CYBER SECURITY FOR LONG TERM EVOLUTION

PUBLIC SAFETY NETWORKS TODAY AND TOMORROW

by Greg Harris,
CIO/G6 CISSP, CAPM, CompTIA Sec+ 2008
Product Manager, Cyber and Information Assurance Solutions
Harris Corporation - Public Safety and Professional Communications (PSPC)

HARRIS®
assuredcommunications®

Cyber Security for Long Term Evolution

Security has become an increasingly important capability for any of today's communications networks, but it has acquired a new and increased level of significance when considered in the context of mission-critical public safety communication networks, and the emergence of LTE (Long Term Evolution) technology. LTE technology is the designated technology of choice by the Federal Communications Commission (FCC) and the broad public safety community to support implementation of fourth generation (4G) broadband networks in the 700 MHz spectrum for public safety.

Legacy mobile networks were largely based on Time-Division Multiplexing/Asynchronous Transfer Mode TDM/ATM transport networks in their wired part. With the wide-scale migration to IP-based transport networks, awareness of and protection against IP-related threats becomes not just increasingly relevant, but essential.

Cyber attacks against all commercial networks have been on the rise in recent years. According to the Identity Theft Resource Center, in 2010, more than 662 security breaches exposed 16.1 million records.[i] And those are just the reported breaches. Significantly, targets for cyber attack will not be limited to commercial networks. The sophistication and frequency of cyber attacks will likely grow over the next few years and those attacks will increasingly seek to penetrate mission-critical communication networks. If not checked, they could have devastating effects, compromising the missions of first responders and even eroding public confidence.

"Cyber attacks against all commercial networks have been on the rise in recent years."

In public safety communications, the dependent relationship between the mission and the reliability and security of the communications network cannot be overstated. Public safety first responders depend on the 24x7 availability of their communications network. It must be available when needed, without exception. Weak and compromised network security reduces reliability and ultimately availability. In today's cyber world, without the proper security measures and features in place, no amount of physical reliability features, such as site hardening and backup power, can guarantee the highest degree of availability required of public safety communications networks.

Our public safety and government partners face rapidly expanding vulnerabilities from network-based attacks, increasing the risks of: loss of mission critical data, denial of service, data corruption, and other damage to systems and infrastructure. Information Assurance (IA) addresses the myriad of threats that impact mission-critical communication systems. Information Assurance is the discipline of protecting information system (IS) resources from malicious and unintended uses, misuse and exploitation while ensuring their availability, integrity, and operational capabilities of intended users, and their mission. First responders rely on a partner that can implement comprehensive Information Assurance (IA) solutions.

Introduction

As public safety agencies extend their communications capabilities from Public Safety Land Mobile Radio (LMR) Project 25 (P25) to the additional data capabilities provided via LTE, security becomes even more important. Even with private LTE networks, public safety agencies may be relying on external providers for data segregation, data privacy, privileged user access, availability, and recovery. Location independence, coupled with the possibility of a service firm as the provider of subcontracted services, creates risks that go beyond the reach of the typical approach to security.

"As public safety agencies extend their communications capabilities... security becomes even more important."

This is especially relevant for an evolved packet core (EPC), which is based on IP transport on all its wired links. While EPC makes the network very efficient, it also requires comprehensive and verified security architecture to ensure protection against the diversity of threats that jeopardize mobile networks, in particular IP-related cyber attacks.

Interoperability requirements and industry standards have driven many industries toward improved and complex security postures as well as enhanced interoperability. The same holds true for networks built with LTE technology. The solution to address this complex security concern is Information Assurance (IA). In its broadest sense, public safety IA for LTE addresses the full range of security issues and risks that could affect the day-to-day operations of public safety agencies today and tomorrow. The requirements of LTE for public safety can make the challenge to provide the highest level of security even more complex. The most common LTE network deployments for public safety will most likely integrate those first responder LTE networks with other private networks, and potentially with commercial networks and LTE carriers. The importance of IA in this type of communications environment is rapidly capturing the attention of public safety agencies across the country and at the Federal government level. In fact, IA for LTE networks is being formally addressed by the proposed governing agencies responsible for LTE security.

Local public safety agencies also are governed by certain federal laws that relate to security. The two major laws are the Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS). HIPAA mandates the privacy and security of medical records, which means that first responder emergency medical services personnel must be able to use applications and devices that can recognize and conform to HIPAA requirements. CJIS has mandates and guidelines for limiting access to criminal justice information and is widely used by law enforcement practitioners.[ii]

The Changing Landscape of Threats

"LTE networks supporting public safety agencies in today's world face unprecedented challenges and threats."

LTE networks supporting public safety agencies in today's world face unprecedented challenges and threats. The reliability of wireless networks in support of public safety operations can literally mean the difference between life and death for responders and a community's citizens. More than ever, the success of U.S. homeland security heavily depends on effective communication among federal, state, county, and local agencies when and where it is needed. Those responsible for protecting the integrity of Public Safety LTE networks must have the experience necessary to properly secure them through the risk management, industry best practices, and strong standards needed to ensure network confidentiality, integrity, authentication, availability, and non-repudiation.

In the past, communication networks used by public safety agencies were circuit switched and built on proprietary implementations. They were closed systems, a term that means they operated independently and were not connected to any other networks. In contrast, today's systems are often inter-networked and rely upon IP-based networking that utilizes standard ports and protocols, and takes advantage of commercial-off-the-shelf (COTS) hardware and software. In the circuit-switched days, the primary security threats were "symmetrical" – the threat was aligned along a specific network perimeter or border. However, today's public safety communications systems, and their expected migration to LTE technology, have brought with them threats that are "asymmetrical," – they can exist either in our own data centers or networks, or can be initiated by a laptop user halfway around the world. The threat landscape has definitely and dramatically changed, and our anticipation of and response to those threats should advance with them.

Security Objectives

This discussion recognizes that virtually all networks deployed in the 700 MHz public safety broadband spectrum will adopt LTE technology, specifically to at least 3GPP Standard E-UTRA Release 8 and associated EPC. A significant portion of the Security Architecture is pre-determined in accordance with the 3GPP standards. Harris Public Safety and Public Communications (PSPC) has adopted the LTE security framework as it relates to the five LTE Security Groups:

1. Network Access Security
2. Network Domain Security
3. User Domain Security
4. Application Domain Security
5. User Configuration and Visibility of Security

These form the baseline security approach. In addition to the five LTE security groups above, we also recommend the implementation of three Supplemental Security & Authentication categories that are recommended by the Emergency Response Interoperability Center (ERIC) Public Safety Advisory Committee report.[iii]

1. Roaming to commercial networks
2. Support for varied application and security requirements associated with a diverse public safety market and the applications and software specific to individual cities, counties, regions, and states
3. Access to the Internet

By leveraging Harris' experience in deploying mission-critical communication systems for the Department of Defense, we have developed a Defense-in-Depth approach to applying just the right amount of security to an LTE network for public safety, providing the following capabilities:

Harris' Defense-In-Depth

If one security barrier is broken, the next security layer will prevent a successful attack.

- Access Control
- Host Security
- Physical Security
- Centralized Logging and Auditing
- Intrusion Prevention and Detection Systems
- Encryption Key Management
- Enterprise Backup (Disaster Recovery)
- Enclave Firewalls
- Automated Vulnerability Management

Taken in its totality, Defense-in-Depth is a critical capability. If one security barrier is broken, the next security layer will prevent a successful attack. For example, if an attacker tries an incorrect password, the security layer may provide an alarm/notification to inform personnel that an excess number of passwords has been attempted. In some instances, Defense-in-Depth may detect the attack and allow various levels of response to the attack to move into place. This could even result in locking down all access to the affected facilities.

How Much Security Is Required?

As those who manage radio systems and networks are aware, the Radio Access Network (RAN) is the most vulnerable to external attacks. With LTE technology and the potential use of more commercially-available user equipment, there will be a tendency to grant more permitted interoperability in line with the LTE protocols established by the 3GPP LTE security standards. This minimum requirement actually calls for a continuous risk assessment process as part of the ongoing operation of the LTE network in order to respond to newly generated threats.

There is a set of best practices guiding IA for LTE networks for public safety. Specific due diligence is required to balance the cost of implementing security measures against the likelihood and impact of a cyber attack. The cost-to-impact balance also must recognize the harsh reality that no single security measure is 100 percent effective in preventing a security breach, and that security breaches will inevitably occur. Therefore, layered security measures must be applied and methods must be developed so that if one security barrier fails, another exists to deter, detect and cope with the threat, or at least create an audit trail for forensic analysis, possible legal actions, and future training. Therefore, a formal risk assessment is crucial when determining the appropriate levels of security for any public safety communications network. In other words, the cost of preventing or coping with security breaches must fit the probable impacts resulting from those security breaches. Within the IA framework, one of the methodologies that has emerged is a Risk Management Methodology consisting of an assessment of risk, vulnerabilities, and threats.

Table 1: Risk Management Methodology

Risk	• Understanding exposure to threats • Assessing likelihood of attack and success • Performing upfront and ongoing risk assessments that attempt to quantify likelihood and cost of a breach
Threats	• Understanding source and means of particular types of attack • Threat assessments are performed to determine best method(s) of defense • Organizations perform penetration testing to assess threat profiles
Vulnerabilities	• Weaknesses or flaws in a system that permit successful attacks • Can be policy related as well as technology related • Vulnerability assessment should be performed on an ongoing basis

Information Assurance: Implementation Driven

IA solutions implemented in LTE networks for public safety must ultimately be implementation-specific, driven by the unique requirements for security of all of the functions within an LTE network for public safety. IA best practices specifically balance the need for security with the need to impose as few additional operating requirements on users of the LTE network as possible.

"By implementing IA best practices within the LTE network, security benefits are available now, and the network also will meet FCC requirements for cyber security and critical infrastructure survivability."

Another key benefit of IA is the application of a minimum number and type of security requirements to ensure interoperability, without limiting the ability of specific jurisdictions, or a future nationwide governing entity, to go beyond these minimum requirements.

In typical corporate networks, security requirements consist of IT best practices. However, on an LTE network for public safety the complexity of stakeholders, systems, devices, networks, and environments precludes just the threshold standard IT security techniques or a one-size-fits-all security solution. Therefore, additional criteria must be used in selecting the IA measures appropriate for the agency.

By implementing IA best practices within the LTE network, security benefits are available now, and the network also will meet FCC requirements for cyber security and critical infrastructure survivability. Further, the LTE network is designed to meet the evolving technical framework of the FCC's Emergency Response Interoperability Center (ERIC), which is required for eventual integration into the planned national Public Safety Broadband network. Finally, these additional criteria must take into account the constraints posed by device and network technologies, legacy systems, organizational structures, compliance mandates, regulatory and legal policies, and cost criteria.

Conclusion

Public safety communication systems are critical capabilities and are essential to the welfare of the country and its citizens. These important assets must be protected with the same rigor as any other critical infrastructure. Malicious cyber attacks on our communication networks have increased dramatically, and these attacks continue to mature in scope and scale, complexity, and sophistication. The need for increased cyber vigilance has never been greater. Enhancing network connectivity and interoperability to both private and public networks improves information sharing and increases situational awareness, but it also elevates the vulnerability of these networks to externally mounted attacks.

LTE networks for public safety must be strongly safeguarded and proactively monitored completely - from end-to-end - in order to avert casual as well as advanced persistent threats. The recommended solution is to implement a comprehensive and well-defined security architecture that is organized and managed on a local, or even national, footprint by a trusted, experienced security engineering resource. Further, this must be as capable as those relied upon by government agencies such as DHS and the DoD.

[i] Identity Theft Resource Center, "ITRC Breach Report 2010 Final," December 2010.

[ii] D. Martinez et al, "Emergency Response Interoperability Center, Public Safety Advisory Committee (PSAC), Considerations and Recommendations for Security and Authentication Security and Authentication Subcommittee Report," May 2011.

[iii] D. Martinez et al, "Emergency Response Interoperability Center, Public Safety Advisory Committee (PSAC), Considerations and Recommendations for Security and Authentication Security and Authentication Subcommittee Report," May 2011.

About the Author

Greg Harris is Product Manager, Cyber and Information Assurance Solutions for Harris Public Safety and Professional Communications business. Prior to joining Harris, Greg was with the Military Medical Command (MEDCOM), assigned as Information Assurance and Governance Program manager for the Southeast Regional Medical Command, Department of the Army. Greg has more than 15 years of Information Technology experience, with emphasis on IP networking, network security, and information assurance. He holds a Bachelor of Science in Business Management from Troy University, and industry specific certifications such as CIO/G6 CISSP, CompTIA Security + 2008, and Certified Associate in Project Management (CAPM).

About Harris

There's a reason Harris is a leading supplier of mission critical communications. Our technology makes critical communications reliable and secure. Our comprehensive line of digital software-defined radio products and systems supports the critical missions of countless public and private agencies; federal and state agencies; and government, defense, and peacekeeping organizations throughout the world.

Harris is an international communications and information technology company serving government and commercial markets in more than 150 countries. Headquartered in Melbourne, Florida, the company has approximately $6 billion of annual revenue and more than 16,000 employees — including nearly 7,000 engineers and scientists. Harris is dedicated to developing best-in-class assured communications® products, systems, and services. Additional information about Harris Corporation is available at www.harris.com.

HARRIS®

Harris Corporation
221 Jefferson Ridge Parkway
Lynchburg, Virginia 24501, USA

1-800-368-3277

http://pspc.harris.com