Smart IoT Devices in the Home

Security and Privacy Implications

Vijay Sivaraman, Hassan Habibi Gharakheili, Clinton Fernandes, Narelle Clark, and Tanya Karliychuk

BEEBRIGHT/ISTOCK

Internet of Things (IoT) devices possess network capabilities and contain at least a part of the application logic, i.e., they have the ability to perform Transmission Control Protocol/Internet Protocol (TCP/IP) communications on their own, and can process some of the sensor data. The IoT thus refers to the network of physical objects embedded with electronics, software, sensors and connectivity to enable objects to exchange data with the manufacturer, operator, and/or other connected devices. At the start of this decade, there were an estimated 12.5 billion IoT devices, almost twice as much as the world's population of 6.8 billion people [1]. The number of IoT devices is expected to grow rapidly in coming years.

These technological changes have tremendous implications for decentralized production control in manufacturing, and are expected to trigger a fourth industrial revolution, following the steam engine, the conveyor belt, and the computer revolution. IoT devices will have a transformational effect on the lives of everyday consumers, too. Australia's largest telecommunications company, Telstra, says the average Australian household in 2017 had 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 AU$1billion annually by 2021 [2]. As the IoT technology becomes embedded in televisions, webcams, smoke alarms, fitness trackers, climate-control systems, lightbulbs and more, it has the potential to save money and time, help people stay fit, healthy, and safe, and enable effortless communication with friends and family. There are important security

Digital Object Identifier 10.1109/MTS.2018.2826079
Date of publication: 31 May 2018

1932-4529/18©2018IEEE

and privacy implications for consumers [3], however; many Internet-connected devices have poor in-built security measures [4] and can reveal private data and information that may harm or embarrass consumers [5]. A 2015 inquiry into data retention by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) [6] mentioned "privacy" nearly 400 times. It said that privacy and security concerns "are closely related, as the potential for security breaches has significant ramifications for the proportionality and privacy risks associated with the proposed scheme."

IoT Consumer Research: Scenario, Test, Evaluate, Propose

In this article, we examine the security and privacy implications of selected IoT devices, building on previous work [7] in this area. Our specific contributions are as follows: First, we developed hypothetical scenarios of household IoT usage. We then tested the security and privacy vulnerabilities of several of these devices, subjecting them to hostile targeting under laboratory conditions. Next, we invited IoT suppliers, consumers, insurers, and regulators to evaluate our results at a workshop. Finally, after examining their reactions and discussing their expectations, we proposed possible approaches to help mitigate the identified risks. We also identified a research trajectory that would begin a new four-step cycle of Scenario-Test-Evaluate-Propose. We wish to emphasize that the workshop phase of our research cycle is as critical as the other phases, and not merely an afterthought. It is this phase that enables us to engage with consumers and understand the contexts in which they use their devices. In doing so, we are in a better position to construct realistic scenarios to guide our laboratory testing.

Scenarios

We created four scenarios in which people are likely to use IoT devices. Our aim was to identify products they would purchase so that we could evaluate their vulnerability under laboratory conditions. All the characters and locations are fictitious, but the scenarios are extremely realistic, and constructed on the basis of direct engagement with consumer advocates.

In the first scenario, the consumer is Tuan, a mid-career private investigator who lives by herself in a regional town in Australia, regularly drives to Melbourne and flies to Sydney to meet with clients. Most of her work involves insurance fraud although she is often asked to track cheating spouses. 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 believes that installing IoT devices would offer some peace of mind. As a sole occupier who desires home security, Tuan buys three IoT devices:

1) a Belkin motion sensor to detect movements inside her house;
2) TP-Link indoor and outdoor motion sensor cameras; and
3) A Nest smoke alarm to send alerts to her smartphone in case of fire.

In the second scenario, the IoT device users are Joe and Lorna Jones, an elderly couple who live in the inner city. Lorna is a bit hard of hearing, wears a pacemaker, and has respiratory difficulties. She is not a regular user of the Internet. Joe has some mobility problems and relies on his medical-alert device when he's away from home. Lorna was playing bowls (lawn bowling) the last time he had a fall, and it took hours before he could get help. Their son, Geoffrey, who lives with his family on the Gold Coast 100-km away, wants a way to monitor his parents' welfare more thoroughly 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. These devices are:

1) Blipcare blood pressure monitor, which sends readings to the web for Geoffrey to check;
2) Withings weighing scale;
3) Withings sleep monitor;
4) Awair air quality monitor; and
5) Netatmo weather station.

In the third scenario, Suresh and Veda Singh live in Sydney's suburbs. They know they have to cool their west-facing house in summer. Although they've trained their three growing children to moderate their electricity usage, it still feels like they're in a losing battle against the large electricity bill that arrives every quarter. While shopping for smart devices intended for use around the home, they also bought an interactive doll for their youngest child. The cute doll has a microphone that "listens" to the child, and replies in a manner similar to Apple's Siri. Their purchases included:

1) a mix of LIFX and Phillips Hue light bulbs for remote-control lighting;
2) a TP-Link power switch to control their appliances; and
3) A Hello Barbie talking doll.

In the fourth scenario, a trendy young city couple place a high priority on their social life. Eddie and Jenny like to listen to music in every room of their home, including on their rooftop terrace. They also spend a lot of time on their mobile devices, and subscribe to the major movie-streaming services. Jenny likes watching the latest movies while Eddie prefers playing computer games. Both have busy professional lives and often work nights and on weekends. They have bought the following devices:

1) Smart TV with Google Chromecast, which plays games and streams videos;
2) Triby portable speaker;
3) Amazon Echo voice-activated assistant;
4) HP Envy smart printer; and
5) Pixstar photo frame, which automatically syncs photos with their Facebook accounts.

Testing

We selected a number of devices based on the above scenarios as well as on product availability and popularity in Australia, 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 evaluating 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.

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 onto 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 computerized 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).

The Results section lists full tables of results showing how each device performed in each category. The results of our tests were consistent and alarming. Every device we tested showed some form of vulnerability in 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. A vivid illustration of these vulnerabilities can be gained by applying them to our four scenarios.

In the first scenario, a former target of Tuan's investigation would be able to sit in a car outside her house and deduce her Wi-Fi network password using freely available software. He would then place 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 his laptop, which he monitors from his home. Essentially, his 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 to see video and read motion-sensor information from Tuan's devices on his laptop at home. He would therefore know when Tuan's devices have been inactive for a few hours. Surmising that Tuan is away, perhaps in Melbourne or Sydney, he drives back to his parking spot in the street outside Tuan's home. He 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 she will never get the smoke alert from her IoT alarm — even though her home has been physically set alight.

In the second scenario, a criminal buys a list of email addresses of people who have recently registered IoT products. One of these belongs to Joe and Lorna Jones. The criminal sends them an email 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 is not sure what the email is about but thinks it sounds interesting. Without thinking, she manages to download the app. The malware immediately disables the Joneses' firewall and enables port forwarding, making them vulnerable to security breaches. Now the criminal is in control. His malware finds unencrypted messages from their weighing scales, enabling him to 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 Joneses' identity and take their social security benefits. He can also use Joe and Lorna's IoT devices to reflect and amplify attacks on other Internet-connected devices. Whenever he likes, he can use the open ports on the Joneses' 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. Note, however, that in general, health monitoring IoT devices do not tend to have many security problems. Although the Awair air quality monitor could stop functioning if it's forced to deal with a large amount of Internet traffic, it encrypts all data sent to the server.

In the third scenario, an opportunistic neighbor sees the Singhs as a potential soft burglary target. He uses a remote device to deliver malware that snoops on local Wi-Fi traffic. The Singhs' IoT devices, especially their power switch and lights, provide a good indication of their presence in, or absence from, their home. More importantly, the neighbor can alter the state of the devices. The Phillips Hue light bulbs do not send encrypted information, so he can turn them on or off and change their color and brightness. The LIFX bulbs have encrypted messages but they can be decrypted with little effort. The TP-Link power switch also uses encrypted data but has a very weak key; it can be broken easily. Under certain conditions, the Hello Barbie doll enables outsiders to listen in on conversations while the doll's talk button is pushed.

In the fourth scenario, a cyber-stalker uses a password-cracking tool to gain access to Eddie and Jenny's Wi-Fi network. Like many others, they have not changed the default username or password ("admin") on most of their devices. Once in, the stalker can use simple request functions to get information on what videos and games they play through Google Chromecast — she might even be able to post a threatening text or video on their television screen. She knows their printer is particularly vulnerable. Using the basic Internet Printing Protocol, she can see any documents they have scanned recently or might even print a threatening or obscene message on the device. Although most of Eddie and Jenny's devices are relatively safe compared with other IoTs tested, the HP Envy printer is an exception. It has poor security protection, with many open ports that are not protected by a password, allowing an attacker easy access. It also allows an attacker to print documents or stop others from printing entirely.

Evaluate

We invited IoT suppliers, consumers, insurers, and regulators to evaluate our results at a workshop. In this section, we discuss their reactions and expectations.

A frequent theme among attendees was that consumer expectations must survive a transition to the digital age. Most consumers of smart-home IoT devices will not scrutinize manufacturers' license agreements, and they cannot be expected to as the agreements 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.

We believe this expectation is reasonable in light of consumers' experiences with non-IoT products. Car buyers, for instance, are only required to ensure that their cars are locked, perhaps parked in a secure garage, and regularly serviced in line with the manufacturer's specifications. They are not expected to also be automotive engineers, mechanics or locksmiths. And yet, the question persists: 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 the security and safety of IoT devices are to consumers [8].

Such a scheme is not without complexity of its own. Security ratings, after all, cannot be static, since security threats evolve continuously. The implications of a low security star rating may be unclear to consumers.

Further, the issue of data ownership and its sharing remains murky [9]. Consumers may expect their service providers will not on-sell data generated by their smart-home IoT devices, for example, despite some license agreements allowing just that. Any ratings system, and improvements to consumer decision making, need to take this into account.

For manufacturers, a major gap exists 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 be patched due to small memory capacity, lack of a management system, the transient nature of network connectivity, or some other issue. In the cases where devices can be updated, the technical demands required to make this happen are beyond the ability of most consumers.

Furthermore, in a world of disarticulated production, it is simply not clear who is most responsible for a security shortfall: is it the company that designs the device, or the one that supplies component software? Or is it the company that supplies the network in which the device is embedded?

Further, manufacturers often focus on price competitiveness rather than security, especially because development costs in this area are high. 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 is 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 do not 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 are not involved in the transaction between buyer and seller — an "externality" in economic terms.

Insurers should reconsider their approach to manufacturers and consumers of IoT devices. The cyber insurance market is said to be worth $3 billion to $4 billion per year, and is growing at 60 percent annually [10]. Companies that sell IoT devices may need to be insured against the possibility that their products may cause harm to their customers, or others. Effective policy is needed to ensure businesses that produce devices unfit for purpose, or that are repeatedly hacked, cannot continue to do so. A business that is compromised, but has taken reasonable steps to resolve the issue — and shows no negligence — should be able to claim on its insurance.

Recently IoT devices have also been made available for extremely intimate and sexual applications with devices enabling remote logging and control [11], even incorporating cameras. In this context other security researchers have identified significant flaws in the implementation of connectivity, privacy, and data management, which they argue is through the poor choice of source code reused from public repositories [12]. In one case privacy protections in the U.S. meant that customers could receive compensation for breaches of their usage data after a court finding that the breach had not been disclosed to customers.

In this context the potential for serious sexual assault leaves device manufacturers clearly open to adverse judgement and reputational damage even if perpetrators of such crimes are difficult to identify and pursue.

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.

Proposal

Resolution of the security risks identified in our study is hampered by the siloed nature of regulation that is now becoming more broadly applicable due to the expansion of communications and forming the IoT. Functions and objects are the responsibility of discrete government departments and regulatory agencies, but the agencies now find themselves potentially responsible for new areas. Further exacerbating this problem is that regulatory standards and benchmarks that apply in one jurisdiction do not necessarily apply within another.

Medical, traffic control, and building management systems, cameras, light bulbs and cars with driver-assist features use an increasing number of IoT devices, yet are regulated by separate government departments. In Australia for example, the Therapeutic Goods Administration within the Department of Health regulates medical devices, whereas the Australian Communications and Media Authority regulates telecommunications, broadcasting, radio communications, and the Internet, and the Australian Competition and Consumer Commission regulates consumer safety and fair trade. Regulating IoT devices will involve input from elements within each of these 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. As in Australia, today's regulatory agencies across the world 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.

We therefore propose a more coordinated and exhortative approach to regulation. Manufacturers will need to be encouraged to build security at the design phase. A "security by default" attitude would see consumers having to deliberately disable rather than deliberately enable security features. A mechanism may need to be found to coordinate software updates among third-party vendors, and to facilitate the coordinated disclosure of vulnerabilities. Here, a role may be found for national cybersecurity agencies, such as the Australian Cyber Security Centre, to coordinate the security knowledge-sharing of developers, manufacturers, and service providers.

Bodies and services that may have been exempt in the past from regulation may also come under future scrutiny due to the evolving need for consumer and community protection. Because of the serious threat to infrastructure, it is conceivable that governments may in the future require Internet service provider networks to comply with network security standards or meet performance benchmarks. Devices provided by manufacturers or Internet service providers to perform network boundary roles, such as home gateways, could be expected to come under higher levels of requirements. This would mean devices shipped with default passwords, for example, could become a thing of the past.

Further research along the lines of the STEP model is needed in order to continue to shed light on the burgeoning field of IoT devices.

Results

Based on the major threats we identified, Figures 1-4 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 did not pass the test but the attack was unsuccessful, it was rated as average (yellow "B" boxes). The grey boxes

Confidentiality										
	Device to Server			Device to Allocation			Application to Device			All
Devices	Plain Text	Protocol	Entropy	Plain Text	Protocol	Entropy	Plain Text	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

FIGURE 1. Confidentiality rating.

show when a particular attribute could not be tested or assessed.

Note these tests were performed at a point in time and may have been improved or further deteriorated since the date of testing in April 2017.

Confidentiality Rating

Confidentially is a measure of the security of data running between the IoT device, the 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 plain text (easiest to hack).

Figure 1 shows how each device performed in confidentiality testing.

- 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 plain text 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. This technique is known as a "man in the middle attack."

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.

Figure 2 shows how each device performed in integrity testing.

- 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 the port 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.

Integrity and Authentication				
Devices	Replay Attack	DNSSEC	DNS Spoofing	Fake Server
Phillips Hue Light Bulb	C	C	C	C
Belkin Switch	C	C	C	C
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

FIGURE 2. Integrity and authentication.

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	C	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	A
Chromecast	A		A	A	C		C

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

FIGURE 3. Access control.

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

- 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.

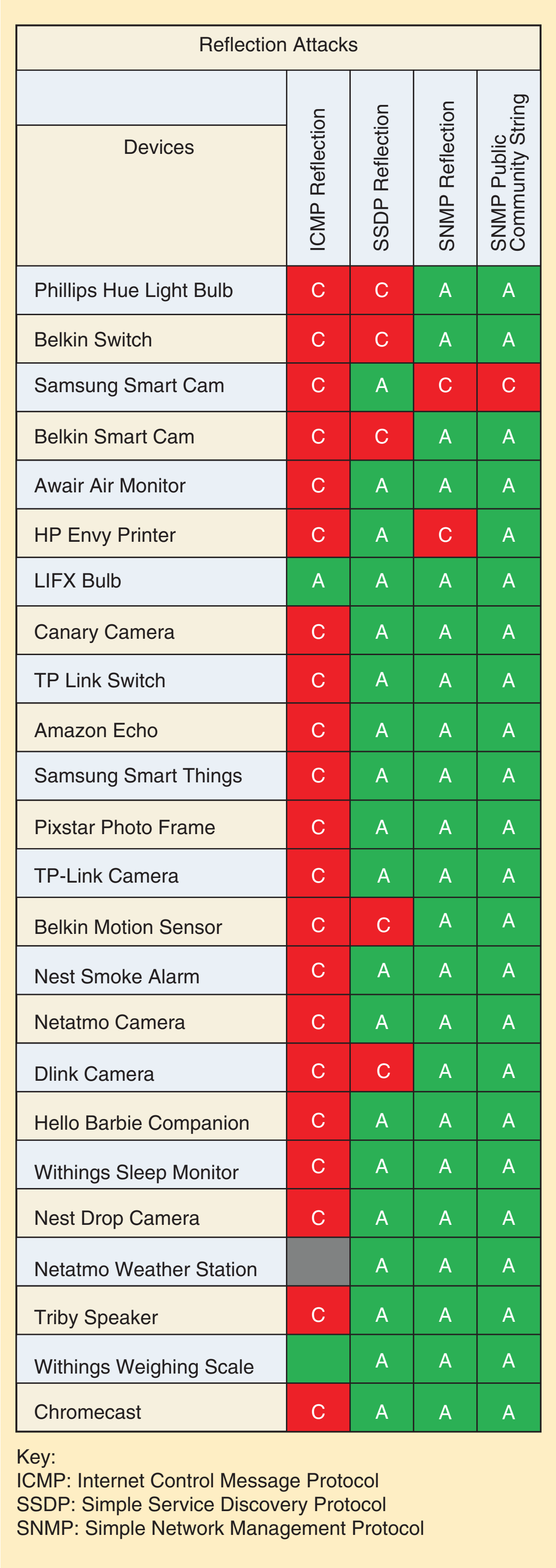
Reflection Attack Rating

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 [13]. 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.

Figure 4 below shows how each device performed.

- 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.



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
Chromecast	C	A	A	A

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

FIGURE 4. Reflection attack.

Current Generation of IoT Devices Vulnerable to Attack

Consumer products connected to the Internet will soon become commonplace in homes and businesses, and will offer customers many productivity and lifestyle benefits. Our study, however, suggests that the current generation of IoT devices is vulnerable to attack in a number of ways. It is a complex problem, and there don't appear to be any "single bullet" solutions to make IoT devices safer or more secure. We hope this article sets the platform for a dialogue between consumers, suppliers, regulators, and insurers of IoT devices to develop appropriate methods to tackle the problem.

Author Information

Vijay Sivaraman and ***Hassan Habibi Gharakheili*** are with the School of Electrical Engineering and Telecommunications, University of New South Wales (UNSW), Australia.

Clinton Fernandes is with the School of Humanities and Social Sciences at UNSW and the Australian Centre for Cyber Security, Australia.

Narelle Clark and ***Tanya Karliychuk*** are with the Australian Communications Consumer Action Network, Australia. Email: research@accan.org.au.

References

[1] D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," CISCO,White Paper, 2011; https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[2] J. Chambers, Executive Director of Product Innovation, comments presented at UNSW workshop (Australia), Apr. 20, 2017.

[3] N. Dhanjani, *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*. O'Reilly Media, 2015.

[4] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Symp. Security and Privacy* (San Jose, CA, USA), May 2016.

[5] F. Loi, A. Sivanathan, H. Habibi Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proc. ACM CCS Workshop IoT Security and Privacy* (Texas, U.S.A.), Nov. 2017.

[6] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. Canberra, Australia: Commonwealth Parliament, 2015, p. 11.

[7] C. Fernandes and V. Sivaraman, "It's only the beginning: Metadata retention laws and the Internet of Things," *Australian J. Telecommunications and the Digital Economy*, vol. 3, no. 3, Sept. 2015.

[8] ZDNet, "No stars for Internet of Things security," presented at AusCERT 2016 Conf., May 27, 2016.

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

[10] "The myth of cyber-security" & "Why everything is hackable," *The Economist*, Apr. 8, 2017.

[11] M. Wynn et al., "How to practice safe IoT: Sexual intimacy in the age of smart devices," in *Proc. ACM CCS Workshop on IoT Security and Privacy* (Texas, USA), Nov. 2017.

[12] R. Chirgwin, "Wi-Fi sex toy with built-in camera fails penetration test," *The Register*, Apr. 4, 2014; https://www.theregister.co.uk/2017/04/04/intimate_adult_toy_fails_penetration_test/.

[13] M. Lyu et al., "Quantifying the reflective DDoS attack capability," in *Proc. ACM* (Boston, MA, U.S.A.), Jul. 2017.