IOT - THE PERFECT STORM

Summary

To the average person IoT means very little. They understand the Internet and use their smart devices for Facebook, Twitter and WhatsApp etc. They trust their banking system and happily purchase goods from Amazon using credit cards or Paypal. They trust that water will flow from their tap at home, the lights will stay on and they assume that they can fill up their gas tank at the petrol station. However, there is a hidden layer of the internet (not the dark web of drug dealers etc) that is becoming more relevant and starting to touch the life of the average person. This paper seeks to outline IoT and Blueskytec's IoT security solution.

Critical National Infrastructure

We take it for granted that the water in our taps will flow, and that the electricity & gas will be there, and that we have a mobile phone signal when we need them. All the utility companies world-wide have started to connect their physical assets (pumps, valves, digesters, mobile phone masts etc etc) to the internet. This connection has been implemented by individual companies in a rather patchy way. Many of the utility companies have not invested in security for their connections with a few disastrous results (Ukraine Power Outage). Many have – the banking sector is a stand-up example of how it can be done properly (probably because it involves money – not water). Many have not – the water industry is appalling. Fortunately, governments have recognised this potential disaster and are mobilising an army of experts to tackle the problem.

Governments are rightly, concentrating on the Critical National Infrastructure (CNI) – Banking, Water, Electricity, Gas, Transport, Communications - and have engaged companies such as Thales, Fortinet, BT, Lockheed Martin, BAE systems, Harris etc to develop solutions.

This is great because these companies are fantastic at producing high tech equipment that can manage the security problems for our Critical National Infrastructure. These are heavyweight solutions that have evolved from military systems and are excellent at providing high grade security.

IT companies

The internet is an enabler. All companies from estate agents and banks through to shipping companies rely on data flowing across the internet for their business. More and more transactions are done "on-line" using payment systems such as PayPal, Visa or Mastercard.

Large IT companies provide the backbone across which this flows and many have excellent products that help protect the internet from attack. All of society rely upon these IT companies to deliver seamless data systems so that their business can reach customers and flourish.

The internet is made up from many hardware systems that "route" individual messages from a customer to a business. As the messages pass through hundreds of "routers" they are diverted to their final destinations. This happens in the time it takes to blink your eves and is seamless. Replies from the business to the customer are routed back along the same path. The path that the messages take is given in the address at the top of your web browser – or its given by a Google search.

The devices that route the messages across the internet are called – you guessed it - "routers" and many companies make routers. These devices are properly designed, implemented in special computer hardware and are very good at their job.

Things on the Internet (IoT)

So we have two types of uses for the internet – Commercial Transactions and Critical National Infrastructure.

We have established that governments and largely defence companies are producing technology for CNI. We have described IT companies enabling commercial organisations to reach their customers (Business to Business – B2B and Business to Customer B2C).

However, there is a third aspect to the internet that has started to be part of the public language – Internet Of Things.

So we have all heard about the Internet of Things, but what does it actually mean. I have seen many explanations but they all seem to require a level of knowledge that surpasses the average Internet user. The simplest definition is "a physical device that connects to the internet but does not have a human interface...".

A few examples of these are:–

- Digital TV Recorder,
- Smart connected Car,
- surveillance camera systems,
- smart home appliances (lights etc),
- Home gas and electricity meters,
- trackers,
- water pumps in sewerage systems,
- assembly robots,
- oil extraction pumps and valves,
- Smart Lifts in hotels.
- Guests doors in Hotels

These are all good examples of IoT. They share common features – simple human interaction (a button for on/off or a volume control), they can all be touched and kicked, they all connect to the internet in a

way that is seamless to humans. The critical point is that it is very difficult to know if a device is internet enabled by simply interacting with it. Take for example a Lift in a hotel. The average user has no knowledge if the lift is controlled by a big computer in the hotel somewhere, of if it is a good old fashioned electro-mechanical system.

In fact in the example of a Lift it is a good bet that in a big hotel with many lifts they are all connected to a big computer in the hotel somewhere. This is so that they can be programmed to anticipate when people will want them. For example, they would all need to return to the bottom floor in the morning as people are arriving to work, and all return to the middle floor in the evening as they are leaving.

This is a classic IoT device it seamlessly and silently works in the background without requiring any human input (save pressing the call button, and the floor number).

However, there is a dark and sinister side to all these devices being connected to the internet – they can be taken over by malicious humans to perform tasks they are not intended for. In the smart lift example, a malicious person controlling a computer could take control of the lift and lock its occupants in the lift, or send all the lifts to the top floor and never come down.

Estimates of around 20 Billion IoT devices being connected to the internet by 2020 have been reported. It will not take long for the whole world to be connected to the internet and in this utopia the criminals will flourish.

Why is this? Well we must delve into the murky world of embedded systems. These are computers that are placed inside physical devices that we use on a daily basis but do not know they are there. Fuel Injection in cars has been around since the early 80's and the reason it became successful is to use of the car computer (ECU). We have all had cars where the ECU needs replacing. Well, this is an embedded system and they are being connected to the Internet and called IoT devices.

The critical point of this is that traditional Embedded Systems have no security, and so engineers that are adding Internet capability to Embedded Systems do not add expensive security, because it was never on the requirements list.

So we now have the perfect storm - 20 Billion IoT devices on the internet without with any security. It is not all bad. CNI (banking, communications, water, oil, electricity) are all actively being protected and IT companies are stepping up the security of their products to try and protect the internet itself. But IoT represents a clear and present danger to the fabric of the Internet and all users on it. It represents a hidden threat that at any moment someone can launch an attack on all the cars in a city to make them stop.

What to do?

The average price for an IoT device is $10 and it runs from a tiny rechargeable battery for weeks on end. They are integrated into everything from devices you wear on your wrist to the knob on your hotel door.

Thus the solutions that are being developed for CNI are not suitable (they cost much $$$, use lots of power and are physically large).

The average IT solution is measured on how fast they can shift messages – the more the better – billions of messages every second. This drives cost, power and physical size. The average smart door in a hotel room only passes a message once every hour at most. This does not need a top-of-the range (or even bottom-of-the-range) IT device its way too much overkill.

So here is a list of things our smart IoT cyber device needs:

- sub $1 device that adds just enough security that will protect the IoT device and that we can distribute across the world.

- It needs to be flexible enough so that OEM engineers can use the device to provide functions that their customers require.

- It needs to allow integration into cloud of computers that a company can manage, so that they can push their security model down to the IoT without compromising the cloud's security.

- It needs to draw no power so it can run from a Lemon for a week! (bit of a tall order) but at least a 3.7v Li-ion battery of 1200mW for 1-2 days.

- Can't me hacked, copied, reverse engineered, altered, subverted or re-programmed

- Must be tiny so that it can be worn on the body

We have the answer

Blueskytec has developed such a device. We have implemented it as a demonstration of the technology into a standard chip (that costs $15). The next stage is to move this to a custom chip and distribute this for around $1. For more information on the technology the next article “Security in IoT” provides more details**.**