KEYNOTE SPEECH

RICHARD MARSHALL (XITEX LIMITED)

Richard is Plenary Chair at Internet of Things Security Foundation and Managing Consultant at Xitex Limited, which provides consultancy on defining and launching wired and wireless connected products with emphasis on creating secure IoT products and their secure supply chains. He has spent over 25 years in the electronics and communications sectors, having worked for Lucent Technologies, Sony, Cisco and also being a founding lead team member at startups Ubiquisys and nSine. At Ubiquisys and subsequently Cisco, after its acquisition of Ubiquisys in 2013, Richard was the Product Manager for their global cloud based activation system for 3G/4G small cells. This role being the security advocate, technology champion and secure manufacturing supply chain architect for the small cells manufactured in Europe and SE Asia.

Richard has held a variety of senior lead engineering roles in the wireless and consumer electronics sectors with a focus on embedded and FPGA-based platforms. In the last 25 years he has been involved in FPGA implementations for a range of applications including custom CDMA wireless and PCM processing, 1 bit DSD professional audio, petrochemical 'down hole' sensing, medical and industrial instruments. Aside from design of products Richard has been deeply involved with new product introduction in production in the UK, USA, Europe and SE Asia, always with a focus of 'on line, on time'.

SUMMARY

The speech will motivate and discuss the following key topics:

- The need for a holistic view on IoT security - point solutions are not sufficient.
- The impact that security has on an IoT device's supply chain and it's lifecycle.
- Delivering secure IoT solutions is more than just security requirements for products but also ensuring the business processes are in place to support the products' life cycle and vulnerability disclosure.
- Raising awareness of the scope and requirements for producing secure IoT products and how the IoTSF compliance programme is intended to help OEMs, Retailers and end users.

TITLE

IoT Security: the need for a holistic view.

ABSTRACT

Security for IoT products and services has a much wider scope than just implementing product security requirements, since it impacts a manufacturers' or service providers' wider business activities. This presentation considers some of the impacts on suppliers that want to launch and support IoT products, not just the product requirements but the wider aspects such as making or procuring a secure supply chain, developing a vulnerability policy to cover all aspects of product life cycle management.

If a product is to become an IoT connected one, consideration has to be given to the implications of what that means. It may not be that a product is being hacked to subvert it's operation but that it is being used as a route to gain unauthorised access to some other device or system. An example might be of a consumer product with wireless connectivity such as Bluetooth, which when taken into a hospital has the ability to subvert medical equipment surrounding it. Alternatively as was demonstrated by the recent DDoS attack on the domain name service provider Dyn, without adequate security a product can be used as a host to mount such attacks, which in that particular case was a relatively small number of ~100,000 of devices generating an estimated peak of ~1.2Tbps of internet traffic. Ultimately one of the most concerning type of attack are those against devices that have safety critical functions such as those in medical, transport and infrastructure installations. Taken in the context safety, security becomes another facet of product quality, with all the ramifications that it brings to the ultimate product issue, that of a product recall.

Given these types of implications and especially the safety aspects, have the product security requirements been captured including the supply chain ones where the manufacture and provisioning of the product are likely to be made by third parties. Are there sufficient quality checkpoints in the proposed supply chain to ensure that insecure product cannot escape the supply chain and there are secure ways of the devices being taken to an end of life state; without these processes there is always the potential risk of unauthorised or compromised product(s) damaging a company's reputation.

Having put together the supply chain elements the operational parts of the business need to ensure that there is a vulnerability disclosure policy in place. As as has been shown recently companies that have not ensured that their senior executives are properly briefed in the event of a disclosure, especially when dealing with the media, can deliver mixed messages with the consequent loss of brand confidence. Albeit not a security related product quality issue but the Samsung Note 7 battery issue is a timely reminder of the kind of impact that can be had on a global brand through a product quality issue and it's consequent recall.

Finally there is consideration as to where organisations can get support in putting the whole product life cycle in place and some of the possible routes to demonstrating that products are trustworthy both for Partners, Retailers and Customers, particularly in this early stage market with an absence of suitable standards and a regulations.