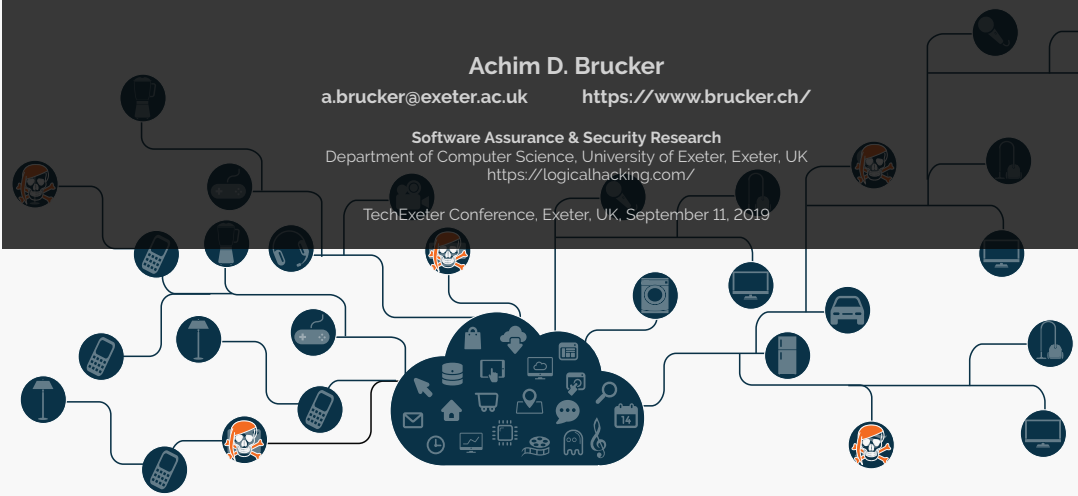
Hacking (Not So) Smart Things 101

Achim D. Brucker
a.brucker@exeter.ac.uk https://www.brucker.ch/

Software Assurance & Security Research
Department of Computer Science, University of Exeter, Exeter, UK
https://logicalhacking.com/

TechExeter Conference, Exeter, UK, September 11, 2019



{*LogicalHacking*}.com

SWCSC South West Cyber Security Cluster

UNIVERSITY OF EXETER

Crock-Pot

Crock-Pot SCCPWM600-V2 Wemo Smart Wifi-Enabled Slow Cooker, 6-Quart, Stainless Steel

★★★★☆ ▾ 318 customer reviews | 121 answered questions

List Price: ~~$149.99~~
Price: $129.99 & **FREE Shipping**. Details
You Save: $20.00 (13%)

In Stock.

Want it tomorrow, May 16? Order within **11 hrs 6 mins** and choose **One-Day Shipping** at checkout. Details
Ships from and sold by Amazon.com in easy-to-open packaging. Gift-wrap available.

- Adjust cook time & temperature using the WeMo Application
- Can be controlled via the WeMo Application or directly on the unit

AIMOX

AIMOX Smart Wifi Stainless Steel Electric Kettle through Smartphone Remote On/Off Switch and Temperature Control,1.7 Liter Teakettles Ikettle

★★★☆☆ ▾ 9 customer reviews | 6 answered questions

Price: ~~$159.99~~
Sale: $99.99 & **FREE Shipping**. Details
You Save: $60.00 (38%)

Only 7 left in stock - order soon.

Want it tomorrow, May 16? Order within **9 hrs 22 mins** and choose **One-Day Shipping** at checkout. Details

Sold by aimox sportband and Fulfilled by Amazon in easy-to-open packaging.
Gift-wrap available.

amazon tap

ALEXA-ENABLED PORTABLE
BLUETOOTH SPEAKER

JUST TAP & ASK
NOW WITH HANDS-FREE MODE

Amazon Tap - Alexa-Enabled Portable Bluetooth Speaker

Amazon

4.0 out of 5 stars 5,815 customer reviews

| 1000+ answered questions

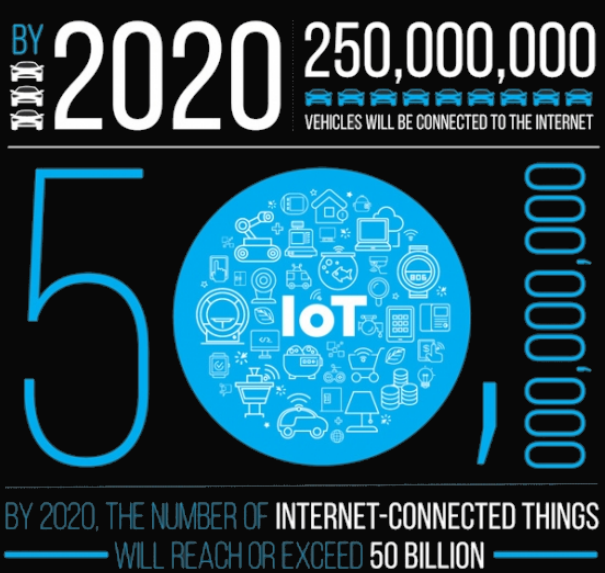
#1 Best Seller in Compact Radios & Stereos

Price: $129.99 & **FREE Shipping**. Details

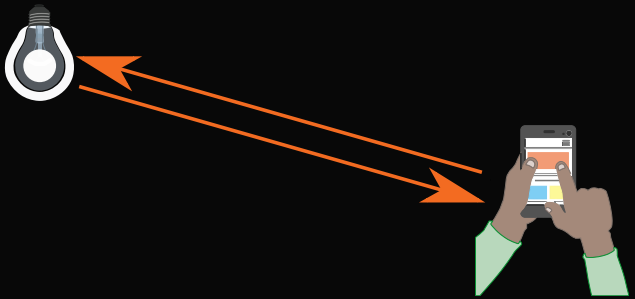
In Stock.

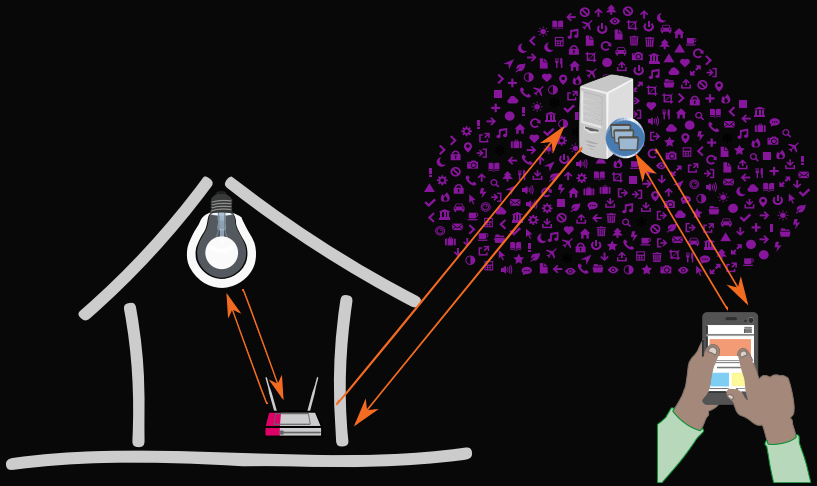
Want it tomorrow, May 16? Order within **11 hrs 44 mins** and choose **One-Day Shipping** at checkout. Details

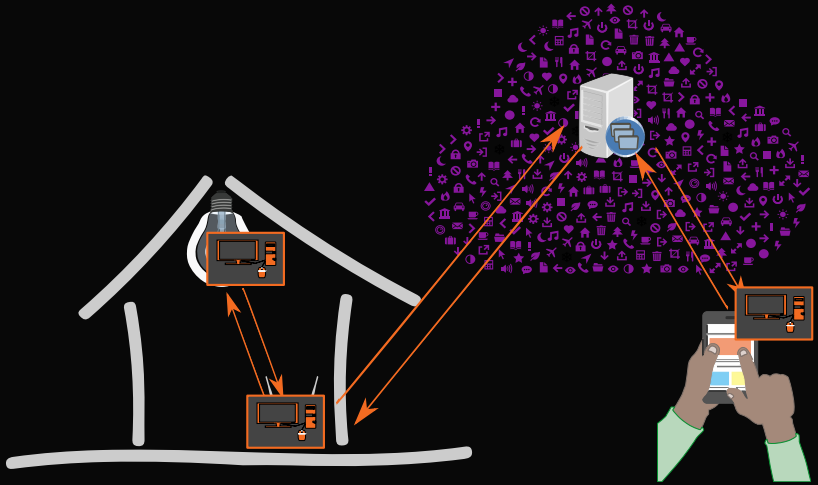
Ships from and sold by Amazon Digital Services LLC. Gift-wrap available.



http://www.comsoc.org/blog/infographic-internet-things-iot







Side Remark

Smart home devices can be cheap

- smart switches are available for as little as one quid
- smart light bulbs starts at four quids

And still, you expect them to

- be secure (think of all the privacy implications of smart devices)
- updated frequently (to fix security vulnerabilities)
- be available (imagine being in the shower and your boiler is not working)

And all that over many years (recall, somebody has to pay for the cloud infrastructure)

1

Side Remark

Smart home devices can be cheap

- smart switches are available for as little as one quid
- smart light bulbs starts at four quids

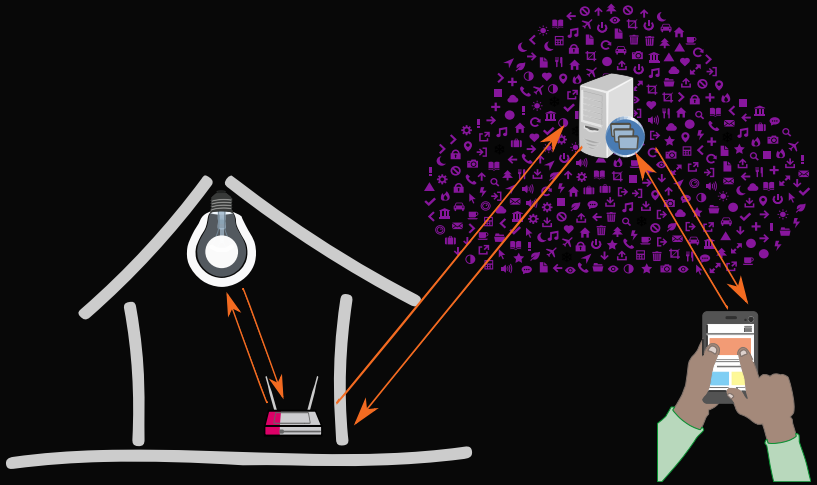
And still, you expect them to

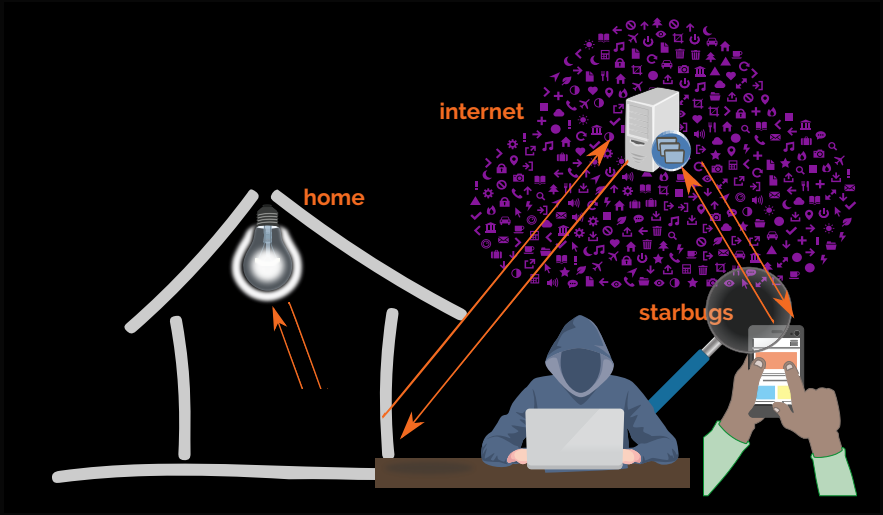
- be secure (think of all the privacy implications of smart devices)
- updated frequently (to fix security vulnerabilities)
- be available (imagine being in the shower and your boiler is not working)

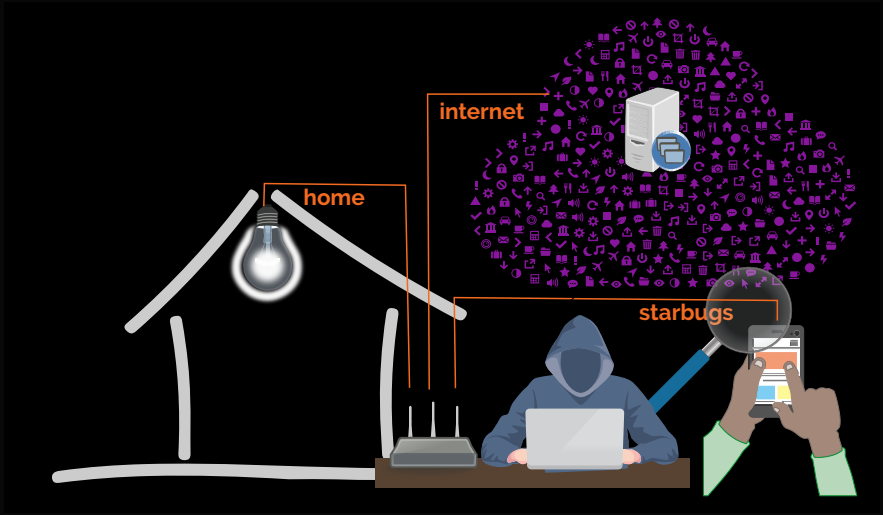
And all that over many years (recall, somebody has to pay for the cloud infrastructure)

Let's have a look at a real device …[1]

[1] All issues discovered by second year students without security knowledge: "from zero to full take over in 15 hours."







Replay Attacks

Live Demo …

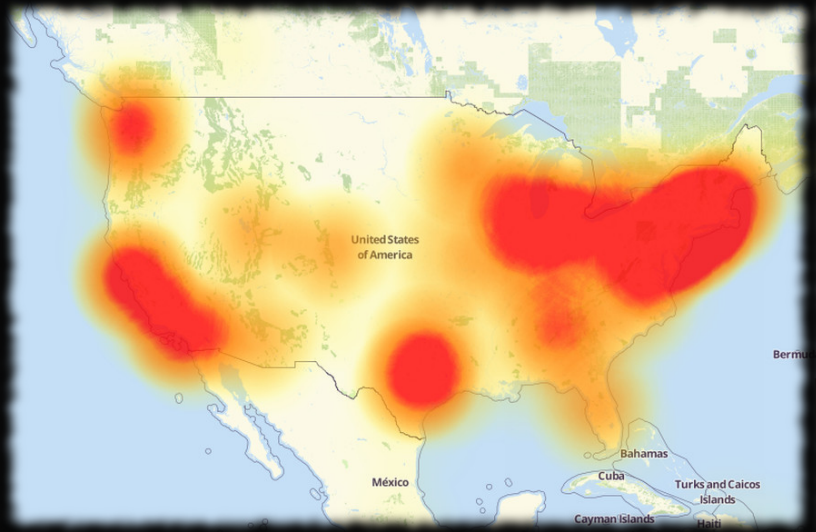
Obtaining "Hashed" Passwords (and Reversing Them)

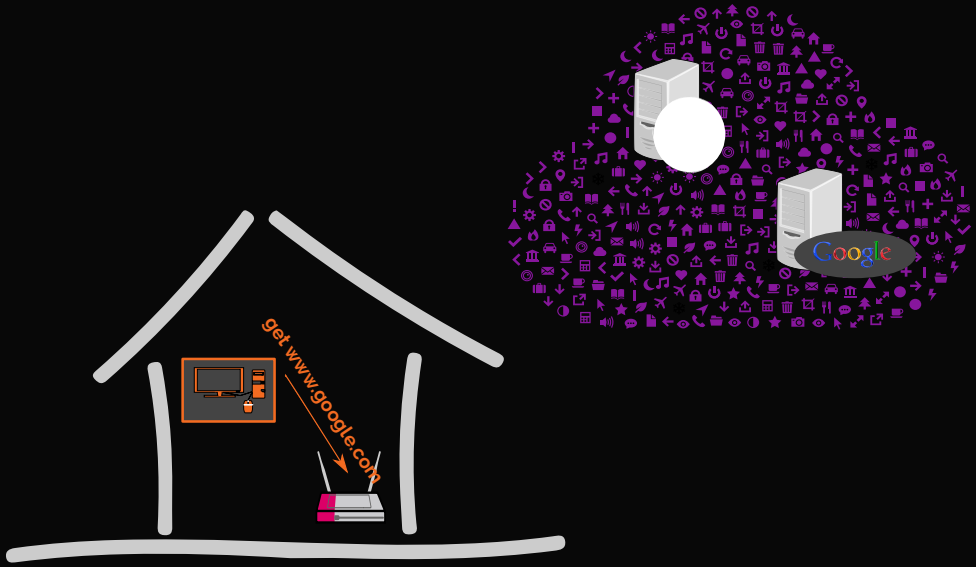
Live Demo …

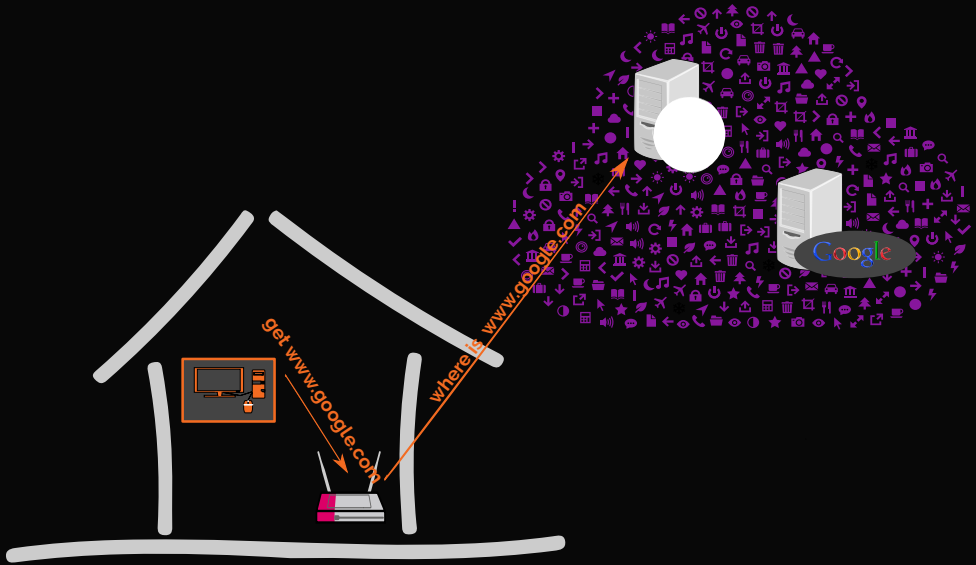
Further Attack Vectors

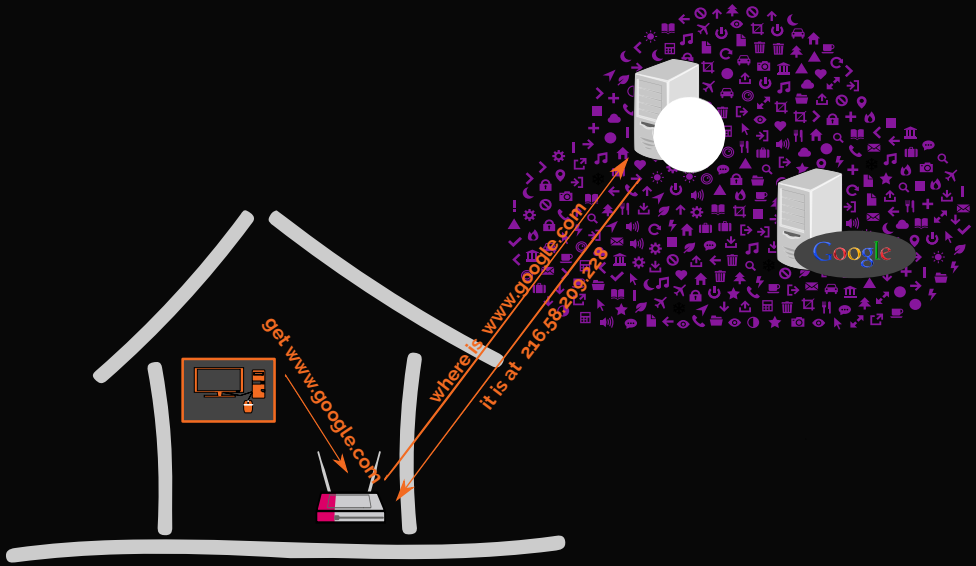
- Attacking the light bulb:
  - during "pairing"
    - the light bulb creates an unsecured wifi network
    - allows to upload new firmware via an insecure connection
  - during operations
    - accepts unauthenticated commands within local network
  - if you throw away the light bulb:
    - your wifi password can be extracted from the device
- Attacking the back-end
  - the back-end use a mix of http and https endpoints: **all** of them can be downgraded to http
  - we've already seen how to obtain password and username
- Attacking the mobile app (was not needed …)
  - disable certificate check

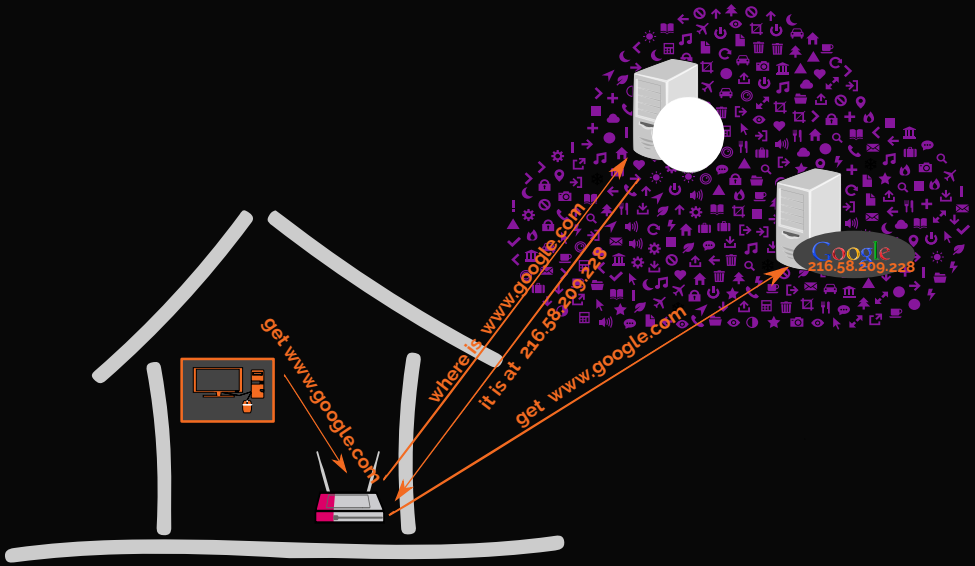

WEB
REPORT
US & WORLD
How an army of vulnerable gadgets took down the web today
Malware known as Mirai is to
by Nick Statt | @nickstatt | Oct 21, 2016
Large DDoS attacks cause outages at Twitter, Spotify, and other sites
Posted Oct 21, 2016 by Darrell Ether
Kate Conger @kateconger
Next Story
Amazon UK - Amazon status back online following huge cyber attack on top sites
AMAZON has been taken down in MASSIVE cyber attack takes websites including Twitter, Spotify and Reddit offline as hackers launch attack on major web host.
By MICHAEL MOORE
18:18, Fri, Oct 21, 2016 | UPDATED: 18:18, Fri, Oct 21, 2016

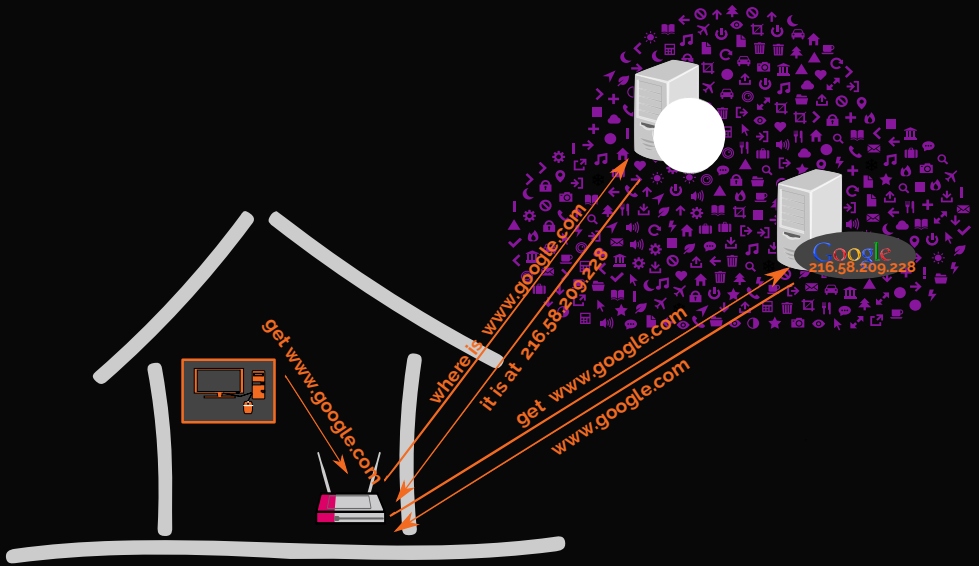


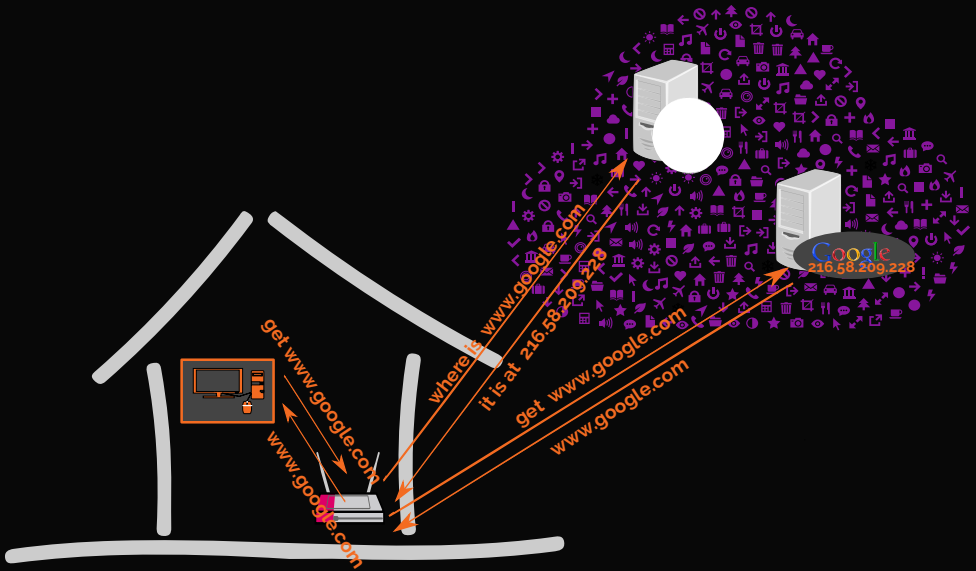








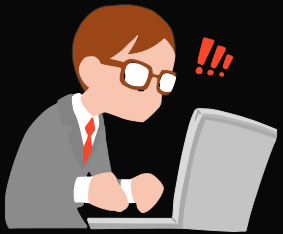




Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer



Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8

Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router

Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7

Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7
- car

Pub Quiz

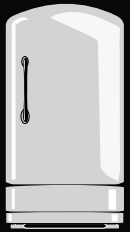
Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7
- car (typical use: 14 years): Windows XP

Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7
- car (typical use: 14 years): Windows XP
- fridge



Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7
- car (typical use: 14 years): Windows XP
- fridge (typical use: 17 years): Windows ME

Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7
- car (typical use: 14 years): Windows XP
- fridge (typical use: 17 years): Windows ME
- LED bulb

Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7
- car (typical use: 14 years): Windows XP
- fridge (typical use: 17 years): Windows ME
- LED bulb (typical use: 20 years): Windows 98

Pub Quiz

Assume, you own a …that is reaching the end of its average life.
Which Operations system from Microsoft was installed, when you bought the device?

- computer (typical use: 5 years): Windows 8
- wifi router (typical use: 7 years): Windows 7
- car (typical use: 14 years): Windows XP
- fridge (typical use: 17 years): Windows ME
- LED bulb (typical use: 20 years): Windows 98

And we complained about the companies still using Windows XP …

Putting Things in Perspective

- This device violates (nearly) all rules of secure design & implementation
- We bought devices from three different vendors:
  - today, I showed the worst one
  - the other two
    - used a standardised architecture using MQTT
    - provide a base level of network security
      (students only found local replay attacks)
    - with access to the device, they can be attacked as well (debug interfaces, JTAG)
- (Relatively) secure smart devices can be build (and still sold very cheap)
- Many cheap devices based on a ESP8266 – yes, the one you know from your Arduino projects, and yes, on many devices you can replace the firmware with your own …

Key Take-Aways

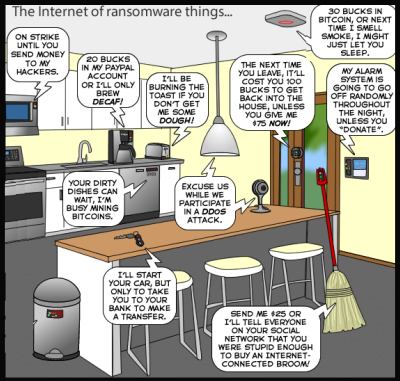
1. Your “smart device” is more likely a pretty dumb device and a server farm (plus a mobile app).
2. IoT security is large software security
3. after addressing the software security issues, focus on hardware attacks, and
4. do not forget the supply chain (and OEM) security!

PS: The group is growing and we are keen to work with (local) industry

Contact:

Dr. Achim D. Brucker
Department of Computer Science
University of Exeter
Streatham Campus
Exeter, EX4 4QF, UK

a.brucker@exeter.ac.uk
@adbrucker
https://de.linkedin.com/in/adbrucker/
https://www.brucker.ch/
https://logicalhacking.com/blog/



http://www.geekculture.com/joyoftech/joyarchives/2340.html

Key Take-Aways

1. Your "smart device" is more likely a pretty dumb device and a server farm (plus a mobile app).
2. IoT security is large software security
3. after addressing the software security issues, focus on hardware attacks, and
4. do not forget the supply chain (and OEM) security!

PS: The group is growing and we are keen to work with (local) industry

Contact:

Dr. Achim D. Brucker
Department of Computer Science
University of Exeter
Streatham Campus
Exeter, EX4 4QF, UK

a.brucker@exeter.ac.uk
@adbrucker
https://de.linkedin.com/in/adbrucker/
https://www.brucker.ch/
https://logicalhacking.com/blog/