SECURING CELLULAR ENTERPRISE IoT SOLUTIONS

SPONSORED BY AERIS

aeris

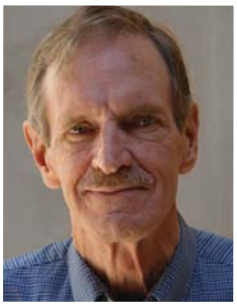
www.aeris.com

beecham research

Shaping the IoT future

THE THREATS ARE GROWING

Robin Duke-Woolley,
CEO, Beecham Research

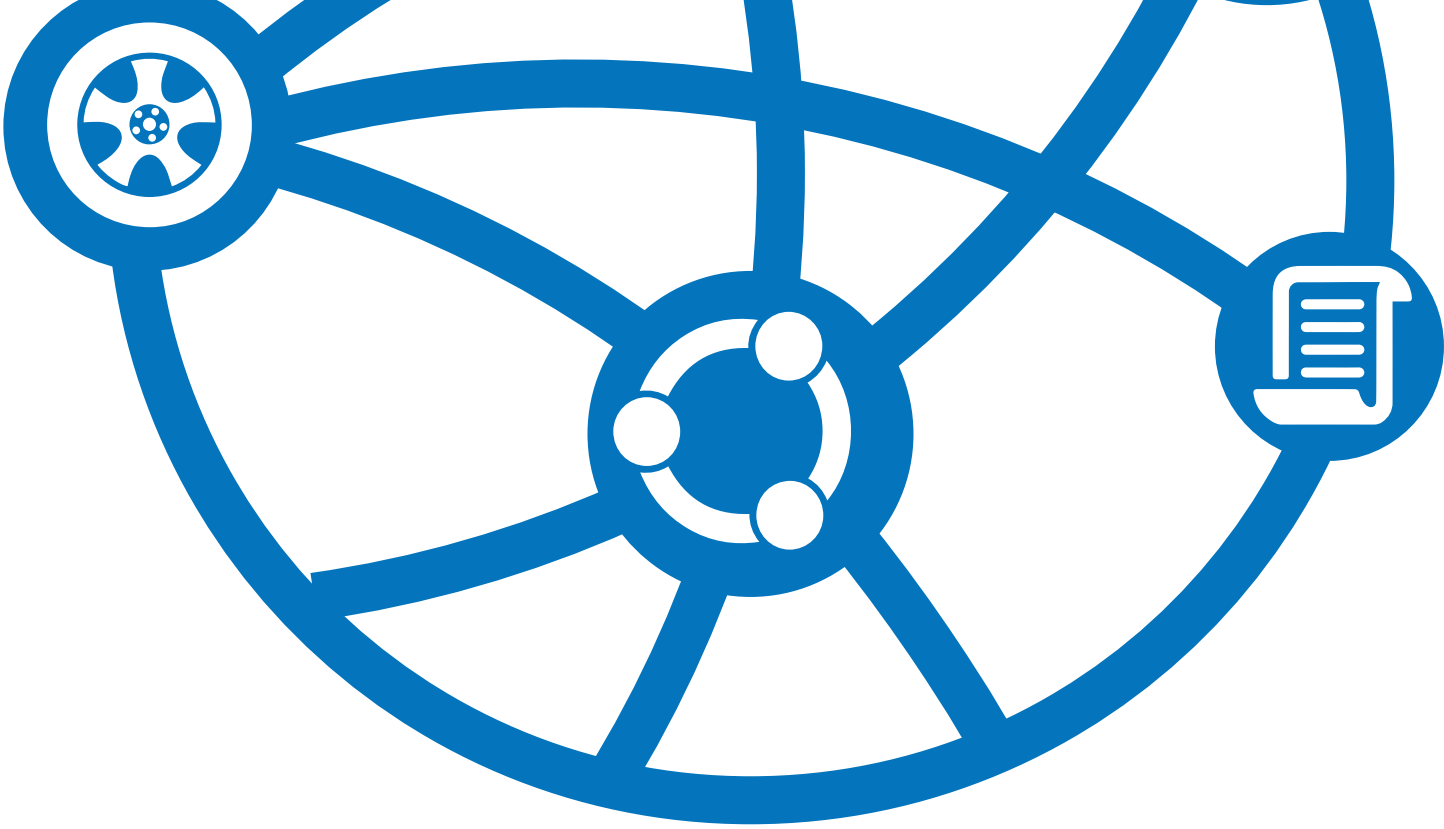


Bill Ingle, Senior Analyst,
Beecham Research

In the first steps on the road to digital transformation of the enterprise, a billion cellular IoT devices have already been connected worldwide. Yet this transformation is just getting going – billions more will follow and growth rates will remain high. This rapid growth of connected devices is not all plain sailing – it brings with it new challenges and new risks, particularly those associated with online security. In the midst of this, Aeris is bringing to market new solutions designed to assist IoT device manufacturers and solution providers address these security issues. These are outlined later in this report.

Numerous cyberattacks have been reported in various IoT sectors. While no one knows for sure how many attacks have not been reported, estimates are "many." These include attacks on banks, telecommunications companies, industrial companies and utilities – all part of what is now termed "critical infrastructure". The specialized equipment used in industrial sectors and the strong security measures used in commercial sectors may have reduced the number of attacks, but only to a limited extent – hackers keep trying and will continue to do so.

For consumer or home IoT there is a different story. 2016's massive Mirai Botnet attack, the largest ever distributed denial of service (DDoS) attack, focused attention on IoT security more broadly than sector-specific attacks. It attacked DNS servers, bringing down a number of major Internet sites in the U.S. and Europe and was launched from connected consumer IoT devices such as CCTV cameras and DVRs.



LEGISLATION ON THE WAY

In the U.S., serious security breaches have jolted state and federal authorities into initiating IoT security legislation; compliance will be an important factor in IoT device and network design and implementation. The EU's GDPR privacy regulations are already impacting IoT solutions, to the extent that data collection of personal information and consent are part of them, while new cybersecurity regulations were approved in March.

California's SB327 bill is a case in point, going beyond existing law focused on protecting consumer privacy. Here's the summary: "This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified."

SB327 is already being rapidly followed by similar bills in other states. IoT devices in many states will soon be required to have built-in security; no longer, for example, will manufacturers be able to ship IoT devices with ADMIN ADMIN for ID and password.

The federal 2019 IoT Cybersecurity Act was passed in March. Its purpose is "to leverage Federal Government procurement power to encourage increased cybersecurity for internet of things devices, and for other purposes." The National Institute of Standards and Technology (NIST) will be in charge of executing the provisions of the act, including integrating its work into current U.S. cybersecurity processes. NIST publications will cover policies and procedures for vendors and contractors providing IoT devices to the federal government, while government agencies will be prohibited from acquiring non-compliant devices.

Developing national standards, establishing testing procedures, etc., takes time and most often follow the market rather than leading it. This means that while IoT vendors offer proprietary security solutions as a new competitive market develops, standards then need to catch up to maintain that market growth. Since the U.S. government is a very large customer, new regulations adopted by government will, in all likelihood, be applied by suppliers to all IoT products and solutions when they are finalized, no matter who the customer is.

In addition to its April, 2016, General Data Protection Regulation (GDPR) privacy act, the EU also approved a new cybersecurity act in March, creating an EU cybersecurity certification framework focused on transparency for cybersecurity assurance of ICT products, services and processes. The framework is based on existing European or international standards.

ASSISTING COMPLIANCE

All of the regulations emphasize how IoT devices are secured and data is accessed. Having proper security in place makes common sense but too often this has been an afterthought. Regulation will force manufacturers to take security into account and not to ship without it – security by design.

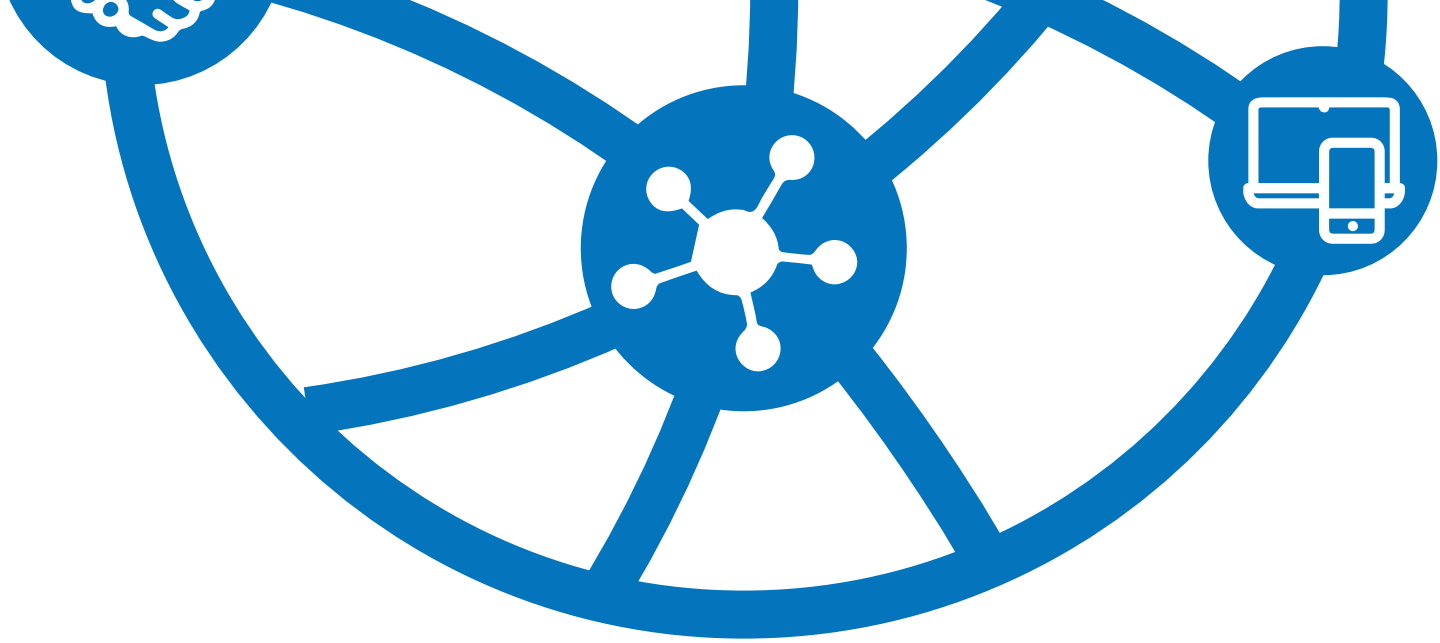
With this in mind, Aeris' solutions help IoT device manufacturers and solution providers comply with upcoming regulations and address both IoT security and operational challenges in three areas: IoT Device Identity, Data Access Security, and Managing Remote Updates. The Aeris IoT security solutions help plan for a scalable 360 degree defense-in-depth incorporating mechanisms to protect, detect, respond, and resolve security challenges.

Point of Vulnerability

Security Vulnerability	Example	Manufacturing Center	Destination Port (Logistics Waystations)	Distribution Center	Customer / Field
Theft of SIMs	Many examples abound in the consumer device space; examples of stolen M2M SIMs growing	✓	✓	✓	
Not in destination country; terrorism threat	Phone/SIMs are often used by terrorists to remotely trigger an IED(1)	✓	✓		
Bad firmware: unauthorized access IN (Read)	(Oct'18) SuperMicro alleged(2) to have allowed Chinese govt. chips meant for spying onto motherboards for large tech companies incl. Apple & Amazon	✓			
Bad firmware: unauthorized access OUT (Changes)	Chrysler recalled 1.4M vehicles when hackers demonstrated they could remotely hijack a Jeep's digital systems				✓
DDoS (Distributed Denial of Service) events	Mirai DDoS attack (Oct '16) caused by default W i-Fi passwords not being changed				✓

Note:
(1) NBCNews - ISIS fighters; Boston Marathon bombing
(2) SuperMicro, Apple and Amazon have strongly disputed the Bloomberg story

Key Security Vulnerabilities across the IoT Device Lifecycle (Source: Aeris)



1. IoT Device Identity
99% of IoT devices send data from sensors to a backend system, where the data is collected, analyzed and processed.

A mechanism for indicating that the devices belong to a particular backend system before they can connect to it is a bare minimum requirement. A typical first generation technique – prone to getting hacked and being misused – is User ID/Password. Transport Layer Security (TLS), a second generation technology, encrypts data and relies on stored certificates for authentication. TLS was designed for computers, however, not IoT devices and is generally unsuited for IoT owing to processor and RAM requirements.

Aeris provides a connectivity service to its customers that includes the SIM used in a customer's device. At the time of manufacture, a secure memory area of the SIM is created. A private encryption key and related applet are added to the secure memory and never exposed in the field to anyone. A random token sent to the applet is signed with the private key and sent to the backend system for verification using asymmetric algorithms in conjunction with a public encryption key. Customers need only plug the SIM into their device to ensure authentication.

Aeris' Zero Touch Provisioning (ZTP) solution enables automated distribution of the public encryption key, solving the challenge of distributing public encryption keys at scale, for example when manufacturing 100,000 or 1,000,000 devices.

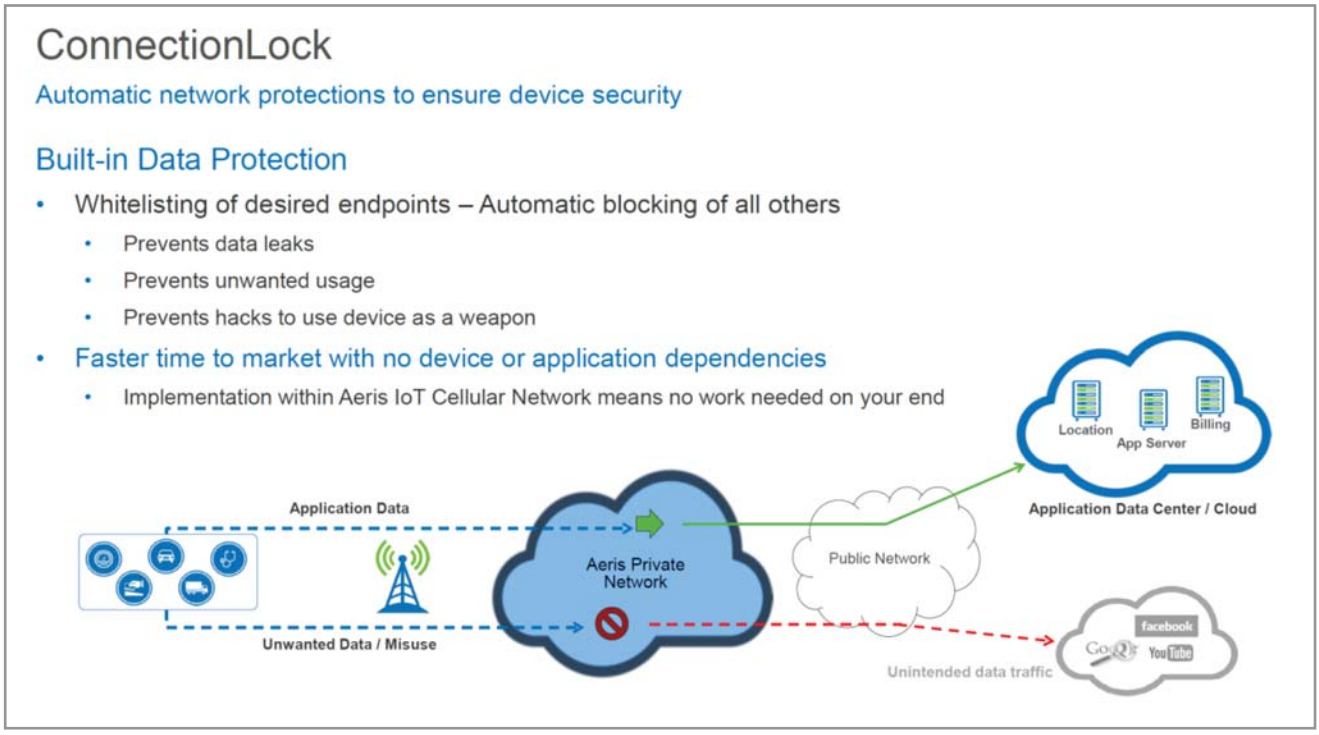
2. Data Access Security
In the 2016 Mirai botnet attack mentioned above, compromised or "weaponized" IoT devices sent massive amounts of data to the servers under attack. Making IoT device security as foolproof as possible starts with securing device identity, but how can you prevent data leaks and avoid having your IoT devices become weapons of mass Internet attacks? How do you ensure that data leaving a device is really going to the intended backend system?

Aeris' ConnectionLock™ solution relies on the fact that all devices communicate over a network before talking to the intended backend. Customers provide information about their authorized and designated backend servers (i.e. intended endpoints) and Aeris configures its network so that customers' devices can only communicate with those endpoints – an enterprise is given the ability to lock down the endpoints their devices can talk to.

In the Mirai botnet attack, the hacked CCTV cameras overwhelmed DNS servers. Had they been connected with ConnectionLock™, the attacks would have failed, as the cameras would only have been able to communicate with their designated backend system servers.

The solution also prevents data leaks enabled by malware put into IoT device chipsets and firmware – data cannot be siphoned off and sent to rogue nations or entities but again, only to designated backend servers, not unintended endpoints.

Lastly, people may take IoT SIMs and plug them into tablets or phones for Internet browsing, creating significant overages and costs. ConnectionLock™ will prevent this from happening.



3. Managing Remote Updates

Zero-day attacks and exploits, especially in IoT devices (due to its scale and geographically dispersed deployment) can have massive implications (example: distributed denial of service attacks), and can spread like wildfire if not contained and fixed in a timely manner. If IoT devices are compromised, mechanisms are needed to detect and quickly fix the devices with software and/or firmware patches. Remote updates of the devices using Over-the-air (OTA) update capability is then very critical; no IoT program should be rolled out without OTA capabilities, whether for security patches or updates that enhance device capabilities. This presents challenges for managing remote updates at scale, especially in highly constrained low bandwidth IoT networks using LTE-M or NB-IoT.

The actual size of updates varies from application to application. With lightweight, constrained devices like asset trackers, updates might range from a few hundred kilobytes to 1 megabyte, with update size increasing as device capabilities are enriched. Updates for a fleet management application might be as large as 50 megabytes. Here, the edge device is more computer-like, with many sub-applications running on it.

One of the many challenges for remote updates, especially with narrowband technologies like LTE-M, is that the networks are highly constrained. With LTE-M, most carriers have deployed a single channel; say they have 10Mb of spectrum – they'll deploy one channel of 1 MHz. Updating hundreds of IoT devices in a single location over a single 1 MHz channel will fail without properly scheduling and managing the updates; they can't all be updated simultaneously.

Knowing where the devices are located is then equally important – are they all at the same cell tower location? Then, too, an enterprise must know when the devices come on-line and go-off-line, especially when using narrowband technologies – where devices do not stay on the network all the time, as solutions are optimized for for low power consumption and long battery life. A challenging situation with LTE-M becomes even more challenging with NB-IoT.

Typically, IoT OTAs are done when devices are stationary. Take an example in asset tracking, when trackers (and the devices being tracked) are sitting in a warehouse. Even in fleet management, updates aren't done with moving vehicles – data collection typically takes place in a single location, such as a depot. Suddenly, hundreds of assets are communicating with one cell tower. If you don't know this and try to update all of them at the same time, your OTAs are going to fail, requiring you to not only track the failures but also implement mechanisms for continuous retries

These challenges are applicable to scenarios for existing IoT deployments as well as new IoT programs that are being rolled out. Enterprises typically utilize home-grown processes or OTA management software for remote update of their devices. These home-grown processes or OTA management software lack information or network awareness to overcome the scale and efficiency challenges as described above. Aeris caters to these situations, providing a set of modern RESTful API's maximizing OTA efficiency.

By using coordinated APIs and carefully scheduling and managing updates, Aeris' solutions create OTAs that are possible, without endless retries. This is especially important when dealing with critical updates that patch security vulnerabilities.

IN SUMMARY

As billions of IoT devices become connected, more all the time, new security risks and challenges will continue to rise as well, even as regulations are enacted to ensure security and minimize the risk of possible cyberattacks. IoT security as a whole will therefore continue to be an evolving area, continuously subject to change.

While IoT providers necessarily offer many proprietary solutions at present, these are ahead of finalized regulatory requirements. Such regulations on the way cover all elements of IoT, including home / consumer IoT not just industrial and commercial or enterprise businesses and not necessarily to the same degree. Such regulations also involve all communication protocols, both wired and wireless. Regarding wireless, a variety of communications technologies and protocols will continue to proliferate. Cellular is just one of these, but with its own high and low bandwidth variations, upcoming 5G developments and recent developments in unlicensed spectrum.

Aeris' solutions for cellular IoT device identity, data access security, and remote update management address today's security risks and help IoT device manufacturers and solution providers comply with existing and near-term regulations in ways that are designed to be easy to implement. As cellular IoT solutions expand into hybrid offerings combining cellular with other communications protocols and in deployments utilizing licensed and unlicensed spectrum, Aeris' security solutions are expected to develop with them.