Whitepaper: Internet of Everything

How to Secure the Internet of Everything

Date: April 2016

Doc Ref: SOS-WP-IoE-0416A

Author: Nick Sharp & Neville Gollan

Table of Contents

Overview

Oxford defines the Internet of Things as "The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data"[1] and the Internet of Everything (IoE) is understood as being the next evolutionary stage. The characteristics of the Internet of Everything include the convergence of people, processes, data, and objects combining communications between machines (M2M), people and machines (P2M) and people (P2P).

With the costs of technology gradually declining and more and more devices centrally connected, organisations are adopting sophisticated ways to improve efficiency and productivity by reducing costs, increasing productivity and potentially increasing revenue.

In 2015 there were 4.9 billion Internet connected devices globally, which represented a 30% increase compared to 2014. According to Gartner's predictions, there will be 25 billion connected devices by 2020[2] . For developing economies, it is expected there will be a higher number of uses for these new technologies, and in some cases due to no legacy technologies needing to be displaced, there will also be greater adoption. For example, China will be one of the largest adopters of IoE within their factories (i.e. manufacturing). Overall, by geography, the United States, China and Europe will lead the charge in the adoption of IoE technologies[3].

In 2015, the primary industry verticals using IoE (in order of size) were manufacturing, utilities and transportation with a total of 736 million connected devices. By 2020, this will change to utilities, manufacturing and government with a total of 1.7 billion devices across these industry verticals alone[4].

To quantify the potential opportunity of IoE, Cisco states that $4.6 trillion will be created in terms of the Value at Stake (VaS) for the Public sector globally from 2013 to 2022. VaS is defined as the potential value that can be created by organisations based on their ability to harness IoE[5]. Likewise, for the Private sector globally IoE will create $19.9 trillion in terms of VaS.

Companies can capitalise on these technological advancements but with any new technology comes risk, particularly when they are exposed to the Internet. Ineffective risk treatment can lead to a potential security event, resulting in disruption to business, reputational risk, revenue loss, and potential regulatory implications. Having a strong focus on security and implementing the right processes to assess and mitigate the risks of new technologies is pertinent to implementing effective and secure solutions.

[1] http://www.oxforddictionaries.com/definition/english/Internet-of-things?q=internet+of+things
[2] http://www.gartner.com/newsroom/id/2905717
[3] http://www.mckinsey.com/insights/business_technology/The_Internet_of_Things_The_value_of_digitizing_the_physical_world?cid=other-eml-alt-mgi-mck-oth-1506
[4] http://www.gartner.com/newsroom/id/2905717
[5] http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf

Benefits of the Internet of Everything

Interconnecting devices with direct Internet access is not new. Improvements in Internet connectivity and speed, coupled with a decrease in the cost of computation devices presents many organisations with an opportunity to benefit from IoE technologies. The innovation being conducted within the IoE space represents significant changes in the manner that information can be consumed, delivering vast benefits to individuals, communities and organisations alike.

Looking at some examples of how organisations are capitalising on IoE solutions, insurance company QBE recently launched the first insurance product to offer custom policies to drivers based on safe driving. This is made possible by a small in-vehicle plug-in device that uses sensors to measure driving habits. This data is then collated for the insurer to calculate a 'DriveScore' (driver safety score). Safe drivers with a good DriveScore will be rewarded with a lower insurance premium. Some of the latest sensors on the market can now provide the capability to validate garage address, recover stolen vehicles and support the validation of claims or post-accident assistance services.

Another interesting development of pervasive IoE computing is in the health industry. In recent years, an Australian healthcare company began to offer several clinical applications via 4G tablets to the hospitals under a Software-as-a-Service model. These clinical applications capture patients' health records and track their journey from admission and identification of the patient through to post-operative stages within the hospital patient system. This allows doctors and nurses to be able to consult with the information from these connected devices in a more productive manner, resulting in faster response times. High availability and scalability is achieved by hosting the infrastructure with Amazon Web Services (AWS).

IoE is here to stay. With the increase in instrumented devices and sensors working to gather decisive data points for decision making, these technologies will enable us to solve complex problems. For example, at the very heart of any smart city program around the world, data is captured from a span of connected sensors, feeding back real-time information to a central command centre, enabling real-time data analytics to be performed. From the correlation of complex data effective decisions can be made by authorities to help reduce traffic congestion, increase emergency response times and enable a better quality of living.

Security Risks and Challenges

But with all new technologies come risks and IoE is no different. Previous industrial systems have typically been closed circuit, but in recent times more systems are available via the Internet for remote access and real-time monitoring. Although interconnection, integration and access have improved the ability to operate these solutions, it also opens up these previously closed systems to Internet based attacks.

Examples of attacks include the Jeep Cherokee that was remotely hacked, allowing

a person to control the car's steering, brakes, and transmission from anywhere in the world[6] . There was also the study by MIT's Technology Review, reporting that computerised equipment in hospitals is dangerously vulnerable to malware. Many systems are already infected due to legacy software systems and the inability for patches to be automatically applied to the devices.

Another potential attack point is with the growing use of smart metering and smart grids used by utility companies to produce more accurate consumption data. According to an Internet threat assessment report conducted by the European crime agency Europol, these meters can be tampered with, with the tools to do so readily available on the Internet[7] . These attacks can result in the meter reporting back incorrect usage data, causing economic loss to the company. Furthermore, if these devices are interconnecting with other components of infrastructure, this may create an entry point for attackers to gain access to other systems.

Researchers at Eurecom, a French technology institute, conducted an analysis of approximately 32,000 firmware images from potential IoE device manufacturers and discovered 38 vulnerabilities across 123 products[8] . During the research, it was also confirmed that some of these vulnerabilities together are affecting at least 140,000 Internet facing devices. Discovered vulnerabilities include poor encryption and backdoors that could allow unauthorised access, opening up hundreds of thousands of devices on a network with potentially serious consequences.

Developing an Effective Security Framework

With any technology strategy it is important that the security requirements for the entire ecosystem are considered and that appropriate risk management measures are adopted. Stated another way; the tenants of information security being confidentiality, integrity and availability are equally applicable to an IoE solution as they are for the traditional use of IT within the enterprise.

Before approving the development of an IoE solution the responsible stakeholders need to obtain a clear understanding on the type and sensitivity of information that will be captured, used and stored. This detail is a fundamental starting point to defining a security framework and conducting a threat & risk assessment. Furthermore, it is quite possible regulatory compliance will apply to the handling of the data type in question.

For example the Australian Privacy Act now includes a set of privacy principles that regulate the handling of personal information by Australian and Norfolk Island Government agencies and private sector organisations that are covered by the by the Privacy Act 1988 (Cth). These principles are called the Australian Privacy Principles (APPs). APP 11 requires an organisation that holds personal information

[6] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[7] https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
[8] http://www.s3.eurecom.fr/docs/usenixsec14_costin.pdf

to take reasonable steps to protect the information from misuse, interference (e.g. cyber-attack) and loss, and from unauthorised access, modification or disclosure. Failure to take reasonable steps to prevent unauthorised access such as a cyber-intrusion may be considered a breach of APP 11[9]. In addition an entity must take reasonable steps to destroy or de-identify the personal information when is no longer needed or they no longer have the rights to retain it.

Beyond the end-use device, the IoE solution will likely rely on web interfaces (API's), intermediary technology and cloud infrastructure. It is therefore highly probable that third-party providers will be engaged for design, build and operations. Consequently, supply agreements need to support the security framework through specific security provisions. The provisions should be prescriptive enough to ensure that the third party clearly understands what is expected of them to perform. Going one step further, the Principal of the contract would be well advised to incorporate right-to-audit clauses to ensure the expected security attributes are upheld.

Moving on from contractual matters, a Threat & Risk Assessment (TRA) should be undertaken by a security specialist. The TRA process will identify potential threats and vulnerabilities most likely to impact the system and recommendations to address risk. The results of a TRA report will inform the development of a Risk Treatment Plan (RTP), with stated controls to treat and manage security risk.
Depending on the technology elements contributing to the overall IoE solution, the security controls will need to address all, or some, of the Domains discussed in the table below.

Domain	Description
Secure Development Lifecycle	Web applications developed in isolation of a Secure Development Lifecycle (SDL) are far more likely to be susceptible to compromise. It is therefore important that secure development standards and practices are defined and incorporated into web applications and API's. The most prevalent web application security flaws have been researched and documented by industry recognised organisations. For example the Open Web Application Security Project (OWASP) is a non-for profit organisation focused on improving the security of software. OWASP has published numerous resources including the OWASP Top 10. This resource outlines the ten most critical web application security risks[10]. The web application security weaknesses can include: 1. Injection Flaws 2. Broken Authentication and Session

[9] http://www.oaic.gov.au/news-and-events/statements/privacy-statements/cyber-attacks-do-not-mean-businesses-are-off-the-hook/cyber-attacks-do-not-mean-businesses-are-off-the-hook
[10] https://www.owasp.org/index.php/Top10#tab=OWASP_Top_10_for_2013

	Management 3. Cross Site Scripting 4. Insecure Direct Object references 5. Security Misconfiguration 6. Sensitive Data Exposure 7. Missing Function Level Access Control 8. Cross Site Request Forgery 9. Using Components with Known Vulnerabilities 10. Invalidated Redirects and Forwards
Authentication & Authorisation	If the IoE solution handles sensitive data (e.g. Personally Identifiable Information) robust authentication and authorisation controls need to be defined and implemented to protect against unauthorised access. Ineffective authentication controls can lead to attacks such as user enumeration, default or guessable passwords, brute-forcing passwords, and client password caching. An Access Control Policy should be developed to determine authentication controls required given the type of connection being made. For example the connection may be Machine to Machine (M2M), Machine to People (M2P) or People to People (P2P). Controls may include: • Strong passwords including minimum password length and complexity • Account lock-out mechanism to limit repeated access attempts from an unauthorised user • Certificate authentication • Multi-factor authentication for accesses to management interfaces After authentication is completed authorisation controls need to be in place to ensure that access to system or data resources is restricted to the appropriate level of permission and no more. The principle of least-privilege required for the function to operate should apply.
Encryption	Sensitive data captured by the device, application or cloud interface needs to be suitably protected when at rest at the collection point or data store and when in transmission across an untrusted network. Applying strong cryptography methods is considered a fundamental security process to protecting sensitive

	data from unauthorised access. Furthermore, management of cryptographic keys and associated hardware and software needs to follow stringent procedures to ensure conformance with the governing policy. The secure management of cryptographic keys should include procedures covering the generation, registration, distribution, installation, usage, protection, storage, archival, recovery, deregistration, revocation, and destruction of key material.
Network	While the premise of an IoE solution is to use the Internet for transmission of data, the organisation should consider how it intends to isolate the supporting infrastructure from unrelated IT environments. The network architecture of the IoE eco-system needs to take into account the items listed below: • Perimeter Security Protection • Zone classification and enforcement • Number of zone enforcement points and capabilities (routers, switches, firewalls, etc.) • Design and capabilities of firewalls protecting the infrastructure • Intrusion detection and prevention systems • Network access controls and authentication • Remote access systems • Endpoint protection
Physical Security	The device/sensor used needs to be suitably protected from a malicious attack. Without proper hardware tampering protection, attackers can debug and modify the device hardware to connect physical management interfaces repeatedly, and upon successfully decoding the acquired data, have access to sensitive information stored in the device. Additionally, the facilities for where data is stored (e.g. datacentre or archive facility) need to provide adequate protection from unauthorised entry. Physical access controls of equipment and data should be designed to ensure the level of access is in line with the principle of least privilege and security policies. These controls should allow for the prevention and detection of unauthorised access.
Patch and Vulnerability Management	Develop and implement both patch and vulnerability management procedures and tools to ensure all devices and software are running the most recent versions and are free from vulnerabilities. This will increase system stability and reduce the possibly of

	vulnerability exploitation. Patch and vulnerability management should tie into internal change management procedures. Performing regular security reviews on the environment is necessary to understand what issues need to be addressed. At a minimum it is recommended that quarterly vulnerability assessments and annual penetration tests are performed. Penetration tests should be performed by specialist firms that can provide an independent appraisal of the risk and report in detail the recommended course of action to improve the overall security posture.
Configuration Management	Define practices to ensure operating systems, applications and networking equipment is configured in a secure manner (hardened) to protect the environment from attacks such as unauthorised access, escalated privileges and denial of service. Furthermore, the organisation would be well advised to develop a capability to readily apply emergency configuration changes to the technologies in use should a critical security event occur.
Incident and Event Management	A management practice is necessary to identify events and address security incidents effectively as they arise. This includes practices relating to; log collection, centralised log aggregation, long term retention, log analysis as well as log search and reporting. Furthermore, an incident response plan should be developed and implemented so potential breaches of sensitive data within the environment can be reported to the designated contact and fixed as quickly as possible. Policies, standards and procedures related to incident management should also be established to include details on how information security incidents are detected, assessed, classified and handled.

Conclusion

With the exponential growth of connected devices and the myriad of digital services at our finger tips, organisations are more reliant on technology to provide the intelligence necessary to operate more efficiently and effectively. However, solutions that rely heavily on the Internet to transmit, and sometimes store information, are at increasing risk of a security incident.

Complex information systems behaving in a cohesive information chain require a comprehensive threat assessment methodology which is focused and relevant to how personal or other sensitive information types will be collected, used and retained. Information security is no longer about an isolated assessment of an IT system but the movement of information throughout its lifecycle.

IoE solutions are rapidly expanding and security must be a primary consideration for organisations looking to adopt these technologies. Defining an effective information security framework that accommodates the threat and risk management needs of new-age technology solutions such as IoE can be achieved. To achieve this however you must consider the end-to-end solution design and all points of data handling.

Appropriate threat risk modelling assessments must be undertaken at the point of evaluating new systems. Additionally, a thorough approach is required for the integration and ongoing management of controls to ensure the IoE solution maintains a solid security posture.

New technologies have the ability to provide vast amounts of value to organisations but like any solution, it comes with its own security challenges.

About Sense of Security

Sense of Security Pty Limited is an Australian based information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. Our strategic approach to security provides our clients with a capability to understand the security risks relevant to their organisation and knowledge to protect their information assets. We provide expertise in governance & compliance, strategy & architecture through to risk assessment, assurance & technical security testing.

For more information please contact us:

Web: www.senseofsecurity.com.au

Email: info@senseofsecurity.com.au

Phone: 1300 922 923

Sense of Security - Compliance, Protection and Business Confidence