CYBERSECURITY BENEFITS OF A PRIVATE LTE NETWORK

UBBA
Utility Broadband Alliance

UBBA CYBERSECURITY WORKING GROUP

Jeff Tufts – Cisco - Chairman
Gary Johnson – Evergy – Co-Chairman
Dan Bayouth – Burns & McDonald
Mike Brozek – Anterix
Scott Burk – Encore Networks
Vicki Carleton – Southern Company
Mark Eaton – Ericsson
Robert Escalle – Sonim Technologies
Jairo Hernandez Guzman – Council-Rock
Bobbi Harris – UBBA
Patrik Ringqvist – Ericsson
Gary Vondrasek – JEA
Aaron Wright – GE
John Yaldwyn – 4RF

UBBA
Utility Broadband Alliance

INTRODUCTION:
UBBA WHITE PAPERS

Utilities and their customers have been focused on electric service reliability since the first systems were installed. The electric grid was complex when built, and it is getting even more complex as we add electrical loads and generation in places not anticipated in the original grid designs. Across the country, homes and businesses that once only consumed electricity are now producing it with the help of solar panels, microturbines, combined heat and power, as well as other sources that now make it possible to reverse the power flow. Reliability standards will be increasingly difficult to meet as the grid changes to comply with modern state and federal regulations focused on service to the consumer.

Complex systems are famously more susceptible to disruption and service degradation than simple systems. Though utilities are redesigning distribution systems and deploying new technology to meet modern demands, the challenge is exponentially increased by the risk of cyber attack exacerbated by greater reliance on data-dependent technologies. There is no single approach or solution to these reliability challenges.

Forward-looking utilities, technology providers, and service companies have come together to form the Utility Broadband Alliance (UBBA), offering members the opportunity to collaborate and share best practices in the deployment and operation of modern multipurpose communications networks. As utilities increasingly need to monitor and control devices on the grid extending all the way to the electricity consumer, they are focusing on wireless communications systems as the most economical and highest performing option to connect those devices. Running fiber to every home and every device on the grid is neither economically feasible nor achievable in the desired short time frame. UBBA members have focused on private wireless systems based on the global LTE standard, finding them an ideal future-proof solution. UBBA working groups will periodically publish papers focused on various aspects of improving electric service reliability.

The following paper focuses on the number one concern and threat all critical infrastructure providers face: cybersecurity.

CYBERSECURITY BENEFITS OF A PRIVATE LTE NETWORK

Electric utilities increasingly rely upon data-dependent technologies to ensure safe, reliable, and efficient operations. Sensors placed throughout the modern power grid collect data about grid conditions, and centralized industrial control systems analyze and act upon that data, sending commands to smart devices in the field to perform physical grid management tasks.

Transporting this data between sensors, control systems, and smart devices requires secure, reliable, resilient, utility-grade communications networks. Selecting a network technology and deployment approach is a critical decision. Where fiber or metro ethernet deployment is not a good fit for financial or logistical reasons, many utilities are looking to wireless broadband networks to extend their ability carry their increasingly voluminous control data. Wireless broadband solutions require radio spectrum appropriate for broadband, a critical input the utility industry has—with just one significant exception—failed to obtain from the federal agency that licenses radio frequencies. Among the many wireless broadband solutions, private LTE, which brings with it an existing ecosystem of LTE products, is the leading option for secure modern grid data communications.

With the increasing reliance upon data for grid control, security of the new data communications network is of critical importance. The utility's Chief Information Security Officer (CISO), chief risk officer, and others will be deeply involved in the selection of the network technology and deployment approach, including evaluation of inherent security features and the security implications of deploying a private, utility-controlled LTE network.

NIST FIVE FUNCTIONS OF CYBERSECURITY FRAMEWORK

IDENTIFY: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

PROTECT: Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

DETECT: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

RESPOND: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

RECOVER: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications

No single wireless broadband data communications solution will fit the needs of all critical infrastructure entities and their industrial control systems. Options range from public carrier services to public/private hybrid networks to fully private deployments. This first paper in the UBBA white paper series provides detail about private LTE networks to help utility decision-makers understand the best-in-class security features of LTE and the value to a utility of possessing complete control over its own data network. The first section describes LTE's security features, and the second section addresses the significant security benefits of controlling a private network. As the paper explains, a private deployment of LTE is a strong choice for improving utility cybersecurity protections.

Many cybersecurity practitioners are familiar with the National Institute of Standards and Technology (NIST) Cybersecurity Framework[1] which is designed to help organizations better manage and reduce cybersecurity risk. The Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program supports critical infrastructure owners and operators like utilities in their use of the NIST Cybersecurity Framework, which defines five Core Functions for cyber risk management.

As suggested in this paper, private LTE deployments offer substantial benefits of these Core Functions.

LTE OFFERS A PARTICULARLY ROBUST SET OF CYBERSECURITY FEATURES

As cyber attackers grow more sophisticated, defenders are developing ever-more powerful and effective mechanisms to prevent, discover, and recover from security incidents. As the newest among mature, proven wireless technologies, LTE not surprisingly offers a particularly robust, up-to-date set of security features. And in a private deployment, the operator has the control to implement any or all of LTE's advanced security features (as well as any additional utility-specific cyber management functionalities), as described in more detail in the second section of this paper.

LTE is focused on security by design. The 3rd Generation Partnership Project (3GPP) constructed the standard with five distinct security feature groups:

1. Network access security
2. Network domain security
3. User domain security
4. Application domain security
5. Visibility and configurability of security

3GPP and the other global standards development organizations are constantly reviewing LTE security and providing updates. 3GPP's Systems Architecture Security (SA3) group is chartered to maintain system security and meets over a dozen times a year to continually address these issues. In response to a recent paper identifying newly discovered vulnerabilities (none of which was exposed in over a decade of commercial LTE deployment), the 3GPP security steering group committed to address the vulnerabilities in the upcoming 3GPP Release 16 for both LTE and 5G networks. Utilities that adopt LTE are "future proofed" through this continual, global 3GPP process.

A core tenet in LTE's creation and evident in many of these feature groups is the idea of allowing more granular control of the network, enabling stand-alone security measures for connections between discrete network elements, each with a different configuration, rather than a single security measure for the entire system. As a result, an attacker wishing to penetrate an LTE network will need to hack discrete protections for multiple elements; in utility legacy networks, security measures typically apply to the entire network end-to-end.

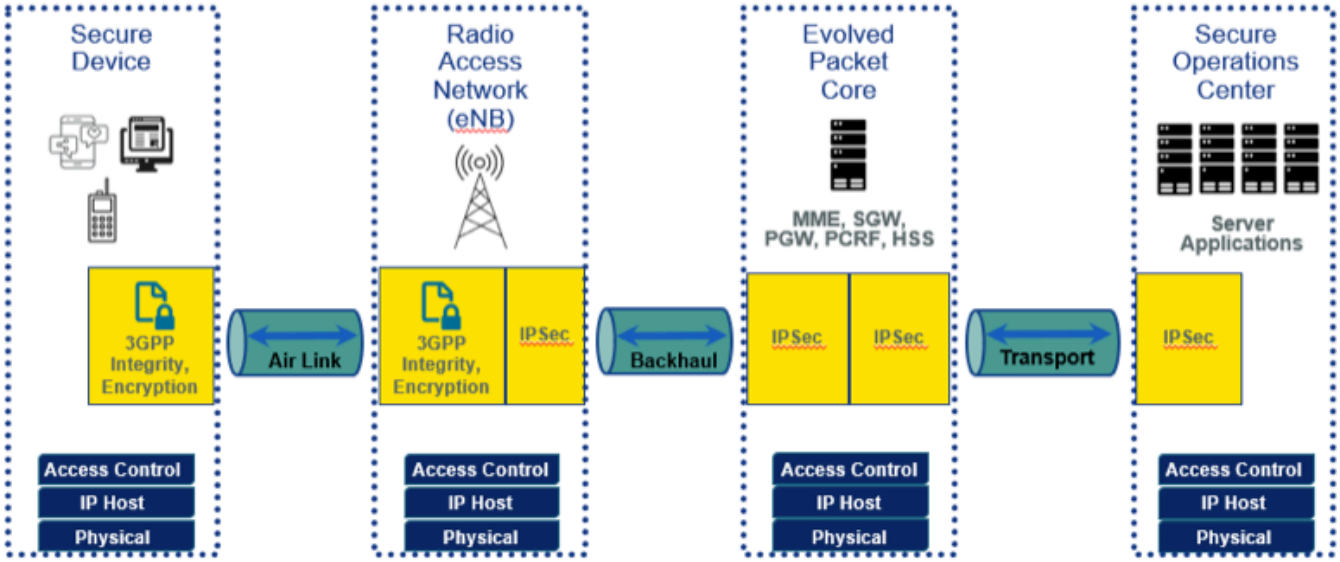
LTE's more granular approach to security is an example of the "defense in depth" practice recommended in 2016 by the Industrial Control Systems Cyber Emergency Response Team of the Department of Homeland Security.[2] In a major step forward, LTE is the only mature wireless technology to enable protection of session set-up and administration signals (the "control plane") separately from the data payload itself (the "user plane"). Regarding the control plane, through its Authentication and Key Agreement protocol LTE separately protects, for example, the links between the SIM in the user's device and three different network elements, two in the core network and one in the radio access network. LTE's adherence to this granular approach results in a many-layered series of barriers to cyberattack on the wireless system.[3]

[1] https://www.nist.gov/cyberframework.

[2] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies (Sept. 2016) ("ICS-CERT Recommended Practice").

[3] Specifically, 3GPP Technical Specification 33.401 defines five security feature groups for LTE (see above diagram). Each of these feature groups addresses certain threats and accomplishes specific security objectives, representing a significant step forward in wireless network security.

LEVERAGE 3GPP SECURITY



This is one way in which LTE represents a strong iterative improvement over its predecessor technologies. Importantly, because of LTE's widespread global adoption, substantial security investment is sure to continue as it evolves into 5G and beyond.

None of this should be surprising; as concern over cyber threats has increased, so too has the degree of cyber protection designed into data communications technologies. The security offered by earlier systems may have been adequate in the past, but newer technologies by design and necessity include stronger cyber protection features. As the most advanced of the proven technologies, LTE should—and does—raise the security bar.

The following review of LTE security features includes both mandatory and optional configurations within the LTE standard. As described in more detail in the second section of this paper, the owner of a private LTE deployment—one that is controlled by the utility—can decide to incorporate any and all of LTE's optional security features, thus strengthening the utility's cybersecurity posture and customizing the network to meet the utility's particular security and operational needs.

CONTROL PLANE PROTECTIONS

As noted above, LTE uses its Authentication and Key Agreement protocol to secure control plane communications separately from user plane data—a major advance. In a good illustration of defense in depth, LTE includes cryptographic protections for control plane communications between the device and three different network elements to prevent attackers from spoofing devices and/or network elements to compromise the system.

To protect control plane communications between the device and the Home Subscriber Service (HSS) core network element, LTE uses an application called "USIM" that typically runs on the Universal Integrated Circuit Card (UICC, which has replaced the SIM card used in older systems). Through USIM, LTE supports not just authentication of the user to the device but also authentication of the device to the HSS, which manages customer information and authorizes the device's access to the network.

The Mobile Management Entity (MME) is also a core network element; it manages device mobility on the network. Using a feature called Non-Access Stratum (NAS) security, LTE verifies, encrypts, and protects the integrity of control plane signaling between the device and the MME separately from other interfaces.

For protection of the device's control plane communications with the radio access network (RAN), LTE employs Access Stratum (AS) security, which provides verification and integrity protection as well as encryption for control plane signaling between the device and the LTE base station, called the eNode-B.

USER PLANE PROTECTIONS

To secure the payload of the communication—the data the user is trying to communicate—LTE enables protections at the IP layer. For the user plane, LTE supports integrity verification and encryption of data sent between the device and the packet gateway, as well as network layer VPN security.

LTE AUTHENTICATION FOR OLDER TECHNOLOGIES

LTE isn't just more secure than legacy systems—it also can help make those older technologies more secure. Private LTE networks can use the full capabilities of the Interworking Function (IWF) that allows for mutual authentication of LTE and Wi-Fi users. Legacy enterprise Wi-Fi users can seamlessly use the same secure authentication protocols and procedures of LTE users in the network. In this way, a private LTE system can help extend the value of some legacy deployments.

PRIVATE NETWORKS GIVE THE UTILITY CONTROL TO IMPROVE SECURITY—TO UTILITY STANDARDS

The LTE standard described above includes certain security measures that are mandatory; it also provides the ability to implement other, optional security features. But whatever communications technology a utility adopts, at least one result is certain: if the utility controls the network, the cyber protections implemented in the network will more likely meet the security goals of the utility—and only the utility. Almost axiomatic, this statement presents a powerful fact that will benefit private network operators addressing today's well-known challenges as well as tomorrow's less certain developments. In short, a utility that controls its own private network can implement all the security features of LTE that it desires—including the optional ones—regardless of a carrier's or other controlling provider's business or operational considerations.

PRIVATE NETWORKS CAN MAXIMIZE LTE SECURITY FEATURE IMPLEMENTATION

A simple example: LTE can be set up to require a PIN to authenticate the user (rather than just the device) to the network. Though this functionality is broadly implemented in Europe, US carriers have rejected it (the PIN option on US devices is a local operating system function only). A utility implementing its own private LTE network can adopt this feature and thereby improve its security posture.

Another simple example: a utility with its own private network will likely use its own internal domain name system (DNS) to assign IP addresses to elements of its core network as a protection against an attacker spoofing a network element and gaining the ability to re-route traffic. A private network provides that control; DNS protection in a commercial carrier network is left to the system operator.

Consider the NAS security feature described above—the additional protections it offers will accrue only to those network operators who choose to implement them. A utility controlling its own LTE network will be able to configure security for the control plane separately from the security of the user plane and thus improve its cyber posture. A utility depending upon a shared, commercial carrier service will almost certainly not realize these benefits, because carriers as a rule do not implement control plane/user plane separation, deeming that measure unnecessary to meet their business requirements.

Similarly, LTE's AS security features, also described above, include the ability to encrypt the transmission set-up information (the actual radio frames at the physical layer) sent over the air interface between the user device and the eNode-B.

One last example: LTE also enables the use of IPSec to secure connections between elements of the RAN and the Evolved Packed Core (EPC) network. This is an optional feature for commercial carriers whereas a utility operating a private LTE network would be able to decide for itself what security measures are appropriate.

Every utility CISO is highly sensitized to the risk of attack from bad actors reaching a utility system via the public Internet. Complete separation from the Internet is a widely recognized best practice that utilities have long implemented for critical control systems.[4] Commercial carrier networks, of course, are connected to the Internet, enabling attackers to launch exploits from anywhere on the globe against utility systems that use those networks. But a utility that deploys a private LTE network controls the extent to which its network will be accessible from the Internet, establishing and enforcing specific measures tightly limiting and securing that connectivity—even to the point of completely "air gapping" its critical control systems, permitting no connection whatsoever outside the network's defined boundaries. A commercial carrier network cannot provide a CISO that level of control and security.

[4] See, e.g., ICS-CERT Recommended Practice at 1 ("Physical separation between corporate and control domains has, traditionally, provided the primary means of protecting" industrial control systems).

PRIVATE NETWORKS OFFER FULL NETWORK VISIBILITY

Despite all the cyber benefits a utility would realize from controlling the architecture and configuration of its own network, perhaps the single most valuable aspect of network control for the CISO is the ability to know, in detail, what is happening on the network. Network visibility can be the difference between knowing the network is under attack and being oblivious to the threat; it can quickly provide information that helps the CISO identify, contain, mitigate, and recover from an attack.

In commercial carrier networks, security issues are by design hidden from the customer, greatly complicating efforts to analyze a security breach. The owner of a private network can deploy sophisticated network monitoring solutions that reduce the critical "time to detect" (TDD) metric. A private network operator can know, for example, if a device on the grid is reporting more frequently than expected, or if each report consists of more data than it should. Though there may be an innocent explanation for the device's unusual behavior, the utility relying on a public carrier network likely would not be aware of that behavior at all. But with a private network, the utility would have full access to security logs, traffic alerts, and network interfaces and analytics. A carrier can be expected to monitor for billing purposes the overall amount of traffic a customer utility sends over the network; the CISO of a utility with a private network can monitor traffic patterns and behavior for cybersecurity purposes.

As demonstrated here, private networks offer control a utility cannot hope to enjoy in a non-private, commercial carrier network environment. And for cybersecurity, control is key. As Southern California Edison wrote this year, "High level security of the network against outside manipulation is essential to reliable operations, and that level of security can only be achieved by a closely owned, controlled and protected network structure."[5]

CONCLUSION

A utility considering a proposal to deploy a private LTE network can be confident that such a network would improve the cybersecurity of the utility's wireless data communications capabilities, based upon two simple, intuitive propositions. The first is that as the newest, most advanced mature wireless technology, LTE includes newer, more advanced security features, and with its vast global market the investment and enhancement of LTE security will continue. The second is that a utility can better protect a private network under its control than it can a public network operated by a carrier where the utility is only a purchaser of a commercial service. A utility implementing a private LTE network for its critical data communications is adopting the latest, most secure mature wireless technology with the greatest degree of utility control to deploy and operate the network in a way that meets its own, specific cybersecurity needs.

[5] Comments of Southern California Edison Before the Federal Communications Commission, In the Matter of Review of the Commission's Rules Governing the 896-901/935-940 MHz Band, WT Docket No. 17-200 (June 3, 2019) at 2.

UBBA
Utility Broadband Alliance

ABOUT UBBA

The Utility Broadband Alliance (UBBA) is a collaboration of utilities and ecosystem partners dedicated to championing the advancement and development of private broadband networks for America's critical infrastructure industries.Members will have access to resources that accelerate theirjourney towards a secure, resilient and future-proof grid.

CONNECT WITH UBBA

Created with utilities for utilities, we're driving the industry toward the next level of connectivity with customers, innovative technology, utility experts and policymakers.

Connect with us today!

(888) 303-7389 | info@ubba.com | www.ubba.com