Can We Make the Internet of Things (IoT) More Secure?

Ming Chow
@0xmchow

What's NOT The Focus of This Talk: Hall of Shame

- "IoT garage door opener maker bricks customer's product after bad review" https://arstechnica.com/information-technology/2017/04/iot-garage-door-opener-maker-bricks-customers-product-after-bad-review/
- "Dishwasher has directory traversal bug" https://www.theregister.co.uk/2017/03/26/miele_joins_internetofst_hall_of_shame/
- "Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings" https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings
- "Hackers Can Easily Hijack This Dildo Camera and Livestream the Inside of Your Vagina (Or Butt)" https://motherboard.vice.com/en_us/article/camera-dildo-svakom-siime-eye-hacked-livestream
- "Nest Thermostat Glitch Leaves Users in the Cold" https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html
- "Just what no one needed: 'world's first smart condom' unveiled" https://www.extremetech.com/electronics/245333-british-company-now-taking-preorders-worlds-first-smart-condom
- "Warning issued over baby monitor, webcam, IoT security… again!" https://nakedsecurity.sophos.com/2016/07/19/warning-issued-over-baby-monitor-webcam-iot-security-again/
- More: @internetofshit (https://twitter.com/internetofshit)

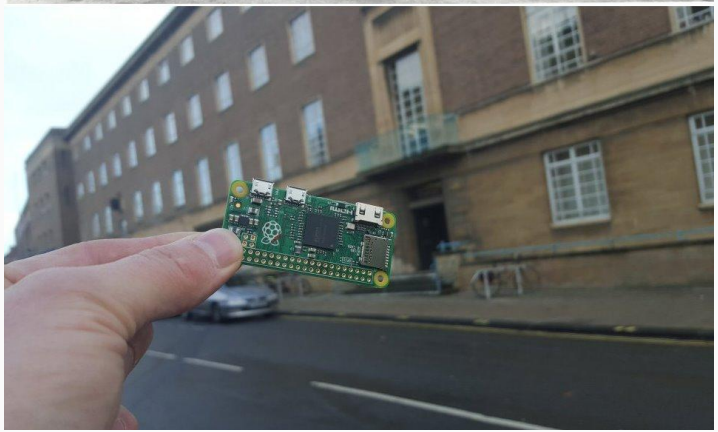
What is the Internet of Things (IoT)?

“...a buzz-phrase used to describe the computerisation of everything from cars and electricity meters to children’s toys, medical devices and light bulbs.” (source: http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security)

“Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of.” (source: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#42d8983e1d09)

How was IoT made possible?

- A CPU
- A plethora of communications protocols (https://www.postscapes.com/internet-of-things-protocols/)
- The cost of technology decreasing
- The cost of Internet connectivity decreasing (e.g., Wi-Fi)
- Internet made widely available
- The physical size of technology shrinking
- The pervasiveness of mobile devices
- “The cloud”
- Barrier of entry to accessing tools and technology is very low



Perspective, 1958 vs 2015: https://www.reddit.com/r/pics/comments/3uc55k/58_years_on/

Why IoT?

- Collecting information
  - Hence, “Big Data” is synonymous with IoT
  - Reasons?
- Money, a billion dollar+ market
  - “IoT is growing at a dangerously fast pace, and researchers estimate that by 2020, the number of active wireless connected devices will exceed 40 billion.” (source: https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/)
  - “Now it’s 2016, and we’re nowhere near 1 trillion IoT devices, or even 50 billion for that matter. The current count is somewhere between Gartner’s estimate of 6.4 billion” (source: http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated)
  - “The Internet of Way Too Many Things” https://www.nytimes.com/2015/09/06/opinion/sunday/allison-arieff-the-internet-of-way-too-many-things.html

“New Tech, Same Old Hacks”

- Not new
- Technology deployed naively
  - Recall RFID tags in the 2000s
- Commonly exposed from IoT devices: open ports, administrative web interface, information leakage
- Techniques to attack IoT devices: scanning, weak or default credentials, updates via FTP, XSS or SQL injection to web interface, open access to server(s), no access control on server (world writable)
  - https://www.rsaconference.com/writable/presentations/file_upload/asd-t10-securing-the-internet-of-things-mapping-iot-attack-surface-areas-with-the-owasp-iot-top-10-project.pdf
- Result of compromising IoT devices: Distributed Denial of Service (DDoS) attacks, botnets

Case Study 1: Mirai

- Terabit scale Distributed Denial of Service (DDoS) attacks from September 2016 to late 2016
- How: using thousands of infected devices, mostly cameras. Devices infected via weak username:password hardcoded on device (e.g., root:root, admin:admin)
- Results: took down Brian Kreb's blog in September 2016; GitHub, Twitter, Netflix, and many major services were affected via DDoS on Dyn DNS in October 2016 (i.e., "all eggs in one basket")
- Source code: https://github.com/jgamblin/Mirai-Source-Code
- Rob Graham's presentation on "Mirai and IoT Botnet Analysis" at RSA Conference 2017: https://vinceinthebay.files.wordpress.com/2017/02/rsac-slides-hta-w10-mirai-1.pdf

Case Study 1A: Deutsche Telekom

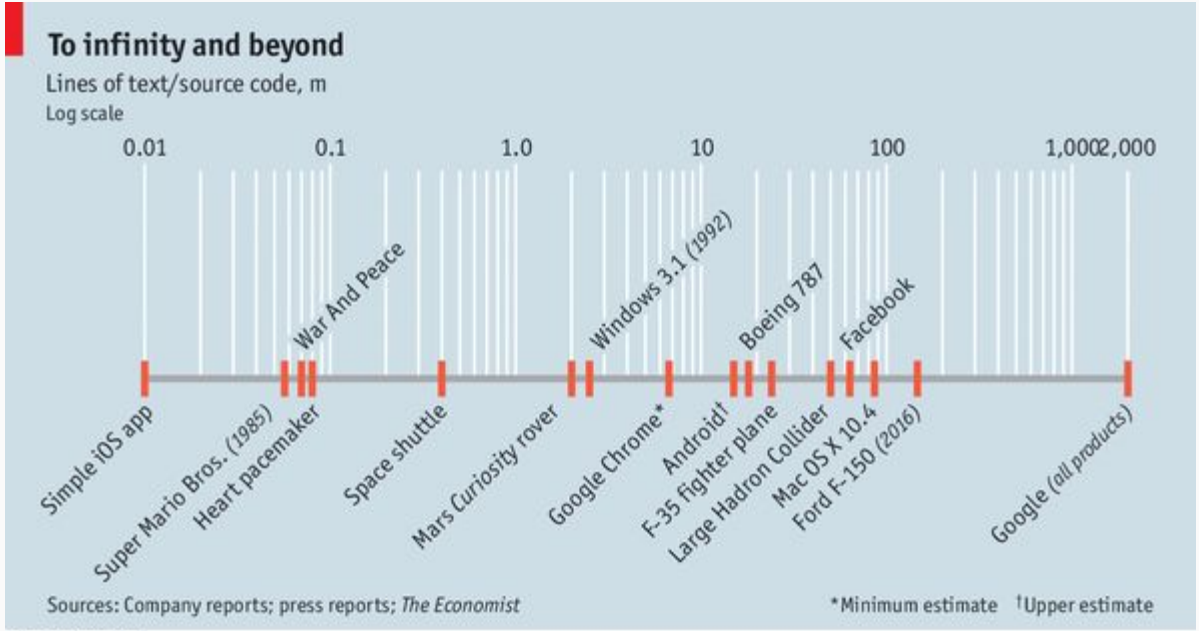
- What happened: “More than 900,000 customers (4.5% customers) of German ISP Deutsche Telekom (DT) were knocked offline”
- How: Routers got infected by a new variant Mirai; “It performs [a] command which should make the device ‘secure,’ until next reboot. The first one closes port 7547 and the second one kills the telnet service, making it really hard for the ISP to update the device remotely.”
- Result: Multi-day outage
- References:
  - http://www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13O0X4
  - https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

Case Study 3: BrickerBot

- Botnet
- What happens: “bricking Internet of Things (IoT) devices around the world by corrupting their storage capability and reconfiguring kernel parameters”
- How: “The bots brick real-world devices that have the Telnet protocol (port 21) enabled and are protected by default passwords”
- How do we know: “...detected via honeypot servers maintained by cybersecurity firm Radware”
- References:
  - https://www.bleepingcomputer.com/news/security/new-malware-intentionally-bricks-iot-devices/
  - https://arstechnica.com/security/2017/04/rash-of-in-the-wild-attacks-permanently-destroys-poorly-secured-iot-devices/

Déjà Vu: Why is This Still Happening?

- Again, not new; “New Tech, Same Old Hacks”
- “The Trinity of Trouble” (Gary McGraw)
  - Connectivity
  - Complexity
  - Extensibility
- https://www.synopsys.com/blogs/software-security/software-security/
- https://freedom-to-tinker.com/2006/02/15/software-security-trinity-trouble/



Perspective on complexity: more lines of code = more bugs

Déjà Vu: Who to Blame

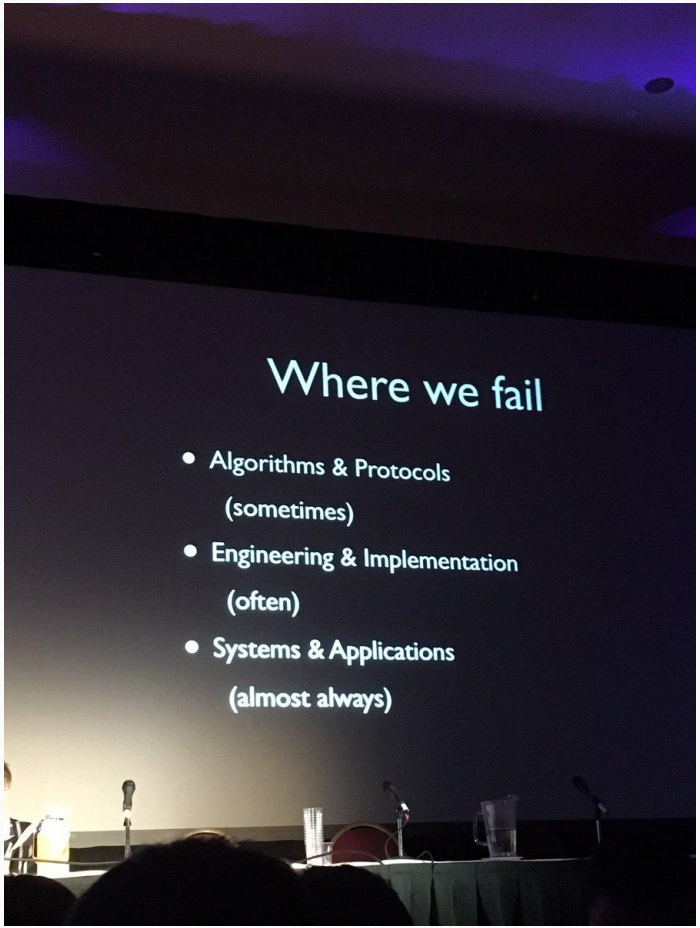
- (heard from Bruce Schneier at USENIX 2004 in Boston)
  - Developers
  - Companies
  - Technology
  - Users --but let’s not go victim blaming

Can We Make the Internet of Things (IoT) More Secure?

"The attackers only have to find one weakness. The defenders have to plug every single hole, including ones they don't know about." --Kathleen Fisher

“Shutting down every risk of abuse in millions of lines of code before people start to use that code is nigh-on impossible. America’s Department of Defence (DoD), Mr Singer says, has found significant vulnerabilities in every weapon system it examined. Things are no better on civvie street. According to Trustwave, a security-research firm, in 2015 the average phone app had 14 vulnerabilities.”

Source:
http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security



From Matt Blaze and Sandy Clark's talk "Crypto War II: Updates from the Trenches" at The Eleventh HOPE Conference in NYC, July 2017

Can We Make the Internet of Things (IoT) More Secure? (continued)

- “Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security” http://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/ > CR partners with Peiter and Sarah Zatko’s Cyber Independent Testing Lab (CITL)
- “Perhaps what is needed is for embedded systems to be more like humans, and I most assuredly do not mean artificially intelligent. By “more like humans” I mean this: Embedded systems, if having no remote management interface and thus out of reach, are a life form and as the purpose of life is to end, an embedded system without a remote management interface must be so designed as to be certain to die no later than some fixed time.” --Dan Geer (transcript: https://securityledger.com/2014/05/dan-geer-keynote-security-of-things-forum/)

Can We Make the Internet of Things (IoT) More Secure? (continued)

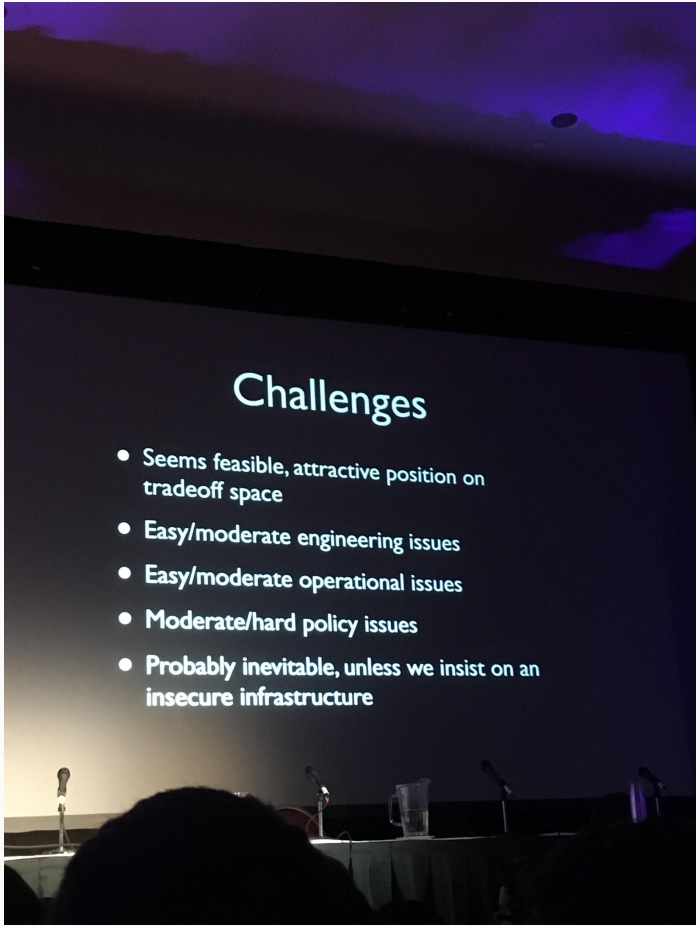
- Educate yourself and others. Visit venues like Sheep City at the Packet Hacking Village at DEF CON or the IoT Village (https://www.iotvillage.org/)
- Make software engineers go through the same rigorous standards as professional engineers (PE)
  - “Programmers: Stop Calling Yourselves Engineers” https://www.theatlantic.com/technology/archive/2015/11/programmers-should-not-call-themselves-engineers/414271/
- Don’t invest in needless things, vote with your wallet

The Most Difficult Questions: The Policy Questions

From Rob Graham's RSA 2017 talk:

- For government policy makers crafting laws/regulations
- What can government do to ward off IoT botnets?

Special note: IoT was the focus in the scenarios presented in the 2017 Atlantic Council Cyber 9/12 Student Competition



From Matt Blaze and Sandy Clark's talk "Crypto War II: Updates from the Trenches" at The Eleventh HOPE Conference in NYC, July 2017

Acknowledgements and Additional References

- Acknowledgements
  - @dotMudge
  - @MattBlaze
  - @sa3nder
  - @ErrataRob
  - @wallofsheep
  - @IoTvillage
  - @cigitalgem
  - @DanielMiessler

- References
  - https://mchow01.github.io/docs/securityofthings2015.pdf