS agencies to implement a series of pilot projects in which the tools and the trustmark framework itself are used to demonstrate trust management for actual Federated ICAM use-cases in the community.

CAD-to-CAD Interoperability

IJIS Institute

Michael Alagna

Michael.Alagna@ijis.org

OVERVIEW

First Responder agencies have long struggled with interoperable communications when responding to a multiple-agency emergency requiring onsite coordination. Until recently, voice interoperability had been the primary concern. Today, however, the First Responder community is focusing on the importance of data interoperability. Next Generation 911 (NG-911) and broadband networks will improve communications during emergencies through a nationwide Internet Protocol-based architecture. A key challenge facing public safety is bridging all these new technology innovations to ensure interoperable information sharing.

CUSTOMER NEED

Critical data supporting incident response and resource management decisions is often not available to all organizations responding to a multiple-agency emergency because the various Computer-Aided Dispatch (CAD) systems used by public safety agencies are unable to electronically exchange information easily, if at all. Most CAD technology was not designed to be interoperable and no data exchange standards are currently in widespread use. As a result, situational awareness suffers and operational inefficiencies are prevalent. To date, improvised interoperability is achieved by developing custom interfaces that can be costly to develop and maintain.

New capability to standardize interoperability between CAD systems used by Emergency Communications Centers to improve public safety.

APPROACH

The project will unite public safety practitioners, CAD solution providers, and standards development organizations in a collaborative environment to



New capability to standardize interoperability between CAD systems used by Emergency Communications Centers to improve public safety.

promote development of requirements, specifications, standards and ultimately conduct technology pilot testing to ensure that interoperability challenges are successfully addressed. It employs a phased approach to reduce risk and allow the resolution of the complex technical environment through step-based consensus building.

BENEFITS

Timely access to all available operational information enables better decision-making, which can easily translate into saved lives. Emergency Communications Centers report average response times are reduced by over two minutes with CAD-to-CAD interoperability. The period following a traumatic injury during which there is the highest likelihood that immediate medical treatment will prevent death is called the "Golden Hour." The recommended amount of time for emergency response for most trauma injuries is less than 10 minutes at the location of the trauma.

COMPETITIVE ADVANTAGE

Supporting the missions of public safety agencies by empowering the electronic exchange of information in a cost-effective and standardized manner will improve responder situational awareness, reduce operational inefficiencies and optimize the response to an incident.

NEXT STEPS

This program will result in recommendations for implementing standards-based interoperable CAD-to-CAD capability as well as operational, technical and training guidance that will ensure a consistent national implementation. The protocols, specifications and/or standards will be drawn from extensive research into best practices and interviews of experts in emergency communication, NG-911 technology, public safety and other relevant fields. Further, the protocols and resultant standard will be verified during pilot tests conducted by Emergency Communications Centers in different locations.

Creating A Cyber-Resilient Public Safety Infrastructure

SecuLore Solutions LLC

Ron Zucker

ron.zucker@seculore.com

OVERVIEW

This R&D project attempts to provide better cybersecurity protections to Emergency Communications Centers (ECC)/Public Service Answering Points (PSAP) through predictive analytics and a robust solution for fast response to identified cyber-attacks.

CUSTOMER NEED

Next Generation 911 (NG911) promises to make emergency services faster and more resilient while providing access to text, voice, video, and phone requests for aid. While an exciting opportunity, this makes the cybersecurity threat to 9-1-1 much more dangerous. The customer needs to create security controls and systems to adapt to NG911 threats.

APPROACH

The project's approach is two-pronged: First, the performer is analyzing Level 2 network traffic and using a Long Short-Term Memory Recurrent Neural Network to recognize some types of malevolent traffic. This approach is called "CyberShapes." So far, the performer has applied this technique to brute-force hacking.

Second, the performer's Guardian service allows it to block very specific traffic temporarily pending PSAP staff review and remediation. Because of the unique needs of ECCs, Guardian is designed to "fail open," allowing traffic to flow in the case of a power failure or network fault.

BENEFITS

The performer's 24x7x365 Security Operations Center (SOC) keeps ECCs safe from attack. But where they are unable to interrogate every connec-



Visualization of a Secure Shell (encrypted) Login

tion or every info packet into or out of a network, its CyberShapes-capable server can examine traffic over unexpected ports and identify innovative attacks to keep ECCs safe. Combined with the Guardian module, the SOC can protect an ECC/PSAP from cyberattacks and distinguish between one that requires immediate response and one that can await action by IT staff.

COMPETITIVE ADVANTAGE

From a technical perspective, the developed ECC cybersecurity solution can do things no other solution on the market can accomplish, including distinguishing success from failure in encrypted brute-force attacks. But the more important aspect of the solution is understanding the workings of an ECC/PSAP and being able to ensure that data flow or throughput is never an impediment to their life-saving work.

NEXT STEPS

The performer is focusing on the vulnerabilities currently being exploited. While brute-force was the first implementation of the solution, the performer is now working to identify and stop an exfiltration attack before it becomes a problem. The project's long-term goals are to see if the approach can be used to detect malware, especially ransomware, and if the solution can protect against Telephony Denial of Service attacks, which are targeting PSAPs across the country.



ONLINE

www.dhs.gov/cyber-research



FACEBOOK

Facebook.com/dhsscitech



EMAIL

SandT-Cyber-Liaison@hq.dhs.gov



YOUTUBE

www.youtube.com/dhsscitech



TWITTER

[@dhsscitech](https://twitter.com/dhsscitech)



PERISCOPE

[@dhsscitech](https://periscope.tv/dhsscitech)



LINKEDIN

www.linkedin.com/company/dhsscitech