5/2/2012

FCC TAB Input

Public Safety Networks and LTE Security Considerations

Anton Kaska, Nokia Siemens Networks

FCC TAB Input

Public Safety Networks and LTE Security Considerations

Nokia Siemens Networks (NSN) is the leading LTE Network solution provider in the world with 54 current networks deployed. As a result of significant investment and development work over the past several years in securing LTE networks, we look to provide input specific to a holistic security approach to be used by the Commission for its success in leading public safety network efforts.

This input is organized with an introduction including some risks and threats, the transport layer, evolved packet core, end device considerations, some key interoperability challenges, and ends with some "soft" considerations such as training and assessments.

Introduction

Understanding the differences between existing LMR, 2G/3G, proposed 4G LTE Networks and specifically how they communicate and function is key to understanding the risks and dangers that FirstNet will be exposed to.

Knowledge of how the network functions between User Equipment (UE), the radio access network, and the core (and the inter-operability between networks) is required to properly address the risks posed to our infrastructure with such deployments.

Confidentiality, Integrity and Availability can be strengthened and risks mitigated to acceptable levels with proper attention to planning, design, implementation, and operation of FirstNet.

Previously, IP traffic did not travel outside the mobile core as in figure 1 below and protective measures were mainly accomplished by actions taken that were core-centric such as firewalls and content security measures applied in the core and on its various edges.

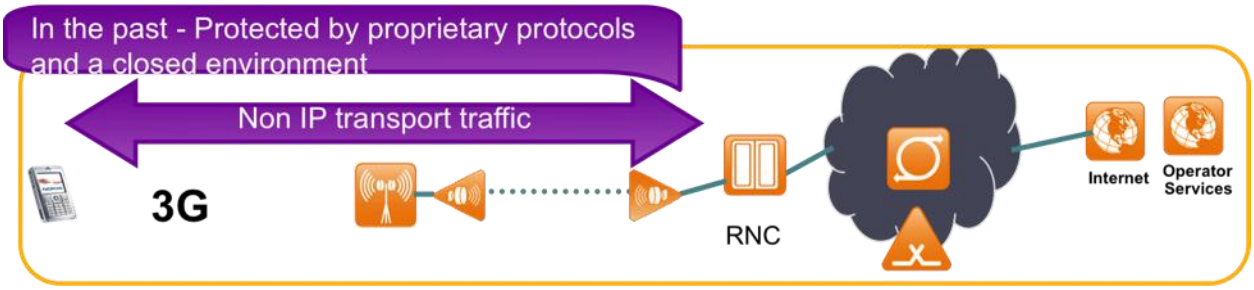

Figure 1

With the advances of LTE, and now legacy 2/3G network evolution, IP traffic travels outside the core terminating within the radio via interfaces on the radio itself (not at an additional device at the tower or bunker/building) as in figure 2 below. In previous mobile network design, IP traffic traveled within the core, the Internet, etc. but never traveled out to the actual radios as it now does. This is the major difference between the network types and what changes the risks associated with mobile networks.

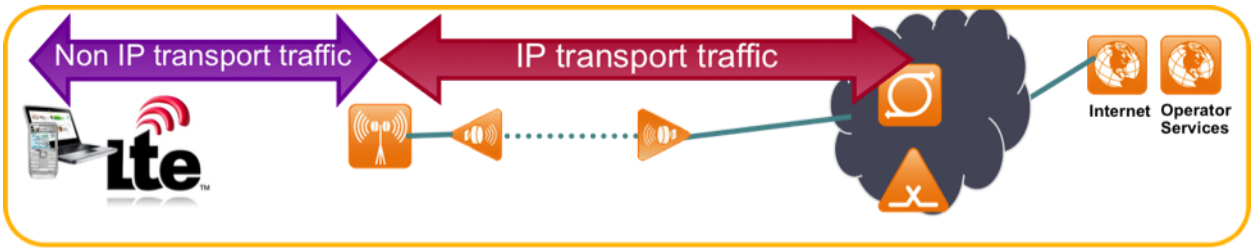

Figure 2

Architecture is key to not only security and successful interoperability of such networks, but also in keeping associated costs down. LTE deployments offer many different methods in which to architect the system and maximize security control points, availability, and flexibility.

The move to LTE networks also presents additional concerns that need to be fully understood by architects, designers, deployers, and operators etc. whom have not previously worked with such networks. Subscriber Data management and security is a clear area where there are additional requirements must be defined and controls that must be deployed.

Threats to LTE network deployments include but are not limited to:

Denial of Service Attacks (IP and Radio based)

eNodeB Spoofing

Eavesdropping of user traffic

Unauthorized access to eNodeB and/or other network elements

These threats can impact the network, its operators and the users in many ways including lack of user participation in FirstNet, inability of first-responders to communicate and operate to their full effectiveness, or even the ability of criminal or hostile intelligence assets to monitor activity on FirstNet.

Simple examples of potential threats could include spoofed radios "proxying" communications or simply not passing it on, physical tapping of networks inside bunkers or via exposed radios on public works type sites typical in such deployments, etc.

Section Summary Points

1. *LTE moves IP traffic outside the core, all the way to the radio which creates new security concerns.*
2. *Security knowledge of LTE Security and its affects to include the core, are critical to architecting a safe and successful system.*

Transport

Transport Security requirements within 3GPP include at least 3 new areas with LTE which are Network Domain Security, Security Architecture and an Authentication Framework as outlined below in figure 3.

Figure 3

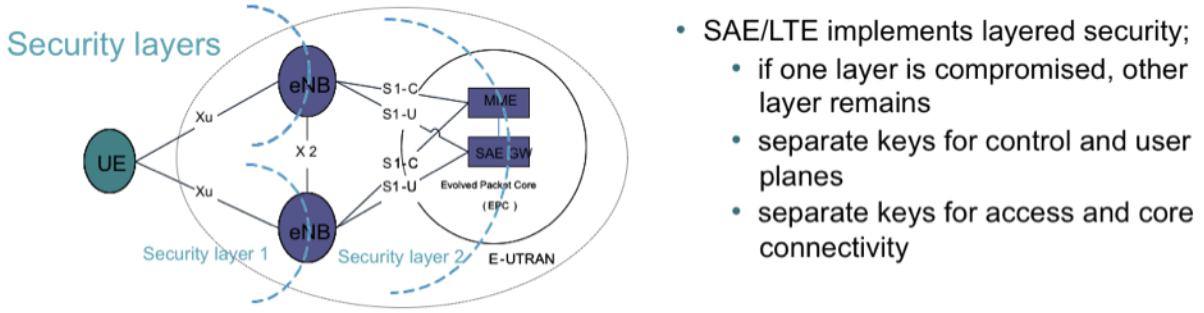

Figure 4

These requirements can and are addressed in network deployments that adhere to these standards and demand high levels of security. They can be simplified for understanding in that one requires IPSEC tunnels off the radio interface and continuing to the core as opposed to from some device at the radio site that is collocated and connected via cable such as a fiber link and that one requires a certificate authority and deployment that is both 3GPP compliant as well as flexible to allow for cross signing between entities at many levels.

Developments in the tapping of fiber are quite advanced and thus, proper adherence to the standards and terminating of tunnels on the interface is ***key*** to maintaining security and avoid risk of surreptitious monitoring.

Additional requirements include specifications for controls on certain traffic types and ability to encrypt traffic within traffic to allow for higher levels of security (e.g.; the ability to use FirstNet by entities requiring US Secret type protections within the network concurrently)

For additional clarity, figure 5 below depicts additional detail on the C Plane (Control Plane) and U Plane (User Plane) protections.

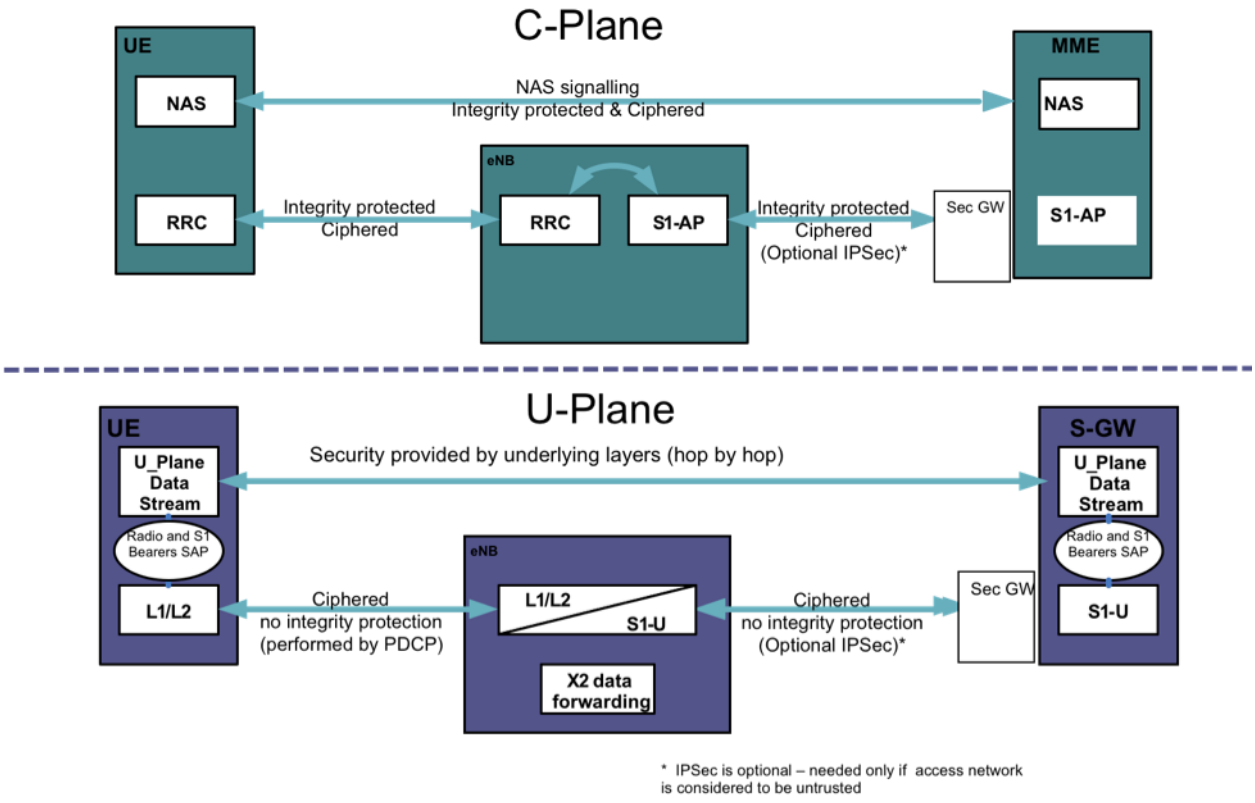

Figure 5

Evolved Packet Core (EPC)

Introduction of an Evolved Packet Core or "EPC" as will occur with FirstNet will result in additional security challenges that are different from those faced in both traditional mobile cores (2G/3G) and those found in typical public safety "Enterprise" security challenges that have supported the Back Office and/or LMR deployments.

If, as is expected, there are users with their own EPC's, the interoperability challenges are significant but not unachievable. Large mobile providers are beginning to work to alleviate risks associated with such challenges and while they have some way to go, the integrators already have been looking at and solving many of these as has the US National Security Agency as the Department of Defense works to build and integrate these evolving networks.

Leveraging current government efforts as well as telecom industry innovation in risk reduction and security will be one of the keys to ensuring deployment of stakeholder EPC's that are interoperable and meet Confidentiality, Integrity and Availability requirements.

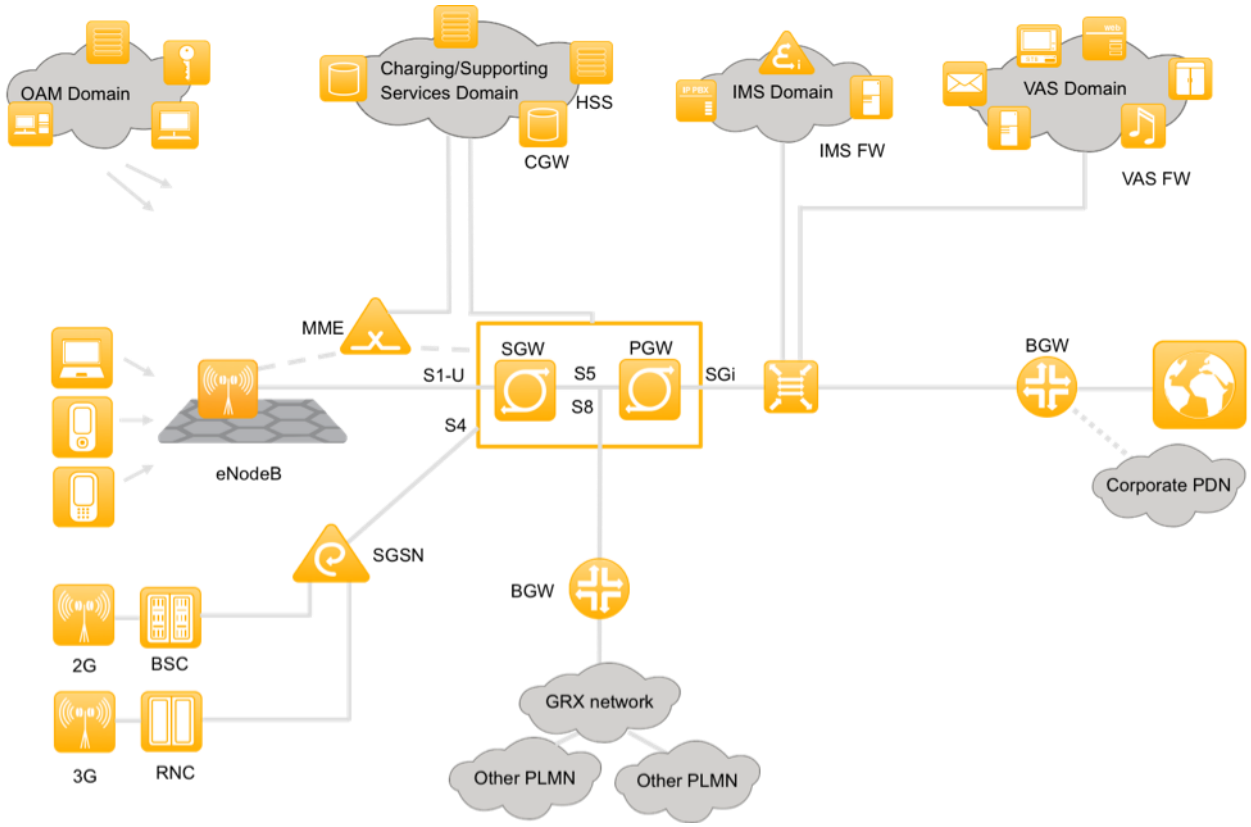

Figure 6

As one can see in figure 6 above showing a typical EPC deployment, adding interaction with other stakeholder cores, a redundant FirstNet core, and even connections with potential non-FirstNet networks in cases of roaming to "normal" LTE networks where there is no FirstNet coverage, an LTE Core Security architecture will require a high level of flexibility, redundancy, and compliance with standardization in use at present and in the future.

Major differences with previous mobile cores and LTE EPC's include a flat and all IP network, simplification of the individual core, and strong design drivers of low latency (critical) and high throughput. These differences pose some unique challenges to security architects of such networks.

While an Evolved Packet Core has many ingress and egress points and users will be secured to the core there are further trials. Within each domain in figure 6 above, there are additional security requirements depending on the risk the domain is subjected to with the value of its data. Deployment of communication specific Secure DNS solutions (3 at minimum in typical core), content security and/or filtering of traffic between specific zones, firewalling of some if not all domains, etc. will be required.

Access technologies in FirstNet are expected to share a common core network as well as distributed cores.

Threats to individual and FirstNet core(s) will include all standard IP threats with the addition of newcomers to emergency responds as a result of additional attack-vectors available as shown in table 7 below.

SPAM OVER INTERNET TELEPHONY (SPIT)	**SPAM OVER INSTANT MESSAGING (SPIM)**
FRAUD AND THEFT OF NETWORK RESOURCES	**CRIMINAL ELEMENTS WITH SIGNIFICANT RESOURCES TO INVEST**
FOREIGN GOVERNMENT INTELLIGENCE	**ANARCHIST/ORGANIZED ATTACKS ON COMMUNICATIONS**

Figure 7

Security measures for minimum deployment should include:

- Authentication and Access control system for users that are portable and flexible to facility interoperability in **all** use cases
- Subscriber data management security. The data that is used by stakeholders, their devices, their applications, etc. that is used, shared either in whole or part depending on the entity, etc. must be able to have enforceable attributes that allow for use case deployment and operation. This is one of the more significant technical challenges and Telecom equipment provider expertise in this area will likely be heavily leveraged for success. (e.g.; cases where an entity can only share part of the information they have for security or safety reasons). Attack vectors (DDoS for example) will

have a network to use that has low latency, high resiliency and maximum throughput unless this is addressed appropriately. Capabilities for some existing telecom solutions in this area include:

- Mobile Number Portability
- SIM based authentication
- User Repository
- Multi Access Subscriber Authentication
- IMS User repository
- "Other" user type repository (vehicular systems, air asset systems, etc)

Interface security and the guaranteeing the confidentiality of data are key

Secure Design of the radio access network is critical when developing intercept gateway architectures.

- Architecture Components
  - Perimeter Measures
    - Operations and Maintenance
    - Charging and Support Services
    - IMS Domain
    - Value Added Services Domain (VAS) which in PSN may include support for EMS or LI specific applications
    - Entity Operational Network Connections (e.g.; Internal City/State/etc. network connections)
    - GRX (roaming)
  - DNS Security
    - MME, SGi, OSS, and S8 interface at a minimum in addition to domain separation requirements discussed elsewhere in this section.
    - Simple and flexible
      - To operate
      - Fast to upgrade/update
      - Central Management
      - Built in security functions/features
      - Full high availability configurations and functionality
      - Forward and caching functions to optimize multiple flows
      - Properly architected deployment to mitigate DNS tunnel traffic
  - Content Security
    - Protect Content
    - Scanning of multiple bearers for such threats as malware, spam, virus, phishing, etc.
      - MMS
      - SMS
      - Messaging
      - Email
      - HTTP (URL, filter, anti malware)
      - FTP/TELNET
      - Point-Multipoint applications

        - Custom/Legacy Applications
    - Deep Packet Inspection and Intrusion Detection
        - Used for security, performance and QoS reasons
            - Maximize use of available bandwidth during events
            - Mitigation of new (zero day) attacks
            - Avoidance of service outages on EPC(s)
            - Prioritize traffic based on event, entity priority, etc.
            - GTP awareness is required for roaming support (current versions and fast track of development to support version change)

Section Summary Points

1. *Successful addressing of security architecture elements*
2. *LIG Deployment with attention to architecture gotcha's*
3. *Subscriber Data Management Security including interface and confidentiality of data in multi-entity and multi security level environments*
4. *Special attention and effort given to authentication and access control security and functional requirements*

End Devices

End device or User Equipment security within FirstNet will present some very specific challenges to an area that is just beginning to be addressed with success in commercial networks. Areas of consideration with end device security include:

- Types of device such as Vehicle, Handset, Aircraft, Fixed/Office System, etc.
- Proper Layering of security across all attack vectors
- The lack of comprehensive solutions in the marketplace

The varying device types expected to be deployed in FirstNet will result in multiple operating systems, multiple versioning, different application software types, connectivity to supporting system data that likely will reside outside FirstNet which may be of higher security classification (or lower).

Attack vectors present may be new to some security architects if they have not previously worked with 4G/LTE networks. This is an important point to mention since in North America, this subject has not

been fully addressed in current network deployments and will result in a reduced knowledge base from which to draw on for the needed security architecture and even approaches to addressing the risks posed.

Potential attack vectors include but are not limited to:

MMS (Virus, Phishing, Spam, DoS, etc)

SMS (Virus, Phishing, Spam, DoS, etc)

**Note: Spam across SMS vectors is a service affecting issue on some networks in N. America*

Web Surfing/Browsing (Filtering, Blacklisting, Malware delivery, virus, phishing, etc)

VoIP (Virus, Phishing, Spam, DoS, Monitoring, etc)

Email (Virus, Phishing, Spam, DoS, etc.)

Other applications such as video streaming (entire range of attacks)

As mentioned in the section covering the Evolved Packet Core or EPC, many of these threats can be addressed in the core or network, however proper security architecture and approaches demand a layered approach and are warranted. End devices can be physically attached to <any> other device that provides an appropriate physical interface (serial, USB, Network, Bluetooth, Wireless/802.11, etc).

Preventing such connections above will not be possible. Security is always best-possible and rarely 100% so the best possible approach (layered) should be taken in this case. Additionally, there are special needs of end devices such as remote-wipe capability and the ability to identify missing/pilfered/compromised devices and then either track their location and movements or prohibit them from authenticating on the network, accessing network resources, or presenting themselves as secure elements on the network when they are not (example, a vehicle that has been physically compromised and trying to join the network in another area)

A typical application of client or end-device applied security is depicted below in figure 8.

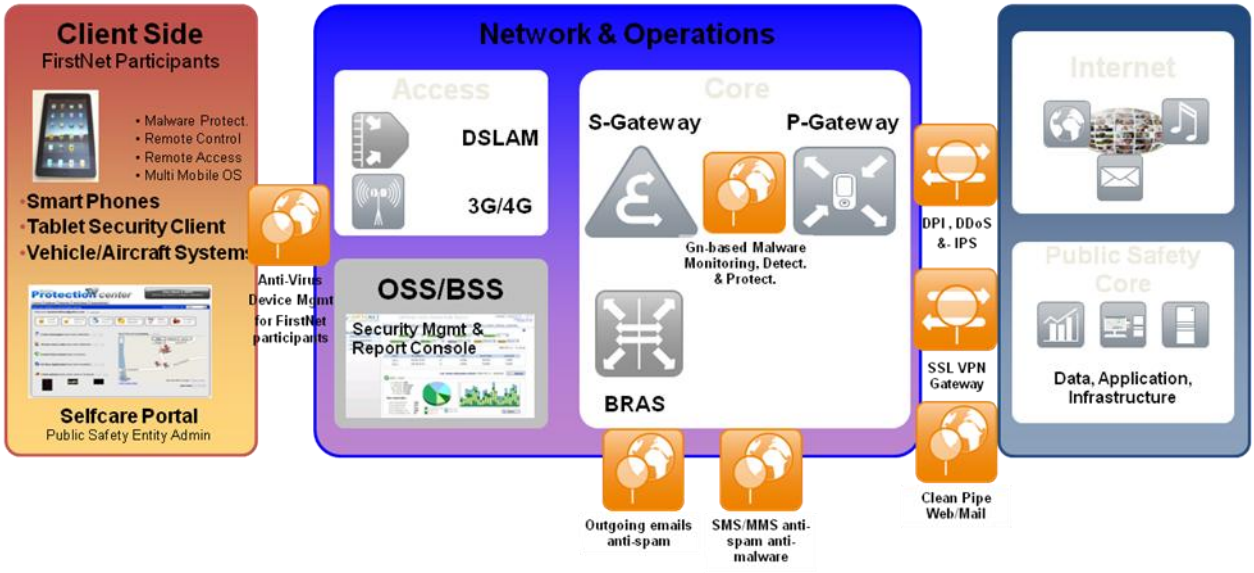

Figure 8

It should be noted that end-device challenges can be addressed either by a Cloud Based approach or serviced/operated by FirstNet. This poses significant privacy challenges by individual stakeholders with their own solutions. More feasibly this would be by an entity (FirstNet operated?) offering a Cloud Based approach in a multi tenancy environment. These environments provide both separation/privacy of various states/entities as well as a centralized / cloud approach to leverage investments, economy of scale, and management/monitoring. Such a Cloud Based approach (leveraging multiple best-in-breed vendor solutions) in a common platform have significant advantages as shown below in figure 9.

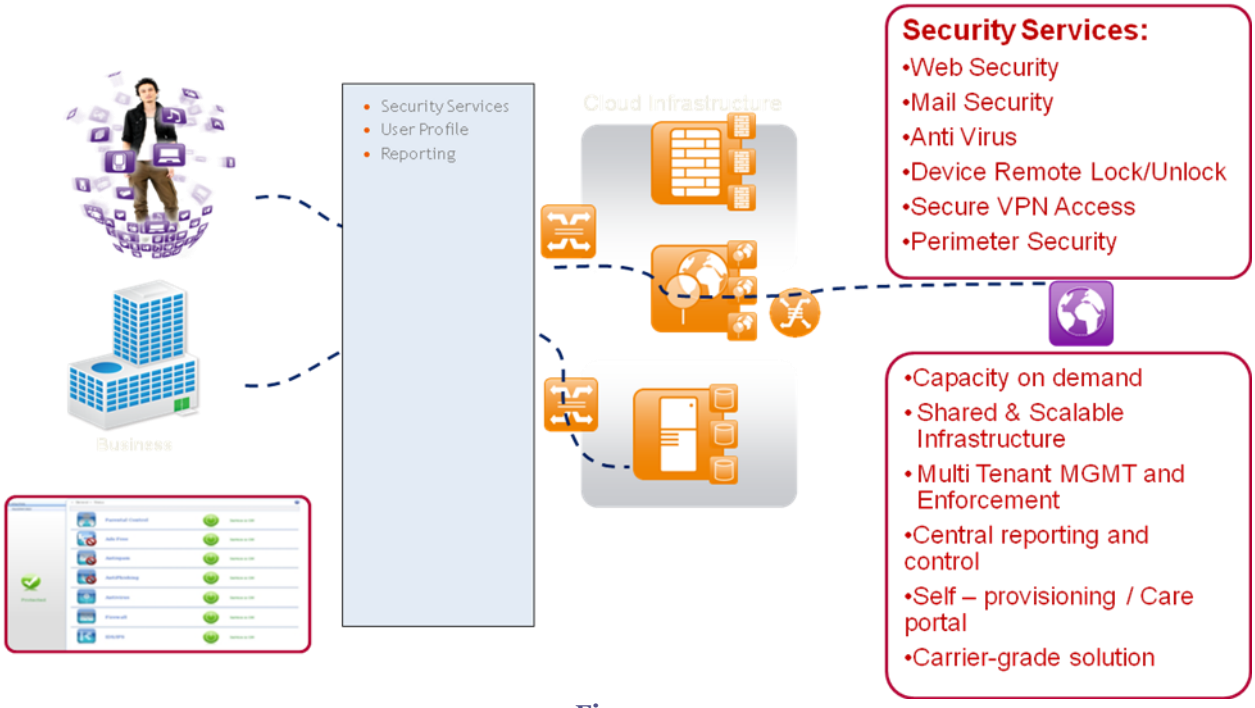

Figure 9

Section Summary Points

1. *Multi-Vector and Multi Layer security is critical including mail, SMS, MMS, Web/HTTP, VoIP, Email, Video, etc.*
2. *Remote wipe capability*
3. *Remote Tracking of compromised/stolen/etc. devices participating in FirstNet*
4. *Cloud Based Multi-Tenancy platform to leverage economies in scale for price as well as management and monitoring*

Key interoperability challenges

Interoperability will either make or break FirstNet acceptance, uptake in use, and continued operation and is arguably the main reason that a FirstNet like capability is needed.

The ability to communicate effectively in any situation is key to being able to successfully handle incidents of any type. While individuals have strong competencies, bringing together those competencies is what makes a successful response to a situation successful.

Interoperability within an LTE Network, utilizing as-yet developed user end devices, will present significant technical security challenges which, if not thought through carefully in the initial stages, can result in tremendous cost overruns, introduce in security risk to our nation's first-responder network, and in the end, could result in the demise of FirstNet.

A non-exhaustive selection of interoperability challenges facing FirstNet and their associated risks is outlined below.

Challenge	Risk / Issue
End User Equipment	Multitude of hardware and OS types introduces significant challenges that likely will NOT be addressed in timely fashion resulting in other mitigation factors being required
Roaming to non-secure LTE networks	Need for communication with our partners in Canada & Mexico as well as non-FirstNet Secure networks for Mutual Aid/LEA and different acceptable standards (e.g.; Use of network components that are forbidden in US Public Safety Networks
Roaming	Roaming as needed in areas of limited FirstNet coverage onto commercial providers
Capacity	Capacity in large scale incidents dictates the network be architected for resiliency and prioritization (multiple levels: city/state/federal, roamer vice home network, police versus fire, etc.)
Privacy and Security	There WILL be a requirement for multi-level, multi-entity, multi-device type, etc access control systems that are both portable and flexible as well as being affordable
Lawful Intercept	Lawful Intercept capabilities must be considered in legal perspective with all entities.
Multi-Level Security Needs	There are clear use cases where multi levels of security will be required (e.g.; Confidential/Secret etc.) and presently there are some technical limitation when architecting such systems with more than "n" entities.
Cost	Multiple end users/groups have privately discussed a concern around the cost of participation, the need to have open applications in order to reduce cost etc.

There are many groups and organizations discussing FirstNet interoperability with regard to security and all are producing some notable results. The DHS Office of Emergency Communications (OES) along with the National Cyber Security Division(NCSD) and National Communications System (NCS) efforts

bringing together both industry and government, operators and users, integrators and others with concerns is uncovering many interoperability specifics and their combined output should be carefully reviewed. The output DHS etc. are developing is more comprehensive than that found in this document.

Section Summary Points

1. *The plethora of end user equipment found in FirstNet will require additional mitigation factors-dictating types of end-user equipment, OS versions etc. will result in lack of support for FirstNet and excessive overhead for participants.*
2. *Foreign Participation (Canada/Mexico/EU) will have issues with regard to lawful intercept platforms and non-approved hardware and vendor platforms. Additional interoperability studies and recommendations will be required.*
3. *Roaming Method of Operations off FirstNet will require analysis, recommendations and determinations of acceptable risk.*
4. *Capacity and prioritization of use will need to be clarified, including state or entity owner of net vice roamer.*
5. *Portable access control and authentication systems need minimum acceptable requirements identified (significant and time consuming effort given lack of user cases, etc.)*
6. *Multiple Security level capability needs to be architected in system from day 1- significant potential variances in designs will require additional research.*
7. *Cost needs to be monitored for end users-success of FirstNet requires users, users must be able to afford participation and all associated costs of a "typical" rural user must be monitored.*

Training, Assessment, and Security Operations

As with all large system deployments, a part of the solution is ensuring that with a plan-develop-implement and operate approach, that the "operate" does not fall by the wayside. Operation when talking about security includes training as well as constant assessments.

Within FirstNet, there will be a need for initial training across the participant spectrum, from the board down through individual users. Additionally, there will need to be recurring security training developed and required, so-called "refresher" training that will occur at a minimum, on an annual basis. This training should include topics such as new developments in technology and the threats they face, an overview of the applicable security policies, etc. and may vary across classes of stakeholders (first responders, intelligence, operations, management, etc.)

Assessments, as with training, are a security process that is never-ending. Following initial assessments and green-lighting prior to launch of FirstNet, there needs to be a regular scheduled set of random assessments across the entire FirstNet Ecosystem. Care must be taken to ensure adequate time for assessment-corrective action- reassessment processes to take place in a timely manner that does not affect launch date deadlines (ensure to leave enough time for assessment and corrections before launch dates).

Section Summary Points

1. *Ensure effective initial security training is developed for all levels of FirstNet Participation.*
2. *Ensure adequate recurring training is funded, developed, scheduled, required, and participants are trained to standard.*
3. *Plan enough time for comprehensive initial and scheduled assessments.*
4. *Allow for corrective action and re-assessments when developing project plans.*

Summary

The challenges in architecting FirstNet are fairly significant with regard to security; however they are not such that they cannot be overcome when leveraging current industry and Department of Defense expertise. Both must be leveraged to take advantage of current market developments and solutions as well as using solutions to some problems the Department of Defense has already overcome in order to ensure success.

The "Section Summary Points" tables following each section in this document are intended to provide overseers a clear overview of some of the notable highlights and it is the hope that this will stimulate further discussion and assist in guiding the coming decisions, design and architecture.