Internet of Things – Making it secure

The development of the internet changed the way our world works, now it's changing again....

The Internet of Things (IoT) will create a world in which physical objects or "things" that are part of our everyday lives communicate securely with each other to anticipate and recognise our behaviour, sense our environment & respond on our behalf and allow us to interact with things in ways previously not possible.

This connected world will enable new opportunities for your business and change the way your customers interact with your products, however, it will also introduce new security threats and challenge the way we address them.

Our starting point

In traditional networks there is a huge body of knowledge and therefore security threats are well understood, how we deal with them is also well defined. Today; a well designed network or cloud solution can be made secure. Most if not all security breaches exploit a defect or oversight in a particular implementation rather than a fundamental weakness so if you get the design right you will have a secure solution. This is partly a result of the fact that such networks have been established for a long time and partly because they are relatively simple in structure. Devices tend to connect using one network, to one platform, to one system/user so the number of permutations is large but manageable. An example might be a Smart meter which connects over the cellular network to a cloud server application – very simple and clearly constrained.

IoT systems

The Internet of Things suddenly introduces a different and less predictable situation; we can have many devices that are communicating over disparate networks to various platforms and numerous other systems/devices. In this situation we have an unimaginable, and in fact indeterminate, number of permutations. So for example a Smart central heating controller could communicate with a mobile phone over Bluetooth while connecting to a cloud server over cellular and sensors over Zigbee!

We can see from this example that we have a device which could be communicating simultaneously with several other devices over different networks, therefore we have devices with multiple interfaces (endpoints for different networks or communications methods) between them, this not only allows traditional threat vectors to be exploited but also introduces Interface vulnerabilities such as depicted in Figure 1.

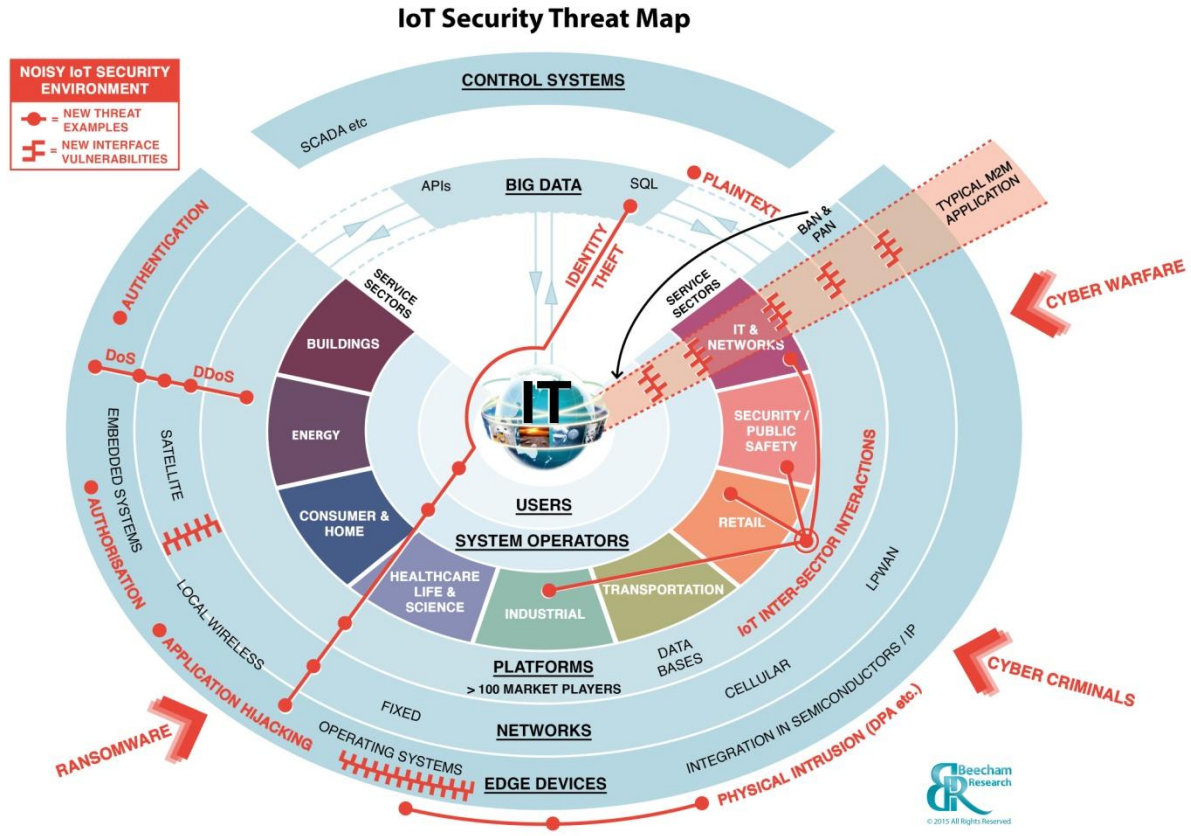

Figure 1

This myriad of threat vectors means that we need to think of solution security in a different way, it must be thought of holistically so that the complete system is secure, it is no good just focussing on one bit of the solution, even if the component you manufacture is secure then a weakness in a connected device or network could be used to compromise on your device, key factors in providing this holistic approach and the desired level of trust will be authorisation, authentication and encryption.

Because of this necessary holistic approach it is important that a complete system or solution is designed from the ground up with security as a major priority, organisations need to be thinking about security from the boardroom down.

When developing a solution for the IoT firstly you need to understand the problem, capturing your user requirements at an operational/product level is one thing but make sure you have complete understanding of the security implications and ensure oversight of the development by all stakeholders. It is also fundamental to consider the full lifecycle of the product you are creating, if you plan a device to be installed and working for 10+ years then you need to consider what might be needed during that time, allowing for new features, changes to security architecture, improved encryption schemes. If you have to do firmware upgrades over the life time of the product and on day one you only have 10 bytes of program memory left then you are likely to have problems!!

Talking about firmware upgrades – there is no point in developing the most secure solution on the planet if someone can install new firmware which disables the security features or disables your ability to do further upgrades – just ask Jeep?

Who owns the problem

With the IoT we are creating a very complicated supply chain with lots of stakeholders so it's not always clear 'who owns the problem'. By way of an example with a simple home application; if you buy a central heating system and controller which requires you to push a button to increase the temperature then if it stops working you contact the company who supplied it. But if you buy a central heating boiler from one company, a wireless temperature controller from another, download a mobile App from another and have a weather station from another supplier then whose job is it to make sure it's secure and reliable? The simple cop-out is to say 'the homeowner bought the bits and connected them together therefore it's their responsibility' – well I'm sorry but that isn't good enough!

Manufacturers can't simply divest themselves of responsibility simply because the home owner bought several component parts from different retailers. As a manufacturer you have a responsibility to ensure that your product is secure and reliable when used in any of the possible scenarios and use cases which means that manufacturers need to work together to ensure interoperability – we all own the problem!

This might come as a shock to some companies/industries but at some level even competitors have to work together to agree and implement architectures and connectivity that is secure and reliable. Standardisation is a good example of this, if you look at the companies actively working together in ISO, ETSI, Bluetooth SIG etc. then they are often fierce competitors but they all recognise the need to work together to define common, secure and reliable platforms around which they can build interoperable products.

Solid foundations

Finally, building on solid foundation; if you develop a solution, on let's say Windows CE, then you know you are building on a platform which is known to be weak therefore nothing you do is going to make it secure. To have a secure and reliable solution you have to build on secure and reliable foundations.

Summary

- Consider security from the start and holistically
- Understand the problem
- Accept your share of the responsibility
- Collaborate with other industry players
- Use solid, reliable and secure foundations

If we do it right the IoT will be fantastic!

About nfs

nfs are leaders and innovators in the NFC and Bluetooth Smart industries specialising in the design and development of products for IoT applications, working with its customers to turn their ideas into market leading solutions. We are committed to creating value for our clients through our expertise and the application of wireless technologies.

Written by Glenn Needham

usingnfc.com