SentryBay

www.sentrybay.com

IoT Security & Privacy

Technical White Paper

June 2015

SentryBay Limited:

UK Headquarters
3 Manchester Square
London W1U 3PB
United Kingdom

ph: +44 (0) 203 219 3060

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

ph: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
ph: +1 (650) 242 8796

SentryBay

www.sentrybay.com

Table of Contents

SentryBay Limited:

UK Headquarters
3 Manchester Square
London W1U 3PB
United Kingdom

ph: +44 (0) 203 219 3060

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

ph: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
ph: +1 (650) 242 8796

SentryBay www.sentrybay.com

IoT Security & Privacy

The IoT ecosystem

The much-anticipated Internet of Things (IoT) is finally happening. Our world is about to be fundamentally changed as billions of devices are made smart and connected. The final technical building blocks are being produced to enable just about everything imaginable to be networked, we will soon live in a networked world of things. It is the latest wave in an ever-faster technological progression.

Nothing will be exempt from change. IoT will network devices in the home, in the vehicle, in the office, in the school, in the factory, on the farm, in public infrastructure, and on our bodies. Wearables will monitor our health and activity. Radical possibilities for enhancing our lives are emerging as objects and data are connected in ways never done before. The IoT is heralding the Connected Society.

A gold rush

Aspects of the California gold rush of 1849, and the oil rush in Pennsylvania ten years later followed by similar events at Spindletop, Texas in 1901, are being repeated today as large companies rush to stake their claim in the rapidly emerging IoT world. Recognising the hugely lucrative potential of IoT, the largest information technology companies in the world are rapidly developing and acquiring technology in order to own a piece of the landscape.

Manufacturers are enhancing just about every device they produce to make them smart (adding computing power) and interconnected. Examples are smart light bulbs and smart electrical plugs. One benefit of smart appliances is smart diagnosis, notifying the service centre of the results of appliance self-fault diagnosis.

To enable smart technology, hardware manufacturers are rushing to stake their claim of the IoT space. Samsung have developed Artik chips, ARM have their Cortex-10 chips, Qualcomm their wi-fi chips, and there are numerous companies producing cheap, low-power IoT sensors such as STMicroelectronics, Samsung and LG. These sensors are designed to be built into just about everything imaginable.

Other giant global corporations rushing to stake their IoT claim such as IBM who have identified their IoT sweet spot in analytics, Booz Allen who have developed an IoT strategy, AT&T who's focus is the connected car with their Drive Studio, and every major global telecommunications

SentryBay Limited:

UK Headquarters
3 Manchester Square
London W1U 3PB
United Kingdom

ph: +44 (0) 203 219 3060

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

ph: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
ph: +1 (650) 242 8796

company rushing to create a part of 5G – the communication channel which will enable mass IoT data transmission.

The operating system used to drive IoT is critical with several technology giants having commenced battle for prominence. An IoT operating system must have a small footprint and be suitable for low-powered devices. Google are developing Brillo, Microsoft are developing an IoT version of Windows 10, Blackberry have their QNX platform, Hauwei have developed LiteOS, Intel have VxWorks, and Contiki is an open source IoT operating system project. The number of powerful players in this area reflects the influential role an operating system has in the IoT ecosystem.

Two major issues need to be overcome: Usability and Security

With the IoT claim rush well underway in the tech sector right now, we will soon see a lot of connected, smart devices, each running one of numerous IoT operating systems, most with their own unique user interfaces. Two significant challenges arise – usability and security. Today, it is difficult enough for the average consumer to cope with different user interfaces on the relatively few smart, connected devices such as their laptop, tablet, smartphone, TV, SatNav, and perhaps heating system. An exponential growth of different user interfaces will put many of the benefits of IoT into the too-hard basket for most consumers. It is too much to expect the average consumer to learn too many different systems.

Today, information security practitioners are battling to cope with the myriad of security threats directed at government, the enterprise and individuals. As the IoT gathers momentum, the attack surface will be exponentially enlarged. New technology, new operating systems, new environments, new devices – all will introduce new security vulnerabilities. Challenges to protect confidentiality, integrity and availability in a Connected World will be exponentially greater. Privacy will be far more difficult to safeguard.

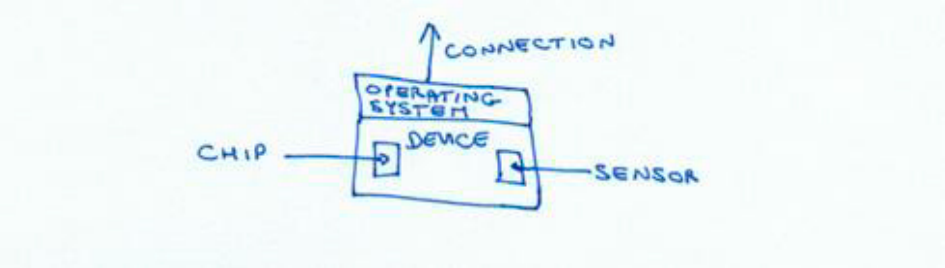
Both the usability and the security challenges are best dealt with through a centralised IoT Command Centre.

SentryBay www.sentrybay.com

A centralised IoT Command Centre to enable the Connected Society

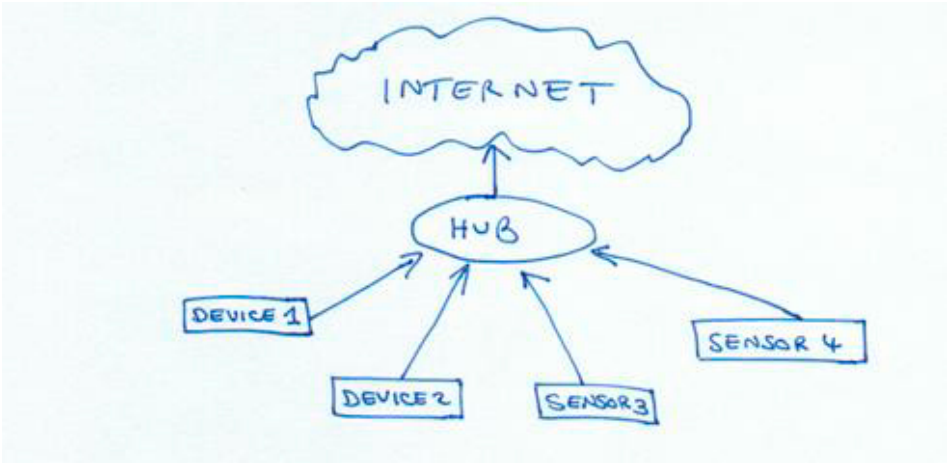
IoT devices vary in complexity from a simple sensor to a more complex device with computing power, an operating system, and connectivity. On the more sophisticated side, a typical device could comprise:

Figure 1: Components of a smart, connected device



IoT devices either connect directly to the internet through mobile networks or Wi-Fi, or connect to a hub through technologies such as Bluetooth, ZigBee or Z-wave. The hub is then connected to the internet. Devices are connected 24/7 – "always-on" – providing continuous, round-the-clock service and data.

Figure 2: Some devices are connected through a hub



SentryBay Limited:

UK Headquarters
3 Manchester Square
London W1U 3PB
United Kingdom

ph: +44 (0) 203 219 3060

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

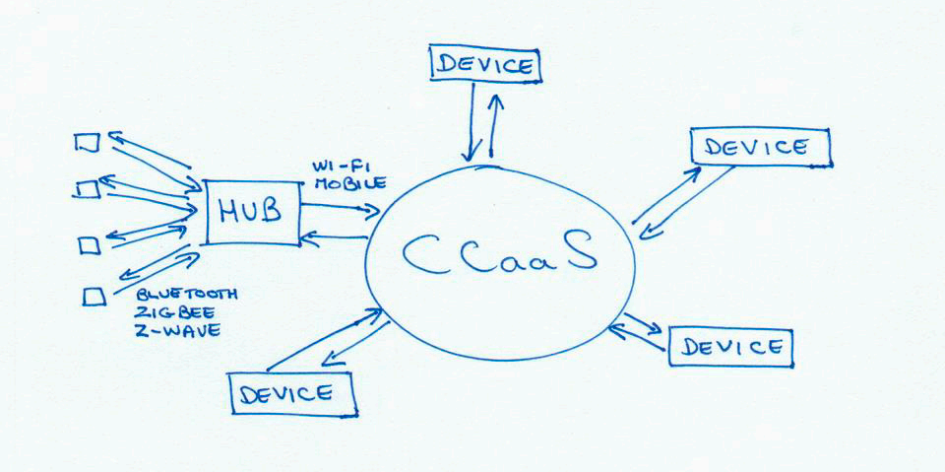
ph: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
ph: +1 (650) 242 8796

SentryBay www.sentrybay.com

A centralised IoT Command Centre enables a user to interact through a familiar interface in a system containing appropriate security technology:

Figure 3: A centralised IoT Command Centre



The Command Centre is cloud-based, providing access from anywhere through any internet-enabled device such as PC, smartphone or tablet. Command Centre as a Service (CCaaS) enables data from differing IoT operating systems to be shared. The Command Centre enables communication between the IoT device and the cloud platform, and between the cloud platform and the device. The connection of large numbers of devices enables the Connected Society. Users interact with the Command Centre in order to:

- - View or change device settings. For example, a user can view the security status of their home (such as check if the garage door is closed), or set personal fitness goals.
- - Viewing IoT analytics
- - Viewing or changing data sharing permissions. Ideally, IoT apps should be transparent and change data sharing permissions.

SentryBay Limited:

UK Headquarters
3 Manchester Square
London W1U 3PB
United Kingdom

ph: +44 (0) 203 219 3060

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

ph: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
ph: +1 (650) 242 8796

SentryBay www.sentrybay.com

Three essential Command Centre as a Service components

1. A Common User Interface (UI) convention

On a PC, the Windows operating system is the platform upon which all user programs run. Even though each program is built displaying a unique user interface, there are certain common characteristics which each UI inherits from the operating system. A window minimise button is one example. This provides the user with a degree of familiarity to all Windows programs.

A suitable model for providing UIs for the IoT Command Centre is similar to that of Wordpress, the open source blogging tool and content management system. Wordpress includes both a template system and a plug-in architecture. Wordpress users wishing to create web content can either use the quick-and-easy template system, or they can start with a blank canvass and employ plug-ins and write their own code. Similarly, an IoT Command Centre should provide IoT device manufacturers the option of either a quick-and-easy template system to create their UI, or a blank canvas and plug-ins to create a more tailored and unique UI. However, the commonality of multiple IoT systems channelled through the same Command Centre provides a degree of familiarity to the user. An IoT Command Centre should leverage the developer community in an open environment.

iYogi have created a partial IoT Command Centre solution with their Digital Services Cloud, where they provide IoT UI templates but no blank canvas and plug-ins. However this solution only partially satisfies one out of these three essential command centre components.

2. Data storage and sharing junction

A Connected Society requires IoT data storage and sharing. And lots of it. The centralised Command Centre provides the platform for managing storage, managing data sharing, and managing M2M communication. Sharing data between IoT systems adds utility to the IoT device function exponentially. In addition, a centralised Command Centre provides the portal to channel analytics from multiple IoT systems.

Command Centre as a Service can also provide traditional BaaS/MBaaS functionality such as push notifications and integration with social networks.

SentryBay Limited:

UK Headquarters
3 Manchester Square
London W1U 3PB
United Kingdom

ph: +44 (0) 203 219 3060

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

ph: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
ph: +1 (650) 242 8796

Users should be able to stream a summary of metrics from the Command Centre through to their smartphone or smartwatch – keeping them in constant contact with their own network of things.

3. Common Security Architecture

As connectivity expands, impacts of security and likelihood of privacy breaches multiplies exponentially. Security is crucial for a Connected Society because of the disastrous potential for things to go wrong. The common security architecture is, by far the most important aspect of the Command Centre.

In a highly-connected society, the loss of confidentiality, integrity or availability can have significant, even life-threatening repercussions. The Command Centre should specify appropriate protocols and security and privacy standards. The IoT Command Centre must be built from the ground-up with security at the core, and include aspects such as:

- Encryption of sensitive data at rest and data in transmission.
- Data classification. All IoT data channelled through the Command Centre must be classified according to criticality and sensitivity. Data associated with the operation of a motor vehicle is an example of critical data, whereas personally identifiable information is an example of data which is sensitive. The security and management of the data is determined by its classification.
- Single Sign-On. Rather than the user managing numerous logon credentials for various IoT devices, all access is through a secure SSO mechanism.
- Sandboxing - keeping applications and data separate.
- Patch management.
- Vulnerability scanning.
- Update management.
- Access management. For example, sensitive data entered on a user device such as logon details, should be protected against key logging attacks. Two-factor authentication could be appropriate to access highly-sensitive data.
- Endpoint hiding – thwarting detection by ensuring network attacks cannot complete network mapping activities.
- Data sharing protocols – ensuring data sharing permissions are user-driven and transparent.
- Connectivity through 5G has significant security implications which need to be addressed in a Connected Society.

Related articles

Securing the IoT – the Command Centre is Cardinal:

http://dwaterson.com/2015/04/15/securing-the-internet-of-things-the-command-centre-is-cardinal/

I am a garage door in the IoT:

http://dwaterson.com/2015/03/16/i-am-a-garage-door-in-the-internet-of-things-iot/

Security implications of 5G:

http://dwaterson.com/2015/03/09/security-implications-of-5g/

SentryBay Limited:

UK Headquarters
3 Manchester Square
London W1U 3PB
United Kingdom

ph: +44 (0) 203 219 3060

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

ph: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
ph: +1 (650) 242 8796