Security Issues in Public Safety Communication Networks

Project Report

Kevin Kuo
Department of Computer & Information Sciences
Towson University
Towson, USA
kkuo1@students.towson.edu

***Abstract*—An exponential increase in the amount of data of sensitive data being transmitted over networks utilized for the public safety mission has raised major concerns regarding the protection and security of such data. This project proposes techniques, technologies, and protocols, which a new First Responder network can adopt and implement in order to protect and secure mission critical data that traverses the network.**

Keywords—public safety; Land Mobile Radio (LMR); FirstNet; First Responder Network; Middle Class Tax Relief and Job Creation Act (MCTRJC) of 2012; First Responder Network Authority; Quality of Service (QoS); Long Term Evolution (LTE); firewalls; Department of Homeland Security; Department of Defense; National Institute of Standards and Technology; 3rd Generational Partnership Project; hotspot; smart phones; tablets; laptops; interference; operation; security; IP security (IPsec); eNodeB; Open Systems Interconnection (OSI) model; TCP/IP; data corruption; data theft; user credential theft; Universal Integrated Circuit Card (UICC); SIM card; International Mobile Subscriber Identity (IMSI); second-generation wireless telephone technology (2G); third-generation wireless telephone technology (3G); Virtual Private Network (VPN); Public Safety Communications Research (PSCR)

I. INTRODUCTION

Public safety communication network are poised for a dramatic evolution from the traditional Land Mobile Radio (LMR) system. First responders recognized the necessity for public safety communication networks to evolve beyond mission-critical voice services to encompass providing mission critical data services. On February 22, 2012, the Middle Class Tax Relief and Job Create Act (MCTRJC) of 2012 required the government managed next generation public safety communication network initiative known as the First Responder Network Authority (FirstNet), to build, operate and maintain the first high speed nationwide broadband network dedicated to public safety, the First Responder network. As the amount of data of sensitive data being transmitted over networks being utilized for the public safety mission has increased exponentially, the protection and security of such data has become a major concern. This project proposes ways in which such data can be protected on the First Responders network.

A. *Items of Interest*

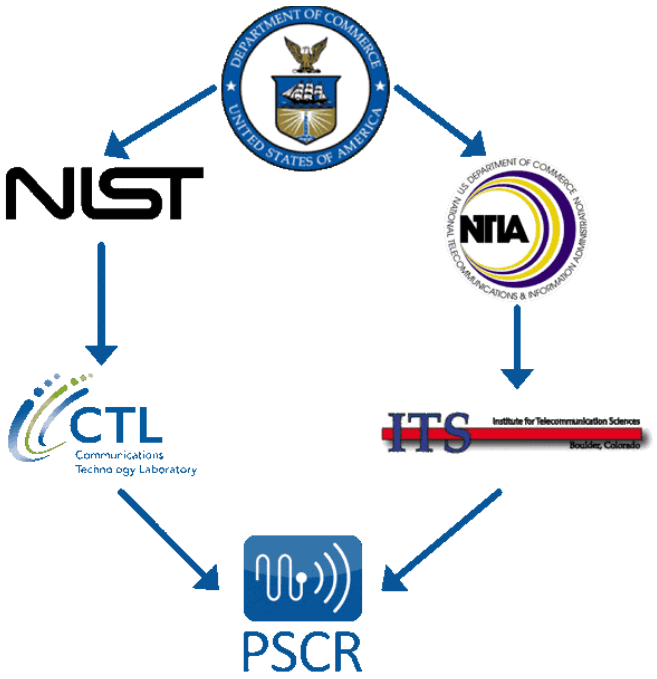
1) Radio Access Network: This consists of the radio base station infrastructure that will connect user devices to the network. These may include cell towers as well as hotspots embedded in vehicles.

2) Public Safety Devices: These are devices that users use to send and receive information over the network. These may include smart phones, tablets, laptops, and other specialty devices. Industry will develop additional types of devices and applications to meet public safety needs. These devices must undergo a variety of testing and certification in areas to include interference operation, and security.

3) Applications: These are the software applications that end users will use in order to access the services they need. The First Responder network will enable the creation of new public safety applications while maintaining support for existing commercial applications to ensure a smooth transition from commercial providers to the First Responder network.

II. Related Work

Fig. 1. Public Safety Communications Research

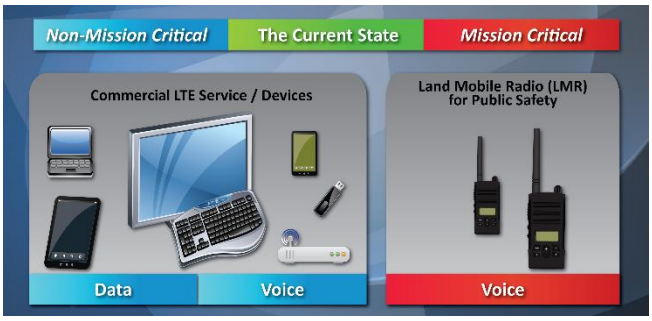


The Public Safety Communications Research program is responsible for addressing key developments regarding priority, pre-emption, and quality of service with regard to FirstNet and the First Responders network. Public Safety Communications Research laboratories provide research, development, testing, and evaluation to improve national communications interoperability. Public Safety Communications Research performs research on the behalf of organizations such as Department of Homeland Security, Department of Commerce, National Institutes of Standards and Technology. Public Safety Communications Research conducts testing and evaluation on audio quality, image quality, indoor wireless coverage, Land Mobile Radio and Long Term Evolution interfacing, Next Generation Networks Priority Services, and security research to include cybersecurity, identity management security, mobile application security, and mobile application/data isolation.

III. Overview

A. Current State

Fig. 2. Current state of public safety communication



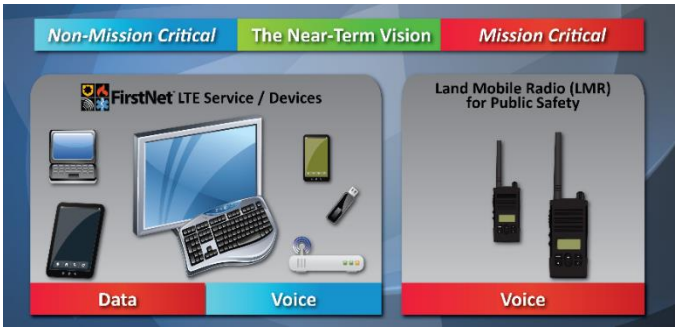
Currently, first responders are relying on Land Mobile Radio (LMR) networks to provide mission critical voice communications. These LMR networks generally meet first responder's needs to have a guaranteed priority access to mission critical voice services. However, most first responder organizations also require use of mobile data services and applications. These services are cannot utilize the LMR network, but are being provided exclusively by commercial carrier data connections. Unfortunately, utilizing these services and applications on the commercial network requires the sharing of resources. This creates significant and ongoing concerns regarding the ability to prioritize such demands appropriately.

B. Near-Term First Responder Network

When the First Responder network launches, the objective of the network will be to provide mission critical, high-speed data and video services that will supplement LMR networks. LMR networks would continue to provide mission critical voice services. First responder organizations will still reply on the LMR networks for mission critical voice services. Therefore, the initial proposed transition will move services and applications that previously utilized the commercial network onto the First Responder network.

In March 2017, the FirstNet team selected AT&T to build, implement, and manage the First Responder network. The vision for the First Responder network has not changed, although, its implementation has been modified since the original conception. The First Responder network will continue to use commercial infrastructure to deliver mission critical data services, but with the addition of application of improved Quality of Service (QoS) assurances for the public safety sector and users.

Fig. 3. Near-Term public safety communication



C. *Long-Term FirstNet*

Ultimately, the First Responder network will offer mission critical voice services along with video and data. Voice services will be provided once Voice over Long Term Evolution (LTE) functionalities, meet or exceed mission critical requirements and standards. Part of the goal of the FirstNet team is to work with industry to ensure this is brought to fruition.

IV. Security Strategies and Protocols

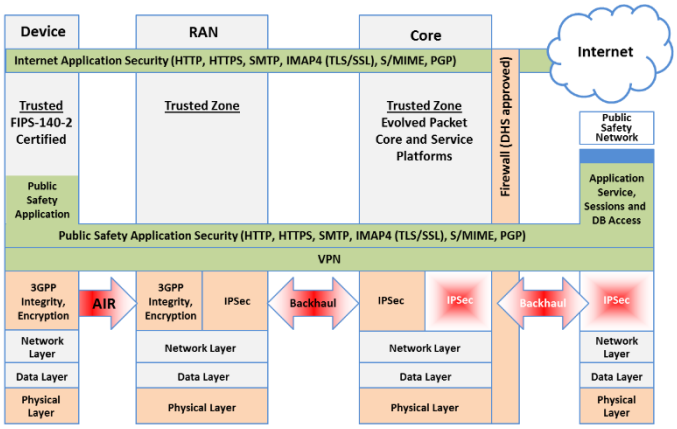
A. *Radio Access Network (RAN)*

There are fundamental changes between second-generation wireless telephone technology (2G) or third-generation wireless telephone technology (3G) and LTE in the way security is provided in a mobile network. There are four primary threats to a mobile IP based network:

- Insider attacks – the abuse of authorized user or administrator rights
- External attacks via IP based networks such as the Internet
- External attacks on physical access to the network on radio interfaces and tampering of small cells
- Attacks from mobile devices

To deal with these issues, LTE implements and utilizes IP security (IPsec) authentication and encryption between the eNodeB – referred to as a cell tower – and the core network. This is designed to protect the integrity of user traffic and network whenever the operator considers the backhaul network to be "untrusted."

Fig. 4. High Level Overview of Infrastructure to End User



IPsec is an open standards framework to help ensure private, secure communications over IP protocol through the use of cryptographic security services. IPsec supports network-level integrity, data confidentiality, data origin authentication, and relay protection. IPsec is integrated into Layer 3 of the Open Systems Interconnection (OSI) model so it provides security for almost all protocols in TCP/IP. IPsec provides a defense in depth against network based attacks from untrusted computers, data corruption, data theft, and user credential theft.

B. *Public Safety Devices*

Universal Integrated Circuit Card (UICC), also known as a SIM card, is responsible for running SIM and International Mobile Subscriber Identity (IMSI) applications. The UICC is the hardware storage location for sensitive information such as a pre-shared key K and IMSI. The IMSI provides subscriber identity which is unique for every subscriber. There is limited access to the UICC via a restricted Operating System application program interface (API) and the UICC performs cryptographic operations for authentication. The LTE network shall not grant access to a 2G or 3G SIM. By not allowing a 2G or 3G device to connect to the First Responder network, the chances of a bad actor mimicking a device is significantly reduced. Authentication and Key Agreement (AKA) protocol is used for devices to authenticate with the carrier to gain network access.

The device itself will also feature two layers of protection to ensure that the user of the device is an authorized users. For example, a device passcode must be entered to access basic features of the device such as text messages, phone, and personal address book. An additional more complex password must be entered

in order to access sensitive services such as mission critical applications, enterprise email, enterprise address book, etc. An example of an enterprise management security container that is used today would be Samsung KNOX. Samsung KNOX is essentially a privileged "container" within the phone that permits the authorized user to access mission critical data services and applications. Samsung KNOX can also be configured to establish a Virtual Private Network (VPN) connection to the mission critical services which would encrypt the data traffic in addition to the standard LTE encryption. By establishing the VPN connection, this ensures data would be secure even under a commercial network. Since devices on the First Responder network will need to be interoperable on commercial networks in the absence of the First Responder network, this capability would be essential.

C. *Applications*

In order to ensure security in public safety communications applications, there must be proper vetting of authorized applications and application settings on the devices. In order to prevent the installation of malicious applications, enterprise management will continually update a list of permissible applications for each specific container within the device. For example, some applications may be allowed to run after entering in the device passcode but not allowed to run behind a more secure container such as Samsung KNOX.

Applications that require web services should continue to make use of Hyper Text Transfer Protocol Secure (HTTPS). HTTPS is the protocol that allows communication between web server and web browser to view web pages securely through encryption. HTTPS uses a Secure Socket Layer (SSL) certificate to create a secure encrypted connection.

Applications that require server to application to server communication should continue to make use of Transport Layer Security (TLS). TLS protocols are located between the application protocol and the Transmission Control Protocol/Internet Protocol (TCP/IP) layer. It facilitates the securing and sending of application data to the transport layer. Since TLS works between application and transport layers, TLS can support multiple application layer protocols. In connection oriented transports, TLS allows the client and server applications to detect message tampering, message interception, and message forgery.

Applications that require messages with digital signatures and encryption will use Secure/Multipurpose Internet Mail Extensions (S/MIME). S/MIME is a protocol for sending digitally signed and encrypted messages. S/MIME is a way for the sender to authenticate the message to its recipients. It provides cryptographic security services for authentication, message integrity, and non-repudiation of origin. Such measures enhance privacy and data security.

V. IMPLEMENTATION INTO EXISTING COMMERCIAL NETWORKS

A. *Performance*

The four key questions regarding performance that will need to be researched are:

- How to manager priority access to the network?
- How to manage priority allocation of network resources?
- How to re-assign or pre-empt connected cell resources?
- How to ensure application performance during times of congestion?

FirstNet also works together with the Public Safety Communications Research to ensure these questions are addressed. One of the critical areas of testing is to develop priority and QoS framework for the network. On an LTE network, the critical resources are uplink and downlink bandwidth. A certain bandwidth is available for all users. However, uplink and downlink transmission speeds are asymmetrical because uplink speeds are dependent on the device where battery power is a significant limiting factor.

B. *Priority and Pre-emption*

Priority is the means by which users, applications, traffic streams or individual streams or individual packets take precedence over others in setting up a service session or forwarding packets during periods of congestion in the network. Public Safety users will require priority access to National Public Safety Broadband Network resources to make their communications an effective tool in the management of incidents and emergencies.

C. *Quality of Service (QoS)*

Quality of service is needed to ensure Public Safety users have access to their mission critical services and applications at the required level of quality for individual needs. Quality of service requires discrimination in the assignment of properties such as bandwidth guarantees, usage limits, latency, accuracy, accessibility and retention.

In order to maintain properly optimized quality of service for public safety users, these five key parameters must be considered:

- Access class allows the device to identify itself as a Normal, High Priority, or Emergency user and allows the device to understand when it is prohibited from connecting to the network.
- Allocation and retention priority allows the network to understand the priority of the user.
- Preemption capability and vulnerability indicators identifies which users can be preempted.
- Quality class indicator allows the network to understand the desired packet forwarding behavior of the Evolved Packet Core (EPC) barrier.
- Bit rate parameters allows the cell tower to schedule and grant bandwidth appropriately.

VI. Conclusion

Security in Public Safety Communications is a massive challenge of integrating multiple organizations and ensuring that mission critical data remains secure. The application of existing technologies, techniques, and protocols into the First Responder network has great potential of making such mission critical data secure in an Unclassified For Official Use Only environment.

VII. Acknowledgement

The author would like to acknowledge and sincerely thank those that provided assistance by proofreading and improving the quality and content of this paper. The author would also like to thank his professor for the opportunity to learn more about this important and relevant topic.

References

[1] "Guiding Principles: FirstNet will have effective security controls that protect data and defend against Cyber Threats," *FirstNet First Responder Network Authority*. [Online]. Available: https://www.firstnet.gov/content/firstnet-will-have-effective-security-controls-protect-data-and-defend-against-cyber-threats#Security. [Accessed: 05-May-2017].

[2] B. Schrier, "Band 14 in every cellular device?," *View from the Top*, 12-Jun-2013. [Online]. Available: http://urgentcomm.com/blog/band-14-every-cellular-device. [Accessed: 10-May-2017].

[3] "700 MHz Public Safety Spectrum," *Federal Communications Commission*, 27-Jun-2016. [Online]. Available: https://www.fcc.gov/general/700-mhz-public-safety-spectrum-0. [Accessed: 05-May-2017].

[4] P. Donegan, "White Paper Authentication as a Service for LTE Base Stations," *Heavy Reading on behalf of Symantec*, May-2012. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/white_papers/heavy-reading-authentication-as-a-service_WP.en-us.pdf [Accessed: 10-May-2017].

[5] "What Is IPSec?," *Microsoft TechNet*, 28-Mar-2003. [Online]. Available: https://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx. [Accessed: 05-May-2017].

[6] "How IPSec Works," *Microsoft TechNet*, 28-Mar-2003. [Online]. Available: https://technet.microsoft.com/en-us/library/cc759130(v=ws.10).aspx. [Accessed: 05-May-2017].

[7] M. Bartock, J. Cichonski, J. Franklin, "LTE Security – How Good Is It?," *National Institude of Standars and Technology*. [Online]. Available: http://csrc.nist.gov/news_events/cif_2015/research/day2_research_200-250.pdf [Accessed: 10-May-2017].

[8] "SSL versus TLS – What's the difference?," *The LuxSci FYI Blog, LuxSci*, 19-Jul-2016. [Online]. Available: https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html. [Accessed: 07-May-2017].

[9] "S/MIME for message signing and encryption," *Microsoft TechNet*, 09-Dec-2016. [Online]. Available: https://technet.microsoft.com/en-us/library/dn626158(v=exchg.150).aspx. [Accessed: 07-May-2017].

[10] "Transport Layer Security protocol," *Microsoft TechNet*, 12-Jun-2014. [Online]. Available: https://technet.microsoft.com/en-us/library/dn786441(v=ws.11).aspx. [Accessed: 07-May-2017].

[11] T. Messer, "HTTP vs. HTTPS: What's the Difference and Why Should You Care?," *Entrepreneur*, 15-Sep-2016. [Online]. Available: https://www.entrepreneur.com/article/281633. [Accessed: 07-May-2017].

[12] "AT&T Selected by FirstNet to Build and Manager America's First nationwide Public Safety Broadband Network Dedicated to First Responders," *AT&TNewsroom*, 30-Mar-2017. [Online]. Available: http://about.att.com/story/firstnet_selects_att_to_build_network_supporting_first_responders.html. [Accessed: 10-May-2017].

[13] "Priority, Pre-emption, and Quality of Service Tutorial: LTE Basic Concepts," *First Responder Network Authority*, 29-May-2015. [Online]. Available: https://www.firstnet.gov/newsroom/blog/priority-preemption-and-quality-service-tutorial-lte-basic-concepts. [Accessed: 05-May-2017].

[14] "Priority, Pre-emption, and Quality of Service Tutorial: LTE Key Concepts," *First Responder Network Authority*, 09-Jun-2015. [Online]. Available: https://www.firstnet.gov/newsroom/blog/priority-pre-emption-and-quality-service-tutorial-lte-key-concepts. [Accessed: 05-May-2017].

[15] "Public Safety Communications Research Division: About PSCR," *NIST*, 09-Nov-2016. [Online]. Available: https://www.nist.gov/ctl/pscr/about-pscr. [Accessed: 10-May-2017]