SCTE·ISBE CABLE-TEC EXPO 2018 | ATLANTA, GA OCTOBER 22-25

2018 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

Securing a Hyper-Connected Society

A Technical Paper prepared for SCTE•ISBE by

Tom Conklin
Vice President of Business Development
Ericsson
6300 Legacy Blvd. Plano, Texas USA
+1 (703) 789-4574
Tom.conklin@ericsson.com

Table of Contents

Title **Page Number**

Table of Contents 2

Introduction 3

A Hyper-Connected Society 3
1. How did we get here? Agriculture as a case study 4
2. Changes in the way software and hardware products are designed 5
3. Intelligent Transport Systems 6
4. E-Health 7
5. Smart Grid 7
6. Manufacturing and Processing 8

Conclusion 8

Bibliography & References 9

List of Figures

Title **Page Number**

Figure 1 - IoT Use Case Diversity 4
Figure 2 - Simple Farming Beginnings 4
Figure 3 - Global Dependencies 5
Figure 4 - Design Concept: Rich Execution Environment vs. Trusted Execution Environment 6

Introduction

Powerful and robust communication networks are a foundation of the global economy, and they are already sparking dramatic transformations in industry and society by enabling new ways of innovating, collaborating, socializing and communicating. While this shift to a hyper-connected, open society brings about many opportunities, it will also introduce many new threats, risks and obstacles. As greater value is extracted from networks and new business structures, the threats are also adapting, becoming more frequent, more sophisticated and more impactful.

A secure communications infrastructure which integrates multiple ecosystems, such as the Internet of Things (IoT) is the foundation for the hyper-connected society. Services for society and business will share similar infrastructure but with different security requirements. We expect next generation networks to enable greater reliability, faster throughput and lower latency as user, device & application demands continue to increase. These requirements call for a new generation of services that ensure end-to-end security across diverse/innovative architectural models. Data integrity and protection is one of the top concerns for operators, enterprises, governments and regulators. As data flows across organizational boundaries and nations, it must be protected at all stages - as it is generated, stored, transmitted, and used over both trusted and untrusted ecosystems.

Future networks will be designed to serve a variety of applications and solutions for people as well as business and connected industries such as manufacturing and processing, intelligent transport, smart grids and e-health. This will result in more complex management of security, privacy and trust across the "things" that make up an IoT ecosystem. And it will also result in far reaching dependencies on the data that is created in one IoT ecosystem and consumers of that data. This paper will examine steps and recommendations for ways to bring a practical approach to securing IoT devices, platforms and ecosystems.

A Hyper-Connected Society

Ericsson is currently predicting 29 billion connected devices by 2022 including about 18 billion IoT devices. Just this year it is expected that the number of IoT devices will surpass the number of mobile phones. We add new ones to our lives now without thinking. Fitness trackers, smart scales, baby and pet monitors, refrigerators, connected cars and other products differentiate from competition through software. And they connect to applications and databases, web pages and other devices with our explicit permission with little regard to security, privacy and trust. When everything takes a username and password as a basic method of authentication providing authorization to produce and consume information that may be very private, it is very tempting to use the same credentials for everything. Product vendors effectively distribute the blame for predictable security breaches to end users by adopting more complicated authentication methods.

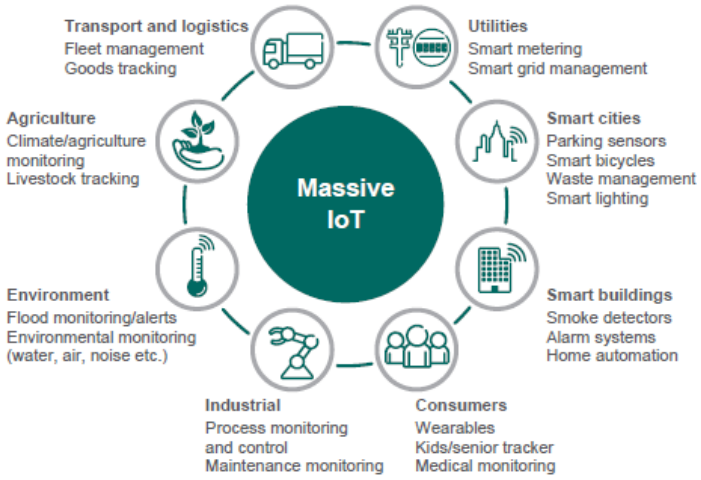

Figure 1 - IoT Use Case Diversity

1. How did we get here? Agriculture as a case study

Figure 2 - Simple Farming Beginnings

It is easy to see that things are changing, but sometimes the benefit of new devices, services, and methods obscures the complexity of their implementation and the risk that accumulates with added convenience and efficiency. Take for example, Agriculture. Originally, man was dependent on rainfall for both their survival and their crops'. Dry or wet years were life or death situations. But there was no interdependence between farmers. They adapted and invented irrigation, which was more predictable, but required an above ground water source like a river or stream. At this stage This limited their capacity to produce and therefore proliferate. Wells, wheels and wind allowed irrigation to be derived from distant or underground sources. There was now some dependence on others, for instance, to not install a dam upstream, or consume too much from the source. Much later diesel pumps and powered irrigation systems allowed better control of both the source and application of water. If it rained too much, the irrigation was not turned on. Dependence on the cost of fuel, availability of parts for the machinery was added to the equation, but more land could be used, and more crops were grown. The systems were improved with rain sensors and automation to reduce the labor requirements and chances for error. A Farmer's success was less more predictable, but at the cost of increased dependence on other factors outside of their control.

On the modern farm today, there are not just many dependencies, there are many interdependencies. Now, farms can be equipped with a matrix of optical and electrical sensors that are GPS located and actively test soil nutrients, moisture, airflow and other conditions. Farmers don't just control irrigation, fertilization, and harvesting dynamically for all parts of the farm based on data from these sensors. They also compare this data with information from multiple weather services to predictively plan for these functions. And they use the data collected to predict crop yield. Data from multiple farms is analyzed by industry and government agencies to predict crop yields and therefore prices, that the farmers can use to plan season to season. Packers, smart transport systems, manufacturers, wholesalers and retailers scale

their businesses based on models of supply and demand, changing costs of labor and fuel, and global consumption. Smart transportation systems, manufacturing and distribution robots and smart grids are tuned and configured based on what has to be trusted information. Governments negotiate treaties and levy taxes based on this data. Monetary transactions from purchasing and selling, to investing, borrowing, and lending happen based on the information. All these players in the economy fed by Agriculture provide and consume data that is critical to all the others.

Figure 3 - Global Dependencies

So while the first farmers would live or die by the rain and their ability to fend off rabbits and deer eating their crops, today's farmers are part of an enormous cascading set of dependencies on their secure connections to places, people, and things. Security of data to ensure its integrity is required to make sure all players in the economy are acting on the right information. Security of access to the network and systems using, transmitting and storing the data is complicated by the sheer quantity and difference of all the devices. Cyber physical-systems like the sensor networks in the Agricultural industry, the smart transport systems, and industrial robots can cause real damage if their security is breached through defect or hack. It is necessary to implement new methods to protect these systems as we move into this next phase. One break in the chain could have global implications if we do not. So, for example, it can't be possible for the farmer to open the door to this whole ecosystem to people with ill intent through deployment of defective, poorly designed or misconfigured sensors. The integrity of the data is too important New methods must be embraced as our dependencies on the interworking of formerly disparate systems grow.

2. Changes in the way software and hardware products are designed

Agile has largely replaced waterfall software development methodology in many sectors. Small, iterative releases of products with few new features, bug fixes and security patches is how things work. This is

recognizable when apps are updated on mobile phones every few weeks. But with IoT, often the software on the devices cannot be upgraded after the product is deployed. Many of these products operate on 2AA batteries that are required to last for five or ten years. The device, say a moisture sensor, turns on rarely, connects to a wireless network, and transmits a small amount of data before going back to sleep. So a mistake in design could have critical impact on securing the systems the device is connected to. And the mistake of trusting the end user to configure secure authentication of the device on the network has been proven.

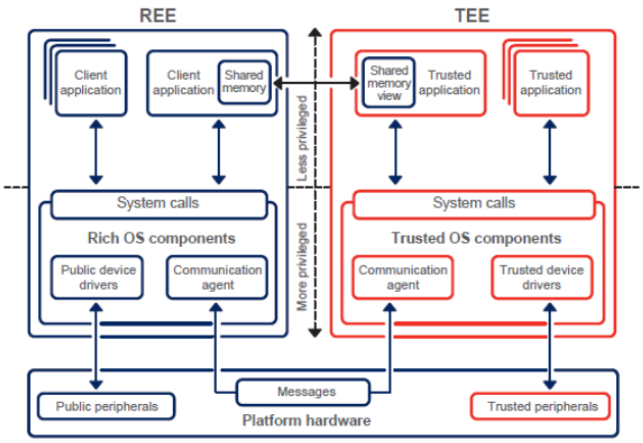

Figure 4 - Design Concept: Rich Execution Environment vs. Trusted Execution Environment

A better approach is to design products with the security built in. While cellular networks have built in authentication and device management, most IoT devices are connected to the network through other interfaces like WiFi, Bluetooth, Zigbee, and NFC from a hub that connects to the Internet through the cellular network. Platforms on the cellular network can facilitate secure bootstrapping of devices and remote application and management of authentication credentials the first time the devices connect. This eliminates user error. Also, the cellular network is a good place for protection from distributed denial of service attacks and rogue devices degrading the trustworthiness of the data provided by a device class. The cellular network is a good platform to apply proven and standards driven security protection to a vast array of IoT devices.

And the proper application of encryption at the device can eliminate the possibility of tampering with the data provided. Devices should be able to verify software updates and boot code cryptographically so that they can't be replaced with malware. A root of trust can be created through separation of these functions logically or even physically through purpose-built ASICs from applications run on the devices in the most sensitive applications.

3. Intelligent Transport Systems

While self-driving cars get much of the attention when it comes to Intelligent Transport Systems, we are still not at a point where systems enabling this technology can be practically hosted in the network. There is just too much at risk. This is an example of a security problem with available solutions that still are not trusted. Guidance and collision avoidance systems for a moving driverless automobile are still largely hosted in the automobile and not just for latency and network reliability concerns. But software is updated, configurations and routes are sent, and traffic and road data is downloaded wirelessly. So, security and trust structures shared between the vehicle manufacturer, the map and navigation source, and

the operator of the vehicle. As with the other use cases, authentication credentials cannot be left up to the end user and authorization profiles need to be shared in real time between public, commercial and private entities. When the technology truly takes off, there will also be privacy concerns about driver behavior and destinations. So, a car's key needs to authenticate the passenger biometrically to ensure privacy and security of the vehicle. Software updates must be cryptographically trusted with keys and block chain before being applied. Rollback to a prior build must be allowed for all systems. And mapping and navigation information must be tracked with block chain before used for any chosen route.

This category also extends to smart cities and control of variable speed limits, traffic lights, tolls, parking spots, and public transport. At the scale of a municipality, there is significant attraction for hackers to disrupt these systems. This is another case where cellular technology can significantly improve security. Standard, hardware-based security for authentication of users for charging for tolls, parking spaces, and express lanes comes with 5G. Also, distributed PCI compliant support for low latency microtransactions is a feature of modern cellular network billing platforms. 5G itself provides very low and predictable latency, high bandwidth, support for low power, low cost devices enabling an economical deployment of hundreds of thousands of sensors, switches, and signals. Automation comes with a risk of its own, though, in that anything that can be automated to fix or optimize itself can also be automated to continuously break itself. Trust structures for system configurations, algorithms, and policies must be in place and audits must be continually run to ensure public safety.

4. E-Health

Because of the high stakes for innovation in healthcare, this use case has always been top of mind for IoT. Saving lives and saving money are easy concepts to sell. At the same time, healthcare is a highly regulated industry with significant interest in privacy, security and trust of data consumed and created. The category extends far beyond IoT to expert systems, doctor / patient portals, and telemedicine. Privacy and trust of data are primary concerns. But the risks get greater when categories like health monitors, pharmaceutical dispensers, surgical and other hospital robots, and elderly patient tracking are considered. It is possible for the "things" in the internet of things to cause real, direct physical harm to people and property.

Care must be taken to design the devices used in E-Health with security, safety and privacy in mind as well as compliance to evolving laws and standards. The price point for many of these devices allows for implementation of hardware encryption, fail safes, and communication and data integrity checks. Because this is so important, government and professional organizations must and will expand regulatory oversight and require more advanced certification of devices against their standards.

5. Smart Grid

Smart grids provide efficiencies through coordination of production, sale, transmission, distribution and consumption of power using information and communications technology. As with the use case, these efficiencies come at the cost of dependencies. All components of this model are potential entry points for bad actors looking to create widespread chaos, demand ransom payments through threat of said chaos, or invade the privacy of consumers. Protection of the smart grid is a critical component of any country's defense strategy as an attack could be debilitating and difficult to reverse.

Many of the vulnerabilities of the smart grid come from the smart part ironically. Unlike the long-lived power equipment and infrastructure, IT equipment typically has a three to five year lifecycle. The mismatch of the lifecycles means that it is very likely that compliance to security standards for the IT equipment will drift as it ages. Automated audit and updating of the equipment and software to maintain

compliance is a good way to avoid this and modern automation and orchestration systems are a good way to counteract this. Besides this, best practices for securing the IT infrastructure, LAN, and WAN are critical as the stakes are high.

The addition of smart thermostats and home automation systems as a popular product category represent a privacy risk that many consumers do not recognize. As these systems adjust temperatures and activate lights and other devices based on the user's habits and presence, access to this information can allow criminals to understand when the house is or is not occupied. This can also be done from a hacked smart meter. Manufacturers of these devices, like others mentioned, cannot place the entire responsibility for security on the end user's ability to maintain and secure a user account.

6. Manufacturing and Processing

Autonomous systems for manufacturing and distribution of goods are becoming more justifiable than ever. In the past, robots replaced humans for jobs that required precision, speed, significant repetition, or hard to find valuable skill sets. As the cost of these robots and their control systems declined, they became useful for replacing humans in tasks humans find unpleasant. And in areas with unreliable labor forces, it is cheaper to automate a job than to train many different people for the same job over the course of a year as they leave too often. Unlike industrial automation systems of the past that required extensive retrofit of the facility, on site IT and automation platform staff, and significant investment, it is possible to buy one robot for a specific purpose. Robots are managed from central platforms on cloud infrastructure to eliminate the need for extra on-site staff. And automation systems can be coordinated between multiple facilities that could be thousands of miles apart. The coordination of order and inventory systems, real time location, collision avoidance and even intelligent transport systems can improve the payback on investment significantly while improving quality and customer satisfaction. But considerations must be made in network design and security to make this possible. There are significant safety concerns for on site personnel that must be mitigated by trusted distribution of system software updates, configurations and orders. Because these systems may be enhanced by adoption of edge networking technologies to reduce latency, distribution of platform logic provides an opportunity for hackers and considerable liability. Application of blockchain to ensure all players in the ecosystem are acting from trusted data is a good solution. And active assurance of compliance to security, privacy, industry standard, and customer service level agreements in a fungible cloudified network is vital. Orchestration and automation of this active oversight can make this efficient. Machine learning and Artificial Intelligence applied to the vast amounts of data created by these systems can aid in the detection and correction of anomalous behavior in real time.

Conclusion

The Internet of Things grows as it makes innovation, efficiency and convenience easy. But it comes at the price of dependencies between previously unconnected systems that significantly escalates the severity of any security breach. While the use cases described have their own set of dependencies, they also collectively have a common set that could be exploited. The GPS network, or public cloud platforms are examples. It is critical that security strategies be employed by the vendors of IoT products, providers of platforms, and deployers of services that consider all dependencies. As the IoT grows, it will be more common for hackers to exploit unexpected dependencies than products or services, as it will be difficult to track them. A start, though, is to employ design, management, and maintenance techniques that are developed with careful thought of these dependencies and ensure security, privacy, and trust of all players in the IoT ecosystem. And devices, networks and services should be audited and tested by independent labs and standards bodies to ensure they will be good citizens in the universe of dependencies.

Bibliography & References

Ericsson Mobility Report, Ericsson November 2016

Ericsson Mobility Report, Ericsson,

5G Security, Ericsson June 2017

Ensuring Critical Communication with a Secure National Symbiotic Network, Ericsson May 2018

Cellular Networks for Massive IoT, Ericsson January 2016

CTIA Cybersecurity Certification Test Plan for IoT, CTIA May 2018

