IoT: Are you safe after a break up?

Jonathan Haddock
Canterbury Cyber Security Conference - 21st January 2020

https://blog.jonsdocs.org.uk
@joncojonathan

About me

- I've worked in IT for over 15 years
- Now the Deputy Senior Information Security Officer formerly a network & security engineer, for three local authorities
- Have run penetration testing courses with the BCS YPISG
- Trained in forensics, penetration testing and incident response

The YPISG is a BCS specialist group - Young Professionals' Information Security Group.

Every role helps with security, whether that's on the service desk or as a developer. I've worked across a number of roles, starting in service desk / desktop support, and each has benefited from experience gained in the others.

If you want to get into IT security, I recommend you specialise in an area you find interesting but make sure you keep your hand in other areas too so you have a broad skill set and knowledge. This will allow you to have informed discussions with different teams, in a way they (and you) can understand.

I also blog about cyber security, development, IT, and occasionally local history at https://blog.jonsdocs.org.uk.

The IoT situation

- Estimated numbers of IoT devices vary, perhaps 7 - 20 billion in 2018[1][2]. UCL research estimates 125 billion devices by 2030[3]
- Generally accepted the number of devices will increase year on year
- Connectivity via wired LAN, WiFi, cellular
- Data sharing, location tracking, behavioural analysis

[1] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (August 2018)
[2] https://www.ericsson.com/en/mobility-report/internet-of-things-forecast (Undated)
[3] https://www.ucl.ac.uk/research/domains/sites/research_domains/files/giot-report.pdf (November 2018)

The numbers of IoT devices vary hugely, not assisted by different definitions. IoT devices exist in the home, in our offices and increasingly on our streets with the rise of “smart cities”. One definition of IoT is a group of interconnected devices, allowing the exchange of information, although conventionally desktop computers, laptops and related equipment is excluded from the definition.

In the home

- 9.5 million UK people estimated to use a smart speaker in 2018[1]
  - Amazon's devices holding the market share
- Approximately 1.5 million smart thermostats in UK homes[2]
- Smart light bulbs allow for personalisation and remote control
- Smart toasters "for precise control"[3]

[1] https://www.emarketer.com/content/amazon-echo-dominates-smart-speaker-market-in-the-uk (December 2018)
[2] https://www.energylivenews.com/2018/04/04/smart-thermostat-usage-hots-up-across-1-5m-uk-homes/ (April 2018)
[3] https://www.engadget.com/2017/01/04/griffin-connects-your-toast-to-your-phone (2017)

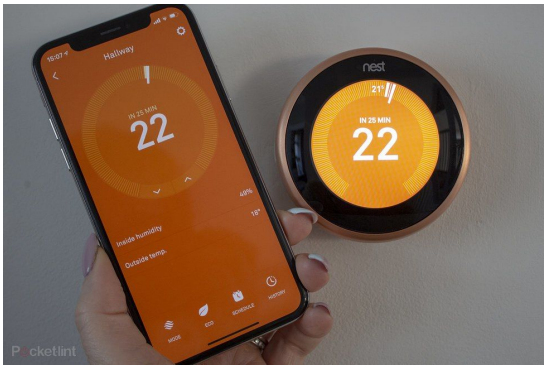
Devices in the home are increasingly online, with smart fridges even able to order food once stocks get low. Sometimes making a home appliance "smart" is a great convenience to the user, and can save money or energy, but other times connectivity can be an annoyance. I'm quite happy that my fridge doesn't order me food and that my washing machine doesn't email me.

I'll come on to the toaster example later.

Controlling IoT devices

- Web portal
- Mobile app
- On site via single console
- Geofencing

Importantly, remote control is a possibility - often a key selling point.



Picture from Pocket Lint

Remote control is a huge selling point for IoT. Being able to tell your heating to come on when you're on the way home can save the shock of a cold house (or help you warm up quickly if you've walked home in a snow storm) and by using geofencing it's possible for the system to do this automatically. Geofencing is when a virtual fence is placed around an area. When you're detected as being in the area, for example 5 miles away from home, an action can be performed due to your proximity.

Similarly, money can be saved by turning equipment off once you're out of range.

Threat landscape

- Often consider the apocryphal “hacker in a hoodie”
- Might consider nation state
- Equipment may be subverted to send spam[1]
- Remote control used to spy on strangers, or send messages[2]

Have you considered members of your family (the insider threat)?

[1] https://nakedsecurity.sophos.com/2017/12/22/washington-dcs-surveillance-cameras-hacked-to-send-spam/ (December 2017)
[2] https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/ (February 2017)

News reports always use the image of a hacker in a hoodie, which doesn’t seem accurate based on the penetration testers that I know. Indeed, there’s likely penetration testers here today and at least one of them is wearing a shirt and tie!

When considering threats we’re quick to picture the outsider that wants to do us harm. Rarely do we think about those close to us, perhaps those with the greatest opportunity. As part of my role, the vast majority of the incidents I have to review are down to genuine insider mistakes - if an accident can be made by an insider, so can a deliberate attack.

All of that said, how many people seriously consider that their home may be a target? “I’m just an individual, no-one is interested in me” or “it’ll never happen to me” are phrases I’m sure we’ve all used.

The problem - abuse through IoT

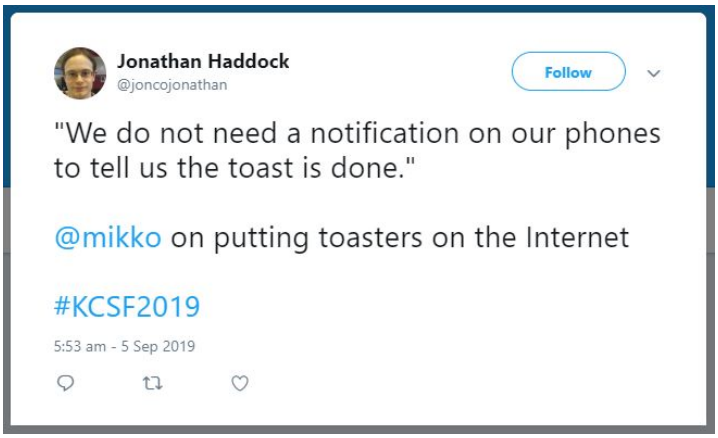
- Sadly abuse through IoT is on the increase[1]
- IoT can be used to control individuals by removing their own control of their environment
- Stalker apps can track people's whereabouts, or spy on their communications
- Internet connected children's toys are being used to play hurtful messages

[1] https://www.ucl.ac.uk/research/domains/sites/research_domains/files/giot-report.pdf (November 2018)

What can be done?

Do you really need it?

- To quote Mikko Hypponen:



Quote from the Kent Cyber Security Forum 2019. My write up is here: https://blog.jonsdocs.org.uk/2019/09/06/kent-cyber-security-forum-2019/

Do you really need it?

- Consider the devices being installed in your home
- Do they provide a tangible benefit?
  - Is there a benefit to multiple people?

Sometimes we want gimmicks but the attraction soon wears off. Similarly, there's no point having a smart light bulb if you then use it just like a normal bulb after the first week. Does the device being installed really provide a benefit to you? Does it provide a benefit to the whole household or just one person?

If you don't really think you'll benefit from the device, seriously consider if you want to install it.

Education

- Often there's one technical person in the home
  - Can lead to dependence unless knowledge is shared
- Showing an interest in the technology, even at a basic level, can help with defence
  - Reduces the knowledge gap between installer and other users
- Knowing what's in the home is important too
- Support services need training in how to deal with the problem

My wife has commented before that if I were to die she wouldn't be able to add anyone to our WiFi. That's not strictly true, as she walks past the guest WiFi password every day, but it does demonstrate the difference in IT knowledge in our relationship. For the record, I don't exert control over my wife, technologically or otherwise.

It's common in the workplace these days to have to sit through some cyber security awareness training. We actively teach employees what a phishing email looks like, what techniques the bad guys use, and how to avoid them. There's no equivalent for IoT, yet a couple of slides in a training session could be really helpful.

Clearly it's not always possible to know what's been brought into the home, but if there's an opportunity to know where the CCTV cameras and light bulbs are it's worth taking that opportunity.

Research by UCL, in their Gender and IoT research report (https://www.ucl.ac.uk/research/domains/sites/research_domains/files/giot-report.pdf) found support services don't have the training to deal with issues surrounding technology. Perhaps if you have a local support charity you could volunteer to provide some training to them, which would also tie in with the British Computer Society's goal to make IT good for society.

Proximity testing

- Technical control: require the controller to be near the device occasionally to get a token or key
  - The IoT device should issue the token, not the smartphone
- Can't use GPS for this
  - Can be spoofed
  - Allows revalidation from outside the building

Token assignment should be done by the IoT equipment, not by the smartphone (otherwise the smartphone could be tricked remotely). This poses a problem for lower powered devices, so perhaps is only necessary for systems with a larger impact (thermostats) rather than smaller gadgets that can easily be removed (e.g. light bulbs).

Proximity testing

- Bluetooth has a shorter range - likely inside the building
- Timeouts need to be reasonable
  - Perhaps a button to invalidate tokens?
  - DoS vs privacy

If access is granted by a token requiring an initial Bluetooth handshake, it is necessary that the token doesn't expire within a couple of days. It's reasonable that the user could be out of the country for a few weeks and monitoring their equipment. Further, any renewal of the token should be transparent to the user - if the smartphone is in range of the IoT enabled hardware the token should be renewed.

There needs to be a failsafe option to allow a local user to cut off remote access by invalidating the token. Clearly this provides the option to provide a Denial of Service attack, but if you're already in the property you have far more options available.

Technical deep clean

- Current option
- Requires removal and / or disconnection of devices
  - Easy for a light bulb, less so for a heating system
- Change of WiFi password disconnects devices
- Complete change of router disables external remote access
  - Options don't work for equipment with its own SIM

The current option is to disconnect IoT devices from the Internet, severing any connection to the third party. While this will work for any gadgets connected via WiFi, any device with its own Internet connection provided by 4G / SIM card is not so easy to disconnect. Powering equipment down would be another option, although depending on the item could cause other issues. Disconnecting a light bulb is easy, and a replacement, "dumb bulb" can easily be installed. If the IoT device is your thermostat, controlling heating and hot water, then disconnecting it may not be such an easy option.

If you have access to the router / WiFi management system it's possible to see which devices are connected at the time. This is useful as it can act as an indicator to show how many devices exist, and how many are left, acting as an "IoT scanner".

Conclusions

- Poor behaviour in society is a people problem, but technology design can help
- Technology companies need to design their systems to be easier to “clean”
  - Removing the IoT device should be as easy as adding
- There needs to be a widespread adoption of a code of conduct in order for the problem to be reduced
  - Cheaper goods unlikely to sign up
- Importantly, the victim is not to blame

Technology should work for all the people, not against them, so improving technology design to help prevent a negative experience is key.

Any questions?

Links and acknowledgements

Refuge are a UK charity that offer help and support to women and children that may have suffered tech abuse:
https://www.refuge.org.uk/get-help-now/

Nest Thermostat & app picture from Pocket Lint
https://www.pocket-lint.com/smart-home/news/nest/148016-google-nest-learning-thermostat-tips-and-tricks

Slide not shown on the day.