#### How to Fix the Internet of Broken Things

#### Presentation at Setii 2018

**Ulrich Norbisrath** 

#### whoami

- http://ulno.net, Ulrich Norbisrath
  email: replace http:// with ulno@
- Adjunct Professor
  - FH Upper Austria
- Independent IoT Consultant/ Inventor/Maker/Artist
- **PhD** from RWTH Aachen University: "Configuring eHome Systems"
- **Research:** Internet of Things, Story Driven Modeling, search support
- **Teaching:** H&B Automation, IoT, SE, Systems
- International teaching and research experience: USA, Germany, Austria, Estonia, Kazakhstan, Singapore, Indonesia, (starting in) Brazil





### Who are U?

- Raspberry Pi?
- Micro controllers? Arduino? ESP8266?
- Maker or part of Maker/Hacker community?
- Teacher?
- Student?
- Designer?
- Marketing expert?





Personal statistic: 30 talks: IoT and Making since 2015, 8 classes: H&B Automation since 2014

#### Outline

- Internet of Things (IoT)
- Awareness/Examples of Breakages
- Contermeasures and a software engineer's perspective
- Let's not make IoT an IoBT (Internet of Broken Things)

# Internet of Things (IoT)

- What does the Internet of Things entail?
- Use phone or laptop to google about IoT, find and note down:
  - 3 domains (included areas)
  - 2 typical devices (appliance or controller)
- 5 minutes time to search
- Discussion

# Internet of Things (IoT)

#### IoT Domains

- Ubiquitous Computing (Pervasive Computing)
- Home automation
- Urban Computing/Smart Cities
- Embedded Computing
- Actor/Sensor Networks
- M2M Communication
- Mobile Computing, Wearable Computing
- Hacking/Making/Remixing
- Big/Actionable Data
- $\rightarrow$  Systems, Connectivity, Data
- Devices and controllers









## What Could Break?

- 20-50 Billion connected devices in 2020
- How could anything go wrong?
- From your head or Google (5 min):
  - What did already break?
  - What will break?
  - Why?

## Causes for Breakage

- Companies assume they can do updates for a fleet of devices
  - They can't
- Automation devices on same network as desktops or other infrastructure
- Default passwords
- Privacy exploitation enforced by corporate entities
- Star topology/ no layered security



### Example Break Downs

- Default passwords in devices and routers
  - Zombie webcams and routers
- WIFI networks very insecure last widely deployed standard WPA 2 from before 2009 (IEEE 802.11w was specified 2009)
  - Deauth attack
  - Krack attack
- Cyber abuse
- Man in the middle attack

#### Zombie Webcams

1 000 000 internet connected cameras attack one infrastructure



- https://www.law360.com/articles/861699/attack-of-the-zombie-webcams-ddos-attacks-and-the-insecure-iot
- https://motherboard.vice.com/en\_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

#### Deauth Attack

- Let me take down your internet for USD 2.50
- Countless denial of service attacks possible
  - Hospitals
  - Service institution
  - Factories
- If both router and client use IEEE 802.11w, not possible (still rarely the case)



#### Krack Attack

- Most WIFI networks
  - All data of clients can be read

(basically all WIFI – even protected ones are like public WIFIs)

- Examples
  - Passwords for local devices are visible in clear text
  - Data filled in forms can be read
  - Patient data visible
  - Insurance and identity data visible



https://www.krackattacks.com/

https://github.com/vanhoefm/krackattacks-scripts

## Cyber Abuse

- Usually domestic
- Thanks to IoT increasing quickly
- Examples:
  - Weird behavior of smart locks, air conditioning, lights
  - Abuser spies and knows too much
  - Prevented transactions

#### Man in the Middle



Image from: http://www.webstepbook.com/supplements-2ed/slides/chapter15-security.shtml#slide41

#### Textbook Advice

- Emphasize security from day one
- Lifecycle, future-proofing, updates
- Access control and device authentication
- Know your enemy
- Prepare for security breaches

**N Hajdarbegovic.** Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. Toptal. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

#### **Counter Measures**

- Awareness
- Layered architectures
- Avoid wireless
- Active and aware community
  - supporting and
  - auditing software and hardware
- Openness about core infrastructure
  - easy to audit
  - easy to update
- Build security into
  - life cycle management
  - maintenance
- Better symmetric encryption than insecure unvalidated asymmetric

#### UlnoIOT (Layered Architecture) Framework and Ecosystem for IoT



- http://iot.ulno.net
- http://github.com/ulno/ulnoiot

Thinkpad image: Robert Kloosterhuis http://www.flickr.com/photos/jemimus/6461569529/ Raspberry: https://www.raspberrypi.org/

#### Layered Architecture (in UlnoloT)



#### Summary

- Let's be aware of security issues in IoT.
- Let's take system architecture into account  $\rightarrow$  think in systems!
- Let's prevent breaking the Internet of Things!

#### References

- N Hajdarbegovic. Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. Toptal. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things
- H Vella. IoT devices and smart domestic abuse: who has the controls? https://eandt.theiet.org/content/articles/2018/06/iot-devices-and-smart-domestic-abuse-who-has-the-controls/
- AJ Shipley. SECURITY IN THE INTERNET OF THINGS Lessons from the Past for the Connected Future. Security Solutions, Wind River, White Paper, 2013. https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr\_security-in-the-internet-of-things.pdf
- **D Goodin.** Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections.

https://arstechnica.com/information-technology/2015/02/lenovo-pcs-ship-with-man-in-the -middle-adware-that-breaks-https-connections/

- C Osborne. Internet of Things devices lack fundamental security, study finds. https://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study -finds/
- DA Hendricks. The Trouble with the internet of Things. https://data.london.gov.uk/blog/the-trouble-with-the-internet-of-things/