Inside job

Security and privacy threats for smart-home IoT devices

UNSW
THE UNIVERSITY OF NEW SOUTH WALES
SYDNEY • AUSTRALIA

accan

Inside job

Security and privacy threats for smart-home IoT devices

Professor Vijay Sivaraman, Dr Hassan Habibi Gharakheili, Professor Clinton Fernandes

May 2017

UNSW
THE UNIVERSITY OF NEW SOUTH WALES
SYDNEY • AUSTRALIA

accan

Inside job: Security and privacy threats for smart-home IoT devices

Authored by **Professor Vijay Sivaraman, Dr Hassan Habibi Gharakheili and Professor Clinton Fernandes**

Edited by **Narelle Clark and Tanya Karliychuk**

Published in **2017**

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

University of New South Wales, Faculty of Engineering
Website: www.engineering.unsw.edu.au
Email: eet@unsw.edu.au
Telephone: 02 9385 4000

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: 02 9288 4000
If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: www.relayservice.gov.au

ISBN: 978-1-921974-10-6
Cover: Design by Richard Van Der Male with image from Shutterstock

This work can be cited as: Sivaraman, V., Habibi Gharakheili, H. & Fernandes, C. 2017, *Inside job: Security and privacy threats for smart-home IoT devices*, Australian Communications Consumer Action Network, Sydney.

Table of Contents

Figures and Tables

Acknowledgements

We would like to acknowledge the students of our research group Arunan Sivanathan, Franco Loi, Minzhao Lyu and Daniel Sherratt for the lab setup and experiments. We also thank Peter Gearin who helped us with the report writing.

Key Findings

We live in an increasingly connected world

The internet gives us the opportunity to enjoy incredible experiences, be entertained and informed, and keep in contact with others across the street or the globe. Wherever we are, and whatever our stage in life, internet-capable devices offer us the promise of unparalleled freedom and flexibility. These devices are also becoming more important for our sense of personal safety and security.

We rely on connected devices

Recent advances in technology have led to the development of devices at work or home that connect to the internet. These “Internet of Things” (or IoT) devices include televisions, webcams, smoke alarms, fitness trackers, climate-control systems – even “smart” light bulbs. They save us money and time. They help us stay fit, healthy and safe. They allow us to communicate effectively with friends and family, or be entertained. The number of IoT devices we use is growing rapidly – there will be billions of internet-connected products by 2020.

With benefits come risks

Current consumer-focused IoT devices, however, are susceptible to attack by those wishing to do us harm. Many internet-connected devices have poor in-built security measures that make them vulnerable, and these flaws have the potential to reveal private data and information that may hurt or alarm us.

All smart-homes are potentially under threat

A typical smart-home with many IoT devices is under significant risk of cyber-attack. This vulnerability compromises data and threatens our personal safety.

The problem is widespread

We tested 20 IoT devices and found that five do not send data in encrypted form, making it easy for intruders to snoop on user information. Four of the devices allowed attackers to manipulate them so they could run fake commands, and two of the webcams tested had weak passwords, making them easy to hack. More than half the devices tested could be rendered dysfunctional after being bombarded with a high volume of attack traffic. Most of the devices tested could be manipulated in some way to participate in attacks on other devices.

Measures must be taken to resolve this issue quickly

Several options need to be considered to manage the potential risk from poor IoT security, ranging from education to legislation. It’s important that consumer groups, manufacturers, regulators and insurers of IoT devices come together to develop appropriate strategies to tackle the problem.

Introduction

What is the Internet of Things?

The Internet of Things (IoT) refers to the technology that allows everyday consumer products to be connected to the internet. Australia's largest telecommunications business, Telstra, says that it's been estimated that the average Australian household in 2017 has 13 internet connected devices and that by 2021 a typical home will have over 30. It's predicted that the collective value of the Smart Home market in Australia will be greater than $1bn annually by 2021[1].

As well as computers, smartphones and tablets, a modern household is likely to have numerous internet-connected devices. Here are some examples:

Entertainment systems:

- Smart TVs
- Games consoles
- On-demand devices, such as Apple TV

Security and safety systems:

- Video cameras
- Motion sensors
- Smoke alarms

Convenience and energy-saving systems:

- Climate-control air conditioning
- Smart light bulbs
- Smart power switches

Healthcare monitoring systems:

- Weighing scales
- Fitness trackers

The IoT revolution

Everyday devices that connect to the internet have already changed the way we live. Here are just some of the ways IoT has revolutionised the Western world, with the promise of much more to come.

- Those who spend much of their time at home – the elderly or those living with disability – can stay in touch with loved ones and receive immediate medical treatment through real-time health-management systems.

[1] John Chambers, Executive Director of Product Innovation, in presentation at UNSW workshop, 20 April 2017

- Householders and businesspeople can have their properties monitored 24 hours a day and be alerted by technology if anything happens that is out of the ordinary.
- Families can use clever devices to save on energy costs and weekly shopping bills.

As technology companies continue to develop IoT technology – as devices become smaller, lighter and more in tune with market demands, and as internet services become faster, cheaper and offer better coverage – more of us will take advantage of these digital solutions to solve our problems.

Project aims

Our objective was to evaluate the extent to which IoT devices might cause harm to consumers through any inherent security and safety vulnerabilities. The specific aims were to:

- Evaluate the privacy and security capabilities of current popular IoT devices.
- Develop representations of "typical" households using IoT devices, and illustrate what threats may emerge for each if IoT security and privacy are compromised.
- Document findings on security concerns in a way that is easy to understand.
- Propose potential approaches to help consumers, policy makers, insurance companies and manufacturers mitigate the identified risks.

Connected risks

It is easy to understand why we're attracted to devices that connect seamlessly with the internet. What is less well known are the security and privacy risks these in-demand consumer products might pose for users.

Many IoT devices are equipped with cameras, microphones and motion and biomedical sensors, and they collect information for a specific purpose. Some of this information is likely to be highly personal and offer significant clues to a user's habits and lifestyle choices.

This would be fine if we knew our data was always safe, but experience tells us that this is often not the case. We have learnt the lesson – through examples in Australia and around the world – that no one is safe from those who wish to do us harm or cause us a degree of disruption. We simply don't know how easy it is for personal information to fall into the wrong hands.

Users face two immediate potential concerns when they connect their household devices with the internet:

- Are the device providers (or their agents) able to collect confidential information without my knowledge?
- Can hackers, eavesdroppers or troublemakers use my personal data to determine where I am or what I might be doing, and how can they use this information?

Either situation may compromise our personal privacy and security. But what would be much more troubling for users is if intruders could effectively control their IoT devices – especially lights, speakers, switches or locks – putting themselves or their families in harm's way. And what would happen if these criminals used household IoT devices to set off even bigger software-led meltdowns?

Despite the IoT industry being relatively young, we have heard many examples of even basic security and privacy measures failing to protect customers of these devices. Some are listed in the later section, *Potential IoT threats*.

Every month, another flood of IoT devices appear on the consumer market – many produced by non-telecommunications companies that have limited experience of cyber-attacks. This gives hackers and chancers more opportunities to exploit or attack vulnerable homes and businesses using internet-connected products.

How IoT users are vulnerable

Criminals, or even enthusiastic troublemakers, can attack IoT devices from anywhere. They don't need to be within Wi-Fi range of their victims. They don't even need to use particularly expensive or sophisticated hardware or software. The tools required for attacks are often freely available.

Here are three common ways that hackers can infiltrate internet-connected devices in the home:

- A hacker equipped with a simple laptop and downloadable software sitting outside a home can gain access to a local Wi-Fi network and manipulate all of the devices connected to it.
- Organised groups can plant malware into IoT devices, or send infected files to users, allowing them to manipulate products any time they choose.
- Hackers based anywhere in the world can launch Dedicated Denial of Service (DDoS) attacks. This is where they can shut down an IoT device, which typically has limited computation ability, by sending it a flood of requests. The device is so busy dealing with the bogus traffic that it can't respond to any legitimate requests.

All of these tactics make devices, and the networks that connect them, susceptible to manipulation and eavesdropping. A few of the devices, for instance, use encrypted language that makes it difficult for non-users to gain access to their data. But others rely on simple text patterns (unencrypted, or *plaintext*), which presents an almost open invitation for savvy hackers to create havoc.

Potential IoT threats

Security and privacy threats for IoT device users come in a variety of forms. These threats can be represented in four ways:

- **Confidentiality:** if a device is unable to keep collected data private within wireless range
- **Integrity:** if a device allows attackers to modify or forge data
- **Access control:** if a device allows attackers to take control
- **Reflection capacity:** if a device allows attackers to amplify and reflect attacks on other internet-connected services

Each of these four threats are outlined in the following boxes.

Confidentiality

Data sent by an IoT device might by "overheard" by an eavesdropper, who can then obtain the data and use it dishonestly. This is why product confidentiality is so important. It's vital that only a receiver and transmitter understand any IoT messages that are sent – not anyone else listening in. This is important for anyone using devices such as health-monitoring units, because they retain highly sensitive and personal information. Even light bulbs that send their "current status" provide an attacker with clues as to whether someone is home, compromising personal security.

When trouble strikes

Industry

Investigators found handheld scanners that monitor inventory at shipping and logistics firms worldwide can be used to compromise company security[2]. Attacks would begin at the company providing hardware and software for the scanners; criminals would install malware on the Windows XP operating systems embedded in the devices. The threat would also be distributed via the company's support website. The scanners would transmit collected data (origin, destination, value and contents of packages) via a customer's wireless network. Once a customer started using the scanner, the malware would send the information to a criminal server.

Barbie

The Hello Barbie was sold as the world's first "interactive doll", capable of listening to a child and responding via voice, in a similar way to Apple's Siri. It connects to the internet via Wi-Fi and has a microphone to record voice. It sends that information to internet-based servers for processing before responding with natural language responses. In November 2015, a security researcher discovered that hackers could steal personal information as well as turn the doll's microphone into a surveillance device. The doll only listens in on a conversation when a button is pressed and the recorded audio is encrypted before being sent over the internet. Once a hacker has control of the doll, however, its privacy features could be overridden. The information stored by the doll could allow hackers to take over a home Wi-Fi network and gain access to other internet-connected devices, steal personal information and cause other problems for the owners, potentially without their knowledge. This vulnerability has since been corrected and the button must be pressed to engage the microphone in later models.

[2] TRAPX Security, "TRAPX discovers 'Zombie Zero' advanced persistent malware", https://trapx.com/trapx-discovers-zombie-zero-advanced-persistent-malware/, July 2014

Integrity

Attackers can compromise the integrity of a device in a number of ways. They might inject fake data into a device or send it fake messages that allow them to gain control. Integrity is about ensuring that any messages received by a device are not modified, deleted or replayed without detection, and that the system performs its intended function without being manipulated. This is important for IoT devices, which should only communicate with the user's server and its associated application. It's also why a strong authentication regime is important.

When trouble strikes

Worms

Researchers uncovered a flaw in the ZigBee wireless technology, which is often included in smart-home devices such as lights, switches, locks and thermostats[3]. They describe a new type of threat in which adjacent IoT devices can infect each other with a worm that spreads quickly over large areas, similar to a nuclear chain reaction. In particular, they verified such an infection that used the popular Phillips Hue smart lamps as a platform. The worm spreads by jumping directly from one lamp to its neighbours, using only built-in ZigBee wireless connectivity and physical proximity. The researchers were able to spread an infection in a network inside a building from a car that was driving past 70 metres away. The attack could be started by plugging in a single infected bulb anywhere in the city. It could then catastrophically spread everywhere within minutes, enabling the attacker to turn all of the city lights on or off, render them useless or exploit them in a massive DDoS attack.

Smart meters

Major security weaknesses in smart meters have been shown to allow attackers to order a power blackout or commit power-usage fraud[4]. Fraudulent customers can program smart meters to allow them to use as much power as they want or "spoof" their neighbour's smart meter identifier code, making it appear that the neighbour is using their electricity.

Heating and garage doors

It's nice to warm up your house on the way home from work. That's why "smart-home connectors" are attractive – they allow customers to adjust their home heating on the thermostat via an app. But hackers detected security flaws in one connected home hub that allowed them to pump up the heat remotely, or worse still, turn it off and allow the pipes to burst. Another example of integrity violation is the HackRF device, created by security researchers to read and reproduce radio-wave signals. Being able to record and replay the signal from a garage door opener may be enough to open the door, even when someone isn't home.

[3] E. Ronen, C. O'Flynn, A. Shamir and A. Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction", Cryptology ePrint Archive, Report 2016/1047, 2016

[4] BBC News, "Smart meters can be hacked to cut power bills", http://www.bbc.com/news/technology-29643276, Oct 2014

Access control

Applying control over who or what can access a system is authorisation. There is evidence that cyber criminals have turned to IoT devices as easy launching pads for large-scale attacks because, with poor access controls, it is easy for hackers to take control. Distributed denial-of-service (DDoS) attacks are where attackers bombard a system with unwanted requests from many different sources and effectively shut the system down. This is a potentially massive problem for IoT users where access controls are often lightweight.

When trouble strikes

Printers

A hacker known as Stackoverflowin, demonstrated how easy it is to gain access to internet-connected printers operating without a firewall[5]. Using a self-made automated script, the hacker scanned for and identified devices with the Internet Printing Protocol (IPP), Line Printer Daemon (LPD) and port 9100 open, and sent rogue print jobs to more than 160,000 targeted devices. Canon, Brother, Epson, HP, Samsung and Konica Minolta models were among those affected. Printed messages warned users their device was "pwned" and was "part of a flaming botnet".

Baby monitors

A Texas family was shocked when someone outside their house started yelling at their two-year-old through a hacked baby monitor. Researchers have found that baby monitors with webcams have a range of vulnerabilities, from weak internal security protocols to easily obtained default passwords.

Cameras

Many internet cameras have default logins and don't prompt users to change them, making the devices an easy target. Hackers can locate routers and other connected devices using IoT search engine Shodan[6]. Bad actors can use the information obtained on Shodan to infiltrate routers with default usernames and passwords. Flaws in smart TVs were discovered that would enable hackers to remotely turn on built-in cameras. While owners were watching TV, a hacker anywhere in the world might have been watching them.

Easy passwords

Default passwords for popular "smart" electric meters brands can be found online, making them easy bait for hackers. And since an electricity company typically installs the device, few homeowners change them. Electricity meters can reveal a significant amount about the habits and whereabouts of residents.

Hacking cars

Hackers were also able to take control of two vehicles, manipulating their steering and brakes. They "hard-wired" a Toyota Prius and Ford Escape to make the steering wheel move sharply at high speeds and disabled the brakes while parking.

[5] Techradar, "Thousands of printers hacked across the globe after critical flaw exposed", http://www.techradar.com/news/thousands-of-printers-hacked-across-the-globe-after-critical-flaw-exposed, Feb 2017
[6] Shodan, https://www.shodan.io/

Reflection attacks

An attacker can use IoT devices to launch attacks on other services on the internet. Large-scale attacks have paralysed internet services by hijacking thousands of IoT devices after injecting them with malware. “Reflection” attacks are where attackers send an IoT device a short query message from a fake IP address, to which the device responds with a long response to the victim. Using this method, attackers can inflict enormous damage, even if an IoT device is secured behind a home gateway. What is particularly scary about reflection attacks is that attackers don’t even need to hijack an IoT device – they just need to send it a “spoofed” query message to which it responds.

When trouble strikes

Inside job

In what sounds like the plot from a science-fiction book, an unnamed university was attacked by its own light bulbs, vending machines and lamp posts in January 2017.[7] *More than 5000 connected devices were hacked to slow down the internet service at the university. They made hundreds of Domain Name System (DNS) look-ups every 15 minutes, causing the university's network connectivity to become unbearably slow or even inaccessible. In effect, the devices attacked their own network.*

When the internet breaks

An estimated 100,000 hacked IoT devices almost broke the internet on 21 October, 2016.[8] *Many were infected with a notorious malware called “Mirai botnet”, which took over cameras and DVRs. This generated multiple DDoS attacks against servers owned by Dyn, a company that controls much of the internet’s DNS infrastructure. The servers remained under sustained assault for most of the day, bringing down sites including Twitter, The Guardian, Netflix, Reddit, CNN and many others in Europe and the US.*

[7] Verizon, “Data breach digest IoT calamity: the Panda Monium”, http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf, Jan 2017

[8] KrebsOnSecurity, “Hacked cameras, DVRs powered today’s massive internet outage”, https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/, Oct 2016

Testing

We selected 20 devices based on market availability and popularity, and carried out detailed tests on each (as well as its supplied mobile app and data server).

These tests ranged from the simple (capturing wireless transmissions from the device to evaluate the contents of the communication) to the complex (making the device communicate to a fake server, and overwhelming the device with fake query messages). We automated the process in a laboratory to make it easier to reproduce and compare results.

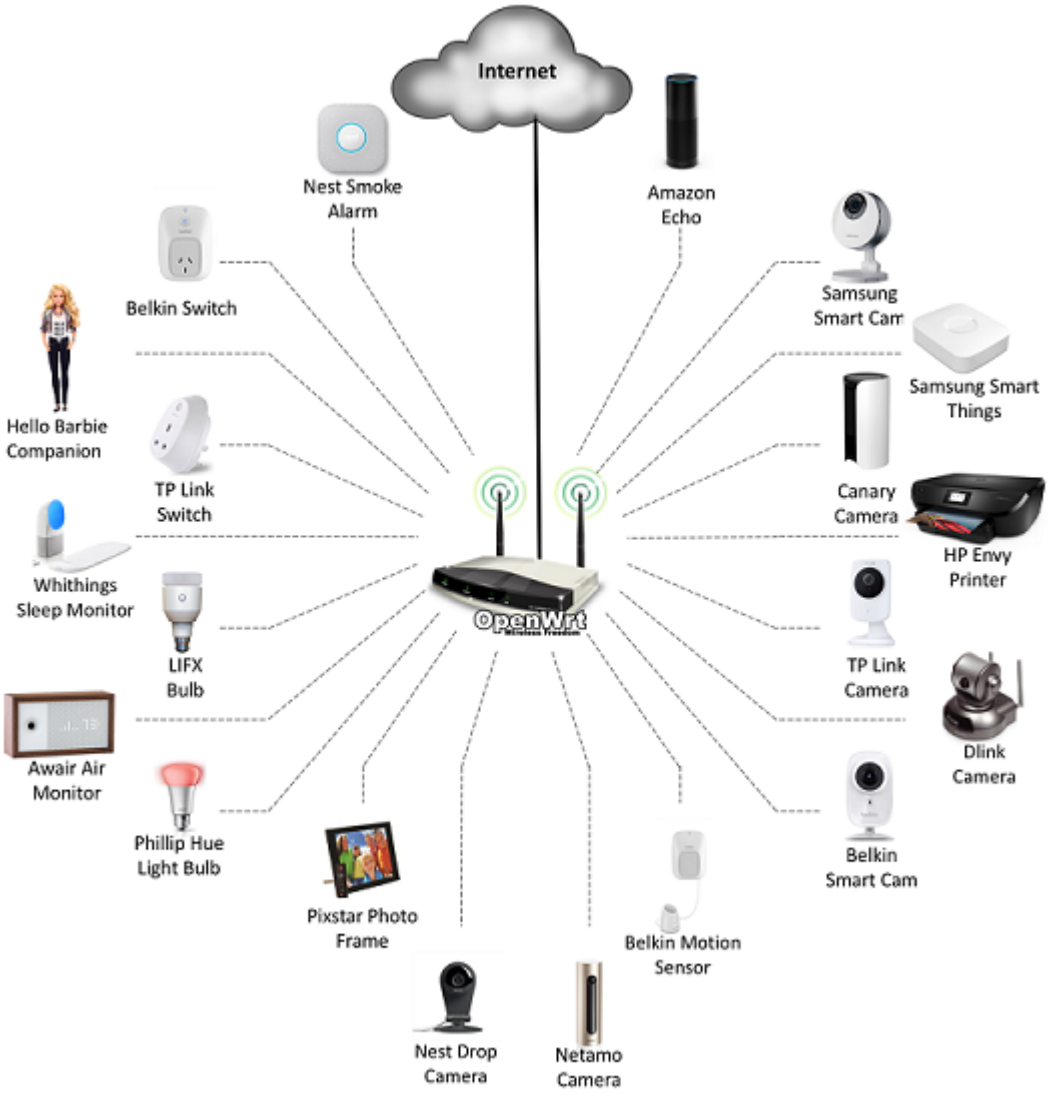

Figure 1: Test lab set up

All of the IoT devices were connected to a home gateway router either through Wi-Fi or via direct connection with an ethernet cable. The applications for the IoT devices were downloaded on to an Android tablet, which was connected to the same router. Checks were performed from a laptop running a digital testing platform called Kali Linux, which was on the same network as the IoT devices.

Using this setup, we ran basic computerised scripts and penetration testing tools to assess the safety and security performance of each IoT device.

The devices tested were:

- Cameras (TP-Link, Belkin, Dlink, Samsung, Canary, Netatmo and Nest Drop)
- Motion sensor (Belkin)
- Smoke alarm (Nest)
- Medical device (Withings sleep monitor, Withings weighing scale)
- Air quality monitor (Awair, Netatmo weather station)
- Light bulbs (Phillips Hue and LIFX)
- Power switches (Belkin and TP-Link)
- Talking doll (Hello Barbie)
- Photo frame (Pixstar)
- Printer (HP Envy)
- Controller (Samsung SmartThings)
- Voice assistant (Amazon Echo)
- Smart TV with Google Chromecast
- Speaker (Triby portable speaker)

Although every device was tested in a laboratory, we were able to accurately determine how each might behave if attacked in real-world conditions. If security or safety deficiencies are detected in a stable lab environment, it is highly likely the same issues will arise in the field… in real homes and businesses.

Results

Our tests were consistent and alarming. Every device we tested showed some form of vulnerability – many allowed potentially serious safety and security breaches. With hundreds of consumer IoT devices emerging over the coming months and years, these tests show that manufacturers must act urgently to combat a range of diverse vulnerabilities.

All of the devices displayed some sort of fallibility in either integrity, access control or reflection capabilities. Many were susceptible to attack in a number of ways. The Phillips Hue light bulb and Belkin switch had notably poor security.

But there was some good news. Devices such as the Amazon Echo, Hello Barbie, Nest Drop Cam and Withings sleep monitor were relatively secure in terms of confidentiality. The Echo, in particular, was a top-rated device in security with encrypted communication channels and almost all of its ports closed to outside attack. The Appendix: How the IoT devices rated lists full tables of results showing how each device performed in each category.

We believe that the surge in demand for IoT products has led many manufacturers to rush to market without ensuring their devices are totally secure. They will need to better understand the ways their products can be compromised, and lawmakers will need to find ways to better protect consumers.

What this means for users

Our results show that all of the IoT devices tested have at least some level of vulnerability to attack. So how would typical users be prone to threats posed by hackers or anyone else wanting to cause them harm?

We created four scenarios in which people are likely to use IoT devices – for reasons of safety, health, energy and entertainment – and consider how vulnerable they might be using products currently available in Australia. While the use cases might be typical, all the characters are completely fictitious.

Case 1: Home security for a single occupier

Figure 2: Case 1 – Home security bundle for a single occupier

The potential victim

Tuan is a mid-career private investigator. Most of her work involves insurance fraud although she is often asked to track cheating spouses. She lives by herself in a regional town in Victoria, regularly drives to Melbourne and flies to Sydney to catch up with clients.

Because she travels quite a bit, and meets a lot of unusual people in her line of work, Tuan is worried about leaving her home unattended. Knowing the benefits of surveillance tools, she believed that installing IoT devices would offer some peace of mind.

The devices

* Belkin motion sensor to detect movements inside her house

* TP-Link indoor and outdoor motion sensor cameras

* Nest smoke alarm to send alerts to her smartphone in case of fire

How security devices are vulnerable to attack

One of Tuan's clients is a woman who recently won custody of her children following a divorce. Tuan was able to prove in court that the woman's husband, Ron, was having an affair. Ron is now looking for revenge. He wants to find some personal details about Tuan and try to intimidate her, or worse.

Once he's sitting in his car close to Tuan's home, Ron deduces her Wi-Fi network password using freely available software. He then quickly walks outside her home and places a cheap battery-powered device beneath her letterbox. This device connects with her home wireless network, capturing all of the information being transmitted by her IoT devices. This information is then sent back to Ron's laptop, which he monitors from his home.

Essentially, Ron's device is performing a "man-in-the-middle" attack on Tuan's motion sensor and camera – both of which send out information that is not encrypted. This makes it quite simple for tech-savvy Ron to see video and read motion-sensor information from Tuan's devices on his laptop at home.

It also means Ron knows when Tuan is away and can choose his moment to strike. Once Tuan's devices have been inactive for a few hours – on a sunny, quiet afternoon when he knows there won't be many kids around – Ron parks his car down the street from Tuan's home.

Certain the home is vacant, Ron uses a denial-of-service attack on Tuan's motion sensor, cameras and smoke alarm by bombarding them with a large number of requests. Unable to cope, these devices simply shut down. This ensures that Tuan will never get the smoke alert from her IoT alarm… even once malicious Ron has set her home ablaze.

Is a home safe and secure with IoT security devices?

No. We feel current customers of IoT home or business security devices are placing themselves at risk.

Despite claims by manufacturers that their IoT devices add an extra layer of home protection, the security frailties built into these products make them particularly vulnerable to software attacks. Unless these issues are addressed, IoT customers are at even greater risk than those who have not invested in these devices.

Case 2: Health monitoring for an elderly couple

Figure 3: Case 2 – Health monitoring bundle for an elderly couple

The potential victims

Joe and Lorna Jones live in inner-city Brisbane. They're independent and in good health for a couple closing in on 90. But their doting son, Geoffrey, who lives with his family on the Gold Coast, wants a way to monitor his parents' welfare that is more thorough than checking in on Skype every couple of days. He has installed a number of IoT devices in their home to allow him to keep a virtual eye on Joe and Lorna's health and wellbeing.

While Joe doesn't mind so much, Lorna finds the constant oversight intrusive on her privacy. She's a bit hard of hearing, wears a pacemaker and has breathing issues, and definitely doesn't care much for the internet.

Joe knows enough about the new-fangled devices to use them in unintended ways (he's worked out that they're a great way to get his son's attention, for example). He has some mobility issues and relies on his medical-alert device when he's away from home. Lorna was playing bowls the last time he had a fall, and it took hours before he could get help.

The devices

* Blipcare blood pressure monitor, which sends readings to the web for Geoffrey to check

* Withings weighing scale

* Withings sleep monitor

* Awair air quality monitor

* Netatmo weather station

How health devices are vulnerable to attack

Lee is part of a Malaysian syndicate that preys on vulnerable people (and devices) across the world. Through connections, he has bought a list of email addresses of people who have recently registered IoT products. One of these belongs to J&L Jones of inner-city Brisbane, Queensland.

From his darkened 15th-floor apartment in Kuala Lumpur, Lee sends an email to all users that contains a link to an app that promises technology customers help with their finances. The app, however, has embedded malware that scouts for IoT devices. Lorna isn't sure what the email is about but thinks it sounds interesting. Without thinking, she manages to download the app. The malware immediately disables the Jones' firewall and enables port forwarding, making them vulnerable to security breaches.

Now Lee is in control. He is able to use Joe and Lorna's IoT products to reflect and amplify attacks on other internet-connected devices. Whenever he likes, Lee can use the open ports on the Jones' Withings sleep monitor, Awair air quality monitor and Netatmo weather station and use them as part of a network of compromised devices to launch massive cyber-attacks.

But Lee isn't finished yet. His malware is able to find any unencrypted messages from the elderly couple's weighing scales and deduce their names, ages, gender, height and weight. From this, he can start hatching a plan for someone else in his criminal syndicate to steal the Jones' identity and take their social security benefits.

Are the devices good for health and safety?

It is important that IoT healthcare devices perform correctly, of course. Any failures can have a major impact on someone's wellbeing. Overall, health monitoring IoT devices don't tend to have many security problems, although they could be used to launch attacks on other networks.

The Awair air quality monitor could stop functioning if it's forced to deal with a large amount of internet traffic. At least it encrypts all data sent to the server.

Case 3: Energy management for a family home

Figure 4: Case 3 - Energy management bundle for a family home

The potential victims

Suresh and Veda Singh live in Sydney's western suburbs. They have three growing kids (Mahendra, Mithali and Latika) and are sick of paying a large electricity bill every quarter. The couple know they have to try to keep their west-facing house cool in summer but also need to educate their kids to remember to turn off lights when they leave a room, but it always feels like they're in a losing battle. The Singhs have decided to take control of their ballooning energy expenses and install some smart devices around the home.

While out food shopping, they also find an interactive doll for little Latika. The cute doll has a microphone that "listens" to Latika and replies in a similar way to Apple's Siri.

The devices

* Mix of LIFX and Phillips Hue light bulbs for remote-control lighting

* TP-Link power switch to control their appliances

* A Hello Barbie talking doll

How energy devices are vulnerable to attack

Juan lives with his mother in the house just over the back fence from the Singhs. Unemployed and desperate for cash, he sees the family as a potential soft burglary target. He thinks he may be able to

use his TAFE-level laptop skills to confuse the family and break into their home when they're vulnerable.

Juan uses a remote device to deliver malware that snoops on local Wi-Fi traffic. Once he is able to detect the Singhs' IoT devices, he uses the malware to check on their status – especially their power switch and lights. This gives Juan a good idea if anyone is home – an ideal scenario for a would-be burglar.

Juan is also able to alter the state of the devices. The Phillips Hue light bulbs don't send encrypted information, so Juan can send them commands – turning them on or off or changing their colour and brightness. The LIFX bulbs have encrypted messages but Juan would be able to decode these with only a little bit of effort. The Singhs' TP-Link power switch also uses encrypted data. However, it has a very weak key for encryption; Juan is able to crack this easily.

What Juan doesn't know is that another hacker has his eyes and ears on the Singhs – specifically Latika's Barbie doll. In far-away Russia, Vladimir is breaking into the device's cloud server, stealing personal information and perhaps even listening in on conversations while the doll's talk button is pushed…

Are energy management devices a smart choice?

IoT devices that claim to make energy systems more efficient might be easy to use but they carry many inherent security flaws. They can give savvy hackers an easy entry into a home – often via a simple transmitted demand.

Devices that appear to be benign, even consumer-friendly items such as remote light bulbs and switches, carry information over the internet that could be vital to criminals or troublemakers wishing to launch attacks.

Case 4: Entertainment and lifestyle for a young couple

Figure 5: Case 4 – Entertainment and lifestyle bundle for a young couple

The potential victims

Eddie and Jenny are in their early 30s and are renting in a fashionable part of Perth. The creative couple love their music, and when they're not out with friends at live venues, they like to listen to new beats in every room of their home, including on their rooftop terrace.

Being young and connected means they spend a lot of time on their mobiles and have all of the movie-streaming services. Jenny, in particular, likes watching the latest flicks. Eddie prefers playing games, and keeps his neighbours awake till the early hours blowing up alien spaceships. Both have busy professional lives and often work nights and on weekends.

The devices

* Smart TV with Google Chromecast, which plays games and streaming videos

* Triby portable speaker

* Amazon Echo voice-activated assistant

* HP Envy smart printer

* Pixstar photo frame, which automatically syncs photos with their Facebook accounts

How entertainment devices are vulnerable to attack

Sven is a lonely widower who lives just two doors away from Eddie and Jenny. He has been keeping an eye on their active (and sometimes noisy) lifestyle, and has often thought of ways to take advantage of them by using his advanced computing skills. He's thinking he might have a bit of fun at their expense… and perhaps make them as miserable as he is.

Sven lives so close to Eddie and Jenny that he is able to use a password-cracking tool to gain access to the couple's Wi-Fi network. Like many others, they haven't changed the default username or password ("admin") on most of their devices. From here, Sven can use simple request functions to get information on what videos and games they play through Google Chromecast – he might even be able to post a threatening text or video on their television screen.

He knows their printer is particularly vulnerable. Using the basic Internet Printing Protocol, Sven can see any documents they have scanned recently or might even print a threatening or obscene message on the device.

Are entertainment devices secure?

Most of the devices Eddie and Jenny bought are relatively safe compared with other IoT devices tested.

The HP Envy printer is an exception to this, with poor security protection. The device has many open ports that aren't protected by a password, allowing an attacker easy access. It also allows an attacker to print documents or stop others from printing entirely.

Overall, entertainment and lifestyle IoT devices don't have as many security vulnerabilities as other devices evaluated. This might be because larger companies familiar with security and safety issues, such as Samsung and Amazon, manufacture many of the devices in this product category.

Implications

What to do about IoT (in)security?

The above scenarios demonstrate how malicious entities, either across the road or across the globe, can snoop on or take control of common household IoT devices. These everyday situations present a serious threat to the wellbeing of their owners, whose devices could also be used to launch cyber attacks on others (a detailed evaluation of the security of each is in the Appendix: How the IoT devices rated).

The problem is large and complex, and there are no easy near-term solutions. A workshop was held at the University of New South Wales, Sydney, on Thursday, 20 April 2017, to present the results and discuss next steps to tackling this challenge. Various entities representing IoT suppliers, consumer groups, regulators and insurance companies attended the workshop to discuss the roles, actions and responsibilities of those groups most affected. This section outlines the discussion held during the day.

Consumers

Attendees felt that consumer expectations must survive a transition to the digital age. Most consumers of smart-home IoT devices will not scrutinise manufacturers' licence agreements, and they can't be expected to as they are frequently complex and unlikely to be enforced. They assume that manufacturers or service providers will supply any software updates necessary to continue running their applications.

Similarly, consumers expect that a smart-home device placed on their home network will not create a backdoor to other devices in their home. More generally, they expect that technical security is someone else's responsibility.

This is a reasonable expectation for consumers. Car buyers, for instance, are only required to ensure their cars are locked, perhaps parked in a secure garage and regularly serviced in line with the manufacturer's specifications. They aren't expected to also be automotive engineers, mechanics or locksmiths.

But how much education is required for a consumer to know that their IoT devices are "safe"? It's possible to foresee the use of a security "star rating" for IoT devices – similar to energy- or water-efficiency ratings on household appliances – that may allow consumers to make informed purchasing decisions. Such a ratings scheme might enable market forces to decide how important consumers see the security and safety of their IoT devices[9].

There are arguments against this: "security evaluations take time, cost money, and always fail to find every possible problem". Not only are the implications of a low security star rating potentially unclear to consumers, but also security threats evolve continuously (since new attacks emerge and IoT software life-cycles are short). How is it possible to keep security ratings up to date?

[9] ZDNet, "No stars for Internet of Things security", http://www.zdnet.com/article/no-stars-for-internet-of-things-security/, AusCERT 2016 conference, 27 May 2016.

Consumers may also feel entitled to expect that their service providers will not sell any data generated by smart-home IoT devices to data aggregators as an additional source of revenue. They won't have the capacity to read through lengthy licence agreements that may permit the service provider to do just that. In general, the ownership of data and its sharing remains very murky[10].

Manufacturers

Manufacturers often face a major gap between consumers' expectations that IoT devices will be kept up-to-date with near-invisible software "patching" and the current reality that many devices simply cannot be updated. While smartphones can be patched with regular updates, the firmware in many IoT devices cannot due to the small memory capacity, lack of a management system, the transient nature of network connectivity or some other issue. In the cases where they can be updated, the technical demands required to make this happen are beyond the ability of most consumers.

Further, manufacturers often focus on price competitiveness rather than security, especially because development costs in this area are expensive. They are more likely to move quickly to the next, more advanced version of their models because that is where the greatest profit lies. The performance of previous models are not likely to concern them, particularly once they're out of warranty.

Manufacturers are also aware that consumers who own webcams and digital video recorders used in DDoS attacks don't personally know the victims, and are not likely to pay too much attention to security features. In such cases, security is something that affects people who aren't involved in the transaction between buyer and seller – an "externality", in economic terms.

For these and other reasons, there may be no feasible market-based solution to the issue of poor IoT security, meaning the onus may fall on regulators.

Regulators

A major implication of our study is that smart-home IoT devices cut across current regulatory silos. They enable the control of functions and objects that are the responsibility of discrete government departments and regulatory agencies.

Medical, traffic control and building management systems, cameras, light bulbs and cars with driver-assist features use an increasing number of IoT devices, yet these are regulated by separate government departments. The Therapeutic Goods Administration within the Australian Government Department of Health regulates medical devices, for example, whereas the Australian Communications and Media Authority regulates telecommunications, broadcasting, radio communications and the internet. Regulating IoT devices will involve input from elements within both entities, and complexity is only likely to increase over time.

The Australian Government Department of Infrastructure and Regional Development regulates vehicle safety, and may require real-time access to data feeds from vehicles using IoT devices. As driver-assistance technologies develop in cars, the need for cross-departmental attention will increase.

[10] The Economist, "The data economy: Fuel of the future", 6 May 2017.

Today's regulatory agencies were created to respond to the rise of earlier technologies. The coming IoT revolution will require new regulatory expertise that cuts across the current set of agencies.

One of the concerns with regulation is its impact on innovation and agility. To reduce this burden, there have been calls[11] for "responsive regulation", with the bottom of the pyramid being "privacy by design" that allows users to monitor and control the life-cycle of data. To ensure the "public health" of IoT, manufacturers could be forced to upgrade software when flaws are found or support "bug bounty" programs that encourage ethical hackers to identify and report flaws so they can be fixed. Users could be forced to change default passwords before using their IoT devices.

Further, companies could be forced to disclose security breaches that affect their products. The issue of liability when damage arises is tricky, and butts up against innovation and agility – even anti-virus software shipped today disclaims liability if your computer gets infected!

Insurers

Just as car insurance premiums vary according to vehicle, its security systems and the experience and track record of its driver, the cost of insuring homes with IoT devices may need to factor in the reputations of the manufacturer and the internet service provider.

Companies that sell IoT devices will need to be insured against the possibility that their products may cause harm to their customers. It is inevitable that a business that produces devices that don't work properly, or are repeatedly hacked, will find its premiums rising. A business that is compromised in this way but has taken reasonable steps – and shows no negligence – should be able to claim on its insurance to avoid going bankrupt.

It's claimed[12] that the cyber insurance market is worth $3 billion to $4 billion per year, and is growing at 60 per cent annually.

[11] M. Richardson, R. Bosua, K. Clark, J. Webb, A. Ahmad, and S. Maynard, "Towards responsive regulation of the Internet of Things: Australian perspectives", Internet Policy Review, 6(1), March 2017.
[12] The Economist, "The myth of cyber-security" & "Why everything is hackable", 8 April 2017.

For consumers: Simple IoT security steps

The following steps are worth considering if you are contemplating any new home internet connected device. Just as the front gate needs the occasional oil and the oven needs cleaning, with any home internet appliance there is likely to be occasional housework and maintenance required.

- Read the manual, and follow any recommended security steps
- Check the packaging to ensure any device you are about to use hasn't been tampered with
- Update the software and set it to auto-update where possible
- Change the password – keep a record in a secure location if you need to, and don’t use obvious ones
- If the device runs additional services in the background, turn off any you don’t need
- Back up important home network data
- Connect devices with cables (not Wi-Fi) where long term connections are desired (eg TVs)
- Place stickers over internet connected cameras and microphones that are not in use
- Turn equipment off at the power switch and disconnect when not needed
- Run an up to date virus checker on home computers and monitor home network traffic levels. If any unaccounted spikes occur, it could be worth investigating.
- Use a good quality home network gateway and set the firewall features to block incoming connections

Conclusions

The rapidly increasing demand for consumer IoT devices poses many security and privacy issues. Consumer products that are connected to the internet will soon become commonplace in homes and businesses, and will offer customers many productivity and lifestyle benefits.

Our testing, however, suggests that the current generation of IoT devices are vulnerable to attack in a number of ways. Hackers, sitting either next door or across the world, can use even quite unsophisticated technology and methods to gain access to personal data within IoT devices. They can also use simple, everyday consumer items to create powerful reflection attacks on other internet networks.

It's a complex problem, and there don't appear to be any "single bullet" solutions to make IoT devices safer or more secure. There is no basic set of agreed security standards or one body in Australia that is capable of overseeing the industry as a whole. The risk with such a fast-moving sector is that basic acceptable standards might become obsolete as quickly as they are established.

The present IoT environment raises many unresolved questions for consumers, manufacturers, regulators and insurers. Of particular concern is whether the cost of regulation and insurance will stifle innovation in the IoT industry. No one wants to turn the software business into something like the pharmaceutical industry, which can spend $1 billion developing a new drug.

It is apparent, however, that consumers will demand greater levels of security and privacy from their IoT devices once they are more aware of the issues involved.

This project, in conjunction with anecdotal evidence in the media, clearly exposes the large-scale lack of security in smart-home IoT devices. We hope it sets the platform for a dialogue between consumers, suppliers, regulators and insurers of IoT devices to develop appropriate methods to tackle the problem.

Authors

Professor Vijay Sivaraman

Professor Sivaraman received his B. Tech. from the Indian Institute of Technology in Delhi, India, in 1994, his M.S. from North Carolina State University in 1996, and his Ph.D. from the University of California at Los Angeles in 2000. He has worked at Bell-Labs as a student Fellow, in a Silicon Valley start-up manufacturing optical switch-routers, and as a Senior Research Engineer at the CSIRO in Australia. He is now a Professor at the University of New South Wales in Sydney, Australia. His research interests span most aspects of internet technologies, including Software Defined Networking (SDN) and the security aspects of the Internet of Things. He has published more than 120 research papers, has been cited more than 2500 times in research literature, and regularly engages with industry on projects ranging from internet performance measurement and enhancement to cyber security.

Dr Hassan Habibi Gharakheili

Dr Habibi Gharakheili received his B.Sc. and M.Sc. (Electrical Engineering) degrees from the Sharif University of Technology in Tehran, Iran, in 2001 and 2004 respectively, and his Ph.D. (Electrical Engineering and Telecommunications) from UNSW in 2015. He is now a Postdoctoral Research Fellow at UNSW. His current research interests include SDN and the security aspects of the Internet of Things.

Professor Clinton Fernandes

Professor Fernandes holds dual appointments at the School of Humanities and Social Sciences at UNSW and the Australian Centre for Cyber Security. His research agenda is linked with the Australian Research Council's strategic priority area of "Securing Australia's place in a changing world". His research within this area includes work on Australia's intelligence agencies, the political and regulatory implications of emerging technologies, Australian foreign relations and defence strategies, and the ability of journalists to report freely in the face of technological, legal and commercial challenges.

Appendix: How the IoT devices rated

Based on the major threats we identified, the following tables show how each IoT device performed in the four categories – confidentiality, integrity and authentication, access control and the ability to withstand reflective attacks.

From this, we gave each device an overall rating for each category. If a device passed a test it was rated “good” (represented by green “A” boxes in the tables); if it failed it was “poor” (red “C” boxes). If it didn’t pass the test but the attack was unsuccessful, it was rated as average (yellow “B” boxes). The grey boxes show when a particular attribute could not be tested or assessed.

Confidentiality rating

Confidentially is a measure of the security of data running between the IoT device, router and our server.

Our tests show whether the communications sent and received were encrypted (the most difficult to read), encoded (hard but not impossible) or plaintext (easiest to hack).

Table 1 shows how each device performed in confidentiality testing.

Table 1: Confidentiality rating

Confidentiality										
	Device to Server			Device to Application			Application to Server			All
Devices	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Privacy
Phillip Hue Light Bulb	A	A	A	C	C	C	A	A	A	C
Belkin Switch	B		A	C	C	C	A	A	A	C
Samsung Smart Cam	A		A	A	A	A	A	A	A	A
Belkin Smart Cam	A		A	A	A	A	A	A	A	A
Awair Air Monitor	A	A	A	A	A	A	A	A	A	A
HP Envy Printer	A	A	A	C	C	C	A	A	A	C
LIFX Bulb	A	A	A	A		C	A	A	A	A
Canary Camera	A	A	A	A	A	A	A	A	A	A
TP Link Switch	A		A	A		C	A	A	A	A
Amazon Echo	A	A	A	A	A	A	A	A	A	A
Samsung Smart Things	A	A	A	A	A	A	A	A	A	A
Pixstar Photo Frame	A	A	A	A	A	A	A	A	A	A
TP Link Camera	A		A	C	C	A	A	A	A	C
Belkin Motion Sensor	A	A	A	C	C	C	A	A	A	C
Nest Smoke Alarm	A		A	A	A	A	A	A	A	A
Netatmo Camera	A	A	A	B	C	A	A	A	A	A
Dlink Camera	C	C	C	A	A	A	A	A	A	A
Hello Barbie Companion	A	A	A	A	A	A	A	A	A	A
Withings Sleep Monitor	A		A	A	A	A	A	A	A	A
Nest Drop Camera	A	A	A	A	A	A	A	A	A	A
Netatmo weather station	A	A	A	A	A	A				A
Triby speaker	A	A	A	A	A	A	A	A	A	A
Withings weighing scale	C	C	C	A	A	A	C	C	C	C
Chromecast	A	A	A	C	C	C	A	A	A	C

- Most of the devices had fairly secure communications in two channels (device to server and user app to server) but were vulnerable when they communicated with their user app.
- Five of the devices – the Phillips Hue light bulb, Belkin switch and motion sensor, HP Envy printer and TP-Link camera – sent data in plaintext rather than encrypted code. This would make it relatively simple for hackers to deduce when a user is at home, based on whether the power switch is on or off, or when the light bulb was last used, for example.
- The TP-Link camera was particularly susceptible to attack. Not only might an attacker view any video and audio footage based on reassembled data, the default authentication password “admin” was easily decoded.

Integrity rating

We checked the integrity and authentication of each device by setting up a fake server to “listen” on the port used by the real server.

Using a number of methods, this fake server communicated with each device to see if it could be authenticated. We also tested to see if the devices could be controlled by outside influences.

Table 2 shows how each device performed in integrity testing.

Table 2: Integrity and authentication

Integrity and authentication				
Devices	**Replay Attack**	**DNSSEC**	**DNS Spoofing**	**Fake Server**
Phillips Hue Light Bulb	C	C	C	C
Belkin Switch	C	C	C	A
Samsung Smart Cam	A	C	C	A
Belkin Smart Cam	A	C	C	A
Awair Air Monitor	A	C	C	A
HP Envy Printer	C	C	C	A
LIFX Bulb	C	C	C	C
Canary Camera	A	C	C	A
TP-Link Switch	C	C	C	A
Amazon Echo	A	C	C	A
Samsung Smart Things	A	C	C	A
Pixstar Photo Frame	A	C	C	A
TP Link Camera	A	C	C	A
Belkin Motion Sensor	A			
Nest Smoke Alarm	A	C	C	A
Netatmo Camera	A	C	C	A
Dlink Camera	A			
Hello Barbie Companion	A	C	C	A
Withings Sleep Monitor	A	C	C	A
Nest Drop Camera	A	C	C	A
Netatmo weather station		C	C	A
Triby speaker	A	C	C	
Withings weighing scale		C	C	
Chromecast	C	C	C	A

Key:
DNS: Domain Name System
DNSSEC: DNS Security Extensions

- These results show that all of the IoT devices were vulnerable to an attack through the Domain Name System (DNS) protocol. This means that attackers could hijack the system and impersonate the legitimate server of the IoT device. They would be protected, however, through proper authentication.
- The two light bulbs that were tested communicated with the fake server, which is a concern.

Access control rating

We tested to see if any ports on a device were “open”, allowing it to be exploited by attackers. Based on this, we launched a password-guessing attack to see if they were protected by strong security protocols.

Each device was also checked to see how much traffic any open ports could handle before they were brought down in a DDoS attack.

Table 3 shows how each device performed in the access control testing.

Key:
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
ICMP: Internet Control Message Protocol
DDoS: Dedicated Denial of Service

- Almost all of the devices had some form of open-port vulnerability. This would enable intruders to communicate with or gain access to the devices.
- Both the Belkin Smart Cam and HP Envy printer exposed a wide range of open ports.
- Disturbingly, both the HP printer and DLink camera had no protection for remote access.
- The last three columns show that most of the devices were susceptible to at least one form of DDoS attack.

Table 3: Access control

Access control							
Devices	**Open Ports (TCP)**	**Open Ports (UDP)**	**Vulnerable Ports**	**Weak Passwords**	**ICMP DDoS**	**UDP DDoS**	**Num. of TCP Connections**
Phillips Hue Light Bulb	C	C	C	A	B	C	C
Belkin Switch	C	C	A	A	C	C	C
Samsung Smart Cam	C	C	C	A	C	C	C
Belkin Smart Cam	C	C	C	A	C	B	C
Awair Air Monitor	B	B	A	A	C	C	A
HP Envy Printer	C	C	C	A	A	A	C
LIFX Bulb	A	B	A	A	C	B	A
Canary Camera	A	A	A	A	C	A	A
TP Link Switch	C	C	C	A	C	C	C
Amazon Echo	C	C	A	A	B	C	C
Samsung Smart Things	C	B	C	A	C	C	C
Pixstar Photo Frame	A	C	A	A			A
TP Link Camera	C	C	C	C	C	B	C
Belkin Motion Sensor	C	C	A	A	C	B	C
Nest Smoke Alarm	B	C	A	A			A
Netatmo Camera	C	C	C	A	C	B	C
Dlink Camera	C	C	C	C	C	B	C
Hello Barbie Companion	A	A	A	A	C	A	A
Withings Sleep Monitor	C	C	C	A			C
Nest Drop Camera	A	B	A	A	C	A	A
Netatmo weather station			A	A			
Triby speaker	C		A	A	C		C
Withings weighing scale	A		A	A	A		A
Chromecast	C		A	A	C		C

Reflection attack rating

We evaluated all of the devices in their ability to “reflect” traffic and overload a victim’s network, forcing it to shut down.

“Amplification” is a type of reflection attack. In this case, the reflection is achieved by gaining a response from an innocent IoT device to a spoofed IP address (a victim machine or server). During an amplification attack, an attacker sends a query with a forged IP address (the victim’s) to the reflector (the IoT device), prompting it to reply to that address with a response. With numerous fake queries being sent out, and with several IoT devices replying simultaneously, the victim’s network is overwhelmed by the sheer number of responses it’s asked to make.

Table 4 shows how each device performed.

Table 4 : Reflection attack

Reflection attacks				
Devices	**ICMP Reflection**	**SSDP Reflection**	**SNMP Reflection**	**SNMP Public Community String**
Phillips Hue Light Bulb	C	C	A	A
Belkin Switch	C	C	A	A
Samsung Smart Cam	C	A	C	C
Belkin Smart Cam	C	C	A	A
Awair Air Monitor	C	A	A	A
HP Envy Printer	C	A	C	A
LIFX Bulb	A	A	A	A
Canary Camera	C	A	A	A
TP Link Switch	C	A	A	A
Amazon Echo	C	A	A	A
Samsung Smart Things	C	A	A	A
Pixstar Photo Frame	C	A	A	A
TP Link Camera	C	A	A	A
Belkin Motion Sensor	C	C	A	A
Nest Smoke Alarm	C	A	A	A
Netatmo Camera	C	A	A	A
Dlink Camera	C	C	A	A
Hello Barbie Companion	C	A	A	A
Withings Sleep Monitor	C	A	A	A
Nest Drop Camera	C	A	A	A
Netatmo weather station		A	A	A
Triby speaker	C	A	A	A
Withings weighing scale	A	A	A	A
Chromecast	C	A	A	A

Key:
ICMP: Internet Control Message Protocol
SSDP: Simple Service Discovery Protocol
SNMP: Simple Network Management Protocol

- Most of the devices were unable to withstand an ICMP reflection attack.
- All devices, except the LIFX light bulb, were susceptible to reflecting some form of attack.
- The Samsung Smart Cam was vulnerable across a number of protocols.

Inside job

Security and privacy threats for smart-home IoT devices