SECURE IOT GATEWAYS

Whitepaper on the need for industry collaboration

nquiringminds

ai • security • iot

IoT Security: understanding the risks, and what can we do about them

Why the big fuss

The Internet of Things (IoT) is the natural evolution of the internet. The internet has made a huge impact on society, changing not just the world economy but transforming the very way that people live their lives. I think we can expect IoT to have a similarly significant - if not greater - impact.

Ericson estimates that:

> Around 29 billion connected devices are forecast by 2022, of which around 18 billion will be related to IoT. [1]

McKinsey predicts that:

> Our bottom-up analysis for the applications... estimates that the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025. At the top end, that level of value—including the consumer surplus—would be equivalent to about 11 percent of the world economy (exhibit). [2]

But as another McInsey paper [3] points out Security issues may represent the greatest obstacle to growth of the Internet of Things. Security is an issue not just because these concerns may impact economic growth, but because the mitigation strategies employed could fundamentally determine the power base of this new IoT economy.

So what exactly is IoT?

Taking three semi authoritative definitions in turn:

> IoT refers to the ever-growing network of physical objects that feature an IP address for

> internet connectivity and the communication that occurs between these objects and other Internet-enabled devices and systems.

https://www.webopedia.com/TERM/I/internet_of_things.html

> IoT has been defined in recommendation ITU-T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

> IoT is the extension of Internet connectivity into physical devices and everyday objects. Embedded with electronics, Internet connectivity, and other forms of hardware (such as sensors), these devices can communicate and interact with others over the internet and can be remotely monitored and controlled

https://en.wikipedia.org/wiki/Internet_of_things

All three definitions describe an aspect of IoT but - particularly from a security perspective - neglect the two most essential characteristics that are critical to understanding the step change in risk.

IoT devices are servers

A lay person's understanding and experience of the internet is generally formed from their experience as a web-client. Whether on a PC, tablet, phone or smartwatch, as a content consumer, a web client will typically make their searches using a web browser. This means that connections are client initiated and produce pull down information for them to view.

IoT devices, typically, invert this relationship. The devices themselves are usually the content generators. These devices "push" information out into the internet, where it is consumed by other devices. IoT devices are more akin to a web-servers than web-clients. This introduces a whole raft of security considerations that need to be addressed.

IoT devices don't directly connect to the internet

The internet is mentioned directly in two out the three definitions above - only the ITU definition takes a more generalised stance. This is illustrative of the important point that a lot of the devices we consider to be IoT devices do not directly connect to or support the internet in the formal sense. SigFox, LoRa, BTLE, Zigbee, Zwave, Ant+ even NB-IoT, are all firmly IoT technologies yet none of them directly support IP. And as we shall see later, this has a profound impact on security.

So what exactly is an IoT device?

It turns out pinning down exactly what it is that constitutes an IoT device isn't entirely straightforward.

If we take an inclusive approach, we could define everything that either directly or indirectly connects to the internet as being an IoT device. This means that IoE devices are now the superset of all traditional (PCs, tablets, phones, servers, etc) and new generation IoT devices.

If we want to be more specific in defining an IoT device we need to consider the industry recommendations as well as the government legislation. This is ongoing activity in many countries (US, UK, France etc). But clearly without a robust working definition of scope this activity will result in hazardous situation.

Consider which of the following examples are IoT devices and which are not:

- Is my PC an IoT device?
- What about my phone and tablet?

- My smart watch?
- How about my Smart TV?
- I have a "dumb TV", but I put a smart stick in the HDMI? Are either of them or both of them IoT devices?
- What about my set top box?
- My network devices: routers, modems and WiFi repeaters?
- My car?
- Smart fridge?
- Internet connected bathroom weighing scales?
- Weighing scales that are not connected to the internet, but connect to my phone over Bluetooth, where my phone connects to the internet?
- An internet connected webcam?
- A normal video camera, connected to a PC, which then serves IP stream to the internet?
- A Bluetooth camera connected to a mobile phone which server and IP stream?>
- A NAS drive which serves media over DLNA?
- A PC which also serves media over DLNA ?
- A GPS tracker device with built in SIM card and IP connectivity?
- A mobile phone which is acting as a GPS tracker?

The list goes on and the number of edge cases expands exponentially but there are two main points to consider:

First, if we are using the term IoT in everyday conversation, the actual definition doesn't really matter that much and we can be quite fluid. But if the term is being used in formal specifications, industry recommendations or government legislation, the interpretation of it becomes a critical business issue.

Second, as we go some way to demonstrate the "device fluidity" in the list above we should not lose sight of the fact that IoT devices introduce a layer of security recommendations. If the security recommendations are to be useful we need to be able to highlight the specific challenges that we need to address.

Why is IoT so hard

Let us put aside the IoT definition problem for now and instead consider the fine grained details of IoT security. What is it about IoT devices that makes the security issues so difficult to address?

For the purposes of this analysis we will focus on domestic IoT devices which are small and typically battery powered for use in the home setting.

No user interface

Your typical IoT device has no (or at least very limited) user interface (UI). It might beep, have a flashing LED and you might have a button you can press with a pencil, but it lacks the rich interactive UI of mobile phones. From a practical standpoint this makes configuration and setup of IoT devices far more challenging. Providing the user with any meaningful feedback on the device status is very complicated.

Physically insecure

Many IoT devices are physically insecure, especially SmartCity and agricultural sensors.

Unlike a web server, which is placed in a physical secure hosting centre, an IoT device could be on a streetlight, in a field, in a garden or on the wall of a house. The risk of physical attack on IoT devices is higher even than for mobile phones, which a user tends to keep close to themselves at all times.

Power, power, power

Some of the hardest security challenges for IoT devices are driven by the low power requirements for sensor devices. If an IoT device cannot be plugged in it needs to run on battery. As a rule of thumb, a minimum battery life of two years is required to ensure its economic usefulness (otherwise the manpower cost of regular battery changes erodes the sensor's business case). However, designing connected devices that regularly take sensor readings and run for two solid years on a reasonable sized battery is far from easy. This basic physical constraint has a major impact from a security perspective.

Power: no I in IOT

The first casualty of this power constraint is the network itself. Typical IP (internet) networks have an overhead that a power efficient network transmission layer cannot support. None of the networks that we associate most closely with IoT support IP protocol natively. These include NB-IoT, LoRa, Zwave, Zigbee, Bluetooth Low Energy, ANT+. This is not an accident but a constraint imposed by the laws of physics.

This simple but unavoidable truth turns IoT into an oxymoron. There is frequently no "I" in IoT.

Our standard portfolio of cryptographic protocols therefore needs to be reconsidered. The super power efficient IoT networks have properties that make developing cryptographic protocols extremely challenging as a result of the fact there's no reliable delivery, small packet sizes, no packet reassembly, asymmetric bandwidths for upstream and downstream and in some instances highly asynchronous data communication (implementing a TLS algorithm would be very challenging).

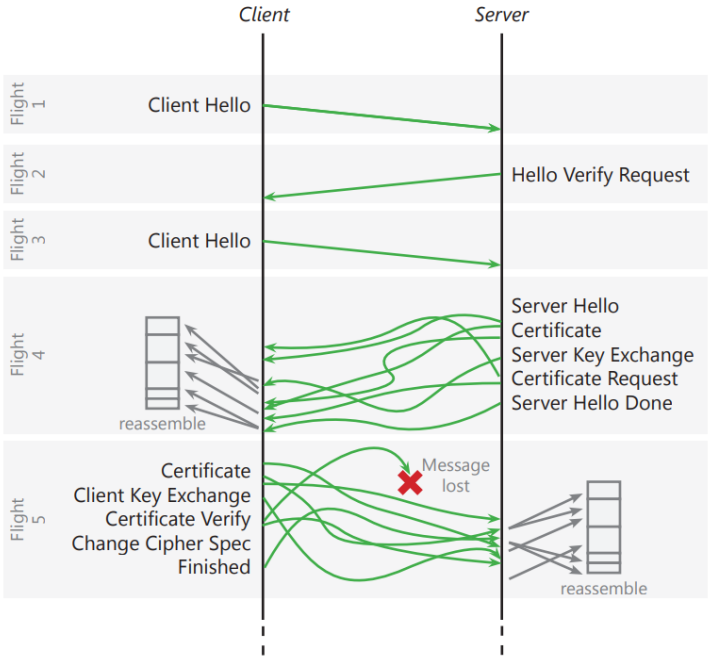
Taking SigFox as an example, its power efficient design has been created to maximise battery life even though it is a propriety implementation. Its network qualities are:

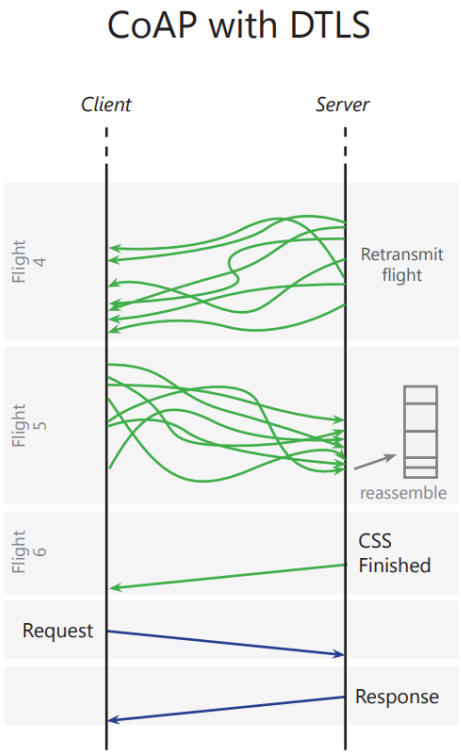
- 12 bytes upstream per messages
- 8 bytes downstream
- 140 messages per day
- only 4 downlink messages per device per day
- no encryption on the wire

The different classes of IoT networks have different properties but none of them are full-fat networks with rich built-in TLS support.

Although this topic becomes very complex very quickly, it is worth noting that even simple processes such as session negotiation becomes intractable when being performed on a constrained network. Hartke and Bergmann's

IETF memo on DTLS obstacles is a good introduction to this problem.





https://www.ietf.org/proceedings/83/slides/slides-83-lwig-2.pdf

https://tools.ietf.org/html/draft-hartke-core-codtls-01

Power: reduced crypto capability

The second impact of the power constraint is the underlying support for cryptographic functions. Low power constraint means low power CPU (and reduced memory footprints). This directly impacts the range of cryptographic functions that can be supported natively on devices irrespective of the qualities of the networks.

Secure storage

A secure device needs somewhere to store its secrets. Whether these are transient session tokens or private keys for secure session negotiation, there will be several requirements to store secrets on devices for differing amounts of time. Secure storage can be complex to implement correctly.

The deep roots of secure boot

Secure storage is in fact impossible to implement and therefore worthless without assured boot. If the code running on the device itself cannot be trusted it is very hard to make any strong assurances about the functioning of the IoT devices. Secure boot is highly silicon

specific and requires deep understanding of software and hardware processes behind it. Secure boot functions are often protected by the silicon vendor for both commercial and security reasons. Therefore when all said and done secure boot only takes you so far up the chain. For the more complex IoT devices we need to start thinking about security implementation of the operating system and update mechanisms as well.

Connectivity

An IoT device should not assume that there is always a public internet connection. This impacts the design of a holistic security system. Centralised CA servers, authentication servers, authorisation servers and resource directories can simplify the design of a secure system immeasurably. However if the internal domestic IoT network ceases to work when the internet goes down then the solution is not useful anymore.

Heterogeneity

Simply put there are lot of different devices available from different manufactures that use different protocols on different operating systems and connect to different services. Given that a security system is only as strong as it weakest link there are a lot of permutations that need to be carefully examined before it is possible to confidently state that an IoT deployment is secure.

Local connectivity

An IoT device may connect to the internet or it may connect locally on an internal network. Smart lighting is usually controlled by local switches and mobile applications on the local network. Similarly smart speakers are typically controlled by remote controls and mobile applications. The IoT packets do not leave the home network.

This introduces a couple of security challenges:

1. How is it possible to implement security that works equally well for connections inside and outside the house?
2. Ignoring the problem of the non-IP IoT networks, how do we implement end to end security for two devices on a local intranet? The normal go-to solution of HTTPS certificates on the open internet simply doesn't work.

Interoperability: security usability

The interoperability of IoT devices is a worthy goal in its own right. There are commercial players incentivised to make it happen and at the same time there are also commercial players who are motivated to create locked-in ecosystems over which they can assert a monopoly.

But setting aside the generalised incentives for ecosystem interoperability, when it comes to security, there should be clear alignment. Having interoperable system wide methods of connectivity and messaging reduces the attack surface of an IoT network considerably. It is true that a systematic weakness in an interoperable protocol design exposes the entire system to attack. However a reasonable argument can be made that focusing the collective attention of a few connectivity pathways is inherently more secure than having multiple proprietary legs.

We should always remember that the end user often presents the single biggest risk to an IT system. As the secure interoperability argument of IoT device is important the human to system usability argument is even stronger. We will only ever achieve usability across a portfolio of

different IoT devices if there is a layer of interoperability.

For instance for a user it makes perfect sense to be able to control which devices have permission to access certain network resources and also which applications have access to certain devices in a centralised way. It could be argued that it would be impossible for the average user to meaningfully do this without a unified management interface.

Update usability

The update problem is in fact just another version of the security usability problem. It is well recognised good practice that to keep services secure it is necessary to regularly update them. For instance the DCMS Code of Practice for Consumer IoT Security specifies several industry guidelines for IoT devices.

https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

But first we should look at the practicalities. Below is a random list of 7 temperature sensors:

https://www.whywelikethis.in/top-7-best-zigbee-temperature-humidity-sensors/

Shang Tong Zigbee Temperature Humidity Sensors
Brook Zigbee Temperature Humidity Sensors
Iyoukesin Zigbee Temperature Humidity Sensors
Elvy Zigbee Temperature Humidity Sensors
Passionin Zigbee Temperature Humidity Sensors
Generic Zigbee Temperature Humidity Sensors
Shang Tong Zigbee Temperature Humidity Sensors

Each of these sensors provides the same functions of temperature and humidity. They work on the same bearer technology (Zigbee) and therefore we can assume they will work interoperably over the same Zibgee network. But if we want to ensure all of them are up to date we will have to follow seven different sets of instructions using seven potentially different update applications.

This is clearly not a sustainable or a sensible position.

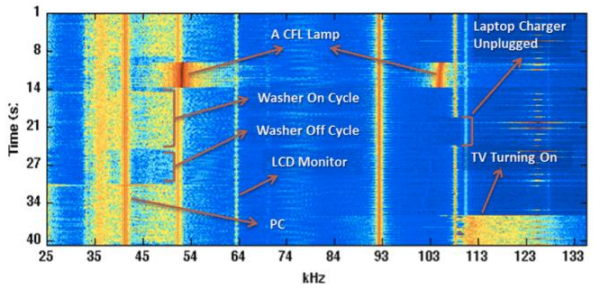
The router problem

Almost all IoT devices have a router. The physics of data transmission means there is usually a short hop before a long hop. Whether a Zigbee, Zwave, or LoRa, there will always be some sort of network concentrator.

So the crux of the issue is that the short hop is likely to be non-IP, meaning it will have to implement some custom end to end crypto between the IoT device and the IoT router. The long hop to the server is likely to be traditional internet in the form of TLS, HTTPS or similar. What this means is the IoT router must decrypt and then encrypt all data leaving the local networks. This makes the router a very attractive attack target as it needs to cache encryption and session secrets.

Information disclosure

A pervasive, always on, fine-grained sensing of the user environment and behaviour will inevitably reveal unexpected information about the user.



https://energyanalyst.co.uk/applying-machine-learning-to-the-electricity-industry/

The above diagram shows that just by looking at fine grained energy consumption data from a smart meter it is possible to identify the use of individual devices on the grid.

This academic paper from Munster University of Applied Sciences goes a step further and shows how to identify what channel a home owner is watching from energy consumption data alone.

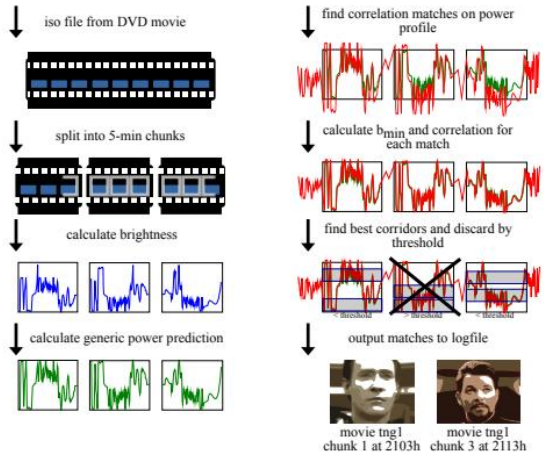


Fig. 8. Work-flow to detect chunks of a movie

In our own company we are using similar techniques to address the Ageing Society Grand Challenge by looking for anomalies and trends from simple user movement data to help spot indications of declining health.

https://www.businessandindustry.co.uk/industrial-strategy/ageing-society-grand-challenge/#

Uber has patents in application to determine how drunk a potential passenger might be by looking at usage data from their mobile phone.

https://techcrunch.com/2018/06/11/uber-applies-for-patent-that-would-detect-drunk-passengers/

In each of the above examples a typical user will not be aware of the potential inferences that can be made through the sharing of seemingly innocuous information.

The security challenges as a result of information disclosure of IoT data will require some major rethinking on data permissioning and the transactional nature of information analytics.

Device ownership/changing

IoT devices may have one or more owners (household members) and over time these owners may change. From a security perspective this means a thorough analysis of device lifecycle over time is required.

Group problem

The final problem to tackle is the device group. This problem is very real, simple to explain and complex to solve.

For instance, take a smart bulb in a particular house. Suppose it requires several bulbs to light a room. They are configured to operate on a virtual circuit so they can be controlled by a single switch (both a real physical switch and a button on an application). It's probably reasonable to assume that in an ideal world it would be possible to buy my bulbs from several

different vendors so that the entire house is not locked into a single bulb supplier.

Skipping over the design, setup and installation phase, the user has been happily living with a smart lit room for 18 months and suddenly a bulb blows. So he or she goes out to the local DIY store and buys a new one.

The question that needs to be asked is, how does the user provision a new bulb on the virtual circuit in a secure, interoperable, easily configured manner?

To reframe the problem slightly, how many standards engineers does it take to change a lightbulb?

When we have solved this problem we will have gone some way to addressing the IoT security challenge

Where are we now?

So how much progress are we making addressing these challenges?

We have bits and pieces but the honest answer is not very far. And in the absence of complete solutions this quote is a reasonable summary of our current trajectory.

> "Despite continued security problems, the IoT will spread and people will become increasingly dependent on it. The cost of breaches will be viewed like the toll taken by car crashes, which have not persuaded very many people not to drive." — Richard Adler - Distinguished Fellow at the Institute for the Future

https://www.pewinternet.org/2017/06/06/theme-3-risk-is-part-of-life-the-internet-of-things-will-be-accepted-despite-dangers-because-most-people-believe-the-worst-case-scenario-would-never-happen-to-them/

There are number of national and international initiatives looking to plug some of the holes, including the UK's own IoT security labelling initiative currently out for consultation.

https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

And of course we have the activities of the IoT Security Foundation https://www.iotsecurityfoundation.org which is an international focus point for the important work that needs to continue in this area.

But in the meantime a few home truths need to be recognised:

One: it's really hard

The list above is just scratching the surface but should hopefully give a sense of just how hard some of these fundamental IoT security challenges are.

Two: its going to take some time

This problem is not going to be fixed overnight. Time, investment and genuine industry collaboration are going to be required to fully address these issues.

Three: the horse has bolted

Basically it's too late. The list of already compromised devices is huge. The list of potentially compromised devices is unknowable. And these security flaws do not just relate to individual devices and manufactures but to entire classes of devices with known vulnerabilities.

Secure IoT Hubs: a practical IoT security strategy

Given the analysis above it is clear we need a containment strategy and not just a prevention strategy. The diversity of devices to be considered, the number of insecure devices that have already been sold and both the complexity and time it will take to achieve industry-wide consensus on workable IoT endpoint security points us to only one workable solution:

IOT security needs to be underpinned at the router level; we need the concept of a secure IoT Hub

The IoT security foundation has already done some excellent work in creating some requirement alignment and putting forward some architectural proposals for both consumer hub and enterprise hubs.

This work needs to be moved forward to the next level if we are to meaningfully address the security risk.

The IoT hub has a central role to play in connecting whole families of IoT devices. It can provide a centralised management and monitoring function across many IoT devices.

The features and functions we might expect of this central component can be broken down as follows:

Foundations

In a normal IoT deployments we have already identified the potential security risks an IoT Hub presents by virtue of the fact it must decrypt and then encrypt data from optimised IoT networks. Even before we start enhancing the IoT Hub with security management features we need to lay the necessary security foundations for an IoT hub implementation. Much of this is simple industry good practice, secure boot, secure storage, credential management, lifecycle management etc. But there is obvious ecosystem benefit in setting minimum standards on these security foundations and establishing industry consensus and momentum to encourage compliance. If we fail to address these basic challenges, even if we fully secure the IoT endpoint devices, the system will still be exposed.

It is worth noting that it is typically harder to fully secure an IoT hub (full stack secure boot) than an IoT device. And where IoT hubs are a necessary part of almost all IoT deployments and where the IoT hub presents a central attack point for many IoT devices this is arguably a far more important activity than securing IoT endpoints.

Containment: network isolation

We need to consider two coarse grained attack scenarios for an IoT network:

1. External and internal entities attacking the IoT device
2. A compromised IoT device attacking entities both inside and outside the network,

where clearly the motivations for (1) is to execute attacks of (2).

A method or reducing the risks of both types of attacks is to implement a network isolation.

We see this as a type of internal firewall where instead of protecting internal network IP assets from external IP attacks we are using similar techniques to protect internal IoT assets from both internal and external attack, in both directions. In the first instance we can partially achieve these objectives by separating the IoT assets from the traditional IT assets. However

this can evolve to more sophisticated containment strategies. The approach also needs to consider the legitimate use case of an IoT device actively communicating with IT assets and how this is managed. The approach must also address head on the question of what constitutes an IoT device.

Management: device updates

We know we have to keep the IoT devices up to date in order to stay secure. We also know that IoT devices are incredibly diverse with very different and sometimes quite complex update procedures.

The IoT hub has a valuable contribution to make here in acting as a centralised user interface to monitor and manage required IoT updates which reduces the administrative complexity for the end user.

This does not mean we have to standardise the physical update process. There are many parallel initiatives that are working on such solutions. This proposal would only require that we standardise the end user notification and control methods. The complexity of the update mechanisms themselves could be hidden behind tools and open source stacks provided by the device manufacturers and development community.

Secure discovery and connectivity

It stands to reason that IoT devices and other IoT architectural elements (various types of IoT hubs) will need to connect to each other on an internal network (the end user's home network).

Making a secure connection between devices on an internal network is not as simple as it might seem. It is necessary to consider in detail how these trusted connections are bootstrapped as well as how to protect these connections from man-in-the-middle attacks. In addition we need to consider how we manage the lifecycle of these connections. Our go-to solution on the public internet and HTTPS certificates doesn't work so well on internal networks.

A centralised IOTHub has a valuable potential role here to help create and manage these secure connections.

Interoperability and permissioning

The interoperability of IoT devices is an issue bigger than security. Nonetheless it is clear that the interoperability of IoT devices has a clear impact on security and vice-versa.

For the owners of IoT devices it seems reasonable to expect to have control over what that IoT devices can connect to and what services the IoT device can access. For us to be able to assert this level of control in a usable way we need a method enabling and disabling these permissions in a common way.

Given the diversity of IoT devices and IoT protocols, implementing this level of control will be impossible in the near or even medium term. It would require major cross industry standardisation across multiple protocols and software stacks. Features introduced at the IoT Hub could make this problem far more tractable.

An IoT Hub almost by definition is a centralised control point from where such permissions could be managed.

However it will not be easy. The notion of an IoT permission will need some cross technology unification of the notion of device identity, user identities and possibly also software and data resource identities. However, if carefully

constructed, it may be possible to create a unified model of IoT permission control which is a critical foundation of usable security for IoT.

User notifications and policy

As an adjunct to the permissioning problem, we need to address the issue of explicit user consent. For IoT this is made more complicated because of the inconsistency and/or lack of usable interface on IoT devices, coupled with the asynchronous nature of IoT notifications.

We believe the transactional messaging model - where users can accept or deny connection requests that we see in social networks - is a proven UI model which has potential to be applied to IoT networks. These messaging notifications should be complemented with an overarching policy that will help determine who gets asked what and how often. Again the IoT Hub is the natural place to implement these policy and notification mechanisms.

Information flow

The information flowing out of the IOT network into the cloud is a significant security issue. An interoperable policy mechanism may give us binary (on/off) control over which device talks to which device's services. Therefore it could be considered reasonable to have control over the quantity and quality of the data that is transmitted and shared with third parties.

For example, if implementing a smart speaker providing voice activated controls, is it necessary to record and send every utterance to the cloud?

If we are implementing a health monitoring system for the home do we need to share every single measurement and movement in the house?

In both cases the answer is no. It is not necessary because it is possible to process some, if not all, of the data locally. This fundamentally reduces the information that needs to be shared with third parties thus reducing our privacy exposure. The way we achieve this is through edge processing.

If we are able to define some edge processing primitives that work interoperably at the IoT Hub this clearly provides major privacy and security benefits.

Monitoring

We have established that insecure, compromised and compromisable IoT devices are currently in circulation. It is reasonable to assume this will continue to be true for the foreseeable future, even with the current momentum behind IoT endpoint security. It is essential therefore that we implement detection strategies. Industry collaboration on initiatives that will speed up and improve the detection rates on compromised IoT devices is an essential component of such a strategy.

The IoT Hub, as a central integration point for IoT data, can assist with this monitoring function. By defining minimal data collection standards and remote access protocols, we can put in place powerful mechanisms that will assist with the early detection and later containment of security threats. Given that this threat is shared across a broad portfolio of stakeholders we can present strong arguments for cross industry collaboration and standardisation of these functions.

Collaborative Security Analytics

The next logical layer in IoT threat detection is the implementation of collaborative analytics to identifying threats from the baseline IoT data.

Most IoT devices will have characteristic behaviours. Messaging activity significantly outside the device's typical behavioural envelope is indicative of a potential threat. Equally, external or internal attacks on IoT devices will have identifying hallmarks.

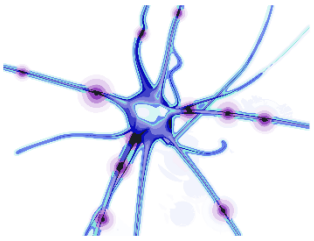
This type of analysis could happen in the cloud or be implemented at the edge. These activities may prove to be proprietary differentiating features of IoT hub vendors or we may conclude that it is in the common good to share certain data. What is clear is that the IoT hub plays a central role in this detection activity.

Protection

Assuming we can successfully gather IoT activity data from different devices and assuming we can implement detection methods to pick up significant threats we then need to be able to do something about it. This is where our containment strategy comes in. Earlier in the document we identified network isolation as being a potential element of an IoT Hub security strategy. If a threat is detected we may have a portfolio of mitigation available to warn the hub owner and service provider through an implementation the network isolation on that device. Again the IoT hub is central to the delivery of such a suite of security mechanisms.

Looking forward

IoT security is a difficult problem that will not be solved overnight. There are a broad range of industry initiatives underway to help mitigate these threats and the IoT security foundation is taking a leading role in this on the international stage. As outlined in this document, the IoT Hub has a critical role to play in the IoT security ecosystem that complements the ongoing endpoint security initiatives. The IOTSF has already undertaken some seminal work in this area by publishing enterprise and consumer reference architectures. These documents do an excellent job in setting out the opportunity and are a first step in generating industry alignment around this topic. However, if we are to meaningfully address the IoT security threats in a realistic timeframe, more effort needs to be invested into this area to deliver results.



nquiringminds

ai • security • iot

Gamma House, Enterprise Road, Southampton Science Park, Chilworth, Southampton, Hampshire, SO16 7NS, UK
Company No: 7452630, Vat No: 103 0537 70, E: info@nquiringminds.com , P: 02381 159 585, F: 02380 000 021