SECURITY CONSIDERATIONS IN AN IOT DRIVEN WORLD

Gemserv

OUR DIGITAL FUTURE

We are already becoming increasingly reliant on digital services and the digital economy. Soon, our homes will be “Smart”, our health and our environments will be monitored, as will our factories, cars, bicycles, hospitals and cities (and probably anything else you can think of).

A multitude of digital services will be available to enhance our lives, increase awareness of our surroundings and protect our environment. We will have autonomous systems governed by AI algorithms making decisions about us and many traditional roles will become obsolete whilst new opportunities are created. Transactions and smart contracts will be stored in the blockchain, and we won’t need trusted third parties. Our packages will be delivered by drone, and our cars will be electric, there will be hover boards, flying cars, the working week will be 4 days (and I probably still won’t get around to painting the spare room).

Realisation of these opportunities will require creation of new business models and development of appropriate services to support them; But as with any new technology, new opportunities come hand-in-hand with risks that we must bear in mind In order to build sustainable, trusted services.

[The challenge we have is by the time you’ve read this opening paragraph the future has snuck up behind you and tapped you on the shoulder]

ENERGY

The backbone of this digital world will rely on energy - without a means to power these digital services none of the above is possible. Combine this with the well-documented challenges posed by climate change, we must supply the necessary power without reliance on fossil fuels. This digital world must be underpinned by clean renewable energy, which in turn will require new technologies and services such as battery storage, demand side response and an intelligent automated smart grid network capable of efficiently balancing supply and demand. Energy will be provided by Virtual Power Plants, alongside more traditional renewable generation, to feed an efficiently managed smart grid in a beautifully orchestrated ballet of automation. A digital world needs smart energy. Without the ability to power our new digital world with renewable energy the future doesn't look quite as rosy, in fact it looks pretty bleak.

Smart Metering is the first step towards a more energy efficient and intelligently managed power grid. Very soon we will see the mass introduction of Electric vehicle charging networks, local distributed generation, and demand side response and home energy management systems. These are all capable of autonomously controlling devices on the edge of the network to efficiently manage our energy usage and protect our environment.

THE INTERNET OF THINGS (IOT)

The IoT can really step up in this scenario, as innovation continues to push the boundaries to develop the solutions required to lead us into our digital future; But there are a few wrinkles we need to iron out before we dive in headfirst, including a number of significant challenges remaining around data security, privacy and ethics.
It's worth noting that where you have an autonomous connected smart grid providing power to a smart connected world and a multitude of digital services driving a digital economy, this is a big target. Any attacker has access to all the same emerging technologies as the rest of us. This integrated network is such a large target that the potential bad actors go beyond the stereotypical lone faceless 'hoodie' sat in a darkened room. They are likely be organised, well-funded, coordinated and highly skilled (and may or may not where hoodies).

We need to look at how we're going to secure the IoT, and it would seem natural to adopt IT security processes as a starting point. We know that Security is a business problem not a technology problem, and we have developed information and cyber security standards and frameworks to address the challenge of securing our data. These build on three core pillars: Confidentiality, Integrity and Availability. Consideration of the three core pillars helps us understand the controls we need to put in place to protect our data and systems. However, despite best efforts, it is still recognised that the advantages still lie with potential attackers to these systems.

In the first half of last year there were an estimated 945 Data Breaches, resulting in the compromise of 4.5 billion records – equating to 291 records exposed every second[1]. IT security does seem to be shifting to a "when" rather than "what if" mindset, and the introduction of GDPR has led to greater transparency and understanding of the current landscape. Information security standards and the three core pillars remain an effective way of identifying and mitigating Information security risks. However, it should be understood that existing standards are not comprehensive enough when it comes to the IoT.

In our digital future, sensing and collecting data alone isn't going to be enough. We need to be able to collect, analyse, and create actions based on that analysis, requiring the use of actuators. We are now entering the world of Operational Technology (OT) and must consider a few additional concepts such as safety and resilience, as our actions can cause physical events to occur in the real world. Traditionally OT systems have been isolated from the IT domain, but as cloud architecture and data analytics services continue to offer greater insights, the method of simply isolating OT and IT is no longer fit for purpose. When designing security management processes for IoT we must take into account both elements – for example "should a smart lock fail open or closed?" The answer must depend on the use case, but to ensure resilience of the system and address safety concerns it should have a method of opening or closing that doesn't rely on connectivity[2].

1 https://www.cbronline.com/news/global-data-breaches-2018

2 https://www.telegraph.co.uk/technology/2018/10/12/glitch-yales-smart-security-system-sees-brits-locked-homes/

SCALE

When analysing IoT security we have to consider the potential scale of the issue. While it is likely that one device being compromised may present a low risk incident, what would happened if one thousand, or one million devices were compromised?

Imagine being able to hack an internet-connected kettle or thermostat (or any other connected device with an actuator function). Being able to control a single instance is likely to result in an unhappy customer, whereas being able to hack one thousand is likely to damage the reputation of the manufacturer. If you could hack one million then you have the potential to impact wider systems including the smart grid. We have seen examples of the unintended consequences that can arise when you create large scale networks in the IT world, for example Facebook.

What started out as a nice way to keep in touch with friends and family has turned into something a little more concerning. Huge amounts of data is gathered about users to provide targeted advertising, which in turn can arguably lead to mass manipulation. Similarly, we have already seen what the IoT is capable of, should large numbers of devices be compromised and controlled, and after the Mirai Botnet incident[3], it's not surprising that the number one security requirement in the recently released European Telecommunications Standards Institute (ETSI) specification for consumer IoT[4] is "No default passwords".

BLURRING MARKET VERTICALS

The IoT is a technology enabler employed across multiple market verticals, from consumer focussed applications through to industrial and medical. We would argue that the development of security for IoT services should not be split by market verticals, but rather adhere to a common minimum baseline, supplemented further based on the risks associated with a given service.

For example, Consumer IoT devices and networks will exist alongside energy market related IoT devices and smart EV charging stations. White goods capable of enrolling in demand side response programs and virtual power plants may in turn operate alongside IoT services related to social care or health. In our digital future we will see interconnected Operational Technology alongside consumer IoT and would therefore argue that security processes should account for this.

3 https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

4 https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

Security competence should also be considered. IT and OT systems have a set of security processes managed and maintained by trained professionals, however in the consumer IoT space the role of security administrator is often undertaken by the homeowner. Basic security provided by a consumer's home router, likely to be a free router supplied by the consumer's ISP, cannot be guaranteed to protect the device, and modifications made to security configurations by the homeowner can also be an important factor here. To counteract this, IoT devices and systems in the home network should have a minimum security characteristic, without requiring intervention by the consumer.

EMERGING REGULATIONS

Security in our digital future will be paramount, and the emerging regulations further highlight the intended direction of travel. DPA2018 (GDPR) came in to force early last year and focuses primarily on the individuals' right to data privacy. The Network Information Systems Directive (NISD), released around the same time, focusses on the security of network and information systems that support the delivery of essential services[5].

The Department of Digital, Culture, Media and Sport (DCMS) code of practice has led to the creation of the ETSI standard for consumer IoT. It lists 13 key security requirements which should be considered a minimum baseline, addressing the "low hanging fruit" of securing consumers IoT devices. It further states that "Poorly secured devices threaten individuals' online security, privacy, safety, and could be exploited as part of large-scale cyber-attacks"[6]. Similar initiatives are moving forward to define IoT security requirements – in particular, the National Institute of Standards and Technology (NIST) have recently published a companion guide to their cyber security framework to address IoT[7], and the European Network for Cyber Security (ENCS) have developed a set of security requirements for smart electric vehicle chargers[8].

5 https://www.ncsc.gov.uk/guidance/introduction-nis-directive

6 https://www.gov.uk/government/news/new-measures-to-boost-cyber-security-in-millions-of-internet-connected-devices

7 https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

8 https://encs.eu/wp-content/uploads/2017/10/EV-Charging-Systems-Security-Requirements.pdf

6

WHERE TO START?

Primarily, we need to analyse the aspects of our IoT systems, including considerations from both IT and OT. Existing information security frameworks such as ISO27001 or the NIST cyber security framework are a good place to start as they are adaptable and flexible enough to be applied to the IoT. However, the differences between IT, OT and IoT must be understood to produce effective controls. When analysing risk and developing security requirements we must consider the physical device, the services it offers, the environment in which it operates and the data it processes.

To achieve this, we recommend that businesses consider the following to understand gaps that may exist around securely managing the IoT:

- Understand the differences between IT, OT, and IoT;
- Use best practice guidelines for IoT security;
- Use established security frameworks;
- Understand the risks in light of the differences;
- Understand the regulatory landscape and how it is changing;
- Consider how assets will be managed across the lifecycle; and
- Build trust, in a digital world trust will be paramount.

The IoT can help reduce carbon emissions, improve efficiencies and drive new business models to create long term sustainable services, but only if the foundations are secure. Using established methods to identify and mitigate risks, combined with an understanding of where the differences lie will be the corner stone to achieving a more secure IoT. Time is short, the future is here.

SEAN GULLIFORD

HEAD OF CONNECTED DEVICES

To get in touch with us contact us at:

London Office

8 Fenchurch Place

London, EC3M 4AJ

Telephone: +44(0)20 7090 1022

Email: connected.devices@gemserv.com

Visit: www.gemserv.com

@gemserv

Ireland Office

Fitzwilliam Hall Business Centre

Fitzwilliam Place, Dublin 2

Telephone: +353 (0) 1 669 4630

@gemservireland

Company Reg. No: 4419878

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS