

Internet-of-~~broken~~-Things

A highly-opinionated overview

[0x73] - The Meet

Øx O P O S Æ C Møætup

April 23, 2019

\$ whoami

- Porto, Portugal
- Invited Assistant Lecturer @FEUP
- Research @FEUP / @INESC TEC
- PhD Student @FEUP

- jpdias.me
- keybase.com/jpdias
- jpmdias@fe.up.pt || jpdias@pm.me

My last talk @ Øx O P O S Æ C

[0x33] April 28, 2016

*A hands-on approach on botnets
for a learning purpose*

What the hell is going on?

The Hacker News 🔍

🏠 Home ✉️ Subscribe 🛒 Deals

Internet-Connected Medical Washer-Disinfector Found Vulnerable to Hacking

📅 March 27, 2017 👤 Swati Khandelwal



Washer-Disinfectors for Surgical Instruments

WIRED SUBSCRIBE

KIM ZETTER SECURITY 02.07.12 02:34 PM

FLAW IN HOME SECURITY CAMERAS EXPOSES LIVE FEEDS TO HACKERS



The Hacker News 🔍 ☰

Someone Hacked 50,000 Printers to Promote PewDiePie YouTube Channel

📅 December 01, 2018 👤 Mohit Kumar



THE INTERNET OF HACKABLE THINGS | By Lorenzo Franceschi-Bicchieral | Feb 27 2017, 9:00pm

Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings

A company that sells “smart” teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

ZDNet 🔍 MENU 👤 EU

Google says 'hidden' microphone in Nest product never intended to be a secret

An error it may be, but invasive it certainly is.

👤 By Charlie Osborne for Zero Day | February 21, 2019 -- 11:22 GMT (11:22 GMT) | Topic: Security

What the hell is going on?

FAST COMPANY

TECH | WORK LIFE | CREATIVITY | IMPACT | AUDIO | VIDEO

08.14.13 | THE CODE WAR

An Easy Exploit Could Leave Philips Hue “Smart Light” Owners In The Dark

TY CAME TO HACKER



The Hacker News

Home | Subscribe

Mirai Variant Adds Dozen New Exploits to Target Enterprise IoT Devices

March 19, 2019 | Swati Khandelwal

npr | SIGN IN | NPR SHOP | DONATE

NEWS | ARTS & LIFE | MUSIC | SHOWS & PODCASTS | SEARCH

AMERICA

S.C. Mom Says Baby Monitor Was Hacked; Experts Say Many Devices Are Vulnerable

June 5, 2018 · 7:18 PM ET

CAMILA DOMONOSKE

leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

let | MENU | EU

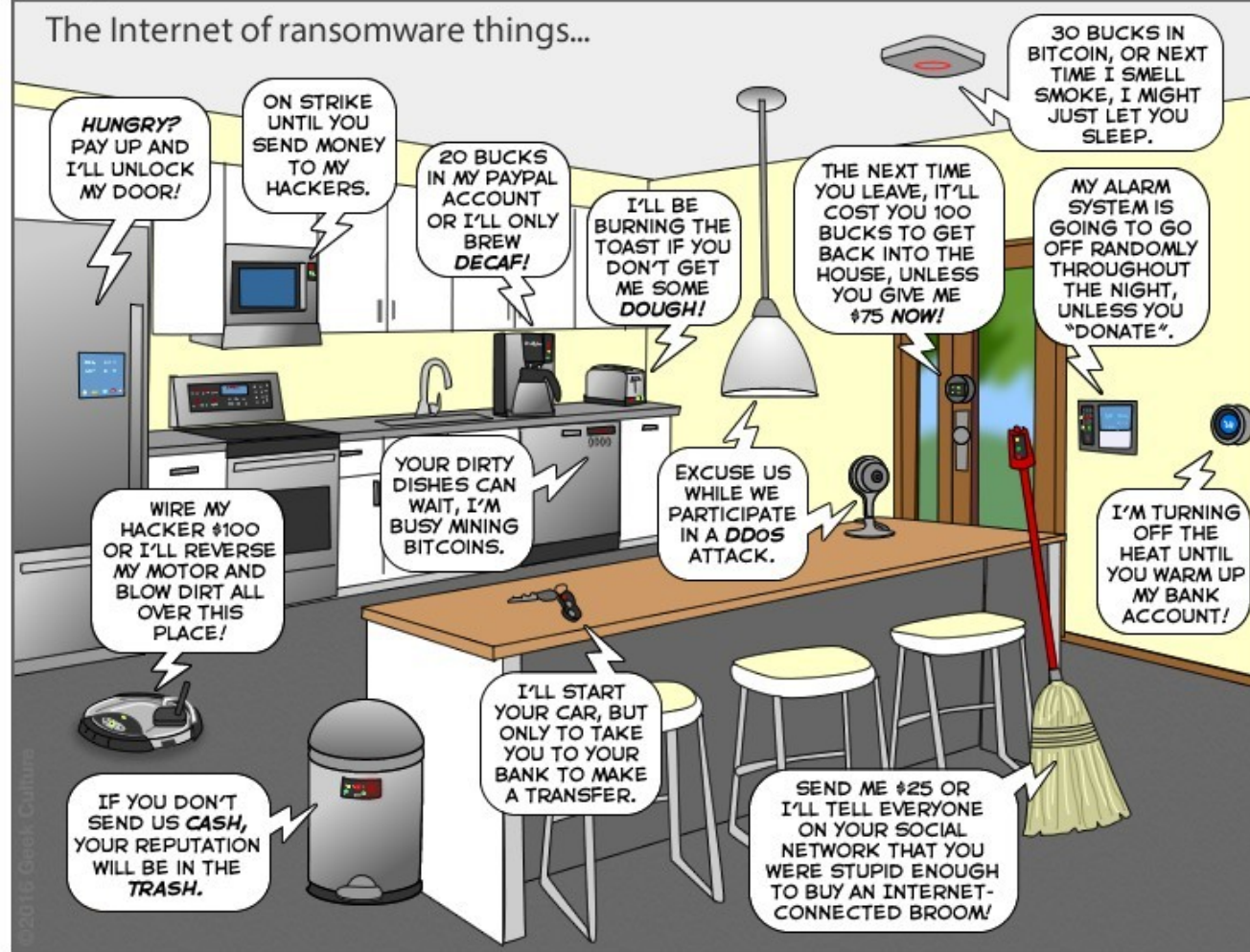
ZDNet | MENU | EU

Shodan search exposes insecure SCADA systems

Hackers are using the Shodan computer search engine to find Internet-facing SCADA systems using potentially insecure mechanisms for authentication and authorization.

By Ryan Naraine for Zero Day | November 2, 2010 -- 07:44 GMT (07:44 GMT) | Topic: Servers

The Internet of ransomware things...



You can help us keep the comics coming by becoming a patron!
www.patreon.com/joyoftech

joyoftech.com

Why is this risk real?

OWASP opinion



OWASP TOP 10

INTERNET OF THINGS 2018

1

Weak, Guessable, or Hardcoded Passwords

Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.



2

Insecure Network Services

Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...



3

Insecure Ecosystem Interfaces

Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.



4

Lack of Secure Update Mechanism

Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.



5

Use of Insecure or Outdated Components

Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.





OWASP TOP 10

INTERNET OF THINGS 2018

6

Insufficient Privacy Protection

User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.



7

Insecure Data Transfer and Storage

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.



8

Lack of Device Management

Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.



9

Insecure Default Settings

Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.



10

Lack of Physical Hardening

Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.



Examples in the wild (Portugal Edition)

- MQTT Connection Code: 0
 - 108 results
 - <https://github.com/Teserakt-io/mqttinfo>
- Xiaomi Devices (MiBox)
 - 20 results
- Home Assistant (<https://www.home-assistant.io/>)
 - 18 results
 - Mostly HTTP
- Domoticz (<http://www.domoticz.com/>)
 - 5 results
- OpenHAB (<https://www.openhab.org/>)
 - Uses Eclipse Jetty Web server
 - 9 results (Version 2)
 - Mostly with open logs

Examples in the wild (Portugal Edition)

- Raspberry Pi's (Raspbian distro)
 - 1888 results (Shodan)
 - HTTP: 350
 - 2222: 92
 - HTTP (8080): 35
 - OSMC: 10
- PiPPLware: PiPplware | The ultimate Linux distro for Raspberry Pi
 - <https://pipplware.pplware.pt>
 - 5 Raspberry Pi's
- Arduino
 - 2 devices
- RTOS (Real Time Operating System)
 - 6 devices

Examples in the wild (Portugal Edition)

- eCos Embedded Web Server (Embedded Configurable Operating System)
 - 188 devices
 - CVE-2017-1000020 (Score: 10)
- Chromecast
 - 39 results
- Sunny WebBox (?) solar energy controller/inverter (?)
 - 2925 results
 - CVE-2015-3964 (Score: 10)
 - **The Sunny WebBox allows central access to your plant data on the Internet via Sunny Portal. Log in as “Installer”. The default password for the installer is: “sma”.**

Web Screenshots (PT)

openHAB 2 Log Viewer (frontail) `tail -f /var/log/openhab2/openhab.log /var/log/openhab2/events.log`

```

2019-04-10 13:40:22.008 [vent.ItemStateChangedEvent] - L3V3 changed from 2400 to 2399
2019-04-10 13:40:22.021 [INFO ] [eclipse.smarthome.model.script.Rules] - Decimal value updated to: 239.90000000
2019-04-10 13:40:22.024 [vent.ItemStateChangedEvent] - NL3V3 changed from 240.00000000 to 239.90000000
2019-04-10 13:40:22.109 [vent.ItemStateChangedEvent] - L2V3 changed from 2405 to 2404
2019-04-10 13:40:22.115 [INFO ] [eclipse.smarthome.model.script.Rules] - Decimal value updated to: 240.50000000
2019-04-10 13:40:22.119 [vent.ItemStateChangedEvent] - NL2V3 changed from 240.50000000 to 240.40000000
    
```

Temperature:

21.5 Celsius

SunnyWebBox SMA Logout

Home

Power: 7178 W
Daily yield: 173 kWh
Total yield: 418.24 MWh

Language: English
Password:

DB91-TX - Compact IP Audio Encoder

DEVA BROADCAST

IN: Analog (Main Analog) 09 Apr 2019 Uptime: 16:44:58 Session: 28d 23:18:47

Inputs	Active connections												
<p>Digital: 0 to -80 dBFS</p> <p>Analog: -5.8 to -4.9 dBFS</p> <p>L dBFS R L dBFS R</p>	<table border="1"> <thead> <tr> <th>Type</th> <th>Status</th> <th>Remote Peer</th> <th>Codec</th> </tr> </thead> <tbody> <tr> <td>IP Audio Server</td> <td>Streaming</td> <td>62.48.165.134:11835</td> <td>PCM</td> </tr> <tr> <td>RTP Sender</td> <td>Streaming</td> <td>62.48.165.134:5000</td> <td>PCM</td> </tr> </tbody> </table>	Type	Status	Remote Peer	Codec	IP Audio Server	Streaming	62.48.165.134:11835	PCM	RTP Sender	Streaming	62.48.165.134:5000	PCM
Type	Status	Remote Peer	Codec										
IP Audio Server	Streaming	62.48.165.134:11835	PCM										
RTP Sender	Streaming	62.48.165.134:5000	PCM										

FW: 1.7.1585 IP Address: 192.168.1.90 (DHCP) Netmask: 255.255.255.0 DNS 1: 62.28.116.41
Serial: 91THB21E MAC: 00:04:A3:91:6C:A4 Gateway: 192.168.1.254 DNS 2: 62.28.40.173

Home Status Soladin Estatística Diário Cons. Diário Prod. Diário GRAPH Comentários [NT]

Janeiro Fevereiro Março Abril Maio Junho Julho Agosto Setembro Outubro Novembro Dezembro
2013 2014 2015 2016 2017 2018 2019 2028 2045 2063 2077

Energia Fotovoltaica Produzida (KWh dia)/ Horas

Day	Production (KWh)
01	1.65
02	2.98
03	3.71
04	2.04
05	2.11
06	1.45
07	1.00
08	2.25
09	1.11
10	0.00
11	0.00
12	0.00
13	0.00
14	0.00
15	0.00
16	0.00
17	0.00
18	0.00
19	0.00
20	0.00
21	0.00
22	0.00
23	0.00
24	0.00
25	0.00
26	0.00
27	0.00
28	0.00
29	0.00
30	0.00

Energia Consumida EDP (KWh)

Month	Consumption (KWh)
Jan	16.80
Feb	14.44
Mar	18.51
Apr	19.56
May	18.81
Jun	23.73
Jul	21.03
Aug	31.97

Prod. Fotovoltaica: 202W Producao Mes: 18.29KWh Consumo EDP: 33855W Consumo Mes: 181.17KWh U: 466V Fator Potencia: 0.99

What have researchers been
working on?

Making things safe? Maybe not.

Demonstration of 5G Connected Cars

Sreekrishna Pandi^{†§}, Frank H.P. Fitzek^{†§}, Simone Redana[¶]

[†]Deutsche Telekom Chair of Communication Networks - Technische Universität Dresden, [§]5G Lab Germany,

Joint Design of Communication and Control for Connected Cars in 5G Communication Systems

Sreekrishna Pandi^{†§}, Frank H.P.Fitzek^{†§}, Christopher Lehmann[†], David Nophut[†],
Domokos Kiss[#], Viktor Kovács[#], Ákos Nagy[#], Gábor Csovási[#], Miklós Tóth[#], Tamás Rajacsics[#],
Hassan Charaf[#], Rainer Liebhart[‡]

[†]Deutsche Telekom Chair of Communication Networks - Technische Universität Dresden, [§]5G Lab Germany,
[#] AIT - Budapest University of Technology and Economics, [‡] Nokia Bell Labs

Smart Community: An Internet of Things Application

Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen, Unive
Jiming Chen, Zhejiang University
Xiaodong Lin, University of Ontario Institute of Technology

Internet of Things and Big Data Analytics for Smart and Connected Communities

**YUNCHUAN SUN¹, (Member, IEEE), HOUBING SONG², (Senior Member, IEEE),
ANTONIO J. JARA³, (Member, IEEE), AND RONGFANG BIE⁴, (Member, IEEE)**

¹Business School, Beijing Normal University, Beijing 100875, China

²Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV 25136 USA

³University of Applied Sciences Western Switzerland, Sierre 3960, Switzerland

⁴College of Information Science and Technology, Beijing Normal University, Beijing 100875, China

A smarter grid with the Internet of Things

*Making the grid infrastructure, meters, homes and buildings
more connected*

A Cloud-Based Internet of Things Platform for Ambient Assisted Living

Javier Cubo * ✉, Adrián Nieto ✉ and Ernesto Pimentel ✉

Universidad de Málaga, Departamento de Lenguajes y Ciencias de la Computación, Campus de Teatinos,
29071 Málaga, Spain

* Author to whom correspondence should be addressed.

Smart Digital Door Lock for the Home Automation

Yong Tae Park Pranesh Sthapit Jae-Young Pyun
Department of Information and Communication Engineering, Chosun University
Gwangju, South Korea
pyt@stmail.chosun.ac.kr, pranesh@stmail.chosun.ac.kr, jyppyun@chosun.ac.kr

A Smart Lock System using Wi-Fi Security

Abdallah Kassem and Sami El Murr
Department of Electrical and Computer and
Communication Engineering
Notre Dame University Louaize, Zouk Mosbeh-Lebanon
{akassem|selmurr}@ndu.edu.lb

Georges Jamous, Elie Saad and Marybelle Geagea
Department of Electrical and Computer and
Communication Engineering
Notre Dame University Louaize, Zouk Mosbeh-Lebanon
{gejamous|mbgeagea|casaad}@ndu.edu.lb

How to mitigate?

Vendors' Opinion



How to solve the problem of having so many *things* connected to Internet?

Connect even more *things*!



What is McAfee Security for TV?

Avast Security & Antivirus

Everything you need
to protect your smartphone.








Or... Antivirus
everywhere!

But why are we exposing so many devices to the Internet!?

Personal opinion

1. If we want a *plug-and-play* IoT, we don't have a choice

					
<i>Cloud Services</i>	Nest Cloud/ Google Cloud	Azure IoT	AWS IoT	iCloud	ARTIK Cloud/ SmartThings
<i>Application Protocols</i>	Weave	AMQP	MQTT	HomeKit	MQTT
<i>Network Protocols</i>	WiFi/Thread	WiFi	WiFi	WiFi/BLE	WiFi/ZigBee/ BLE/Thread
<i>Operating Systems</i>	Linux/Android Things	Windows IoT	Linux/AWS Greengrass	iOS	Linux/ARTIK

Vertical Silos (from <https://iot.mozilla.org/>)

2. We want to use "smart assistants" and stuff

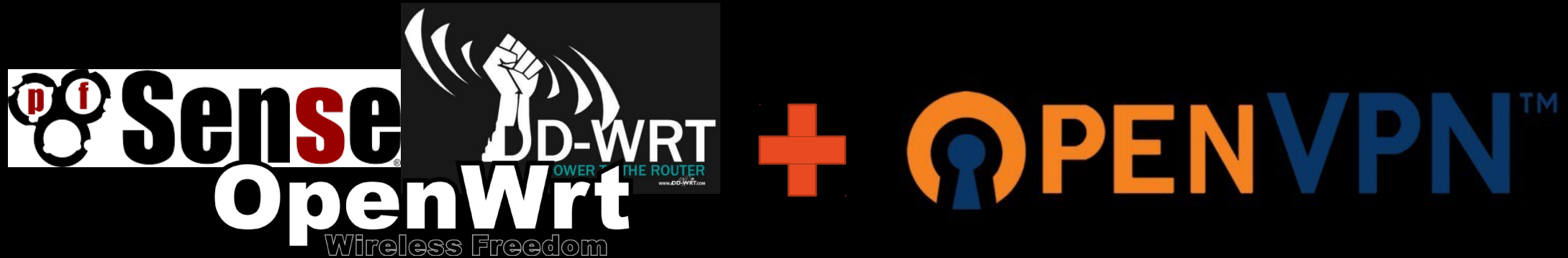


3. We simply don't know what the hell is going on {category of devices}



So, what now?

The DIY solution



- VLAN segregation
- VPN for limiting what is exposed (local-only interactions)

PS: Firewalls don't solve the problem of security-broken devices.

Main idea? Not exposing anything beyond your local network.

But my apps don't work
anymore...

Expected result.

What about a *silver-bullet*?

- More documentation about the *things*
- Adoption of standards?
 - Mozilla IoT Project Things
- Stop reinventing the wheel
 - (e.g.: communication protocols)
- Make things local-first instead of remote-first

What about a *silver-bullet*? (source: Twitter)

- Customers **must** be notified if security updates are no longer occurring for a given device. (@daeken)
- Proper channels for reporting vulnerabilities. (@daeken)
- Minimize attack surface. (@daeken)
- Keep third-party software up to date. (@daeken)

- No cloud service should ever have access to your sensitive home devices or even know what you're doing. (@creationix)
- Devices should always work when you're at home, even without Internet connectivity. (@creationix)
- Communicating with devices while at home should have far less latency than is typical. (@creationix)

Good Examples

- IKEA Trådfri
 - Works out of the box, Local-only Hub, Based on Open-Standards
- Philips Hue
 - Local-first, Update locally (using Hue App)
- Hubitat
 - Local-first, extended compatibility
- Ring Alarm
 - “Your Ring Alarm usually communicates with you or your monitoring service through the internet. Any time your Base Station loses its connection to the internet, regardless of the cause, a cellular backup system kicks in that will allow the system to continue to monitor your home.”
- Mozilla WebThings
 - “(...) allows users to directly monitor and control their smart home over the web, without a middleman.”
- OpenHAB, Domoticz, Node-RED and other DIY solutions

Final Remarks

- Don't connect things directly to the Internet!
 - It's ~~impossible~~ hard to have good security in a microcontroller.
 - Vendors love telemetrics/statistics of *everything*.
 - Use gateways, make them cross-compatible ~~and take my money~~.
 - And end vertical silos (interoperability is nice).

Useful Links

- Your guide to the Internet of Things Sh*t
 - <https://internetofshit.net/soon>
- The search engine for Internet-of-Things
 - <https://www.shodan.io/>
- OWASP Internet of Things Project
 - https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Thank you

jpdias.me

keybase.com/jpdias

jpmdias@fe.up.pt || jpdias@pm.me