SECURITY CHALLENGES AND CYBERCRIME

ELAINE COOK, PAUL KEARNEY

Securing the Internet of Things.

Cybercrime is big business with devastating consequences, from loss of intellectual property, customer details and finances to loss of brand values and hard-won customer loyalty.

In the first 10 months of 2014, 11 major companies across the retail, financial, and restaurant industries reported their security had been breached. Tens of millions of credit card numbers were stolen along with personal information. Credit card numbers from those breaches continue to show up in fraudulent transactions today. One of the first questions that managers responsible for security ponder after containing such a breach must be "how did this happen?" followed by "what do we do to prevent it in the future?".

There are a number of factors that potentially increase the security challenges:

- Threats are getting smarter and more sophisticated – and they are growing in number and diversity. Not all hacks are technology-based; using social engineering techniques such as phishing, hackers attempt to persuade and trick users into opening fake linked sites with their login credentials. Other advanced persistent threats aim to remain undetected for as long as possible, gradually expanding their knowledge of the system until control can be taken and the system exploited.
- The growth of mobile devices such as tablets, smartphones and other dedicated Internet connected devices, whilst improving individual and team productivity, have challenged security teams to provision fast and responsive yet secure access to systems.
- The trend of bring your own device (BYOD) has spread through many organisations in an attempt to allow virtually any employee's own tablet or phone to connect to the company's network yet the implications of this strategy are far reaching in terms of security.
- The increasing use of cloud-based services, whether public or private, has opened up more threat scenarios. There is no doubt that using application and storage as a service makes a lot of financial sense but, in so doing, the responsibility of access to the data and networks gets entrusted to a third party.
- The growth of the Internet of Things (IoT) opens up security threats both from the myriad of devices and from the analysis and control applications they all feed.

This article examines this last point in more detail; the risks inherent in connecting ever more devices to the network, mitigating those risks, and identifying essential security capabilities. As well as assessing and mitigating against risks at the design stage, in-life risk management is important; this article goes on to outline a continuous holistic approach to security management.

The Internet with added Things

The accelerating trend for networked sensing and processing devices to be attached to and embedded within physical objects in the natural and built environment is leading to the Internet of Things. Such "Things" include:

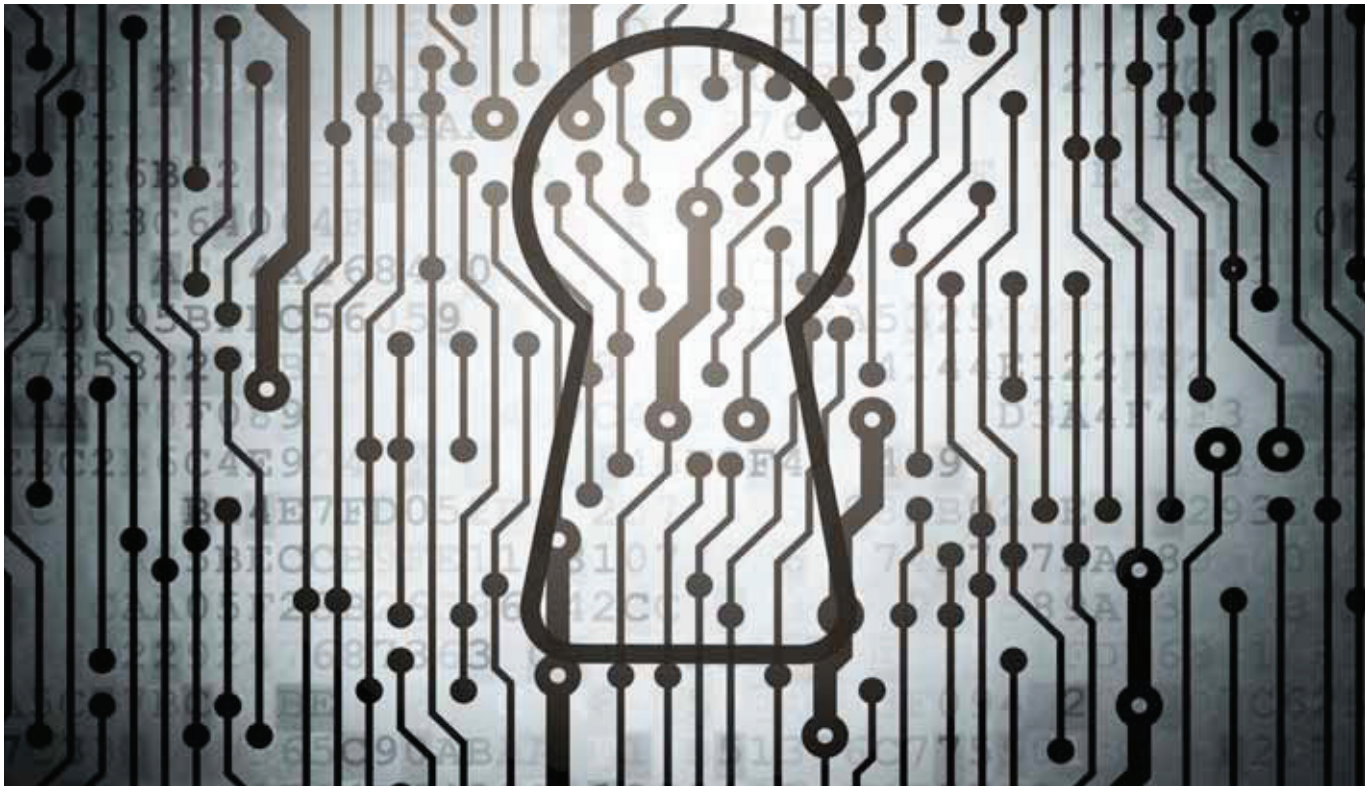
- Personal, wearable and implanted electronics.
- Health care equipment.
- Smart meters and controllers.
- Surveillance and security cameras.
- Systems in vehicles.
- Environmental sensors.
- Traffic monitoring sensors.
- Factory automation and industrial control systems.
- Robots, autonomous vehicles, etc.

The IoT is not a separate Internet for physical objects, but rather adds physical objects to the existing Internet effectively integrating the physical and cyber-worlds. The IoT means not only that the cyber-world can observe the physical world in increasing detail, but also that the cyber-world can affect the physical world directly through control systems, actuators, etc, as well as by passing information and instructions to people.

Risk assessment

The IoT cannot be considered in isolation from other trends in ICT, such as cloud computing, Big Data, analytics, ubiquitous high speed networks, personal electronics/smartphone developments, software defined data centres and networks. Most if not all of the advanced applications enabled by IoT also require the other emerging technologies and vice versa. Such application areas include smart cities and transportation networks, healthcare, smart energy/utility grids, smart agriculture, and smart buildings.

It follows therefore that securing the IoT is not solely about the properties of devices themselves but about whether the risk of



operating a system/application in a particular usage context is acceptable to that application's stakeholders. Assessment of security risk must take into account both the likelihood and consequences (impact) of security breaches. Conventionally, security risk covers the following types of impact:

- **Failure of confidentiality** – unauthorised parties are able to use the information or other services provided by the application. Protecting the rights of the subjects of information (as opposed to its owners) is known as privacy, though another distinction is that privacy is covered by regulations protecting personal data.

- **Failure of integrity** – unauthorised parties are able to interfere with the correct operation of the application.

- **Failure of availability** – an unauthorised party is able to deny legitimate users access to the system.

Assessing security risk on an IoT domain basis

IoT can be viewed as having three main domains or layers:

- **A device domain** – consisting of local networks of devices connected to wide area networks via gateway devices. This simplifies some of the challenges by confining diversity issues to the local networks – the gateway devices expose a standardised interface to the rest of the application.

- **A data domain** – requiring Big Data technology in many applications - to hold the potentially very large amounts of data and enable it to be analysed to yield actionable information.

- **An application domain** – making use of the collected and analysed data, making decisions based on it, and potentially sending commands back to the devices via the relevant gateway devices.

In simple cases, the application domain may consist of an app on a smartphone, the data domain as cloud-based storage, and the device domain a home network. At the other end of the scale, there could be a highly diverse collection of device networks owned and operated by different organisations feeding data into a multi-tenant store operated by a data broker, which in turn makes the data available to multiple subscribing organisations, who apply it for their own individual purposes.

The IoT device domain introduces particular vulnerabilities that can be exploited by attackers. It generates large amounts of potentially sensitive data that can be misused, and it can take actions affecting the physical world, including potentially the safety of its inhabitants. This is examined further in the section below.

While the distinctive properties of IoT applications arise from the device domain, their consequences permeate the whole system. Each of the domains has a different mix of security concerns, and looking at security on a domain-by-domain basis simplifies the overall problem by allowing those concerns to be considered separately. However it is important also to look at the holistic properties of the complete system to ensure that all significant risks are identified and treated.

Some of the more ambitious IoT applications are extremely complex, which magnifies the security problem in non-linear fashion by

adding/creating new vulnerabilities and making consequences much more difficult to predict. Furthermore, it is likely that devices/device networks will serve multiple applications and end-users, and the same goes for the data storage and analysis services, coupling applications to form even larger and more complex systems and raising further security challenges.

The security of things

The nature and diversity of the devices being added to the Internet bring security challenges that are different from conventional computers, including the following:

- Many manufacturers of IoT devices have not had the lengthy and bitter learning experience regarding security that ICT providers have. There have been numerous press reports recently of webcams and other network-connected consumer devices that have been trivially-easy to compromise.

- The devices are often in exposed locations allowing physical access to attackers.

- They often communicate wirelessly, making interception, eavesdropping, impersonation, man-in-the-middle attacks, jamming, etc, easier that in wired networks.

- They often have limited computational (and electrical) power meaning it is not practical to perform computationally expensive (and power hungry) conventional cryptographic operations. New algorithms are required, or other measures taken to avoid the need for encrypted communication and crypto-based authentication and integrity measures. The diversity of devices with different cryptographic capabilities mean that there will need to be negotiation or intelligent decision-making to select a mutually compatible protocol that provides sufficient security in the context.

- They often have no external power supply and so must rely on batteries or be powered via the communication medium (like passive smart cards), so power consumption is a major issue. Amongst other things, this means communications will have to be managed carefully, which needs to be factored in to design of security and management protocols. The short range of communications of low-powered further devices means that communication opportunities may be intermittent and depend on other devices coming with range.

- Like the computers we are familiar with IoT devices will need to have security patches and operating system upgrades on a regular basis to remove newly identified vulnerabilities. As well as the impact of limited communication opportunities, patch management for a large number of diverse and distributed devices will pose a severe management headache.

- Many types of IoT device will be difficult and/or expensive to deploy/replace in the field. This is likely to lead to severe legacy issues as old devices continue to operate alongside successive new generations.

- Some IoT devices can take actions with safety consequences, e.g. vehicle and healthcare devices.

- The data produced by IoT devices has the potential to reveal a lot about our lives, leading to privacy concerns. Such data could also be used by criminals (e.g. to work out when a building is empty) and terrorists.

Dealing with threats

Typically any organisation's security technology infrastructure has been built up in silos, with multiple security processes developed for specific purposes: anti-virus software (sometimes multiple varieties running simultaneously to detect different viruses), firewalls, gateway security, encryption etc.

An organisation is likely to contain a broad plethora of these software products and services to enable real-time analysis of security information management and security event management. These multiple layers exist across the IT infrastructure, leading to more data to oversee and making it harder to figure out what's going on. But detecting and responding to individual attacks means that organisations are always behind the curve.

By the time defenders have contained one incident another is potentially brewing. Instead, businesses need to move to a continuous approach to incidents, where attacks are expected, and systems learn patterns of behaviour making anomalies easier to spot.

Continuous monitoring of the entire network, looking for patterns, anomalies and triggers will generate significant amounts of data. Big data analytics will be required to turn this data into actionable insights that businesses can respond to in real time.

Implementing an holistic approach

IT security teams need to review how their security architecture is currently implemented. Most IT systems are in continuous use so it makes sense that the security response is continuous too. Detection of the threat at an early stage and the way it occurred is crucial to building a knowledge map of network and application vulnerabilities. Amassing threat detection or so-called "threat intelligence" information into its own dedicated database will greatly aid an understanding of application, device and network weaknesses for the future and potentially help pave the way to a more predictive response to threats in real-time.

In addition to making IT security monitoring a continuous operation, it should be implemented across all layers; from the network stack, transport packets, end-points operating systems, devices, information content, users (people and machines) and applications. By making it possible to communicate through the entire network stack layers will ensure that even the humblest of compact IoT sensors can communicate a potential attempt, for example, to communicate without a trusted key, to become immediately visible to monitoring staff.

Networks and platforms

The network is rather hard to define on paper now. In the broadest context it represents every user on the network whether sat in an office, out "on the road' or an IoT sensor on an air-conditioning plant. Using firewalls, access control lists and packet inspection are some of the tools that are available but it doesn't keep every threat out or isolated. The next stop for a threat that penetrates the network is the platform. Comprising virtually every server, desktop, laptop, tablet and smartphone, there is a lot to consider.

And when talking about networks and platforms we mustn't forget to mention one aspect of the user community. Most businesses have a system of privileges that control who has access to certain data, systems or administration rights. These are typically controlled by passwords. There are two common failings with the traditional password system which increases the risk of hacking: firstly resorting to easy-to-remember passwords or across multiple accounts, and secondly (almost the exact opposite) of creating unique passwords containing a randomised string of characters that users are unable to remember and therefore are locked out. Moving to multi factor identification, including biometrics, making it easier for users to prove their identity and harder for hackers to usurp, has to be the goal of the industry.

Hardening platforms and devices

Traditionally the domain of anti-virus and anti-malware software they attempt to keep viruses and rootkits out. Malware developers however are getting rather adept at moving down the stack of devices in an attempt to get below any anti-virus or anti-malware software, and below the operating system in order to get into the boot code. In this way they can disable any anti-virus / anti-malware software in place, corrupt drivers and control communications. Defending platforms from such low-level attacks is the job of hardware techniques such as secure boot.

When communicating across the network, platforms should use whitelisting techniques to allow communication between devices and applications. The default access parameter should always be set to 'deny' and the use of guest or anonymous logins absolutely banned.

AUTHORS' CONCLUSIONS

The proliferation of smart, networked devices observing and interacting with the physical world poses many security challenges as well as significant business opportunities. Security professionals should not try to stand in the way of progress, but rather should develop techniques and processes that allow continual innovation to be managed securely. An holistic / systems-based approach should be adopted, whereby threats, vulnerabilities and consequences are used to assess the risk of operating a proposed IoT application in a given environment. If the level of risk cannot be reduced to an acceptable level by applying available and affordable security tools and technique, then the ambitiousness of the application should be scaled back until the level of risk becomes manageable.

Having assessed the risk to be acceptable, nevertheless it is important that security should be a core and comprehensive part of in-life management so that threats can be better identified and managed. This needs to be a continuous process, not one that is just responsive after the event. Computer networks, devices and systems are constantly under attack and will continue to be so. Gathering security and threat intelligence will greatly help an organisation's ability to detect and take active steps to prevent hacker attacks becoming so disruptive. In time, and with the proper security measures in place, the organisation can get better at predicting potential hacker events.

One way to reduce risk is to partner with experienced, knowledgeable and trusted service providers. Over time, we, as a community of researchers, innovators and practitioners, will advance the state of the security art to enable increasingly complex deployments to be tackled with confidence.

ABOUT THE AUTHORS

Elaine Cook

Elaine Cook has worked for Intel for 17 years in the non-PC part of the business that has evolved into the Internet of Things (IoT). With a history in Operations, Pricing, Product Marketing and Marcom, she is a passionate advocate for how IoT can enrich people's lives and transform businesses. She is a multi-year Intel veteran and has more than 15 years' experience of working in the evolving field of Embedded Computing and the Internet of Things.

Paul Kearney

Paul Kearney is Chief Security Researcher in the Security Futures Practice, BT Technology, Service and Operations. He joined BT in 1997 having previously gained a BSc and PhD in Theoretical Physics and worked in the defence aerospace and personal electronics industries. Paul has specialised in information security and business continuity research since 2001. Paul has played a leading role in several European collaborative research projects, is a member of the Group of Experts for the EUREKA CELTIC programme, the HORIZON 2020 Secure Societies Advisory Group, and the steering committee of Working Group 3 (Secure ICT research and innovation) of the EC Network and Information Security Platform. In addition to his BT position, Paul is now Professor of Cyber Security (part time) at Birmingham City University.

ABBREVIATIONS

IoT	Internet of Things
IP	Internet Protocol

ITP INSIGHT CALL

Want to talk to the author?

To discuss this article and its content, join in the ITP Insight Call on 22 February, 2016.

To book onto the call visit: https://www.theitp.org/calendar/