WWW.BLUESKYTEC.COM

BST TECH – QUESTIONS AND ANSWERS

1. **What is BST IP?** - Blueskytec (BST) IP is an integrated solution of hardware and software items for securing IoT.
2. **What does it look like?** - it is available in a number of forms (1) as a set of files that are used in the design phase of an IoT product (2) in a physical chip (3) in a chip on a circuit board (4) in a demonstration device (5) in a full IoT product.
3. **What is IoT?** - A physical product with a tiny computer that connects to the internet – requiring little or no human contact.
4. **Where do I find IoT devices?** - in everything, in your hotel door, the traffic lights in the street and railways, medical implants on your body, the message board in a subway, many in the car – work coffee machine, vending machine, smart doors, alarm systems, elevators, cctv systems, hospital MRI scanners, infusion machines, gas pumps, cash point, payphone, sewerage valves and pumps, electricity sub-stations, heart pace makers, toasters, TV's.....
5. **Uh? Toasters – Why is a toaster being connected to the internet? And what benefit does that have for me?** - well nothing. The toaster is not connected to the internet for the benefit of the customer – most customers would not know if it is connected or not. It is connected for the benefit of the manufacturer, so that they know how it's being used. Tesla records all data from their customer's cars, and has amassed 1.6 Billion miles of data of how they are being driven!
6. **What is the problem?** – Until recently there was no problem, but criminals have found that most IoT has no security and have started hacking it.
7. **Why?** – why not, to create chaos and anarchy. Because it's there and the want to demonstrate power or winning a competition, because state actors are waging warfare, for money, to destroy a competitor or a competitors capability, human nature!
8. **How does that effect me?** - Ransomware! Every device you touch has the potential to be an IoT device – from your hotel door, smart meter – to your car. If these are hacked they can stop working whilst you are using them! We have witnessed ransomware attacking the UK National Health Service and computers worldwide on Friday 13th May 2017. Now imagine every car, MRI scanner, medical implant, automatic infusion machine, traffic light, sub-way signal in a major city

is targeted, encrypted and stopped until a ransom is paid. You would soon pay up if your medical implant was being hacked!

9. **OK I understand something important like my car or my medical implant, but I don't care if my coffee machine is hacked or not!** - Well yes, we agree that we don't care if our toaster or coffee machines are hacked. But criminals use the toaster or coffee machine as a back door into your computer network, and from there they access your computers and files. A new coffee machine installed in your office is the perfect host for a Trojan that infects your network and steals valuable IP. This could be on any device in your company, from vending machines, lifts to the smart recycling bin and HVAC (heat and ventilation Air Conditioning) system. We do not vet every company that supplies equipment to our companies and any of them could have been compromised to install malware in their products. Take for example Vending Machines. It would be easy to compromise the security in the local vending machine company that supplies the products for your vending machine, because they are likely not to take security as seriously as you. However, once the criminals are into their network, they can infiltrate your network through the maintenance and supply ports on the vending machine in your office. Now multiply this through your entire supply chain of Office items (from stationary, toiletries to the built environment) and you can see the attack vector for IoT is very serious. Even if your local vending machine supplier takes security seriously they might have a compromised toaster or coffee machine in their staff kitchen!
10. **So why don't manufactures secure them?** – Money! It has not been at the top of the things customers look for when making a purchase, not at the top of the sales person's list of sexy features and not at the top of the engineers requirements list.
11. **Why don't we get the engineers to build secure IoT?** - We could – great security already exists, but it's way too expensive for IoT. IoT computers are usually less than $10. We need just enough security for IoT at a rock bottom price (<$1). We need to persuade engineers and companies to design them into IoT at the getgo.
12. **Why has no one got a solution?** - All technology firms compete against each other on features and price – bigger is better – right? No one has reduced the features for security to produce chips

for <$1. But they are starting – Intel has announced the development of a secure IoT chip for everyone in the world to use. It's just a matter of time.

13. **What is the size of the market?** - Big. Estimations for IoT are 20 Bn devices by 2020. But some estimate that by 2030 everyone on the planet will interact personally with 10-100 IoT devices on a daily basis – that puts the upper estimate at 2000 Bn devices. If everyone has some sort of medial implant (several in one body maybe) then the market is very large and continuously expanding.
14. **Who is your target market?** - there are 2 major markets for this type of technology, Systems suppliers and Original Equipment Manufacturers.
15. **What are systems suppliers?** - These are companies that take standard off-the-shelf products and connect them together to build a system for their customers. They do not manufacture any original equipment but will design and manage the cloud and desktop/smart device software for the system.
16. **What are Original Equipment Manufactures?** These are businesses that have an established or new product portfolio and want to add IoT security to this. They can take our IP and integrate this into their board or chip. However, many OEM's do not have a chip capable of integrating the security at the correct price point for IoT. They are usually focused on other parameters.
17. **How can BST help?** BST would work with the OEM to develop their new IoT product at the lowest price point for security. We have demonstration chips and wearable technology that can be used immediately to integrate the OEM's cloud access software to show the benefits to their customers.
18. **What about time to market – how does this help?** A custom chip for a IoT device like a medical implant (ASIC) will take time and money to develop. However, the BST IP would help the OEM on the time-critical paths for market trials and would de-risk the integration phases. The ASIC could then be developed out of the time-critical phases and be introduced in a staged and managed manor.