Billions and billions of IoT devices are coming, are they really secure?

IoT Security: the issue with protecting billions of IoT sensors and devices, when many of them have limited CPU processing power and are running on batteries.

To hear from the experts, Planet Earth is on the verge of the next big techno-clysmic event, to be carpeted by low-cost ubiquitous wireless sensors reporting virtually everything imaginable, on people, at home, on the road, in the air, in the cities, in the enterprises, at the hospital. So where are all the promised billions and billions of IoT devices? Why aren't they under every rock as we were led to believe? What's the problem? Cost? Technology? Regulation? Cheap silicon, reliable wireless connectivity, mass consumer adoption of technology abound – what could be missing?

Well no… There's one small problem that was also swept under the carpet, oh yeah, that pesky security thing.

With new hacks announced weekly, and as government, health, and energy grids get taken over, governments around the world attempt to pacify the public into believing that they are considering these vulnerabilities seriously and will help solve this escalating threat on society. Are they?

To understand, first let's take a look at the IoT wireless connectivity industry. The majority of IoT devices will be dumb sensors and in fact be quite epigrammatic. In reality they will measure some simple data (personal, environmental, physical, etc…) and report this data typically via some wireless connections to the cloud a handful of times each day, week or month. They're not going to be streaming video or having lengthy conversations because most of them are very small and battery powered. They need to run for several years on a tiny battery or an energy harvesting power supply. Realistically these IoT sensors can only send a few messages each day.

Conversely, it is obvious that the mobile network operators (or MNOs), driven by the GSMA at its core, have little grasp of the real world uses for IoT. The GSMA and its member companies stand by a model in which IoT devices consume data at rates of hundreds of kilobits per second. Understandably that is what MNOs want to sell, but it's simply not what IoT devices need. If we are going to achieve the nirvana of billions of devices, then connectivity and silicon need to be cheap, cheaper, and uber-cheap. Cheaper and simpler than GPRS, much simpler than the new NB-IoT or LTE-M offerings, and easier to manage than the future 5G. The cellular industry has yet to realize that the reason we don't already have billions of IoT devices is that even GPRS

is way too expensive and complex to implement for a personal or environmental sensor. In other words, you don't use a sledgehammer to kill a flea.

So back to IoT security; what is the current status of IoT security?

Let's just recap the last IoT couple of years with a sampling of 3 newsworthy events….

First the major grid cyber attack in the Ukraine, which was blamed on a state nation attempting to disrupt the Ukrainian grid by shutting down the country's substations. Post-mortem details that malware was injected into power-grid computers to turn them off, using malware to send control messages to the substations. Fortunately, as these "valid" commands seemingly originated from the central control system, the substations performed an orderly shutdown without causing any permanent harm to the grid – lucky for the power grid. Next time they won't be so lucky. Turning them all on again en masse could do even more damage, as restoring power when demand is unknown will burn out equipment on the grid, which gives a hacker the capability to cripple every country so reliant on the flow of power. Ukraine aside, just imagine what would happen to the US or Japan if even 10% of the power grid was shut down?

The second very public incident involved Nest thermostats in the US, which started to turn off, leaving their owners in freezing homes. That problem was allegedly caused by a simple bug in a software upgrade. The bug caused the internal battery to drain. At the same time, the UK Hive thermostat experienced a similar problem, where an upgrade directed thermostats to ramp the temperature up to an equatorial 32 degree Celsius. Coincidence? Both were rectified quickly; however aside from consumers annoyed that their thermostats were not as smart or reliable as they had been told, these events were certainly not shrugged off by security experts. Coincidental simultaneous bugs, or hack-attack?

The third issue was a report by the UKs Daily Mail about a smart gas meter, which stopped working. It reported a British Gas customer who had smart gas and electricity meters installed. Three months after installing, on a very cold morning the gas meter turned his gas off. A field technician blamed the battery (which is supposed to last fifteen years). It is unknown if this was an isolated incident, but it is every bit as important as a hacked pacemaker. Life and death is not measured in percentages, nor a failing battery (which should have been auto-detected in any case). Even more recently hackers have reported on how easy it is to hijack the latest Smart Meters making sensationalist claims that they could be caused to explode. While exploding meters are very unlikely, they could turn off the power to the home and cause damage to equipment inside or allow the home to be more easily entered by disabling alarms that might be connected via the smart meter. There is a drive to make the house smart too by using the meter as the focal point, now that should really worry you!

In the fourth issue, hackers were able to get into an unnamed casino network through its Internet-connected thermostat controlling the temperature of the fish tank located in the lobby of the casino. The hackers exploited a vulnerability in the thermostat to get a foothold in the network and once there, they managed to steal the high-roller database of gamblers and then pulled it back across the network, out the thermostat, and up to the cloud.

Were all these problems due simply to sloppy engineering, or were they the result of black hat hackers? The lack of a clear, definitive analysis is perhaps just as revealing.

In the world of connected devices, faults like this should set alarm bells ringing, as failing embedded software either indicates bugs which needs to be fixed - more likely poor quality control, or more worrying an abyss of security vulnerabilities.

Poor software or terrorist friendly? In his world, every connected device can be hacked – because today's devices simply are not designed to be hacking sentient, nor actively thwart hacking.

What about 802.11 Security ?

A lot of effort has been put into the connectivity aspects of 802.11 derived such as Wi-Fi (802.11ah), Zigbee and Z Wave. However they have relied upon SSL, SHA, peer-to-peer authentication, and Trust-Zones. In fact 802.11 has mediocre and easily hacked security designed in. Sadly each and every one of these security mechanisms implemented in 802.11 have been hacked, and both Google and Cisco, two of the industry's giants frequently warn users of breaches in 802.11. Additionally 802.11 implementations rely upon on-board CPU to not only process math intensive encryption/decryption algorithms, but must by design exchange multiple messages between devices in order to authenticate with each other, which makes these systems extremely vulnerable to hacks. This in fact was the way WPA-2, the strongest encryption standard used by most WiFi networks today got cracked not long ago, by manipulating and fooling the 4-way handshake protocol. This type of "heavy" processing by definition requires expensive and power-hungry silicon solutions. Heavy CPU and multiple message exchanges generated by encryptions like WPA-2 simply drain the battery, need high computing power and cannot realistically satisfy the needs of the IoT sensor model of small, infrequent, random and cheap data transmissions.

One of the largest market for IoT using 802.11 is the home market. Vendors such as Samsung and LG have targeted this market but have both experienced embarrassing hacking publicity. For many sensors around the home, it may not matter if they can be overheard. It matters more if malicious packets can be injected, as that can lead to false alarms, the transmission of incorrect data back to the server, or the annoyance of something being turned on/off – a home security alarm for instance. Imagine what it could be with medical sensors monitoring people with chronic conditions.

One fundamental issue for consumers that has yet to receive the necessary attention, is how to easily add new wireless IoT devices to a home network while preventing rogue ones from attaching. The act of adding any consumer device to a network can be daunting (and in a majority of cases is a massive barrier to adoption) to most users and potentially restricts any company's potential sales. Pairing and authentication are two of the most difficult aspects of wireless IoT, as ease of use and security work in opposition to each other.

Consider swapping devices in and out without opening security vulnerabilities is a real challenge. This means working out how to distribute security keys safely around your system. This level of security simply does not exist in today's IoT products and will not exist if manufacturers continue on their current trajectory.

To the rescue: NB-IoT, LTE-M, SigFox, LoRA, LPWAN?

We can all trust in the combined expertise of modern technology and service providers to have learned the lessons for the needs of a secure network – right? Well not so fast. The problem is that 3GPP (the 3rd Generation Partnership Project), the standards body which has been responsible for the 3G, 4G and 5G mobile standards, enigmatically ignored the needs for Internet of Things even while GSMA paid lip service to IoT. 3GPP members failed to design something to replace the old 2G workhorse GPRS, which is still responsible for most of today's machine-to-machine (M2M) communications. Instead, GSMA spent all of their efforts designing high power, high speed, expensive variants of 4G to support the burgeoning dynasty of smartphones, none of which is any practical use for the Internet of Things. Self-serving to say the least.

Not surprisingly, this GSMA omission was seen as an opportunity, and LPWAN (Low Power Wide Area Network) technologies appeared in the form of SigFox, LoRA, LPWAN et alia to take advantage of GSMA's ignoring the IoT requirements for very simple devices. To address this challenge, GSMA directed the 3GPP body to specify their own solution, one of which was ultimately named the Narrow Band Internet of Things (NB-IoT). NB-IoT's pedigree provided a modicum of security due to its reliance on SIM cards for user authentication/verification. However, as would soon be realized, NB-IoT really merely satisfied the MNO's parochial requirement to protect their revenue source, and did nothing to specifically address security concerns for providers of IoT device vendors begging for a secure network.

In fact NB-IoT does not protect any IoT device from a rogue hacker, as long as the hacker has a valid SIM. It is unlikely that an NB-IoT providers would keep a blacklist of SIMs (circular logic in fact).

So what is the optimum IoT connectivity which can reduce cost yet provide the vital missing security? As indicated above, the IoT market will be too large for one single wireless technology, therefore many solutions will be offered and ultimately find their niche; for example NB-IoT or other cellular technologies, which deliver higher data rates with better command and control mechanisms, will be attractive to customers who are

willing to pay more. LoRa might be more attractive in private networks, and Sigfox for the lowest segment with limited uplink and practically no downlink but overall cheapest cost.

HOWEVER - the problem with multiple different standards is, “which one does a manufacturer choose if they’re shipping a global product?” One support call would completely kill any profits from the addition of a different wireless system to tens of devices; how can vendors guarantee security with so many connectivity standards?

Consider for example, NB-IoT does not provide a practical nor efficient provisioning method. Putting SIM cards into billions of devices is simply impractical. Yet every MNO’s IoT solution always requires SIM cards. Additionally, the MNO desire to add location suggests that they are all locked into a technology frenzy, rather than understanding what the market really needs. The dream of a $1 NB-IoT endpoint still seems a long, long way away. The licensing of the NB-IoT modem will always prevent the best price point even as patents lapse – the exact opposite market objective of IoT.

Further, history has proven that people will attempt to hack into IoT products. Not necessarily for any malicious reason, but because it’s fun. It’s the first thing any IT professional will do – and that’s just the White Hats. We’re not even talking about the mythical pimply faced teen looking for something to do between video games. The fact is that IoT designers need to think carefully about what level of security a product needs, and it is quite obvious that this requirement is not being considered seriously. Just go to any IoT product or service website, and try to find how the product’s authentication and verification works without the equivalent of a 2.3Ghz CPU powered by a car battery!

Due to the obvious absence of a credible standard or solution, all of the emerging IoT sensor-based devices that employ wireless for control and monitoring create their own proprietary wireless protocols. These are designed and tested in isolation, and have little security. The tools that support these IoT chips and reference designs make it very easy for designers to get prototypes up and running and bring the resulting products to market, but they generally leave security implementation to the designer.

In summary, IoT wireless security is difficult, homegrown, and remains an afterthought with only lip service paid to the security problems or hand waving at all the options - but which option?

So what’s the answer?

Clearly multiple forms of wireless technologies will and must emerge to satisfy wireless IoT issues of range, data speed, and cost. However it is also clear that IoT by definition cannot be a system of homogeneous devices, all relying on a single means of wireless connectivity. Pragmatism means systems will be developed to cover a broad range of technologies: Bluetooth LE, Zigbee, Z-Wave, LoRa, Sigfox, NB-IoT, LTE-M, Wi-Fi to name just a few. Connectivity is simply not the major issue of IoT.

The most important issue is how to provision uniform rock-solid security across all technologies so that the operator has only one security mechanism to deal with and can consistently keep it updated and invulnerable to attack.

Vendors and consumers need to know and trust in a single security scheme, which is unambiguous, and simple and inexpensive to implement across multiple technologies and applications. It does not make any sense for a service provider or company to implement multiple security systems: one requiring SHA, a second with SIM cards for authentication while requiring a separate means of encrypting data, and a third which is based entirely on proprietary silicon relying on Trust-Zones (e.g. ARM), and then a multiple different methods of data encryption (AES128, Blowfish, TripleDES, PGP). This multiplicity of security standards would increase management expenses exponentially, as well as create multiple weak points in a system – simply impractical and totally hackable.

IoT requires a method that eliminates both multiple battery draining message exchanges, and CPU intensive calculations.

It should have the latest un-hacked encryption method designed for short, infrequent, IoT messages and highly constrained devices, which randomly updates its security keys. Such a system should make it mathematically impossible for any hacker to "sniff" sufficient amount of packets in order to hack any single sensor in less than 20 years. The design should prevent even a single breach to allow an en masse access to the network. The security system should be self-aware such that even in the attempt to hack – the hacker should be immediately identifiable by the system. Machine learning should recognize emerging attacks, reverse out the hacker's path, and characterize the hacking intelligence as it attempts to adapt and subvert the security system – in other words learn what the hacker is learning – and then calculate a tactical response to stop him.

Follow us at www.iotaBEAM.com or look for iotaBEAM on your social media (LinkedIn, Twitter, Instagram or Facebook) to learn more about how we have been able to resolve these issues with StarDust™, the enduring security solution for low complexity IoT sensors and devices.