ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 September 2015 www.computerfraudandsecurity.com

Featured in this issue:

Securing small businesses – the weakest link in a supply chain?

The UK government has announced the investment of £1m into a new scheme to help SMEs boost their cyber-security, and has issued guidelines for small businesses.

But is this enough and should larger companies be spending money on helping to secure their smaller partners and suppliers? Tracey Caldwell discusses some of the risks and threats faced by the supply chain and provides industry commentary on the issues and recommendations arising.

Full story on page 5…

The security issues of the Internet of Things

The Internet of Things (IoT) was first envisaged in the last century, but interest has picked up in the past 15 years or so. And there are many potential benefits.

However, owing to the wide range of sectors involved and their impact on everyday life, the security issues can have serious consequences, causing damage, disruption to operations or, in some scenarios, even loss of life. Colin Tankard of Digital Pathways looks at how we might head off these problems.

Full story on page 11…

Big data – the future of cyber-security or its latest threat?

Big data allows organisations to detect anomalous behaviour in near real-time by consolidating data from numerous sources into one large database.

But adoption is still only at the very early stage and commercial options are limited, although a range of cloud-based services are expected to emerge over time. A key issue here is that big data expertise in either an information security or wider sense is still thin on the ground, which means that such systems need to be treated with caution, explains Cath Everett.

Full story on page 14…

US Internal Revenue Service admits to much bigger attack using stolen information

The US Internal Revenue Service (IRS) has revised the number of people affected by scammers using stolen data back in May.

The IRS was the target of a massive data-trawling attack in which criminals used personal data acquired from breaches of other organisations in an attempt to retrieve further information from the IRS systems. At the time, it was reported that around 100,000 people had their data illegally accessed via the Get Transcript service on IRS websites that allow taxpayers to retrieve past tax records. The Get Transcript service was subsequently

Continued on page 3…

Contents

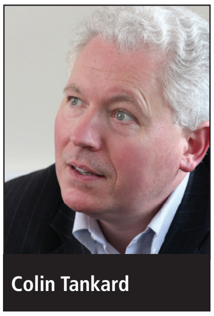
NEWS

FEATURES

REGULARS

The security issues of the Internet of Things

Colin Tankard, Digital Pathways



Colin Tankard

The Internet of Things (IoT) was first envisaged in the last century, but interest has picked up in the past 15 years or so. It is a vision whereby potentially billions of 'things' – such as smart devices and sensors – are interconnected using machine-to-machine technology enabled by Internet or other IP-based connectivity.

A recent study by the McKinsey Global Institute estimates that the IoT will have a potential economic impact of $3.9tn-$11.1tn per year by 2025 across nine settings – homes, offices, factories, retail environments, worksites, human health, outside environments, cities and vehicles.[1] Estimates vary widely regarding how many IoT devices will be connected, but an often quoted statistic is from Cisco, which estimates that 50 billion objects and devices will be connected by 2020.

Potential benefits

There are many potential benefits from embracing the IoT. Verizon estimates that currently some 10% of organisations have adopted IoT extensively and that, by 2025, those that do so will be 10% more profitable than those that do not. They will be better empowered to innovate, disrupting both established players and new entrants, and will afford their customers better experiences, see accelerated growth and improved performance, and will be able to improve safety and reduce risk. For example, IoT will enable new ways to protect inventory, equipment and machinery, even in remote locations or over large areas.

According to a recent survey by the SANS Institute covering organisations of all sizes, 66% of respondents are either currently involved in or are planning to implement IoT applications involving consumer devices, such as smartphones, smartwatches and other wearables. Smart buildings systems are increasingly being implemented as operations management systems get connected to networks. The IoT holds much promise for the energy, utilities, medical devices and transport sectors, which will see the highest levels of adoption in the near term, according to SANS, as well as smart buildings.

Smart buildings

Smart buildings are those in which the various systems, such as lighting, heating, ventilation, air conditioning and security, are connected. In terms of security, connected alarms, sensors and tracking devices will make threat detection easier and remotely activated cameras and other networked security equipment will help to improve physical security. Other benefits are higher operational efficiency, more safety and comfort, and lower cost of operation as systems pass data freely back and forth.

> ***"The IoT holds much promise for the energy, utilities, medical devices and transport sectors, which will see the highest levels of adoption in the near term"***

The EU has identified further development of smart buildings as an imperative for achieving its goals of a proposed improvement in energy efficiency of 27%

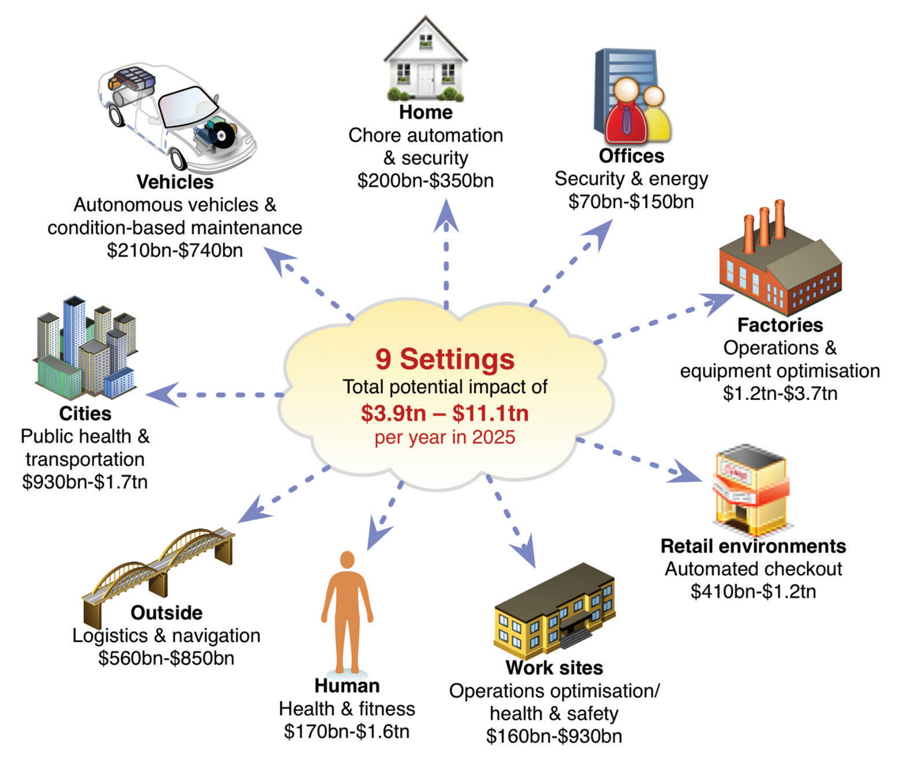


Figure 1: Nine settings identified by the McKinsey Global Institute and their global impact by 2025.

by 2020, potentially 30% by 2030, under the Energy Efficiency Directive set out in June 2015. It states that new buildings now use half of the energy that they did in the 1980s owing to the use of new, smart technologies.

The US is also focusing on this sector, aiming to increase energy efficiency in buildings as well as reduce energy costs. It passed the Smart Building Acceleration Act in May 2015, which it is hoped will be a catalyst for increasing the transition to smart building technology across the country, in both the public and private sectors.

Security issues

While the IoT holds much promise, many security issues have been uncovered. Owing to the wide range of sectors involved and their impact on everyday life, such security issues can have serious consequences, causing damage, disruption to operations or, in some scenarios, even loss of life. In a smart building – where systems ranging from HVAC (heating, ventilation and air conditioning), lighting and door access controls, to video surveillance and elevators, are all interconnected – a security threat that is exploited to disrupt power or lighting could cause loss of life if it were something like a hospital. In office buildings, a door access control that is hacked could provide an intruder with unauthorised access. Issues with IoT devices are far from hypothetical: one example of a threat is the Stuxnet worm, which has been seen to be able to disrupt industrial control systems, causing extensive damage.

"A different stance needs to be taken. Security needs to be built into products by design. It cannot be bolted on afterwards"

A range of security risks have been uncovered in the devices themselves that make up the IoT. OWASP has identified the top 10 such issues involved with IoT devices:[2]

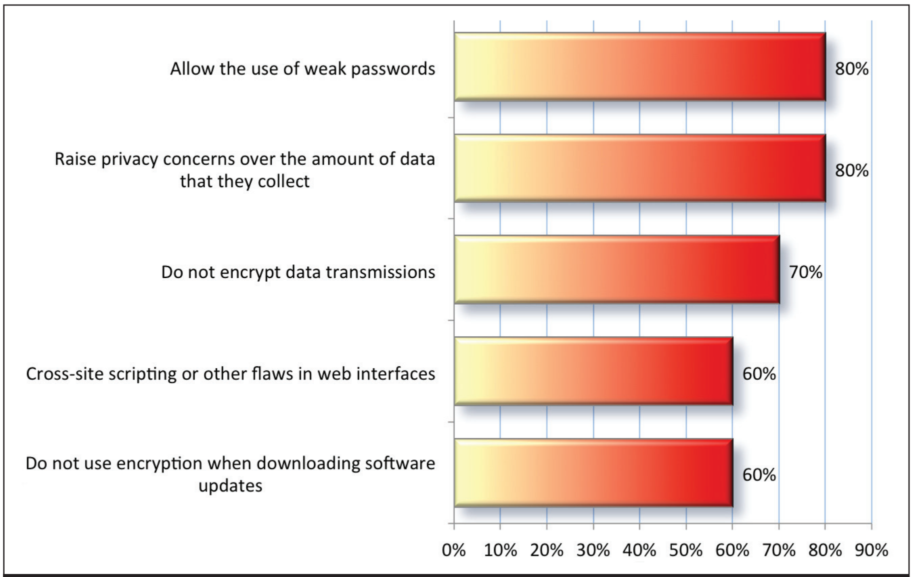


Figure 2: Device-level IoT security vulnerabilities. Source: HP Fortify.

- Insecure web interface.
- Insufficient authentication/authorisation.
- Insecure network services.
- Lack of transport encryption.
- Privacy concerns.
- Insecure cloud interface.
- Insecure mobile interface.
- Insufficient security configurability.
- Insecure software/firmware.
- Poor physical security.

This is echoed by recent research undertaken by HP Fortify, the findings of which are shown in Figure 2. Overall, it found that 70% of the most commonly used IoT devices contain security vulnerabilities and there are an average of 25 security concerns per device.

Among the reasons for this is that many IoT devices are not developed with security in mind. Many contain embedded software, often proprietary firmware, which is problematic to patch and upgrade, leading to vulnerability and configuration management issues. Many devices do not undergo any kind of security review. According to SANS, just 52% of IoT devices undergo security evaluations or testing prior to production.

Solving the security challenges

To solve the security challenges of IoT devices, a different stance needs to be taken. Security needs to be built into products by design. It cannot be bolted on afterwards. There are moves, such as the position being taken by the US Food and Drug Administration regarding medical equipment, to encourage manufacturers and facilities to ensure that appropriate security safeguards are built in from the start of the design process, as well as to remain vigilant regarding new risks and threats as they are uncovered. This is especially important since it has already been demonstrated that implantable medical devices such as pacemakers and defibrillators can be remotely hacked and exploits such as changing dosage levels of insulin pumps have been accomplished from a distance of up to 300 metres. As well as this, the University of Michigan has shown that the majority of hospital devices use Windows XP or Windows 95 operating systems, which are extremely vulnerable to computer malware, and many monitoring systems use open wifi connections that can be hacked.

Building in security by design means that controls need to be introduced at the operating system level, should use the device's hardware security capabilities and should extend right up through the device stack to the applications it deploys.

In order to address security throughout the device lifecycle, from the initial design to the operational environment, software vendor Wind River states that there are five essential requirements:

1. Secure booting – the authenticity and integrity of software on a device should be verified via a digital signature attached to the software image and verified by the device to ensure that it has been authorised to run on that device and that there are no runtime threats or malicious exploits present. Only then will it be allowed to load.
2. Access control – mandatory or role-based access controls should be built into the operating system. If compromise of any component is detected, access to other parts of the system should be minimised as much as possible. This will help to minimise the effectiveness of any breach of security.
3. Device authentication – a device should authenticate itself at the point at which it is plugged into the network, prior to receiving or transmitting data. Machine authentication only allows a device to access a network based on credentials that are stored in a secure storage area.
4. Firewalling and IPS – each device needs to have a firewall or deep packet inspection capability for controlling traffic, but this requires that protocols are needed to identify malicious payloads hiding on non-IT protocols. And these protocols need to be industry-specific since – for example, smart energy grids have their own set of protocols governing how devices talk to each other.
5. Updates and patches – the ability to deliver software updates and patches to thousands of devices in a way that conserves limited bandwidth and intermittent connectivity of embedded devices, while ensuring that there is no possibility of functional safety being compromised, is a necessity.

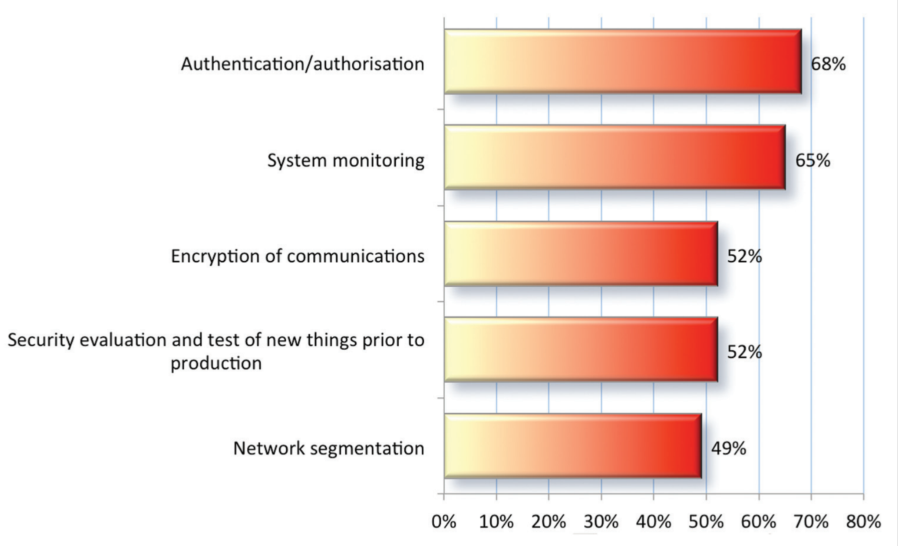


Figure 3: Top controls currently in place for securing the IoT. Source: SANS Institute.

Essential steps

It is unlikely that security will become an over-arching requirement in the design process any time soon. There are also standards that need to be developed before this happens and it is also likely that some form of regulation or specific industry pressure will be required in order to force manufacturers to place the necessary emphasis on security.

Organisations should look to limit what is allowed in the workplace, considering the risks versus the benefits, and look at how systems are interconnected and therefore how risks such as malware infections can be spread.

> ***"Systems will need to be used to link physical and network security together to enable a total view of incidents, enabling management to make decisions regarding the threat posed"***

Organisations also need to find a way to enforce data protection policies on all devices in use and to control what data people can access. Identity and access rights should be tightly managed in order that all devices and connections are authenticated and authorised, and controls should be placed on what information can be viewed and how it is communicated and stored. All data held on devices or in transit should be encrypted to safeguard it from unauthorised access or loss. In terms of devices that are lost or stolen, device management tools that extend to remote data wipe should be considered, especially for consumer devices that are personally owned.

For devices used for business operations, systems will need to be used to link physical and network security together to enable a total view of incidents, enabling management to make decisions regarding the threat posed and how it can be controlled. This requires that all IoT devices are managed the same way as other equipment connected to the Internet and the network. All activity should be closely and continuously monitored to look for anomalies from normal baseline behaviour and organisations should ensure that all devices are correctly configured and are operating properly.

Where anomalies are uncovered, organisations need to have workflow and escalation procedures in place so that those in charge of security are alerted promptly to any potentially serious security threat or incident. This will help greatly in the time taken, and therefore cost, for remediating problems. It is essential that all procedures and processes are documented, completed in a compliant way and an audit trail is generated to provide evidence of the effectiveness of actions taken.

Figure 3 illustrates the controls that organisations currently have in place for controlling IoT devices in the workplace according to the SANS Institute.

Remain vigilant

While it could be said that the IoT is still in its infancy, IoT devices and increased connectivity are being seen across a wide range of sectors. Many will be familiar with consumer-oriented smart, highly connected devices and these are invading the workplace. Organisations are still grappling with the BYOD phenomenon that has an increasing array of personally owned smartphones and tablets being used for work purposes, creating headaches for many in terms of managing them and controlling what sensitive data can be accessed. Now this is being extended to wearables such as smartwatches and health and fitness monitoring devices.

But the industrial IoT holds the greatest promise, offering to improve productivity, ease safety issues and reduce operational costs in a wide range of scenarios and industries.

Organisations would be well advised to thoroughly research the risks involved in each scenario in which IoT devices are deployed and to communicate with employees, partners and customers about security and privacy risks, especially, where sensitive data is at risk. This should include both consumer devices that they wish to purchase and use to interact with corporate information, as well as how devices used, for example, in smart buildings should be closely monitored and maintained. One point of failure in a hyper-interconnected network can initiate a chain of events that could have catastrophic consequences.

The IoT appears to be an unstoppable force and the rising tide of devices cannot be turned back. Until security issues are solved, organisations need to be vigilant, ensuring that they weigh-up the security risks against the benefits to be gained, putting appropriate controls and policies in place, and keeping a constant eye over what is connected to their networks and how devices are performing.

About the author

Colin Tankard is managing director of data security company Digital Pathways which specialises in the design, implementation and management of systems that ensure the security of all data whether at rest within the network, mobile device, in storage or data in transit across public or private networks.

References

1. Manyika, J; Chui, M; Bisson, P; Woetzel, J; Dobbs, R; Bughin, J; Aharon, D. 'Unlocking the potential of the Internet of Things'. McKinsey Global Institute, June 2015 Accessed Aug 2015. www.mckinsey.com/insights/business_technology/the_Internet_of_things_the_value_of_digitizing_the_physical_world.
2. 'OWASP' Internet of Things Top 10 Project'. OWASP. Accessed Aug 2015. www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project.

Big data – the future of cyber-security or its latest threat?

Cath Everett

Cath Everett, freelance journalist

Everyone seems to be talking about big data lately. The much-vaunted ability to analyse large diverse data sets very quickly really does appear to have become the hottest of hot tech topics over the past few years. In fact, big data, despite being such an over-used term, has even managed to worm its way into mainstream public consciousness – mainly because of the insights it has been able to afford by finding patterns in what often appears to be unrelated information.

Killer app

In an industry context, meanwhile, a raft of glowing articles have emerged in the computer press recently extolling the technology's virtues and dubbing it the future of cyber-security – or alternatively claiming that information security is big data's killer app. But is there any truth in such hyperbolic statements? And if so, what is this future likely to look like? As usual, views are mixed.

According to Peter Wood, chief executive of information security consultancy