The Internet of Things (IoT) often conjures up images of a futuristic global network where automated houses pay the utility bills, switch the heating/lights on and order the shopping. In reality, IoT is already with us. Our smart TVs communicate with other devices and the world at large, accessing internet content and conversing with our tablets/smartphones via the games console. Soon smart meters will join the ranks, controlling our gas and/or electricity supply, reporting readings and sending faults to the nearest engineer. Eventually, all of these devices will be brought together and protected to some degree by the home hub.

IoT comprises any object capable of being read or of passing information over a network, be it an inert unpowered object bearing an RFID tag or an active agent that relays and receives data via the internet. Due to the diverse nature of these objects, numerous methods of connectivity are employed – from Wi-Fi to Bluetooth, to ZigBee and NFC – that communicate via the proxy of a home gateway. These paths of communication enable the home network to relay data to and from the network and to third parties, but every one has been shown to be vulnerable to attack under the right (or wrong) circumstances.

Interestingly, CORDIS, the European Union’s Community Research and Development Information Service, notes that ‘information security is a major concern of IoT... Past experience... shows that they are sometimes neglected during the design phase, and that integrating features to safeguard them at a later stage creates difficulties, is costly and can considerably reduce the quality of the systems. It is therefore crucial that IoT components are designed from their inception with a privacy – and security-by-design mindset.’ The inference is that IoT needs to be secure before launch, but given that these devices are already using compromised communication standards, we may already have failed.

IP is something that protocol hackers are all too familiar with and the criminal fraternity are already getting to grips with exploiting IoT. One need look no further than the Sony debacle when Sony’s servers were hacked revealing the usernames, passwords, credit card details, security answers and physical addresses of Playstation gamers. On that occasion the attack was perpetrated against a remote server, but the advent of IPv6 could bring the battle much closer to, and even into, the home.

Launched in June 2012, IPv6 is designed to alleviate the shortage of IP addresses associated with its predecessor, IPv4.
IPv6 uses 128-bit addresses enabling it to award a far higher number of unique addresses not just to users but to devices and objects too. The expectation is that IPv6 will allocate a block of addresses to a household, enabling these devices to ‘come online’ independently. Many of the devices previously hidden behind one IP address will become publically notable and more exposed as a result. IPv6 uses globally unique static IP addresses, making it possible to track a single device’s internet activity. While privacy extensions can counter this, they do not protect the user if cookie tracking is enabled or if only one or two hosts are using a given network prefix and the tracker is aware of this. The only way of locking down these addresses would be for the ISP to assign a dynamic network prefix via the Dynamic Host Configuration Protocol (DHCP).

In addition to the vulnerability of the wired broadband hub, it’s also worth noting the vulnerability of the wireless communications used by many IoT devices. The price point of the physical equipment required to capture and manipulate wireless communications previously deterred hackers, with the hardware required (amplifiers, demodulators/modulators, detectors, filters, mixers, etc.) setting back the user several thousand pounds. But the emergence of Software Defined Radio (SDR) has eliminated these barriers to entry and it is now possible to acquire highly sophisticated equipment capable of replicating the actions of a mobile base station, for instance, for just £800.

The capabilities of SDR should not be underestimated. Capable of performing highly complex hacking procedures, it can enable even the most inexperienced hacker to capture, relay or jam mobile communications over WiFi, Global System for Mobile (GSM), Digital Enhanced Cordless Telecommunications (DECT) and General Packet Radio Service (GPRS) networks. Hackers already familiar with IP and hacking ‘over-the-wire’ will be able to readily apply the same skillsets to ‘over-the-air’ communications, leading to an upsurge in wireless hacking and paving the way for IoT attacks.

During our investigations, we conducted experiments in hijacking wireless smart meters, for instance. On one occasion we were able to intercept the wireless signal between a gas boiler and its paired thermostat from up to 150 metres, replay the signal and cut off the boiler; a relatively trivial attack, but this could have profound implications, enabling the hacker to create false readings or terminate services. On a larger scale this could be extremely disruptive, altering or disabling utility supplies for thousands of users for miles around with very little traceability.

Today, the smart meter is still relatively isolated, but the expectation is that it will join other devices over a dashboard in the near future. One example of this is ‘The Connected Home’ offering of AlertMe, the company that recently partnered with British Gas to launch its Remote Heating Control service. AlertMe brings together ZigBee-enabled devices around the home, allowing them to interact with internet devices via the proxy of a home gateway, which is then controlled via AlertMe’s cloud. The plan is to add new devices and applications over time such as electricity, home security, smoke detectors, lighting, locks and keypads, potentially handing over the very keys of the home to a central server and creating a new attack vector.

Let’s be clear, there is no security issue with AlertMe’s system that we are aware of. The issue here is the ZigBee standard, which, while it requires very little energy and is extremely efficient, continues to be susceptible to attack. It is prone to interference, for example, and in the event of a jam its frequency hopping capabilities are poor. Attempts have been made to secure ZigBee through authorisation and preconfigured security keys but this requires additional system management, and out-of-the-box ZigBee transmission security can be woefully inadequate with keys transmitted in the clear and thus subject to interception.

In the future IoT will become even more complex, with physical objects given their own cyber counterparts to enable the user to interact with them online. The CORDIS report suggests that we will go ‘from a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create a new IoT’. These objects will sometimes have their own IP addresses, be embedded in complex systems and use sensors to obtain information from their environment (e.g. food products that record the temperature along the supply chain) and/or use actuators to interact with it (e.g. air conditioning valves that react to the presence of people).

Eventually the world we live in will have a mirror image online and we need to think about how we will secure these interlinked entities. As we peer through the looking glass and see our world reflected in 1s and 0s, the danger is that we may just have created a warren of rabbit holes for unwelcome guests.

References

About the author
Greg Jones is Director of Digital Assurance and has nearly 20 years of commercial technical experience spanning network development, network and system design/architecture, operations, IT and the wider technical security and delivery ramifications associated with professional services.

Greg’s areas of expertise include security assessment, secure systems design, and holistic security management. Greg started his career as a programmer with IBM over 20 years ago and holds a Master of Science from the Royal Holloway University of London.

Greg Jones can be contacted at greg.jones@digitalassurance.com