Internet of Things

Security

Oskar Wieczorek

Institute of Computer Science, University of Wroclaw

December 12, 2018

Agenda

1. Agenda

2. 7 IoT security failures

3. 7 IoT security challenges

4. 6 IoT good security practices

7 IoT security failures

7 IoT security failures

1. Dyn cyberattack

7 IoT security failures

1. Dyn cyberattack

- October 21, 2016

7 IoT security failures

1. Dyn cyberattack

- October 21, 2016
- DDoS attack on systems operated by DNS provider Dyn

7 IoT security failures

1. Dyn cyberattack

- October 21, 2016
- DDoS attack on systems operated by DNS provider Dyn
- accomplished by requests from IoT devices botnet that had been infected with the Mirai malware

7 IoT security failures

1. Dyn cyberattack

- October 21, 2016
- DDoS attack on systems operated by DNS provider Dyn
- accomplished by requests from IoT devices botnet that had been infected with the Mirai malware
- Anonymous and New World Hackers (?), "an angry gamer" (*Forbes*), "script kiddies" (*FlashPoint*)

7 IoT security failures

1. Dyn cyberattack

Figure: Various devices targeted by Mirai malware

7 IoT security failures

1. Dyn cyberattack

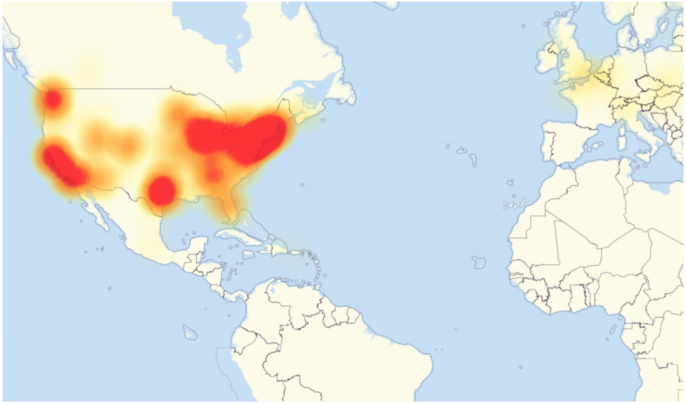


Figure: Map of areas most affected by attack

7 IoT security failures

1. Dyn cyberattack

Services affected by the attack:

AirBnb
Amazon.com
Ancestry.com
The A.V. Club
BBC
The Boston Globe
Box
Business Insider
CNN
Comcast
CrunchBase
DirecTV
The Elder Scrolls Online
Electronic Arts
Etsy
FiveThirtyEight
Fox News
The Guardian
GitHub
Grubhub
HBO
Heroku
HostGator
iHeartRadio
Imgur
Indiegogo
Mashable
National Hockey League
Netflix
The New York Times
Overstock.com
PayPal
Pinterest
Pixlr
PlayStation Network
Qualtrics
Quora
Reddit
Roblox
Ruby Lane
RuneScape
SaneBox
Seamless
Second Life
Shopify
Slack
SoundCloud
Squarespace
Spotify
Starbucks
Storify
Swedish Civil Contingencies Agency
Swedish Government
Tumblr
Twilio
Twitter
Verizon Communications
Visa
Vox Media
Walgreens
The Wall Street Journal
Wikia
Wired
Wix.com
WWE Network
Xbox Live
Yammer
Yelp
Zillow

7 IoT security failures

1. Dyn cyberattack

Mirai – modus operandi

1. Locate and compromise IoT devices to further grow the botnet.

7 IoT security failures

1. Dyn cyberattack

Mirai – modus operandi

1. Locate and compromise IoT devices to further grow the botnet.
2. Launch DDoS attacks based on instructions received from a remote C&C.

7 IoT security failures

1. Dyn cyberattack

Mirai – default passwords list:

root xc3511
root vizxv
root admin
admin admin
root 888888
root xmhdipc
root default
root juantech
root 123456
root 54321
support support
root (none)
admin password
root root
root 12345
user user

admin (none)
root pass
admin admin1234
root 1111
admin smcadmin
admin 1111
root 666666
root password
root 1234
root klv123
Administrator admin
service service
supervisor supervisor
guest guest
guest 12345
guest 12345

admin1 password
administrator 1234
666666 666666
888888 888888
ubnt ubnt
root klv1234
root Zte521
root hi3518
root jvbzd
root anko
root zlxx.
root 7ujMko0vizxv
root 7ujMko0admin
root system
root ikwb
root dreambox

root user
root realtek
root 00000000
admin 1111111
admin 1234
admin 12345
admin 54321
admin 123456
admin 7ujMko0admin
admin 1234
admin pass
admin meinsm
tech tech
mother fer**

7 IoT security failures

1. Dyn cyberattack

Mirai – user-agents:

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7

7 IoT security failures

1. Dyn cyberattack

Mirai – "Don't Mess With" List:

127.0.0.0/8 - Loopback
0.0.0.0/8 - Invalid address space
3.0.0.0/8 - General Electric (GE)
15.0.0.0/7 - Hewlett-Packard (HP)
56.0.0.0/8 - US Postal Service
10.0.0.0/8 - Internal network
192.168.0.0/16 - Internal network
172.16.0.0/14 - Internal network
100.64.0.0/10 - IANA NAT reserved
169.254.0.0/16 - IANA NAT reserved
198.18.0.0/15 - IANA Special use

224.*.*.*+ - Multicast
6.0.0.0/7 - Department of Defense
11.0.0.0/8 - Department of Defense
21.0.0.0/8 - Department of Defense
22.0.0.0/8 - Department of Defense
26.0.0.0/8 - Department of Defense
28.0.0.0/7 - Department of Defense
30.0.0.0/8 - Department of Defense
33.0.0.0/8 - Department of Defense
55.0.0.0/8 - Department of Defense
214.0.0.0/7 - Department of Defense

7 IoT security failures

1. Dyn cyberattack

Mirai – a territorial predator

The following scripts close all processes that use SSH, Telnet and HTTP ports:

```
killer_kill_by_port(htons(23)) // Kill telnet service
killer_kill_by_port(htons(22)) // Kill SSH service
killer_kill_by_port(htons(80)) // Kill HTTP service
```

7 IoT security failures

1. Dyn cyberattack

Mirai – a territorial predator

```
table_unlock_val(TABLE_KILLER_ANIME);
// If path contains ".anime" kill.
if (util_stristr(realpath, rp_len - 1, table_retrieve_val(TABLE_KILLER_ANIME, NULL)) != -1)
{
    unlink(realpath);
    kill(pid, 9);
}
table_lock_val(TABLE_KILLER_ANIME);
```

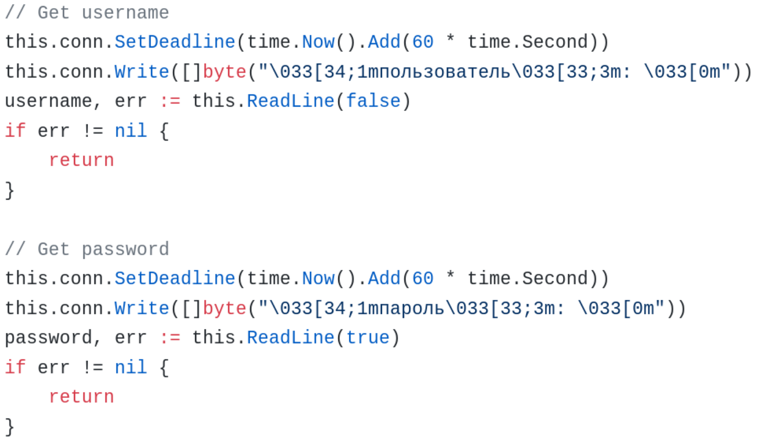
Goals:

1. Help Mirai maximize the attack potential of the botnet devices.
2. Prevent similar removal attempts from other malware.

7 IoT security failures

1. Dyn cyberattack

Mirai – trace amounts of Cyryllic



```
// Get username
this.conn.SetDeadline(time.Now().Add(60 * time.Second))
this.conn.Write([]byte("\033[34;1mпользователь\033[33;3m: \033[0m"))
username, err := this.ReadLine(false)
if err != nil {
    return
}

// Get password
this.conn.SetDeadline(time.Now().Add(60 * time.Second))
this.conn.Write([]byte("\033[34;1mпароль\033[33;3m: \033[0m"))
password, err := this.ReadLine(true)
if err != nil {
    return
}
```

7 IoT security failures

2. Chrysler's UConnect hack

7 IoT security failures

2. Chrysler's UConnect hack

- in 2015 two hackers Charlie Miller and Chris Valasek hacked 2014 Jeep Cherokee using 0-day vulnerability

7 IoT security failures

2. Chrysler's UConnect hack

- in 2015 two hackers Charlie Miller and Chris Valasek hacked 2014 Jeep Cherokee using 0-day vulnerability
- the hackers targeted the Uconnect board computer using WiFi

7 IoT security failures

2. Chrysler's UConnect hack

- in 2015 two hackers Charlie Miller and Chris Valasek hacked 2014 Jeep Cherokee using 0-day vulnerability
- the hackers targeted the Uconnect board computer using WiFi
- the results were announced at the Black Hat USA 2015 security conference

7 IoT security failures

2. Chrysler's UConnect hack

- in 2015 two hackers Charlie Miller and Chris Valasek hacked 2014 Jeep Cherokee using 0-day vulnerability
- the hackers targeted the Uconnect board computer using WiFi
- the results were announced at the Black Hat USA 2015 security conference
- after issuing a patch Chrysler announced a recall for 1.4 million vehicles

7 IoT security failures

2. Chrysler’s UConnect hack

7 IoT security failures

2. Chrysler's UConnect hack

Breaking into WiFi:

- the Wi-Fi password is generated automatically, based on the time when the car and it's multimedia system — the head unit — is turned on for the very first time.

7 IoT security failures

2. Chrysler's UConnect hack

Breaking into WiFi:

- the Wi-Fi password is generated automatically, based on the time when the car and it's multimedia system — the head unit — is turned on for the very first time.
- moreover it turned out that Chrysler's cars is generated before the actual time and date is set and is based on default system time plus a few seconds during which the head unit boots up.

7 IoT security failures

2. Chrysler's UConnect hack

Breaking into WiFi:

- the Wi-Fi password is generated automatically, based on the time when the car and it's multimedia system — the head unit — is turned on for the very first time.
- moreover it turned out that Chrysler's cars is generated before the actual time and date is set and is based on default system time plus a few seconds during which the head unit boots up.
- hackers were left with a few dozens passwords to check

7 IoT security failures

2. Chrysler's UConnect hack

Taking control over the car:

- ECU sends messages at regular interval

7 IoT security failures

2. Chrysler's UConnect hack

Taking control over the car:

- ECU sends messages at regular interval
- if the hacker injects a fake message, the ECU temporarily disables non-critical systems (multimedia, speedometers, locks, etc.)

7 IoT security failures

2. Chrysler's UConnect hack

Taking control over the car:

- ECU sends messages at regular interval
- if the hacker injects a fake message, the ECU temporarily disables non-critical systems (multimedia, speedometers, locks, etc.)
- the hackers also hacked into Parking Assist Module

7 IoT security failures

3. Washington DC CCTV system hack

7 IoT security failures

3. Washington DC CCTV system hack

- 9-12 January 2017

7 IoT security failures

3. Washington DC CCTV system hack

- 9-12 January 2017
- James Graham, Mihai Alexandru Isvanca and Eveline Cismaru

7 IoT security failures

3. Washington DC CCTV system hack

- 9-12 January 2017
- James Graham, Mihai Alexandru Isvanca and Eveline Cismaru
- 123 of the 187 cameras used by the Metropolitan Police Department of the District of Columbia

7 IoT security failures

3. Washington DC CCTV system hack

- 9-12 January 2017
- James Graham, Mihai Alexandru Isvanca and Eveline Cismaru
- 123 of the 187 cameras used by the Metropolitan Police Department of the District of Columbia
- the internet-connected computers behind the cameras were sending "ransomware-laden spam emails"

7 IoT security failures

3. Washington DC CCTV system hack

- 9-12 January 2017
- James Graham, Mihai Alexandru Isvanca and Eveline Cismaru
- 123 of the 187 cameras used by the Metropolitan Police Department of the District of Columbia
- the internet-connected computers behind the cameras were sending "ransomware-laden spam emails"
- the attack was halted on 12 January after the MPDC's IT network administrator discovered that multiple cameras had been disabled.

7 IoT security failures

4. Samsung smart TVs

7 IoT security failures

4. Samsung smart TVs

- 2015

7 IoT security failures

4. Samsung smart TVs

- 2015
- It turned out that some Samsung smart TVs are sending users' voice searches and data over the internet unencrypted, allowing hackers and snoopers to listen in on their activity. It had been believed that the information was encrypted.

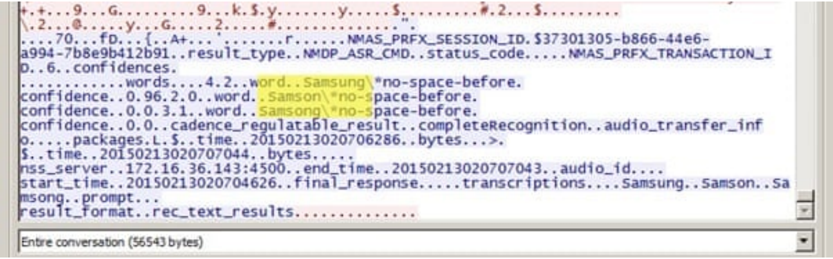
7 IoT security failures

4. Samsung smart TVs

- 2015
- It turned out that some Samsung smart TVs are sending users' voice searches and data over the internet unencrypted, allowing hackers and snoopers to listen in on their activity. It had been believed that the information was encrypted.
- In some Samsung models, neither the audio, nor the text returned was encrypted.

7 IoT security failures

4. Samsung smart TVs



```
+.+...9...G.........9...k.$.y.......y.....$..........#.2...$.........
\.2...@.....y...G.....2.....#..............".
....70...fD...{..A+...'........r......NMAS_PRFX_SESSION_ID.$37301305-b866-44e6-
a994-7b8e9b412b91..result_type..NMDP_ASR_CMD..status_code.....NMAS_PRFX_TRANSACTION_I
D..6..confidences.
............words....4.2..word..Samsung\*no-space-before.
confidence..0.96.2.0..word..Samson\*no-space-before.
confidence..0.0.3.1..word..Samsong\*no-space-before.
confidence..0.0..cadence_regulatable_result..completeRecognition..audio_transfer_inf
o.....packages.L.$..time..20150213020706286..bytes...>.
$..time..20150213020707044..bytes.....
nss_server..172.16.36.143:4500..end_time..20150213020707043..audio_id....
start_time..20150213020704626..final_response.....transcriptions....Samsung..Samson..Sa
msong..prompt...
result_format..rec_text_results..............
```

Entire conversation (56543 bytes)

Figure: Text send without encryption as a result of voice recognition of the word "Samsung"

7 IoT security failures

4. Samsung smart TVs

> *”Samsung takes consumer privacy very seriously and our products are designed with privacy in mind. Our latest Smart TV models are equipped with data encryption and a software update will soon be available for download on other models.”*
>
> Samsung spokesman

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

- 2016/2017

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

- 2016/2017
- the doll "My friend Cayla" claimed to be the first world interactive doll

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

- 2016/2017
- the doll "My friend Cayla" claimed to be the first world interactive doll
- the doll is equipped with a microphone, bluetooth connection, and Internet access

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

- 2016/2017
- the doll ”My friend Cayla” claimed to be the first world interactive doll
- the doll is equipped with a microphone, bluetooth connection, and Internet access
- it was revealed that that the communications between the Cayla doll and the parent's app were not sufficiently protected

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

- 2016/2017
- the doll "My friend Cayla" claimed to be the first world interactive doll
- the doll is equipped with a microphone, bluetooth connection, and Internet access
- it was revealed that that the communications between the Cayla doll and the parent's app were not sufficiently protected
- child recordings were sold to third-parties for targeted advertising

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

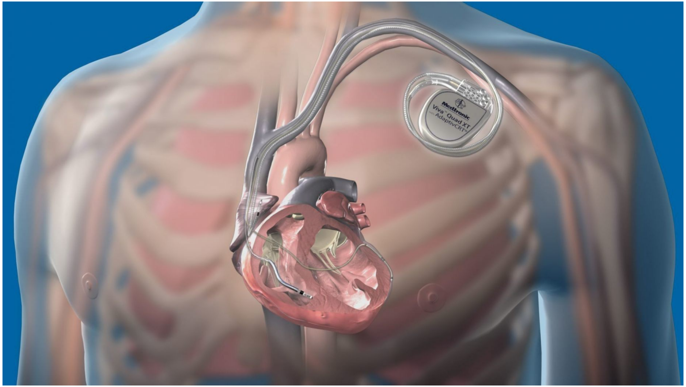
- 2016/2017
- the doll ”My friend Cayla” claimed to be the first world interactive doll
- the doll is equipped with a microphone, bluetooth connection, and Internet access
- it was revealed that that the communications between the Cayla doll and the parent’s app were not sufficiently protected
- child recordings were sold to third-parties for targeted advertising
- the doll was banned in Germany and the parents were told to destroy the dolls

7 IoT security failures

5. My Friend Cayla - The Internet of Toys

7 IoT security failures

6. Connected cardiac devices



7 IoT security failures

6. Connected cardiac devices & insulin pumps

- 2012

7 IoT security failures

6. Connected cardiac devices & insulin pumps

- 2012
- FDA (Food and Drug Administration) confirmed that St. Jude cardiac devices have vulnerabilities that could allow a hacker to access a device

7 IoT security failures

6. Connected cardiac devices & insulin pumps

- 2012
- FDA (Food and Drug Administration) confirmed that St. Jude cardiac devices have vulnerabilities that could allow a hacker to access a device
- a hacker could potentially deplete the battery or administer incorrect pacing

7 IoT security failures

- 2011

7 IoT security failures

- 2011
- Barnaby Jack (researcher at McAffee) hacked his insulin pump using an Arduino module that cost less than $20. to access a device.

7 IoT security failures

- 2011
- Barnaby Jack (researcher at McAffee) hacked his insulin pump using an Arduino module that cost less than $20. to access a device.
- In April 2012 Jack demonstrated a system that could scan for and compromise insulin pumps that communicate wirelessly. With a push of a button on his laptop, he could have any pump within 300 feet dump its entire contents, without even needing to know the device identification numbers.

7 IoT security failures

- 2011
- Barnaby Jack (researcher at McAffee) hacked his insulin pump using an Arduino module that cost less than $20. to access a device.
- In April 2012 Jack demonstrated a system that could scan for and compromise insulin pumps that communicate wirelessly. With a push of a button on his laptop, he could have any pump within 300 feet dump its entire contents, without even needing to know the device identification numbers.
- In July 2013 Jack died a week before he was to give a presentation on hacking heart implants. According to the coroner's report, Jack died of an overdose of drugs.

7 IoT security failures

7. Hackable Sniper Rifles

7 IoT security failures

7. Hackable Sniper Rifles

7 IoT security challenges

7 IoT security challenges

1. Insufficient testing and updating

Companies are too careless when it comes to handling of device-related security risks. Most of these devices and IoT products don't get enough updates while, some don't get updates at all. Early computer systems had this same problem, which was somewhat solved with automatic updates. IoT manufacturers, however, are more eager to produce and deliver their devices as fast as they can, without giving security too much of a thought.

7 IoT security challenges

2. Brute-forcing and the issue of default passwords

Example: Mirai.

7 IoT security challenges

3. IoT malware and ransomware

Traditional ransomware used to encrypt or lock user's data and ask for a ransom.
In IoT: a hybrid of both malware and ransomware.
Example: IP cameras.

7 IoT security challenges

4. IoT botnets aiming at cryptocurrency

The open-source cryptocurrency Monero is one of the many digital currencies currently being mined with IoT devices.

7 IoT security challenges

5. Data security and privacy concerns (mobile, web, cloud)

Example: Samsung smart TVs issue.

7 IoT security challenges

6. Small IoT attacks that evade detection

Instead of using the big guns, hackers will most likely be using subtle attack small enough to let the information leak out instead of just grabbing millions and millions of records at once.

7 IoT security challenges

7. AI and automation

Using autonomous systems to make autonomous decisions that affect millions of functions across large infrastructures such as healthcare, power and transportation might be too risky, especially once you consider that it only takes a single error in the code or a misbehaving algorithm to bring down the entire infrastructure.

6 IoT good security practices

6 IoT good security practices

1. Authentication

Never create a product with a default password which is the same across all devices. Each device should have a complex random password assigned to it during manufacturing.

6 IoT good security practices

2. Debug

Never leave any kind of debugging access on a production device. Even if you are tempted to leave access on a non-standard port using a hard-coded random password, in the end it will be discovered. Don't do it.

6 IoT good security practices

3. Encryption

All communications between an IoT device and the cloud need to be encrypted. Use SSL/TLS where appropriate.

6 IoT good security practices

4. Privacy

Ensure that no personal data (including things like WiFi passwords) is readily accessible should a hacker gain access to the device. Use encryption for storing data along with salts.

6 IoT good security practices

5. Web Interface

Any web interface should be protected against the standard hacker techniques like SQL injections and cross-site scripting.

6 IoT good security practices

6. Firmware updates

Bugs are a fact of life, often they are just a nuisance. However security bugs are bad, even dangerous. Therefore all IoT devices should support Over-The-Air (OTA) updates. However those updates need to be verified before applied.

The end

Thank you for listening!