WHITE PAPER

Taking charge of the IoT's security vulnerabilities

January 2017

www.canonical.com

Contents

Building a secure, reliable platform at the core

The IoT has almost infinite capacity to enrich our lives and add value. However the major security issues that currently loom over the industry are threatening to derail the IoT's hard-earned progress to-date. By listening to, and understanding, end users, Canonical believes it has identified the route to righting past wrongs and putting the IoT back on track.

It's easy to forget that the 'Internet of Things' was only coined as a concept in 1999, but the issue of security has been its achilles heel from the very beginning. Today, Gartner has estimated that there are around 6.4 billion connected things in use[1] but it warns that the costs of securing these 'things' is rising.

IoT as a concept was first named in 1999

As the IoT has continued to develop and grow, so too have the threats involved, and the consequences of poor security. This situation reached a tipping point in late September 2016 when KrebsOnSecurity.com, the site of security researcher Brian Krebs, was hit by the biggest DDoS attack on record. This headline-grabbing attack was instigated by a BotNet of around 145,000 IoT devices (mainly webcams and DVRs) compromised by Mirai malware. Barely a month later, Ars Technica reported[2] on yet another BotNet that had infected almost 3,500 IoT devices in just five days. At around the same time, the Mirai BotNet was used to launch a vast attack on US and European internet infrastructure, bringing down sites including Twitter, Paypal and Spotify. These attacks[3] are only going to get worse with the presence of such vast numbers of easily-compromised devices in the market.

> "What has just happened is not a minor bump in the road, it's an asteroid-size rock blocking the way. Every company involved with the Internet of Things should place mitigating the threat of these IoT botnets at the top of its agenda."
>
> Glynn Moody, Ars Technica[4]

[1] gartner.com/newsroom/id/3165317
[2] arstechnica.com/security/2016/11/new-iot-botnet-that-borrows-from-notorious-mirai-infects-3500-devices/ (Nov 2016)
[3] theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault (Oct 2016)
[4] arstechnica.co.uk/business/2016/10/future-of-the-internet-iptv-ddos-iot-security-issues/ (Oct 2016)

Following the launch of Canonical's secure IoT operating system, Ubuntu Core 16, we set out to examine public attitudes and behaviours towards IoT connected devices. We polled 2,000 consumers to find out:

- Does the public realise that connected devices can be used to attack other devices?
- Are IoT security issues putting people off buying IoT devices?
- Is the public aware of the risks IoT/Smart Devices pose?
- Who do they think should be responsible for securing devices?
- How often do they perform updates themselves?

Our findings highlight a significant disconnect between how we in the industry view things and how users perceive the IoT. They also make it clear that consumers want devices that just work, and don't require substantial interaction to make them secure. This is especially true given that many IoT devices offer no real user-facing interface. IoT security is a concern that consumers simply want 'taken care of' with minimal or no interaction from them.

One in five people claim to be 'more distrustful' of IoT / smart home devices in the wake of recent IoT security issues and have been put off buying them.

So how do we address this fact? Ultimately the IoT industry needs to step up and take on responsibility for keeping devices up to date. It needs to be realistic about consumer behaviours and how little action they are likely to take to mitigate security problems. And most importantly of all, it needs to do this quickly, because unless this issue of security is addressed convincingly, it could represent a genuine threat to the entire future of the IoT.

We believe that with Ubuntu Core we are already addressing many of these issues. But what do developers need to do now?

Through this whitepaper we will cover three key interconnected topics that will ultimately help the industry with a blueprint to move forward:

1. The main IoT security vulnerabilities and why they exist
3. Current approaches to IoT security and why they aren't working
2. Ubuntu Core's blueprint for better IoT security

IoT security issues and why they exist

In the post-match analysis of the attacks on his site, and on others, Brian Krebs himself identified several core issues with IoT devices. He suggests it's due to these fundamental IoT security vulnerabilities that so many devices are open to the exploits that led to the DDoS attack on his site:

- Hard-coded passwords – Devices shipping with no password or a standard 'admin' password that can be easily discovered and exploited.
- Fundamentally weak security at both the software and hardware levels – Beyond the password many products are simply not designed with security best-practice in mind. To secure a design, configuration bit streams should be encrypted and protected. At a hardware level, devices should also be fitted with tamper protection, zeroization, and secure key storage to reduce the chances of an attack. Unfortunately while there are IoT security principals in place to recommend such considerations, they are not actively enforced.
- Lack of software updates – When a security exploit is discovered, updates are not always rolled out in a timely fashion. Sometimes they are not rolled out at all.
- The size of the opportunity – With billions of vulnerable IoT devices having entered the market in the past couple of years, IoT devices represent an attack vector that offers ease and scale arguably unmatched by any other DDoS method. As the IoT becomes increasingly integrated into business and society we can expect attacks to become more organised and increasingly orchestrated for profit.

> "HP estimated in 2014 that 70 percent of most commonly use IoT devices were vulnerable to attacks, while International Data Corporation says that by 2017, 90% of organisations will have a breach related to IoT."
>
> Sekhar Sarukkai via esecurityplanet[5]

SO WHY DO THESE IOT SECURITY VULNERABILITIES EXIST?

There are a wide range of reasons and none of them stand in isolation. The industry must address all of these issues convincingly in order to restore confidence in the IoT amongst businesses and consumers, and minimise the chance of future security problems.

[5] esecurityplanet.com/network-security/ransomware-and-the-internet-of-things-a-growing-threat.html (May 2016)

Some of the more prominent root causes of IoT security vulnerabilities include:

SHORT PRODUCT LIFESPANS

There's a gold rush occurring in many areas of the IoT. It's not hard to see why: With huge device numbers predicted the opportunities are enormous. The production of (often simple, low cost) devices can present companies with an encouragingly low barrier to entry into the IoT market.

But every gold rush has its losers. When thousands of companies rush into a space in which many of the risks and business models are not yet proven it's only to be expected that you'll see a reasonable number of company failures.

> "Over two-thirds of the Internet of Things projects will fail"
>
> Sushil Pramanick, IBM[6]

Although few official figures or estimates exist, a huge number of IoT companies (perhaps the majority) barely make it through a single 9-18 month product lifecycle before failing. Even more fail after they have launched products to market, ending the possibility of any future security updates and, calamitously, leaving vulnerable devices in the field. Acquisition and subsequent deprioritisation of IoT products can have the same effect; leaving IoT devices unsupported and ripe for hijacking.

Much of the time, the problem is also closely related to the product lifespan. Short product runs and low profit margins simply leave many companies feeling little incentive to provide costly long-term support as there is no additional profit to be made.

POOR DESIGN

Even where companies last the distance, issuing regular security updates, or ensuring security best practice in the design of core software and passwording, may be uneconomical, or otherwise not regarded as a priority. This is particularly true where driving down device cost is the absolute priority, or where devices are produced by transient brands.

At other times the decision not to design with the appropriate level of security in mind is taken consciously. For example, many companies want their devices to be easy to use, and regard anything other than default passwording as 'too fiddly' for most consumers.

[6] ibmbigdatahub.com/blog/why-over-two-thirds-internet-things-projects-will-fail (Jan 2016)

TAKING OWNERSHIP

It's not always clear who (at what production stage) should actually be responsible for ensuring the security of IoT devices. Disconnects between different companies involved in the production process mean that, in many cases, security is treated by too many parties as a 'someone else's problem'.

This is not helped by the fact that security during the development and maintenance cycles is almost always seen as a cost center, with different departments hoping to pass the buck further down the line rather than being the ones to absorb the additional costs.

The result of this mentality is potential security holes being left open at all stages of the design process, with physical vulnerabilities being built into hardware, undocumented backdoors being incorporated within the operating system, and a lack of updates opening further vulnerabilities at the application level. Even minor considerations such as how a user conducts a factory reset can impact the security of an IoT device. As such, all stages of the design process should incorporate some consideration for the end security of a device.

While manufacturers and sellers of IoT devices may be happy to pass off responsibility for securing devices, the public is under no illusion as to who to blame: 57% see ensuring a device's security credentials as a clear responsibility of those who provide or manufacture the device.

LACK OF REGULATION

Although wider regulation is all-but inevitable right now there's not much concrete legal obligation for companies to design devices for security (beyond fear of any anticipated brand damage or lawsuits that might result).

In regulatory terms recent events have made IoT security issues more front-of-mind. There have been calls in both the US[7] and Europe[8] for tighter regulation. Both the FCC and FTC have been called[9] on to address IoT security (though at the ISP rather than the device-level), and the Department for Homeland Security has recently been motivated to issue[10] a set of broad guidelines for securing the Internet of Things.

Overall, regulation needs to be applied across-the-board and quickly. Vendors also need to be well-prepared from the beginning of their design cycles to accommodate basic security considerations, or else face potential financial penalties at a later date.

> "IoT makers who have gotten a free pass on security for years are about to discover that building virtually no security into their products is going to have consequences. It's a fair bet that the European Commission's promised IoT regulations will cost a handful of IoT hardware vendors plenty."
>
> Brian Krebs, KrebsOnSecurity[11]

[7] computerworld.com/article/3141803/security/us-lawmakers-balk-at-call-for-iot-security-regulations.html (Nov 2016)

[8] http://techweekeurope.co.uk/security/european-commission-push-iot-security-regulations-198826 (Oct 2016) and silicon.co.uk/security/european-commission-push-iot-security-regulations-198826 (Oct 2016)

[9] rt.com/usa/369430-internet-things-fcc-cybersecurity/ (Dec 2016)

[10] dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (Nov 2016)

[11] krebsonsecurity.com/2016/10/europe-to-push-new-security-rules-amid-iot-mess/comment-page-1/ (Oct 2016)

A lack of standardisation in how security updates are delivered and implemented

Users often lack the will or wherewithal to update devices themselves, and in any case many IoT devices lack a UI that would allow them to do so. Security updates therefore must be automatic, and require a mechanism for reliable delivery. It is clear the industry cannot rely on the public to update their devices.

However, even where over-the-air security updates are generated in a reliable and timely manner, there is generally no guarantee that they will reach the device or be installed correctly. Nest for example has had a few well documented failed updates that effectively broke their devices leaving their consumers out in the cold. Ultimately devices need to be safeguarded against faulty updates with a centralised, standardised transactional update and rollback mechanism.

The proliferation of 'one-off' and device-specific IoT platforms

For years one of the favoured approaches to creating IoT devices has been to develop a custom-built OS – usually based on some variety of Linux, and often with a degree of 'lock-in'. This trend is nothing short of a disaster waiting to happen. The more OS variants there are in the market, (whether based on open source or proprietary technology), the more potential methods for exploitation, and the harder these exploitation methods will be to track and address. Also, having billions of devices running on different OSs will make it incredibly difficult for the industry to establish any centralised regulation of code or updates. While there are benefits to maintaining biodiversity within the IoT ecosystem, collaboration is required to ensure that standards are met and maintained and that devices are kept up-to-date and secure. A single open source code base, both in terms of the OS and the apps that run on it, would render it quicker and simpler for companies or the open source community to patch devices when required.

Ubuntu's research asked respondents how often they had consciously updated the firmware on their connected devices (including IoT, smart home and connected devices such as routers but excluding computers and phones):

- Only 31% of consumers that own connected devices perform updates as soon as they become available.
- A further 40% of consumers have never consciously performed updates on their devices.
- Nearly one in ten (8%) didn't even know what firmware was

THE FIX

With so many vulnerabilities and so many companies betting their future on the IoT you'd expect there to be many existing solutions and approaches that are already successfully tackling them. You'd be wrong. Let's look in more detail at why current approaches aren't working, if these were possible. This is exactly the situation that has emerged in the world big software.

Current approaches to securing the IoT: and why they aren't working

While it's true there are a number of approaches to addressing IoT security, most of them, to-date, have either been flawed, or simply don't go far enough to address the issues at hand...

THE EC 'STICKERS' INITIATIVE

In October 2016 the European Commission announced[12] plans to develop a new labelling system to help identify potential security flaws built into IoT devices; the idea being that an IoT device would literally be 'labelled' with its potential vulnerabilities.

While the intentions behind this initiative are positive, at a practical level it simply doesn't work. Few IoT developers are aware of the vulnerabilities within their devices before they launch, with most security holes emerging over time. As a result, any information printed on physical labels will rapidly fall out of date.

At the same time, the use of such stickers could be seen as sending a negative message to the IoT community, telling them that it's ok for suppliers to sell devices with security issues, as long as the person purchasing the device knows that they are taking a risk.

Unfortunately the risks involved in buying an insecure IoT device extend far beyond the buyer's own network. When a device can contribute towards the takedown of a multinational corporation the choice to knowingly buy a vulnerable device suddenly seems wildly irresponsible.

Ultimately what the industry needs isn't stickers, but a better method of securing IoT devices in the first place.

IOT SECURITY BODIES AND FOUNDATIONS

Several independent organisations and initiatives such as the IoT Security Foundation[13] have sprung up around the world, attempting to establish 'IoT security best practice'. While this is a step in the right direction, membership of such organisations is voluntary. This will do little to address improper security provision amongst commoditised IoT device manufacturers, where poor security often emerges as a symptom of a 'drive to the bottom' on price.

[12] theregister.co.uk/2016/10/10/eu_commission_preps_iot_security_privacy_rules/
[13] iotsecurityfoundation.org/

BETTER EDUCATION

Providing consumers with better education regarding IoT security principles would appear to be a sensible way to address security concerns. But the fact is most consumers just aren't that motivated to secure their devices.

Consumer education will take a while to penetrate but several governments around the world have already launched costly campaigns (such as the UK's £4m 'Cyber Aware' campaign) to encourage consumers to be more cyber-aware in their use of connected devices. Despite this, Canonical's consumer research found that nearly half (48%) were unaware that connected devices in their home could be used to conduct a cyber attack and 37% believe they are not "sufficiently aware" of the risks that connected devices pose.

Education is also a somewhat reactive solution to security issues, and it won't do much to address the introduction of fundamental vulnerabilities at the device and network level. And this is the key point: As long as consumers continue to be sold vulnerable devices, those devices will pose a risk to the systems of others.

The industry doesn't need a 'sticking plaster' approach to dealing with security: Instead it needs a way to eliminate any potential vulnerabilities from devices before they can cause issues.

ENCRYPTION AND DATA AUTHENTICATION

The need for encryption and data authentication is, thankfully, relatively well-rooted in most IoT device designers' minds. Protocols such as SSL should be used wherever data is transported online, and appropriate wireless encryption should also be in place. However, the use of such basic measures is by no means universal, and is often overlooked or poorly implemented due to cost constraints in the design process.

Again, the issue is the lack of any obligation for companies to put encryption in place. In any case, even where it is properly implemented, encryption alone is far from a flawless method of securing devices or ensuring data privacy, and may be rendered moot if a Bad Actor gains physical access to a device or network.

The case for standardisation and cross government/industry collaboration seems clear, especially in addressing more challenging and fundamental security concerns. For example, in a price-sensitive market, manufacturers will be incentivised to keep the overall Bill of Materials (BOM) of their devices as low as possible. They will do this by integrating lower-grade components that may be insufficient to handle future security upgrades. Until companies are required to futureproof their devices, IoT hardware restrictions are likely to continue to be an issue.

48% of consumers are unaware that connected devices in their home could be used to conduct a cyber attack.

37% believe they are not "sufficiently aware" of the risks that connected devices pose.

‘PLUG AND PLAY’ HOME FIREWALLING

Several companies have taken steps to creating simple ‘plug and play’ methods of securing the boundaries of home IoT networks. Generally-speaking however, firewalls and antivirus approaches have not had a good reputation as threat-mitigators. Additionally, as with much of IoT security there is no obligation to put such measures in place. It is also hard to imagine litigation being levelled at every home or organisation with an insecure network. And how can the industry ensure that networks are safeguarded in a standardised, reliable manner?

While there is merit in all of the above approaches, it’s clear that, overall, current methods are failing to adequately safeguard the IoT against the kind of massive exploits the industry has seen in recent months.

What’s needed is a fundamental rethink; an approach that deals with the problem right at the Core.

The Ubuntu Core blueprint for better IoT security

By closely analysing the IoT's security vulnerabilities and the failings of existing approaches Ubuntu believes it has the formula to address IoT security issues for good, with its nine point blueprint for better IoT security:

1. THE INDUSTRY HAS TO START WITH THE OS

Without a doubt the most critical point at which the industry must address IoT security is that of the end-device itself, specifically the most fundamental element of those devices, its OS.

In an ideal world all IoT devices would have multiple levels of protection. Networks would monitor traffic, secure gateways would route and remove hostile traffic, and every device would sit behind a properly-configured firewall. But we don't live in an ideal world.

In reality the IoT cannot rely on such measures being consistently applied. In the case of consumer IoT technology in particular, it is unrealistic to expect users to reliably keep the boundaries of their networks secure. And even if every consumer had the skills of an IT professional, 'security by architectural design' would still be a flawed approach due to the necessary complexity of its implementation.

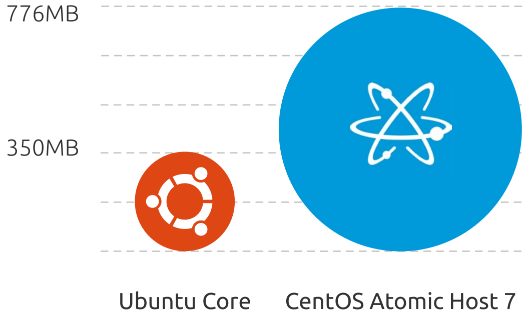
The first assumption that should be made when securing the IoT is that devices will be deployed in an insecure environment, because in most cases they almost certainly will. Therefore IoT devices, and the IoT OS they employ, must be acknowledged as the most critical point at which security should be considered.

2. ANY IOT OS NEEDS TO BE DESIGNED FROM THE GROUND UP FOR SECURITY

Security is the IoT's biggest challenge: An OS designed for the IoT should not shy away from this simple fact. When security is treated as an afterthought, as is the case with so many OSs, patching vulnerabilities becomes a never-ending battle; no sooner is one addressed, than another appears. Traditional approaches to OS design simply present too many opportunities for incursion. First and foremost, what is required is a radical rethink of OS architecture that regards security as the Alpha and Omega.

3. THE OS SHOULD BE KEPT SIMPLE WHILE MAINTAINING APPROPRIATE FUNCTIONALITY

Any IoT OS needs to be streamlined. IoT devices often have little budget in terms of CPU cycles, memory, and storage. And Ubuntu Core is extremely streamlined.



OS image size

But lowering size and increasing simplicity is about much more than getting an OS to fit/run on a device; it's also a philosophy that helps to make an OS more secure. The less complexity, the fewer points of vulnerability.

This principle can be seen in Ubuntu Core's architecture, which is composed of a minimum of three compressed files called snaps:

- One contains the Kernel and other device drivers, the kernel snap
- One contains the OS itself , the OS snap
- One contains the manufacturer configuration and device enablement data, the gadget snap

In addition additional applications can be installed on the device, each packaged as a snap.

4. THE OS SHOULD FEATURE A CENTRALISED UPDATE MECHANISM

Canonical believes strongly that the ability to update software reliably and automatically must be the beating heart of any secure IoT OS. This is particularly true when many IoT devices will be connected and then forgotten about, or will become physically hard to access, with no UI through which to update them.

With Ubuntu Core, whenever a device checks for updates, the Ubuntu Store or a device manufacturer's branded Store can be configured to act as the primary gatekeeper. If an application ('Snap') update is made available by its creator it can only be installed if it is approved by Canonical or the device manufacturer. In ensuring the timely delivery of authenticated updates, and by providing a mechanism that helps to shield users from the negative consequences of poor applications or vendor failure, Canonical mitigates some of the biggest security issues faced by the IoT.

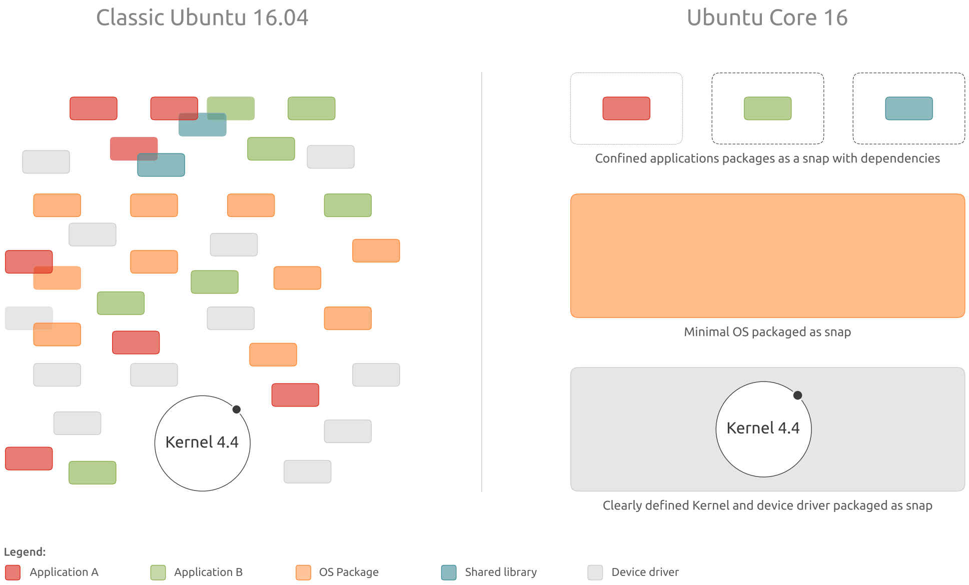
In ensuring the timely delivery of authenticated updates, and by providing a mechanism that helps to shield users from the negative consequences of vendor failure, Canonical mitigates some of the biggest security issues faced by the IoT.

5. THE OS SHOULD FEATURE AUTOMATIC, INBUILT ROLLBACK OF UPDATES

Should an update fail, devices running Ubuntu Core will automatically roll back to the last known working configuration, thus maximising the chances that devices remain not only secure, but also functional.

6. FILES SHOULD BE READ ONLY BY DEFAULT AND REQUIRE UNIVERSAL DIGITAL AUTHENTICATION TO BE REPLACED

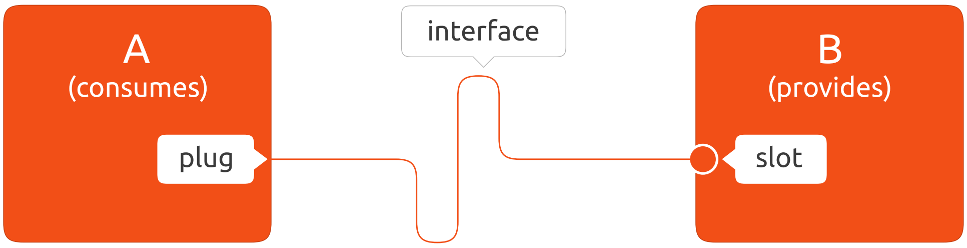
Snaps on the Ubuntu Core file system offer additional security because they are read-only and digitally signed. This allows a far greater opportunity to examine the integrity of each snap before installation and guarantee this integrity over time. The result is a system that can be secured from startup to shutdown.


Classic Ubuntu 16.04
Ubuntu Core 16
Kernel 4.4
Confined applications packages as a snap with dependencies
Minimal OS packaged as snap
Kernel 4.4
Clearly defined Kernel and device driver packaged as snap
Legend:
Application A
Application B
OS Package
Shared library
Device driver

Classic Ubuntu 16.04 compared to Ubunut Core 16

7. APPLICATIONS SHOULD BE SELF-CONTAINED AND SANDBOXED

By default, all snaps are segregated in their own restrictive sandboxes, minimising the damage that can be done by malevolent or malfunctioning applications. By default it is thus impossible for a snap to access another snap's data. Snaps can still share data and functionalities with other snaps from the same vendor, and with a very limited number of additional core system elements. However, in order for two snaps to talk to each other, they generally have to establish a specially-defined interface.



Snaps interface

8. THE OS SHOULD FEATURE FAMILIAR ARCHITECTURES AND KNOWN CODING METHODS

Although not essential, development within a known framework and ecosystem is of clear benefit to the security of an IoT OS. There are additional benefits to working according to known techniques, (any such OS will get off the ground quicker, and likely be more portable). Most importantly however, if it leverages the talents of large, pre-existing coding community, security issues will likely be addressed more quickly.

9. SECURITY SHOULD NOT RESTRICT THE OPEN AND INNOVATIVE NATURE OF THE IOT

Perhaps most importantly, security measures should not involve a 'walled garden' approach. Canonical believes that remaining Open Source is key to fostering the spirit of innovation at the heart of the IoT. Thus, while closed-source Snaps are available, anyone can choose to develop their own Snaps and upload them to GitHub. Users can even examine the code behind Ubuntu Core itself.

Ubuntu Core represents a chance to combine the best of both worlds – the centralised control and close oversight of proprietary systems, and the Open Source philosophy of Ubuntu – in order to provide a fully-secured IoT OS suitable to a wide range of applications.

So what have we learned?

The IoT is too valuable to let security vulnerabilities derail its progress.

As this paper has shown, too many of the solutions proposed for IoT security today involve either mitigating security issues after-the-fact, or living in a world where IoT security problems are the accepted norm. This does not need to be the case.

Our survey has listened to the views of users and highlighted just how few consumers are security savvy and are keeping their connected devices up-to-date. In order for the IoT to truly succeed, there needs to be a better system in which devices are automatically kept up-to-date without placing the full burden of security at the consumer's doors.

The IoT industry needs to step up and take charge, but manufacturers and software developers can't be expected to permanently update and manage devices that they may have sold 10 years previously.

What is needed is a standardised infrastructure for the IoT, allowing vital security updates to be managed, rolled out – and if needed – rolled back, at the OS level. Executed effectively, this will have the biggest and most immediate effect on overall IoT security.

This is the challenge that Canonical is addressing with Ubuntu Core – a centralised operating system, which can take the burden of IoT security away from manufacturers, designers and, most importantly, the end user. Already in use in a vast number of connected devices, including digital signs, robots, and the majority of self-driving cars, Ubuntu Core presents a solution tailor-made for the security needs of today's IoT.

How do I find out more?

For further information about Ubuntu Core, please visit **ubuntu.com/core**

Canonical Limited, Registered in England and Wales, Company number 110334C Registered Office:
12 - 14 Finch Road, Douglas, Isle of Man, IM99 1TT VAT Registration: GB 003 2322 47