IoT, S stands for security

HackDay UdG

17 de febrer de 2018

Index

HACKING LLIURE

Index

HACKING LLIURE

About us

Hacking Lliure (@HackingLliure)

- Ethical and social aspects of infosec
- Use and creation of FLOSS
- Technical workshops and talks in wireless security, passwords, RE, stego, IoT...

HACKING LLIURE

About us

Hacking Lliure (@HackingLliure)

- Ethical and social aspects of infosec
- Use and creation of FLOSS
- Technical workshops and talks in wireless security, passwords, RE, stego, IoT...

HACKING LLIURE

About us

Hacking Lliure (@HackingLliure)

- Ethical and social aspects of infosec
- Use and creation of FLOSS
- Technical workshops and talks in wireless security, passwords, RE, stego, IoT...

HACKING LLIURE

About us

Gerard Finol (@GerardFinol)

- Maths + Info at UB
- Co-Founder of Hacking Lliure
- gerard@hackinglliure.org

Arnau Gàmez (@arnaugamez)

- Maths + Info at UB
- President and Co-Founder of Hacking Lliure
- arnau@hackinglliure.org

HACKING LLIURE

Index

HACKING LLIURE

What is IoT?

The **Internet of Things (IoT)** is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.

What is IoT?

Internet of Shit
@internetofshit

Siguiendo

2015: why not put a chip in that thing
2017: fuck it, put a chip in it

HACKING LLIURE

Let’s see some examples...

HACKING LLIURE

Let's see some examples...

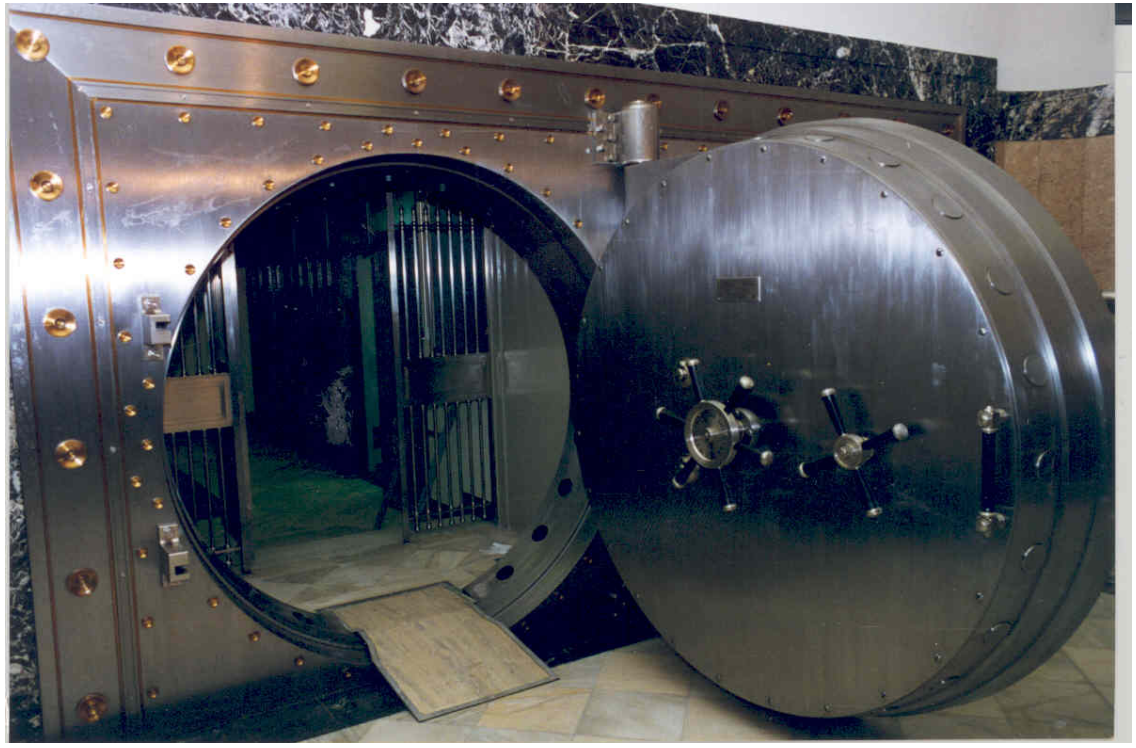
HACKING LLIURE

Index

HACKING LLIURE

What about security in IoT?

You may be thinking of something like. . .



HACKING LLIURE

What about security in IoT?

You may be thinking of something like. . .

HACKING LLIURE

What about security in IoT?

But it is more like...

HACKING
LLIURE

Index

HACKING LLIURE

Teddy Bear

https://motherboard.vice.com/

HACKING LLIURE

Cayla

Banned In Germany: Kids' Doll Is Labeled An Espionage Device

February 17, 2017 · 11:51 AM ET

BILL CHAPPELL

https://www.npr.org/sections/thetwo-way/2017/02/17/515775874/banned-in-germany-kids-doll-is-labeled-an-espionage-device

Mirai botnet

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Mirai botnet

Unlike other botnets, which are typically made up of computers, the Mirai botnet is largely made up of so-called "internet of things" (IoT) devices such as digital cameras and DVR players.

Because it has so many internet-connected devices to choose from, attacks from Mirai are much larger than what most DDoS attacks could previously achieve. Dyn estimated that the attack had involved "100,000 malicious endpoints", and the company, which is still investigating the attack, said there had been reports of an extraordinary attack strength of 1.2Tbps.

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

HACKING LLIURE

Jeep car

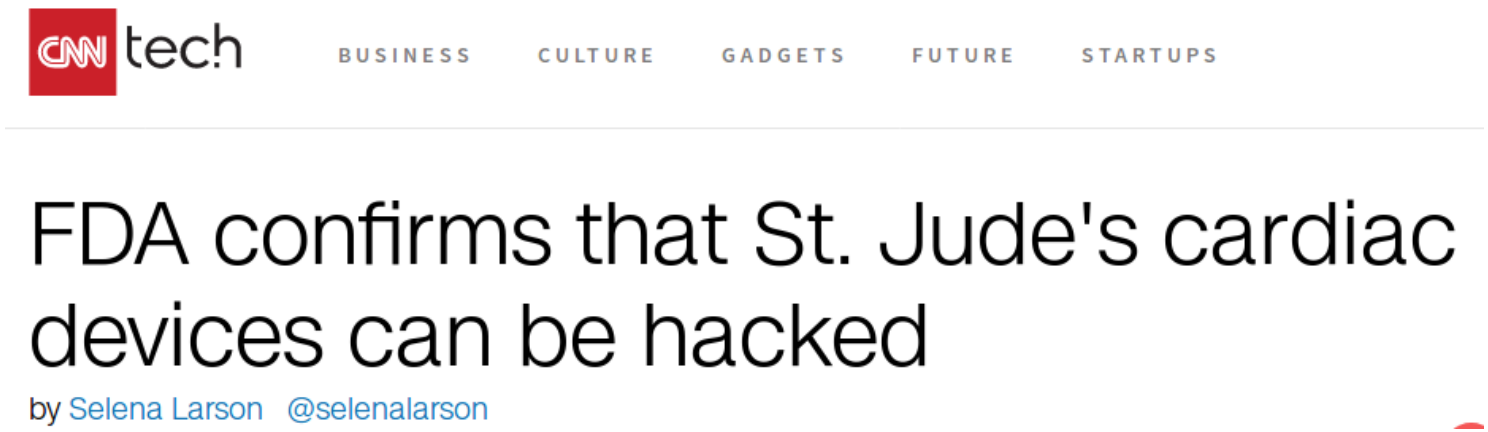
Black Hat USA 2015: The full story of how that Jeep was hacked

August 6, 2015

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

HACKING LLIURE

Cardiac devices



money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/

HACKING LLIURE

Sex toy

SEC Consult SA-20180201-0 :: Multiple critical vulnerabilities in Whole Vibratissimo Smart Sex Toy product range

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Thu, 1 Feb 2018 11:30:22 +0100

```
We have published an accompanying blog post to this technical advisory with
further information:

https://www.sec-consult.com/en/blog/2018/02/internet-of-dildos-a-long-way-to-a-vibrant-future-from-iot-to-iod/index.html
```

http://seclists.org/fulldisclosure/2018/Feb/0

HACKING LLIURE

Sex toy

1) Customer Database Credential Disclosure
The credentials for the whole Vibratissimo database environment were exposed on the internet. Due to the fact, that the PHPMyAdmin interface was exposed as well, an attacker could have been able to connect to the database and dump the whole data set. The dataset contains for example the following data:

- Usernames
- Session Tokens
- Cleartext passwords
- chat histories
- explicit image galleries, which are created by the users themselves

http://seclists.org/fulldisclosure/2018/Feb/0

HACKING LLIURE

Sex toy

```
3) Cleartext Storage of Passwords
The user passwords were stored unhashed in cleartext in the database.
If an attacker gained access to the database (e.g. via credential disclosure),
he could have been able to retrieve the plaintext passwords of users and abuse
their privileges in the system.


4) Unauthenticated Bluetooth LE Connections
The sex toys are connected without prior authentication to the app, which is the
standard use case. For example one of the identified Bluetooth services allows
to read the current device temperature. Other services, which can be
accessed without prior authentication are:

-) Setting the "intensity" of the current vibration pattern
-) Reading various values (Temperature, etc)
```

http://seclists.org/fulldisclosure/2018/Feb/0

HACKING LLIURE

Samsung's smart TV

Samsung's Tizen OS is apparently full of security holes, 'the worst code I've ever seen'

Ben Schoon - Apr. 4th 2017 6:31 am PT @NexusBen

https://9to5google.com/2017/04/04/samsung-tizen-security-holes/

HACKING LLIURE

Samsung's smart TV

Don't talk in front of your smart TV – it may be listening

Staff Writer 9 February 2015 28 Comments

0 shares

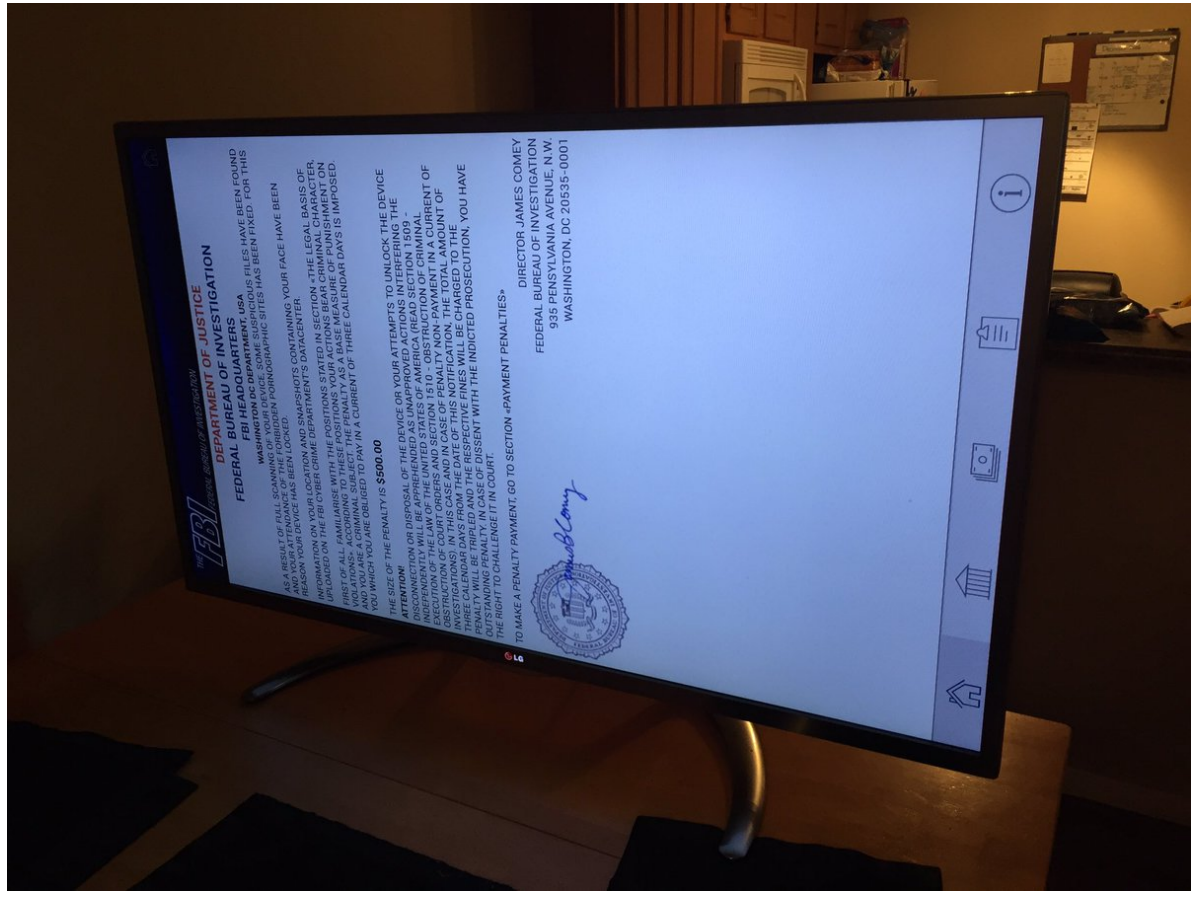
Email address Subscribe

Samsung is warning its customers not to talk about personal information in front of their smart TV, as the device may be "listening" to the conversation.

https://mybroadband.co.za/news/security/118471-dont-talk-in-front-of-your-smart-tv-it-may-be-listening.html

HACKING LLIURE

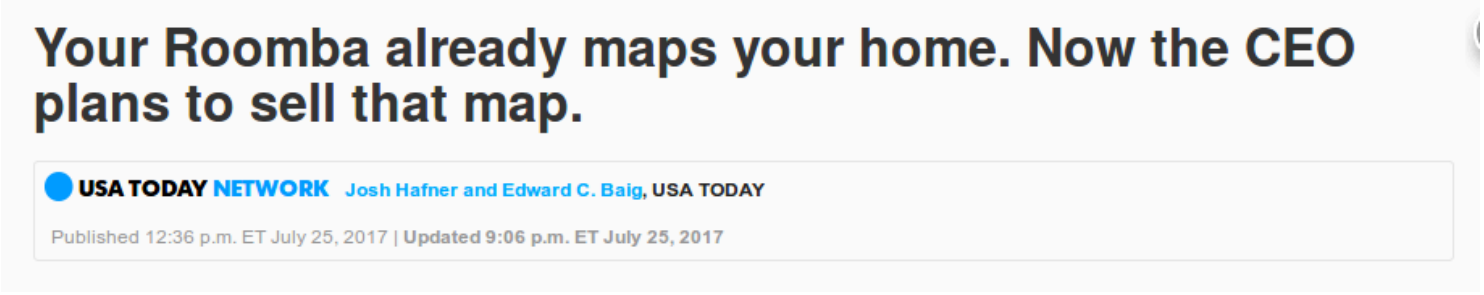
Ransomware



https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/

HACKING LLIURE

Roomba



Your Roomba already maps your home. Now the CEO plans to sell that map.

USA TODAY NETWORK Josh Hafner and Edward C. Baig, USA TODAY

Published 12:36 p.m. ET July 25, 2017 | **Updated 9:06 p.m. ET July 25, 2017**

https://www.usatoday.com/story/tech/nation-now/2017/07/25/roomba-plans-sell-maps-users-homes/508578001/

HACKING LLIURE

Index

HACKING LLIURE

General Approach & Workflow

What is Shodan?

SHODAN

HACKING LLIURE

Index

HACKING LLIURE

What about UdG's IoT?

HACKING LLIURE

Let’s play

HACKING
LLIURE

Index

HACKING LLIURE

Conclusions

- No security standards or regulation
- IoT fever cared about $$ and not security
- People keeps reusing passwords and not changing default credentials

HACKING LLIURE

Conclusions

- No security standards or regulation
- IoT fever cared about $$ and not security
- People keeps reusing passwords and not changing default credentials

Conclusions

- No security standards or regulation
- IoT fever cared about $$ and not security
- People keeps reusing passwords and not changing default credentials

Conclusions

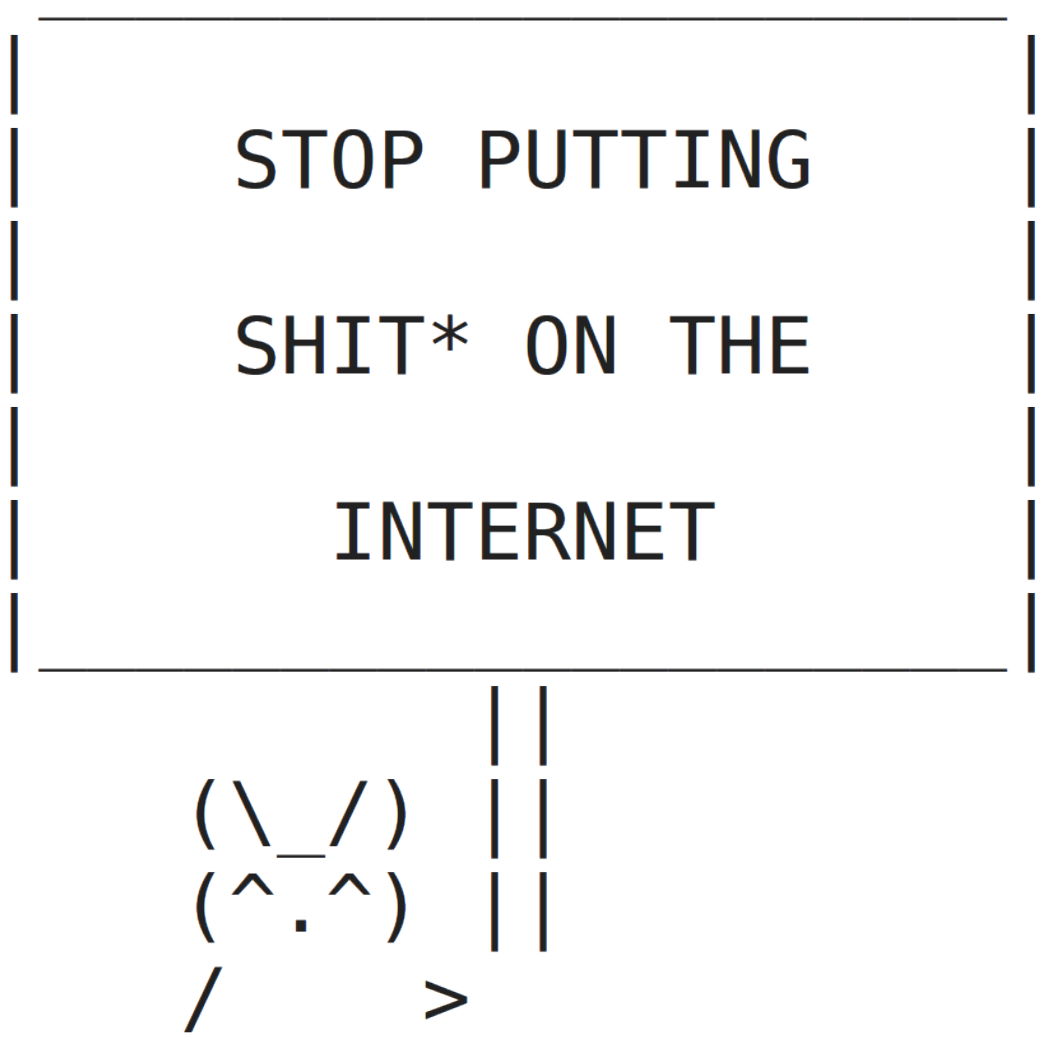
- No security standards or regulation
- IoT fever cared about $$ and not security
- People keeps reusing passwords and not changing default credentials

Security by default > Optional security > No security at all

IoT

HACKING LLIURE

Conclusions



HACKING LLIURE

Thank you

HACKING
LLIURE

Q&A

HACKING
LLIURE

https://hackinglliure.org

@HackingLliure

info@hackinglliure.com

HACKING
LLIURE