Experimental Evaluation of Cybersecurity Threats to the Smart-Home

Arunan Sivanathan, Franco Loi, Hassan Habibi Gharakheili, and Vijay Sivaraman
Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia.
Emails: a.sivanathan@unsw.edu.au, f.loi@student.unsw.edu.au, h.habibi@unsw.edu.au, vijay@unsw.edu.au

***Abstract*—Consumers are increasingly buying Internet-connected appliances, referred to as the Internet of Things (IoT), for their homes. These IoT devices can collect a lot of data and enable users to manage their smart home environment. However, it can also pose huge risks to consumers privacy and security. A remote intruder who may illegitimately access these devices can obtain information for his gain or harm other entities. This paper aims to experimentally evaluate vulnerabilities of consumer IoT devices against cyber-attacks. We first develop a number of test suites to conduct our evaluation in four categories: *confidentiality* of data exchanged by IoT devices, *integrity and authentication* of their communication, their *access control and availability*, and their capability to *reflect* DDoS attacks. We then give each IoT device an overall rating (good, average, poor) based on threats we identified in each category. Lastly, we apply our evaluation to four representative households namely home security, health monitoring, energy management, and entertainment which collectively include 17 consumer IoT devices that are available on the market, and illustrate what threats may emerge for each household if IoT devices are compromised.**

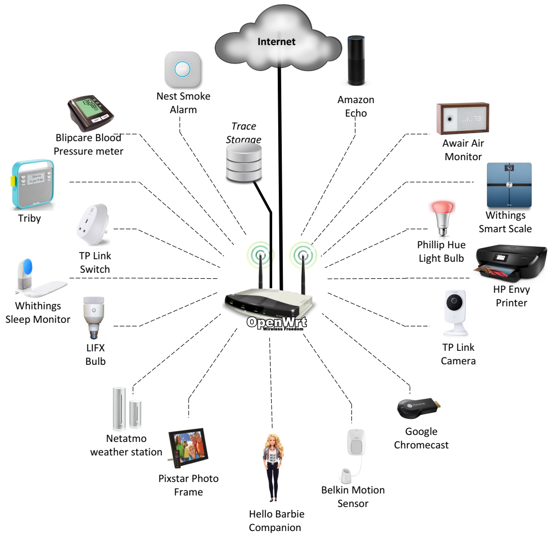


Fig. 1. Testbed showing the IoT devices and gateway

I. Introduction and Background

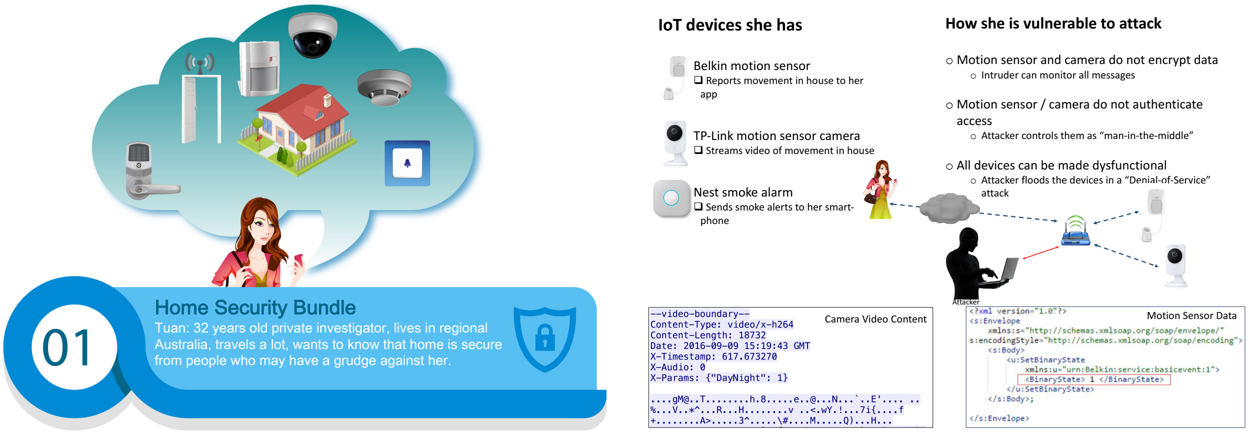
The internet gives us the opportunity to enjoy incredible experiences, be entertained and informed, and keep in contact with others across the street or the globe. Wherever we are, and whatever our stage in life, internet-capable devices offer us the promise of unparalleled freedom and flexibility. These devices are also becoming more important for our sense of personal safety and security. These "Internet of Things" (IoT) devices include televisions, webcams, smoke alarms, fitness trackers, climate-control systems - even "smart" lightbulbs. 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 IoTs in use is growing rapidly - there will be 12.2 billion of Internet-connected devices by 2020 [1].

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 further hurt or alarm us. A typical smart home with many IoT devices is under significant risk of cyberattack. This vulnerability compromises data and threatens our personal safety. Many security vulnerabilities in IoT devices have been identified and reported by prior work [2]–[4]. For example, the experimental studies carried out in [5] shows that the current status of lightbulb and power switch can be monitored and tampered by sniffing and replaying certain packets (violating confidentiality and integrity); measurement of smart meters were spoofed [6] (violating integrity); thousands of printers exposed to the Internet with no authentication were exploited to print threating messages [7] (violating access control); 100,000 infected IoT devices were used as launchpads conducting large-scale DDoS attack to DNS servers [8] (violating access control);household IoT devices were recruited to reflect DDoS attacks toward a victim server, even they were seemingly protected by home gateways [9]. Further, search engines such as shodan [10] and Inseccam [11], that are discovering vulnerable IoT devices and exposing them to public Internet, make it an effortless task to launch a cyberattack.

This paper[1] aims to experimentally evaluate vulnerabilities of consumer IoT devices against cyber-attacks. Our specific contributions are as follows:

- We develop test suites corresponding to four categories of security vulnerabilities namely confidentiality of data they communicate with other devices locally/externally; integrity of connections they make to/receive from other entities; access control and availability of IoT devices; and their capacity in reflecting unwanted traffic that can contribute to a DDoS attack.

[1] Funding for this project was provided by the Australian Communications Consumer Action Network, ACCAN Grants Scheme round 2016.


01
Home Security Bundle
Tuan: 32 years old private investigator, lives in regional Australia, travels a lot, wants to know that home is secure from people who may have a grudge against her.
IoT devices she has
Belkin motion sensor
❑ Reports movement in house to her app
TP-Link motion sensor camera
❑ Streams video of movement in house
Nest smoke alarm
❑ Sends smoke alerts to her smart-phone
How she is vulnerable to attack
○ Motion sensor and camera do not encrypt data
○ Intruder can monitor all messages
○ Motion sensor / camera do not authenticate access
○ Attacker controls them as "man-in-the-middle"
○ All devices can be made dysfunctional
○ Attacker floods the devices in a "Denial-of-Service" attack
Attacker
Camera Video Content
Motion Sensor Data

```
--video-boundary--
Content-Type: video/x-h264
Content-Length: 18732
Date: 2016-09-09 15:19:43 GMT
X-Timestamp: 617.673270
X-Audio: 0
X-Params: {"DayNight": 1}

....gM@..T........h.8.....e..@...N...`..E'.... ..
%...V..*^...R...H........v ..<.wY.!...7i{....f
+........A>.....3^.....\#....M.....Q)...H...
```

```
<?xml version="1.0"?>
<s:Envelope
    xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding">
    <s:Body>
        <u:SetBinaryState
            xmlns:u="urn:Belkin:service:basicevent:1">
            <BinaryState> 1 </BinaryState>
        </u:SetBinaryState>
    </s:Body>;

</s:Envelope>
```

(a)

(b)

Fig. 2. Home security (a) persona, (b) cyber attack.

- We apply our test suites to IoT device and rate them assessing their security by three levels of A (good), B (average), and C(poor), in each of four categories.
- We develop representations of "typical" households using 17 off-the-shelf IoT devices, and illustrate what threats may arise when security of their devices are compromised. It is important to note that our scenarios are hypothetical for the narrative, but devices vulnerabilities are not - we have experimentally evaluated these security issues in our laboratory environment.

The rest of this paper is organized as follows: §II describes our security evaluation criteria. We highlight the cuber-security threats to IoT devices in four typical households and present our security rating to individual devices in §III. The paper is concluded in §IV.

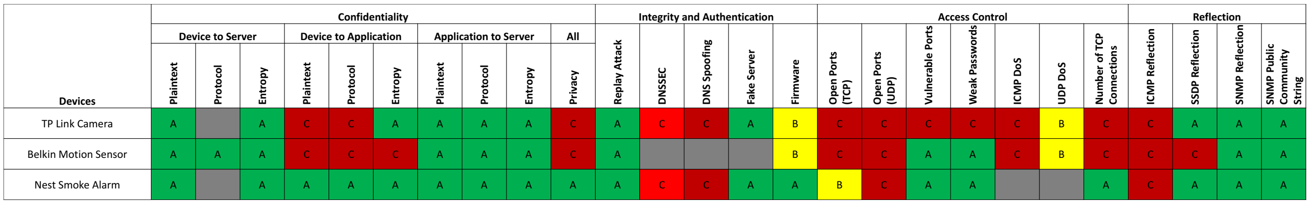
II. Security Evaluation Criteria

We develop and carry out several tests on individual IoT devices as well as their supplied mobile app and corresponding Internet-based servers. Our tests are ranging from simple (capturing wireless communications from/to the device to evaluate the confidentiality of exchanged data) to complex (probing the device if it responds to a fake endpoint, and overwhelming the device by spoofed messages) inspections. We develop a number of Python scripts and use penetration testing tools (available on Kali linux) to assess the security performance of each IoT device. We assess each device against four criteria namely confidentiality, integrity and authentication, access control and availability, and reflection as explained next.

Confidentiality is an important aspect of security which involves ensuring the exchanged data between endpoints cannot be understood by snoopers. If an IoT device does not communicate in a confidential manner, it not only exposes the users private data but also provides attackers with information of the device that can be exploited further to launch more serious attacks to other devices or networks. We measure the confidentiality of a device using various methods such as analyzing the payload of packets whether those are human-readable or not, determining the entropy level of packets and identifying the security protocols like SSL/TLS. These analyses reveal the confidentiality level of the communication as "plaintext" – where all information is in human-readable text, "encoded" – where data is not human-readable but can be reverted into plaintext by applying the some decoding algorithms, or "encrypted".

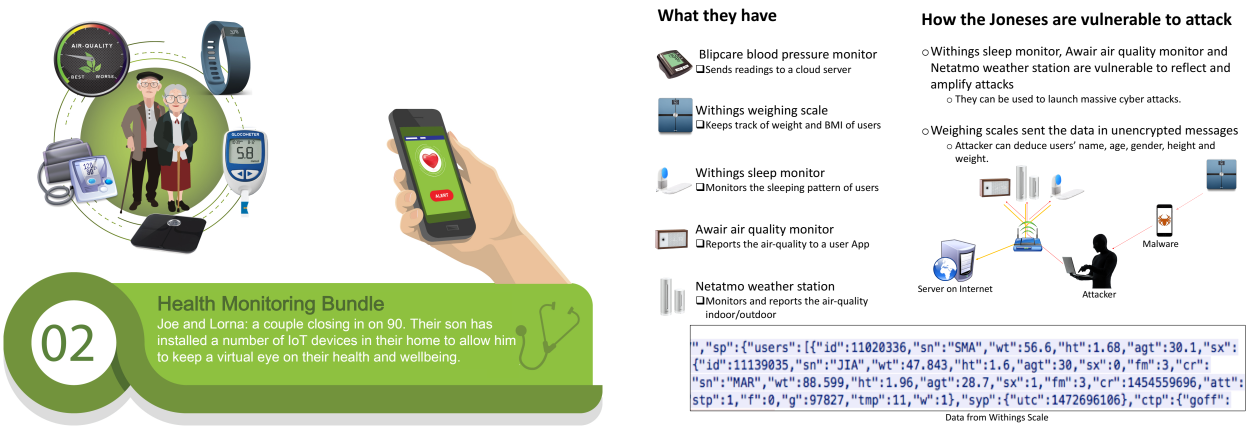
We next evaluate the integrity of communications to check if a given device communicates only with indented endpoints (either cloud servers or local devices) and does not respond to spoofed packets. To ensure that the integrity is not violated, the IoT device needs to perform a proper authentication with all endpoints it communicates with and verify all data it receives (e.g. firmware update). We test the integrity by checking if the device responds to spoofed packets (replay attack, DNS spoofing, or fake servers). We also test if the device is DNSSEC enabled – this protocol helps perform authentication, preventing DNS spoofing using a set of keys.

We consider the access control and availability of an IoT device to identify how easily an attacker can gain access to/control over the device, and to determine whether it is susceptible to a DoS attack which can have serious implications for users (e.g. surveillance camera or health monitoring devices can become unavailable). We, therefore, use following measures for each IoT device: the number of open TCP and UDP ports (using port scan), vulnerable ports that provide remote access (checking SSH, Telnet), existence of default credentials (e.g. admin/admin), and the maximum rate of



Devices	Confidentiality										Integrity and Authentication					Access Control							Reflection			
	Device to Server			Device to Application			Application to Server			All																
	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Privacy	Replay Attack	DNSSEC	DNS Spoofing	Fake Server	Firmware	Open Ports (TCP)	Open Ports (UDP)	Vulnerable Ports	Weak Passwords	ICMP DoS	UDP DoS	Number of TCP Connections	ICMP Reflection	SSDP Reflection	SNMP Reflection	SNMP Public Community String
TP Link Camera	A		A	C	C	A	A	A	A	C	A	C	C	A	B	C	C	C	C	C	B	C	C	A	A	A
Belkin Motion Sensor	A	A	A	C	C	C	A	A	A	C	A				B	C	C	A	A	C	B	C	C	C	A	A
Nest Smoke Alarm	A		A	A	A	A	A	A	A	A	A	C	C	A	A	B	C	A	A			A	C	A	A	A

Fig. 3. Security rating for security persona


AIR-QUALITY
BEST
WORSE
GLUCOMETER
58
ALERT
02
Health Monitoring Bundle
Joe and Lorna: a couple closing in on 90. Their son has installed a number of IoT devices in their home to allow him to keep a virtual eye on their health and wellbeing.
What they have
Blipcare blood pressure monitor
❑Sends readings to a cloud server
Withings weighing scale
❑Keeps track of weight and BMI of users
Withings sleep monitor
❑Monitors the sleeping pattern of users
Awair air quality monitor
❑Reports the air-quality to a user App
Netatmo weather station
❑Monitors and reports the air-quality indoor/outdoor
How the Joneses are vulnerable to attack
○ Withings sleep monitor, Awair air quality monitor and Netatmo weather station are vulnerable to reflect and amplify attacks
○ They can be used to launch massive cyber attacks.
○ Weighing scales sent the data in unencrypted messages
○ Attacker can deduce users' name, age, gender, height and weight.
Malware
Server on Internet
Attacker

```
","sp":{"users":[{"id":11020336,"sn":"SMA","wt":56.6,"ht":1.68,"agt":30.1,"sx":
{"id":11139035,"sn":"JIA","wt":47.843,"ht":1.6,"agt":30,"sx":0,"fm":3,"cr":
"sn":"MAR","wt":88.599,"ht":1.96,"agt":28.7,"sx":1,"fm":3,"cr":1454559696,"att":
stp":1,"f":0,"g":97827,"tmp":11,"w":1},"syp":{"utc":1472696106},"ctp":{"goff":
```

Data from Withings Scale

(a) (b)

Fig. 4. Health monitoring (a) persona, (b) cyber attack.

incoming traffic that it can handle.

Evaluating the reflection capability of IoT devices is important since they are increasingly contributing to DDoS attacks launched towards popular service providers across the Internet. During reflection attacks, devices send a large amount of packets to victim servers in response to traffic with a forged source IP address of the victim. We test the ability of reflection for individual IoT devices using standard protocls including ICMP, SSDP, SNMP, and SNMP public communication string.

III. Security Threats to Households

We now consider four scenarios in which people are likely to use IoT devices - for reasons of safety, health, energy management and entertainment. We identify the security vulnerabilities of devices in each households and illustrate possible attacks can be launched via malwares or from remote endpoints.

A. Home Security Bundle

Fig. 2(a) shows our home security persona. Tuan is a 32-year-old private investigator. Most of her work involves insurance fraud although she is often asked to track cheating spouses. She lives by herself in Geelong, Victoria, and 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 piece of mind.

She equipped her home with following sensors

- 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

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.

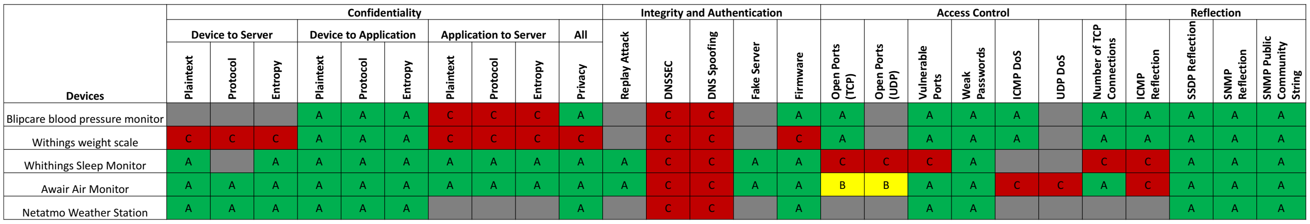
Once he's sitting in his car close to Tuan's Geelong home, Ron deduces her Wi-Fi network password using freely available software. He then quickly walks outside her home and places a cheap battery-powered device beneath her letterbox. This device connects with her home wireless network, capturing all 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.

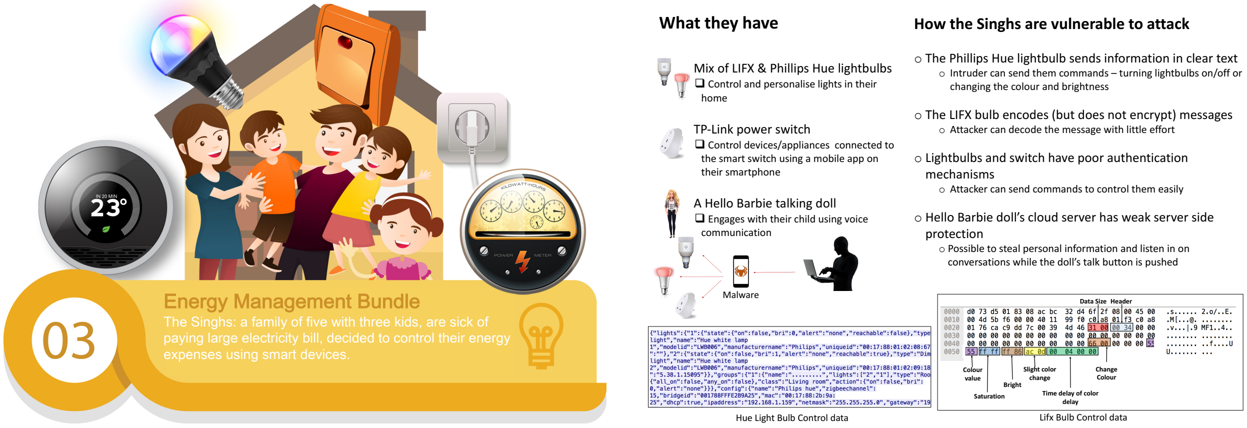
Certain the home is vacant, Ron uses a denial-of-service attack on Tuan's motion sensor, cameras and smoke alarm by bombarding them with a large number of requests. Unable to cope, these devices simply shut down. This ensures that Tuan will never get the smoke alert from her IoT alarm even once malicious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

Our evaluations show that Belkin motion sensor and TP-Link camera send data in plaintext as depicted in Fig. 2(b).



	Confidentiality										Integrity and Authentication					Access Control							Reflection			
	Device to Server			Device to Application			Application to Server			All																
Devices	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Privacy	Replay Attack	DNSSEC	DNS Spoofing	Fake Server	Firmware	Open Ports (TCP)	Open Ports (UDP)	Vulnerable Ports	Weak Passwords	ICMP DoS	UDP DoS	Number of TCP Connections	ICMP Reflection	SSDP Reflection	SNMP Reflection	SNMP Public Community String
Blipcare blood pressure monitor				A	A	A	C	C	C	A		C	C		A	A		A	A	A		A	A	A	A	A
Withings weight scale	C	C	C	A	A	A	C	C	C	C		C	C		C	A		A	A	A		A	A	A	A	A
Whithings Sleep Monitor	A		A	A	A	A	A	A	A	A	A	C	C	A	A	C	C	C	A			C	C	A	A	A
Awair Air Monitor	A	A	A	A	A	A	A	A	A	A	A	C	C	A	A	B	B	A	A	C	C	A	C	A	A	A
Netatmo Weather Station	A	A	A	A	A	A				A		C	C		A			A	A					A	A	A

Fig. 5. Security rating for health persona


IN 20 MIN
23°
03
Energy Management Bundle
The Singhs: a family of five with three kids, are sick of paying large electricity bill, decided to control their energy expenses using smart devices.

What they have

Mix of LIFX & Phillips Hue lightbulbs
❑ Control and personalise lights in their home

TP-Link power switch
❑ Control devices/appliances connected to the smart switch using a mobile app on their smartphone

A Hello Barbie talking doll
❑ Engages with their child using voice communication

How the Singhs are vulnerable to attack

○ The Phillips Hue lightbulb sends information in clear text
  ○ Intruder can send them commands – turning lightbulbs on/off or changing the colour and brightness

○ The LIFX bulb encodes (but does not encrypt) messages
  ○ Attacker can decode the message with little effort

○ Lightbulbs and switch have poor authentication mechanisms
  ○ Attacker can send commands to control them easily

○ Hello Barbie doll's cloud server has weak server side protection
  ○ Possible to steal personal information and listen in on conversations while the doll's talk button is pushed

{"lights":{"1":{"state":{"on":false,"bri":0,"alert":"none","reachable":false},"type
light","name":"Hue white lamp
1","modelid":"LWB006","manufacturername":"Philips","uniqueid":"00:17:88:01:02:08:67
":""},"2":{"state":{"on":false,"bri":1,"alert":"none","reachable":true},"type":"Dim
light","name":"Hue white lamp
2","modelid":"LWB006","manufacturername":"Philips","uniqueid":"00:17:88:01:02:09:18
":"5.38.1.15095"}},"groups":{"1":{"name":"........","lights":["2","1"],"type":"Roo
{"all_on":false,"any_on":false},"class":"Living room","action":{"on":false,"bri":
0,"alert":"none"}}},"config":{"name":"Philips hue","zigbeechannel":
15,"bridgeid":"001788FFFE2B9A25","mac":"00:17:88:2b:9a:
25","dhcp":true,"ipaddress":"192.168.1.159","netmask":"255.255.255.0","gateway":"19

Hue Light Bulb Control data

```
0000  d0 73 d5 01 83 08 ac bc  32 d4 6f 2f 08 00 45 00   .s...... 2.o/..E.
0010  00 4d 5b f6 00 00 40 11  99 f0 c0 a8 01 f3 c0 a8   .M[...@. ........
0020  01 76 ca c9 dd 7c 00 39  4d 46 31 00 00 34 00 00   .v...|.9 MF1..4..
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 66 00 00 00 00 55   ........ ..f....U
0050  55 ff ff ff 86 ac 0d 00  04 00 00                  U....... ...
```

Lifx Bulb Control data

(a)

(b)

Fig. 6. Energy management (a) persona, (b) cyber attack.

This makes it relatively easy for hackers to deduce when a user is at home, based on the binary state of the motion sensor. The TP-Link camera streams video/audio in plaintext (the video/audio header is human-readable even though its data doesn't seem so in Fig. 2(b)). This data can be sniffed by an attacker and then used to reassemble the video/audio data thus allowing them to view all the video and audio captured by the camera. Surprisingly, it is revealing not only the video and audio data but also the authentication password required for logging-in to the device – the password is exposed in the basic authentication field like "YWRtaW46WvdSdGFND0=" which is a Base64 encoded version of "admin/admin" that can easily be decoded. Using this credentials attacker can gain the full control of camera easily.

According to our rating shown in Fig. 3, we believe that customers of IoT home or business security devices are placing themselves at risk due to poor rating (i.e. red cells labeled as C) in confidentiality and access control. 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 various attacks. Unless these issues are addressed, IoT users are at even greater risk than those who have not invested in these devices.

B. Health Bundle

Fig. 4(a) illustrates the health persona. Joe and Lorna Jones live in Spring Hill, 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 intrudes a little 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). 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.

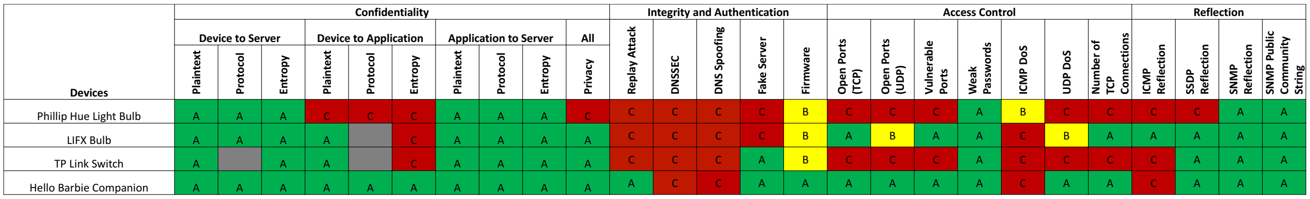
What they have

- 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

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 belong to J&L Jones of Spring Hill, Queensland.

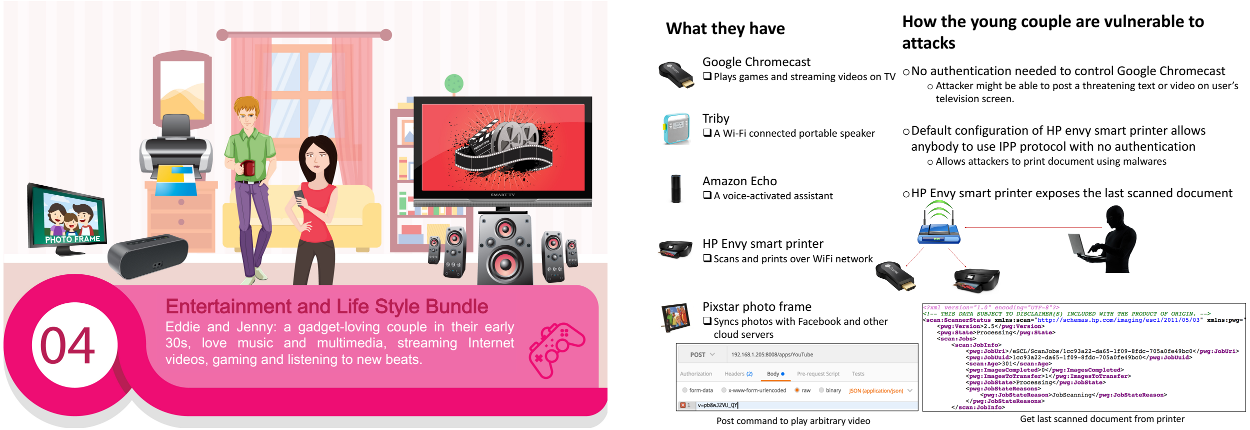
From his darkened 15th-floor apartment in Kuala Lumpur, Lee sends an email to all users that contains a link to an app that promises technology customers help with their finances. The app, however, has embedded malware that scouts for IoT devices. Lorna isn't sure what the email is about but thinks it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



Devices	Confidentiality										Integrity and Authentication					Access Control							Reflection			
	Device to Server			Device to Application			Application to Server			All																
	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Privacy	Replay Attack	DNSSEC	DNS Spoofing	Fake Server	Firmware	Open Ports (TCP)	Open Ports (UDP)	Vulnerable Ports	Weak Passwords	ICMP DoS	UDP DoS	Number of TCP Connections	ICMP Reflection	SSDP Reflection	SNMP Reflection	SNMP Public Community String
Phillip Hue Light Bulb	A	A	A	C	C	C	A	A	A	C	C	C	C	C	B	C	C	C	A	B	C	C	C	C	A	A
LIFX Bulb	A	A	A	A		C	A	A	A	A	C	C	C	C	B	A	B	A	A	C	B	A	A	A	A	A
TP Link Switch	A		A	A		C	A	A	A	A	C	C	C	A	B	C	C	C	A	C	C	C	C	A	A	A
Hello Barbie Companion	A	A	A	A	A	A	A	A	A	A	A	C	C	A	A	A	A	A	A	C	A	A	C	A	A	A

Fig. 7. Security rating for energy management persona



Entertainment and Life Style Bundle

Eddie and Jenny: a gadget-loving couple in their early 30s, love music and multimedia, streaming Internet videos, gaming and listening to new beats.

What they have

Google Chromecast
❑ Plays games and streaming videos on TV

Triby
❑ A Wi-Fi connected portable speaker

Amazon Echo
❑ A voice-activated assistant

HP Envy smart printer
❑ Scans and prints over WiFi network

Pixstar photo frame
❑ Syncs photos with Facebook and other cloud servers

How the young couple are vulnerable to attacks

- No authentication needed to control Google Chromecast
  - Attacker might be able to post a threatening text or video on user's television screen.
- Default configuration of HP envy smart printer allows anybody to use IPP protocol with no authentication
  - Allows attackers to print document using malwares
- HP Envy smart printer exposes the last scanned document

```
1 v=pb8wJ2VU_QY
```

Post command to play arbitrary video

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- THIS DATA SUBJECT TO DISCLAIMER(S) INCLUDED WITH THE PRODUCT OF ORIGIN. -->
<scan:ScannerStatus xmlns:scan="http://schemas.hp.com/imaging/escl/2011/05/03" xmlns:pwg="
    <pwg:Version>2.5</pwg:Version>
    <pwg:State>Processing</pwg:State>
    <scan:Jobs>
        <scan:JobInfo>
            <pwg:JobUri>/eSCL/ScanJobs/1cc93a22-da65-1f09-8fdc-705a0fe49bc0</pwg:JobUri>
            <pwg:JobUuid>1cc93a22-da65-1f09-8fdc-705a0fe49bc0</pwg:JobUuid>
            <scan:Age>301</scan:Age>
            <pwg:ImagesCompleted>0</pwg:ImagesCompleted>
            <pwg:ImagesToTransfer>1</pwg:ImagesToTransfer>
            <pwg:JobState>Processing</pwg:JobState>
            <pwg:JobStateReasons>
                <pwg:JobStateReason>JobScanning</pwg:JobStateReason>
            </pwg:JobStateReasons>
        </scan:JobInfo>
```

Get last scanned document from printer

(a) (b)

Fig. 8. Multimedia (a) persona, (b) cyber attack.

connected devices. Whenever he likes, Lee 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.

As shown in Fig. 4(b), Lee's malware is also able to sniff unencrypted messages sent 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 Jones' identity and take their social security benefits.

Overall, health monitoring IoT devices don't seem to have serious security problems as shown by our rating table in Fig. 5. Although they could be used to reflect attacks to other servers or networks. Most of them are susceptible to some form of reflection attack like ICMP, SSDP, SNMP. Meantime, the Awair air quality monitor could stop functioning if it is bombarded by a large amount of ICMP traffic.

C. Energy Management Bundle

Fig. 6(a) shows our chosen household with energy management bundle. Suresh and Veda Singh live in London, UK. 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.

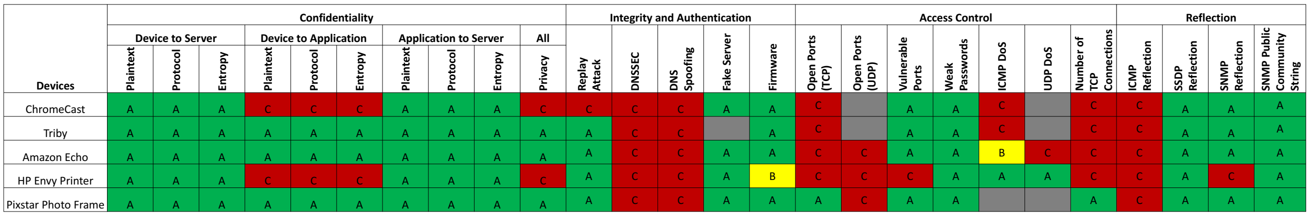
What they have

- 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

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 vocational-level computer 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 some devices. We note that Phillips Hue lightbulbs don't send encrypted messages as shown in Fig. 6(b). Juan, therefore, can easily read the current status of the bulb, or even send commands to the bulb using simple `POST` methods - turning it on/off, or changing its colour/brightness. Further, the mobile application of LiFX uses encoded UDP packets to control the LIFX bulb when they are on the same LAN, thus allowing Juan to decode LiFX messages with little efforts. Considering the Singhs' TP-Link power switch, the exchanged data is not in plaintext but its entropy value is fairly low suggesting that the traffic of the power switch could possibly be encoded or poorly encrypted. By guessing that the data is sent in JSON format (i.e. {data}), Juan attempts to XOR the first byte with the character "{" to obtain the single byte key. Juan then applies the key to



Devices	Confidentiality										Integrity and Authentication					Access Control							Reflection			
	Device to Server			Device to Application			Application to Server			All																
	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Privacy	Replay Attack	DNSSEC	DNS Spoofing	Fake Server	Firmware	Open Ports (TCP)	Open Ports (UDP)	Vulnerable Ports	Weak Passwords	ICMP DoS	UDP DoS	Number of TCP Connections	ICMP Reflection	SSDP Reflection	SNMP Reflection	SNMP Public Community String
ChromeCast	A	A	A	C	C	C	A	A	A	C	C	C	C	A	A	C		A	A	C		C	C	A	A	A
Triby	A	A	A	A	A	A	A	A	A	A	A	C	C		A	C		A	A	C		C	C	A	A	A
Amazon Echo	A	A	A	A	A	A	A	A	A	A	A	C	C	A	A	C	C	A	A	B	C	C	C	A	A	A
HP Envy Printer	A	A	A	C	C	C	A	A	A	C	A	C	C	A	B	C	C	C	A	A	A	C	C	A	C	A
Pixstar Photo Frame	A	A	A	A	A	A	A	A	A	A	A	C	C	A	A	A	C	A	A			A	C	A	A	A

Fig. 9. Security rating for multimedia persona

the encrypted message and is able to extract the message in plaintext. Using this weak encryption used in the TPLink power switch Juan is able to crack it easily.

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. Energy management IoT devices might be convenient to use but our evaluations show that they carry many inherent security flaws, as shown in Fig. 7 – they have poor integrity and access control measure as well as fairly poor access control. They can give savvy hackers an easy entry into a home - often via a simple transmitted demand.

D. Entertainment

Fig. 8(a) shows entertainment bundle of a couple. Eddie and Jenny are in their early 30s and are renting in a fashionable part of New York City. 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.

What they have

- 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

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/password on most of their devices: "admin"/"admin"). From here, Sven can use simple RESTful `GET` request to retrieve information on what videos they play via Google Chromecast he might even be able to `POST` a threatening text or video on their television screen since any YouTube contents can be played on the Chromecast by using the REST API as shown in Fig. 8(b).

He knows their printer is particularly vulnerable. He can print with no authentication by using Internet Printing Protocol given the print command message is crafted properly. In addition to that, Sven can see any documents they have scanned recently using the exposed system files, as shown in Fig. 8(b). The device has many open ports (9 TCP ports and 10 UDP ports) that aren't protected by any password, allowing an attacker an easy access. It also allows an attacker to print documents or stop others from printing entirely by keeping a connection to TCP port 9100.

According to our evaluation shown in Fig. 9, some of entertainment and lifestyle IoT devices (suc as Amazon Echo, Triby speaker, and Pixtar photo frame) seem fairly secure (rated as good and labeled green A in many criteria) . However, The chromecast and HP printer exhibit serious vulnerabilities (poor rated in confidentiality and integrity) .

IV. 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 experimental evaluation, 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 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 paper, in conjunction with anecdotal evidence in the media, clearly exposes the real large-scale lack of security in smart-home IoT devices. We believe that our findings can set the platform to inform consumers, suppliers, regulators and insurers of IoT devices to develop appropriate methods to tackle the problem.

References

[1] Cisco Systems. (2016) Visual networking index (VNI). http://www.cisco.com/.

[2] TRAPX Security. (July 2014) TRAPX discovers Zombie Zero advanced persistent malware. https://trapx.com/trapxdiscovers-zombie-zero-advanced-persistent-malware/.

[3] N. Dhanjani, *Abusing the Internet of Things*, 2015.

[4] E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," in *Proc. IEEE Symposium on Security and Privacy (SP)*, May 2016.

[5] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in *Proc. IEEE Conference on Communications and Network Security*, San Francisco, USA, Oct 2014.

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

[7] Techradar. (Jan 2017) 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.

[8] KerbsOnSecurity. (Oct 2016) Hacked cameras, DVRs powered todays massive internet outage. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

[9] M. Lyu, D. Sherratt, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Qantifying the Reflective DDoS Attack Capability of Household IoT Devices," in *Proc. ACM WiSec*, Jul 2017.

[10] Shodan. https://www.shodan.io/.

[11] Insecam. http://www.insecam.org/.