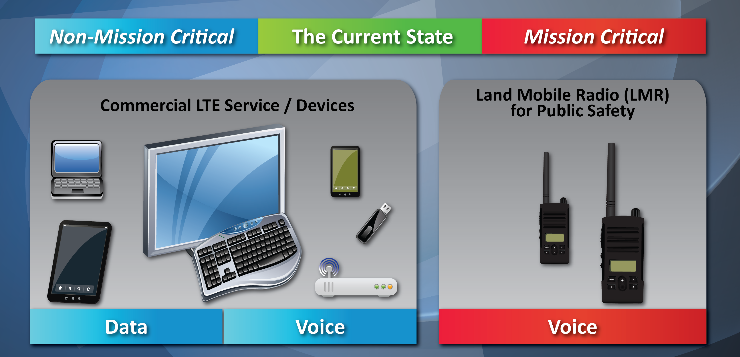
# Security Issues in Public Safety Communication Networks

## Introduction

Public safety communication networks are poised for a dramatic evolution from the traditional Land Mobile Radio 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 Creation Act (MCTRJC) of 2012 required FirstNet, a government managed next generation public safety communication network initiative known as the First Responder Network Authority, to build, operate, and maintain the first high speed nationwide broadband network dedicated to public safety. However, the exponentially increasing amount of sensitive data being transmitted over networks being utilized for the public safety mission caused great concern over the protection and security of such data. This project proposes ways in which such data can be protected on the FirstNet network.

### Current State

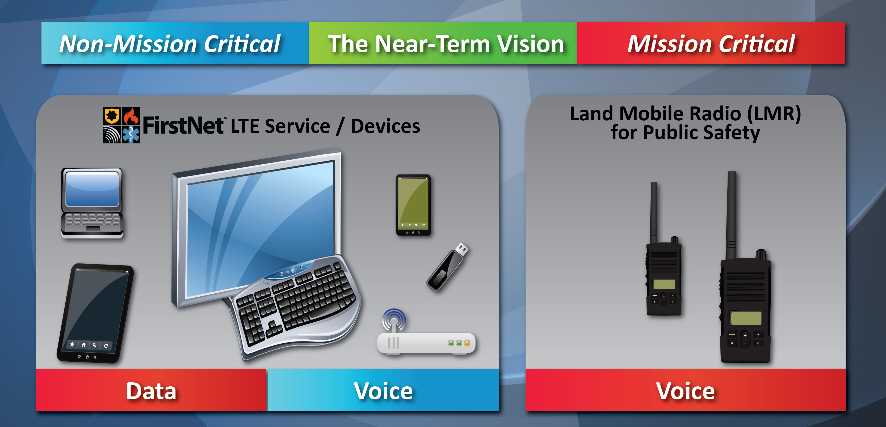
Currently, first responders are relying on Land Mobile Radio networks to provide mission critical voice communications. These Land Mobile Radio networks generally meet first responder’s needs to have a guaranteed priority access to mission critical voice services. However, most first responder organizations require mobile data services and applications which are being provided exclusively by commercial carrier data connections. Unfortunately, utilizing these services and applications requires the sharing resources with the commercial network which creates significant and ongoing concerns regarding the ability to prioritize such demands appropriately.



### Near-Term FirstNet

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

However, in March 2017, FirstNet selected AT&T to build and manage FirstNet. The vision for FirstNet has not changed, although, its implementation has been modified. FirstNet will continue to use commercial infrastructure to deliver mission critical data services with the application of improved Quality of Service (QoS) assurances for the public safety sector and users.



### Long-Term FirstNet

Ultimately, FirstNet will offer mission critical voices services along with video and data. Voice services will be provided once Voice over Long Term Evolution functionalities meet or exceed mission critical requirements and standards.

## Purpose

The purpose of this project is to propose techniques, technologies, and protocols which FirstNet can adopt and implement inn order to protect and secure mission critical data that traverses the network. Security will be designed into all radio access networks, devices, and applications used on FirstNet. Firewalls will enforce stringent security policies developed in cooperation with Department of Homeland Security and Department of Defense to meet National Institute of Standards and Technology requirements. The FirstNet design will be using 3rd Generational Partnership Project standards for encryption as well as other security measures and best practices.

### Items of Interest

#### Radio Access Network

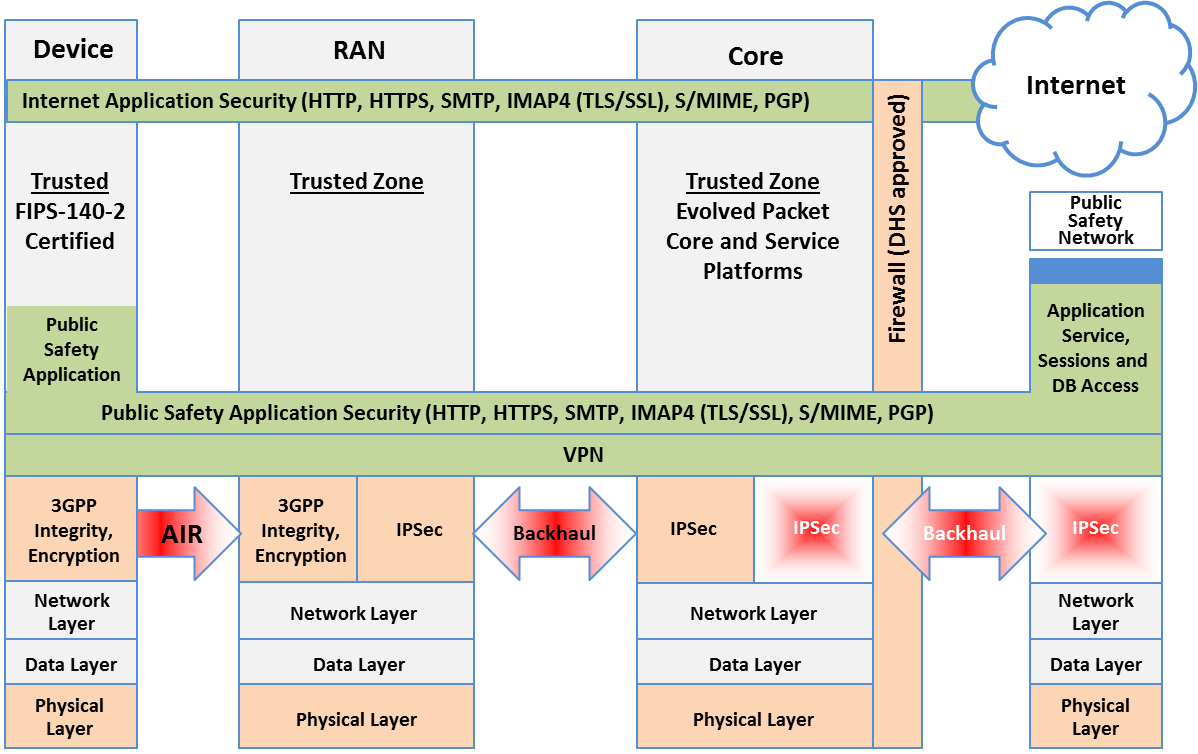
This consists of the radio base station infrastructure that will connect user devices to the network. These may include cell towers as well as hotspots embedded in vehicles.

#### 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 any other specialty device. Industry will develop device types 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.

#### Applications

These are the software applications that end users will use in order to access the services they need. FirstNet 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 FirstNet.



## Radio Access Network (RAN)

There are fundamental changes between 3G and LTE in the way security is provided in a mobile network. There are four primary threats to a mobile IP based network:

1. Insider attacks – abuse of administrator rights
2. External attacks via networks such as the Internet
3. External attacks on physical access to the network on radio interfaces and tampering of small cells
4. 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 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”.

IPsec is an open standards framework to help sure private, secure communications over IP protocol through the use of cryptographic security services. IPsec supports network-level integrity, data confidentiality, data origin authentication, and replay protection. IPsec is integrated into Layer 3 of the Open Systems Interconnection 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.

## Public Safety Devices

Universal Integrated Circuit Card (UICC), also known as a SIM card, is responsible for running SIM and IMSI applications. The UICC is the hardware storage location for sensitive information such as a pre-shared key K and International Mobile Subscriber Identity (IMSI). The IMSI provides subscriber identity which is unique for every subscriber. There’s limited access to the UICC via a restricted Operating System 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 FirstNet, the chances of a bad actor mimicking a device is significantly reduced. Authentication and Key Agreement 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 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 FirstNet will need to be interoperable on commercial networks in the absence of FirstNet, this capability would be essential.

## 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 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.

## Performance

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

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

FirstNet also works together with the Public Safety Communications Research. One of the critical areas of testing is to develop priority and quality of service 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.

### 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.

### Quality of Service

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:

1. 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.
2. Allocation and retention priority allows the network to understand the priority of the user.
3. Preemption capability and vulnerability indicators identifies which users can be preempted.
4. Quality class indicator allows the network to understand the desired packet forwarding behavior of the EPC barrier.
5. Bit rate parameters allows the cell tower to schedule and grant bandwidth appropriately.

## 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 FirstNet has great potential of making such mission critical data secure in an Unclassified For Official Use Only environment.

## References

* <https://www.firstnet.gov/content/firstnet-will-have-effective-security-controls-protect-data-and-defend-against-cyber-threats#Security>
* <http://urgentcomm.com/blog/band-14-every-cellular-device>
* <https://www.fcc.gov/general/700-mhz-public-safety-spectrum-0>
* <https://www.symantec.com/content/en/us/enterprise/white_papers/heavy-reading-authentication-as-a-service_WP.en-us.pdf>
* <https://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx>
* <https://technet.microsoft.com/en-us/library/cc759130(v=ws.10).aspx>
* <http://csrc.nist.gov/news_events/cif_2015/research/day2_research_200-250.pdf>
* <https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html>
* <https://technet.microsoft.com/en-us/library/dn626158(v=exchg.150).aspx>
* <https://technet.microsoft.com/en-us/library/dn786441(v=ws.11).aspx>
* <https://www.entrepreneur.com/article/281633>
* <http://about.att.com/story/firstnet_selects_att_to_build_network_supporting_first_responders.html>
* <https://www.firstnet.gov/newsroom/blog/priority-preemption-and-quality-service-tutorial-lte-basic-concepts>
* <https://www.firstnet.gov/newsroom/blog/priority-pre-emption-and-quality-service-tutorial-lte-key-concepts>