Making it safe to connect

Addressing the wicked challenges of security in IoT needs co-ordinated action.

Not so long ago, the Internet of Things (IoT) was seen as a quiet revolution. More recently, IoT has hit peak hype and attracted a great deal of attention from the media, as analyst and vendor forecasts have been somewhat optimistic. Regardless of what you think of the bulging numbers and the speciation of IoT products and services being announced, it is clear the rise of connected 'things' and the low costs of technology are creating disruptive forces throughout all industrial sectors, and felt in virtually all corners of modern life.

Technology is dual purpose; it can be used for good, yet it can also be used in ways which expose unwelcome threats. With IoT, security is a top three challenge and moving to a regular board room agenda.

Applications are typically composed of many moving parts – devices, gateways, networks, sensors, actuators, storage, compute, software, people and so forth – and much of this is impossible to guarantee in action.

The familiar adage that 'complexity is the enemy of security' and 'security does not compose' is ever real in the IoT context. Conceptually and practically, IoT is moving in the opposite direction to where security experts would like it to be – and it's moving at an accelerating rate. If this wasn't challenge enough, cost, convenience, lack of standards, questionable ethics and the threat of heavy handed regulation and blunt law combine to create a motley dynamic of the 'IoT wild west'.

From an industry perspective, we have to think carefully about our outputs and resist the urge to abandon caution in pursuit of quick, short-term profits.

An arms race?

Security is often described as an arms race and perfect security is asymptotic. We begin with the technical aspects of course but that is not, and will not be, sufficient. The IoT industry will need to develop new working practices across convergent groups whilst cultures evolve. Supply chains will also need to collaborate in effective ways to avoid the vulnerabilities that exist between organisational boundaries and promote a duty of care towards the customer throughout. This is crucially important – adversaries will test defences for weakness across the entire system and often need only one flaw in the armour to get their intended payload.

The status with IoT today is variable. Whilst some parts are quite robust, certain segments are woefully inadequate and certainly not fit for purpose. With cyber-crime on the increase and IoT attracting attention, there is now significantly more at stake than financial fraud and industrial espionage. At the risk of 'scaring the children', it is not an over statement to mention that, with hyper-connected systems, the potential for sabotage of our critical national infrastructure could threaten us more substantially – even physically.

It is not hard to find IoT hacker stories in the news – in fact, they're rife. A short overview such as this cannot do it justice, however here are a few examples: The story of the year in 2015 was arguably the Jeep Cherokee hack, but other connected car hacks include the Tesla and the

INTERNET OF THINGS SECURITY FOUNDATION

Formed as a response to existing and emerging threats in Internet of Things applications, the mission of IoTSF is to help secure the IoT in order to aid its adoption and maximise its benefits. To do this, IoTSF will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems.

IoTSF promotes the security values of a security first approach, fitness for purpose and resilience through operating life.

IoTSF is an international, collaborative and vendor-neutral members' initiative, driven by the IoT eco-system and inclusive of all parties including technology providers and service beneficiaries.

Mitsubishi Outlander. At the other end of the 'thing' scale, lightbulbs have the potential to compromise your home network – in July 2016, vulnerabilities were discovered in the Osram Lightify range. And poorly secured IoT devices are already being 'zombified', amassed into armies and and turned against specific targets. Recently, the high profile security blogger Brian Krebbs had his website taken down by a 620Gbit/s distributed denial of service (DDoS) attack from IoT devices. That episode was eclipsed almost immediately by an attack on French hosting firm OVH with a datastream that peaked at more than 1Tbit/s.

The rise in ransomware is also beginning to target IoT devices and scales very neatly as a criminal business model. We have also witnessed curious behaviours in 2016; one 'grey hat' organisation deliberately targeted a medical equipment company's share price and monetised a vulnerability report via short-selling the stock.

Many of these reported issues could be avoided in relatively simple ways as some vendors are making it easy for the hackers and criminal gangs. In far too many cases, these attacks are possible because even the most remedial of precautions have not been attended to, such as default passwords, hard coded passwords and no encryption. This really is '101 stuff' and, as David Rogers, CEO of Copper Horse Solutions says, 'we can't carry on like this'.

Finding hacker stories is easy; which, by itself, provides a sense of the scale and scope of the problems. Spreading fear, uncertainty and doubt is also easy, but not very helpful. We are engineers, we are technologists, we are entrepreneurs and we need to act. We need to acknowledge the problem, understand the threats and make informed decisions to manage the risks at every level. We need to provision defences in depth and, given the 'many moving parts', our efforts need to be co-ordinated.

Solving the challenges

But who owns the problem and how do we start to solve the challenges of security in IoT?

On 23 September 2015, the IoT Security Foundation (IoTSF) was launched as a non-profit organisation seeking to meet the bigger picture challenges of IoT security head on. Its objective is to catalyse change by working collaboratively to deliver accessible, actionable and low cost – free – best practices to industry. And that's just for starters. Whilst cyber security is advanced in certain quarters, the pressing and immediate issues in IoT are significantly more remedial and we must start with basics. We have to level the bar, then raise it from almost zero assurance levels (in some sectors), then ratchet upward from there.

IoTSF has started with the creation of five priority working groups. Each group has been tasked with creating high quality guidance which can be easily consumed by industry. Those priority groups are:

- **Self-Certification Framework**. A structured approach to implementing security measures. This aims to be easy to adopt, have minimal cost/overhead and applicable to any organisation in the IoT supply chain.
- **Connected Consumer Products/Smart Home**. The unregulated consumer space was prioritised for guidance due to the acuteness and volume of reported issues.
- **Vulnerability Disclosure**. A template and guidance documentation to help connected product organisations setup the mechanisms to be 'vulnerability-ready'.
- **The IoT Security Landscape**. Reference architectures which map sector implementations and inform the vulnerability areas and points of attack.
- **Patching Constrained Devices**. A consideration of what is required to patch and maintain the hygiene of resource constrained IoT devices.

> “We need to acknowledge the problem, understand the threats and make informed decisions to manage the risks at every level. We need to provision defences in depth and, given the 'many moving parts', our efforts need to be co-ordinated”

One year old

It may not feel like it, but the IoT is still nascent and IoTSF itself is just one year old. As any start up knows, you have to get organised and mobilise. IoTSF has done that and is already making an impact. There is a great deal more planned for 2017 now that the initiative is firmly up and running, most notably addressing sectors beyond the connected consumer and connected home.

We encourage readers to do their part where possible in reducing the threats of IoT – whether you're a provider, buyer or consumer. Let's make it safe to connect.

IoT Security Foundation

https://iotsecurityfoundation.org