Ubiquity, security, and you - Malware, security and the Internet of Things

Heather Goudey - Independent Researcher
Jasmine Sesso - Microsoft

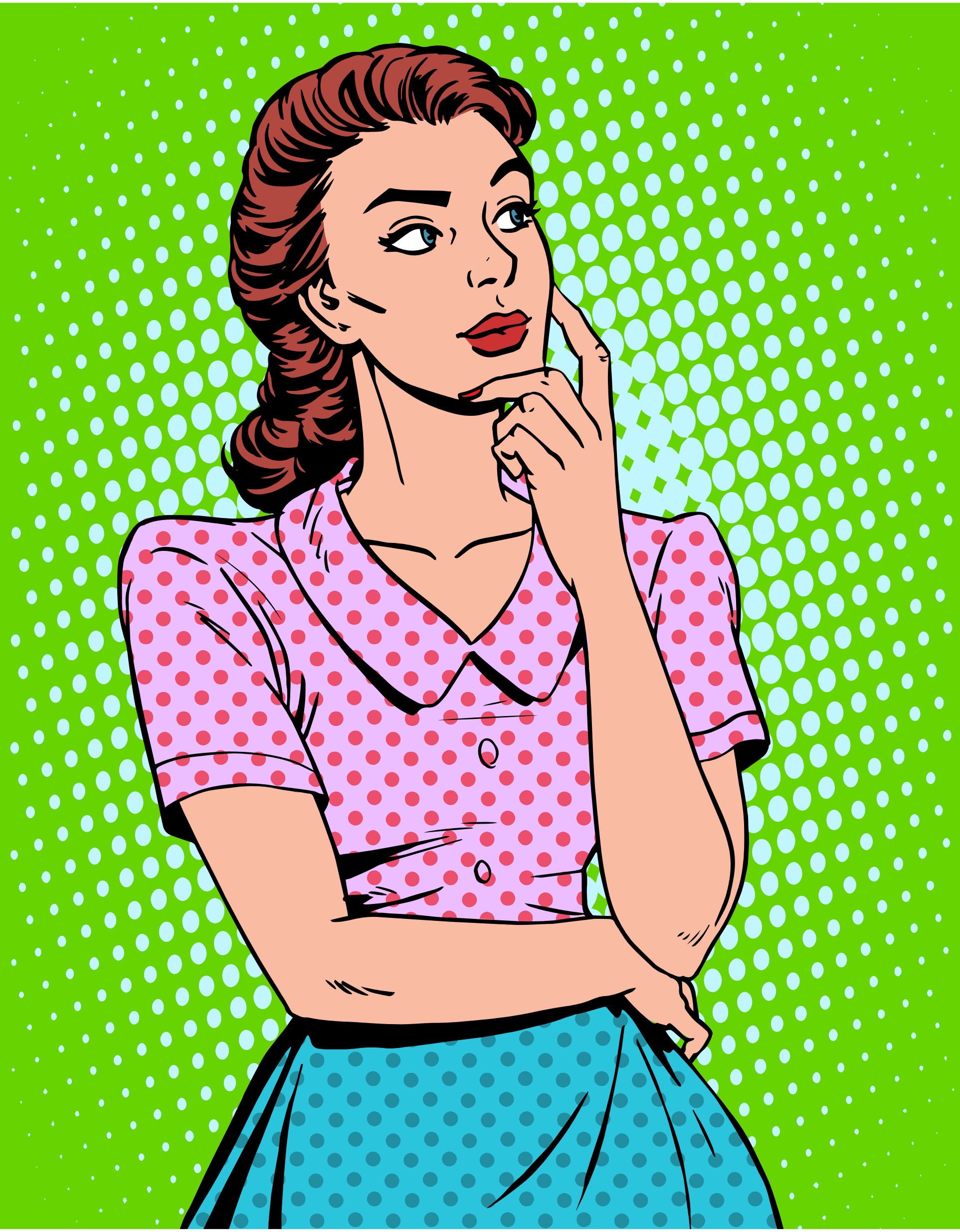
Microsoft

The Internet of Things

An Internet, **but better** because the information it captures, contains and consumes is created and managed by 'things' unfettered by the highly fallible intrusion of human-generated data.

But what is it **really?**

At a functional level, the IoT is an omnipresent mix of billions of IP-connected embedded objects, smart devices, sensors and actuators with web services in between.



More importantly, **what does it mean?**

→Some **very** big numbers

→**Massive impacts** – economic and otherwise

→**Infinite possibilities** – smart cities, smart houses, smart healthcare, smart industry, etc.

But there is a dark side...

What’s the **problem?**

The security challenges of the IoT arise specifically out of its functional and conceptual characteristics.

→Scope and scale

→Dynamicity

→Heterogeneity

(Ning, H., Liu, H. & Yang, L.T. in "Cyberentity Security in the Internet of Things")

Scope **and** scale!

The scale is beyond the capacity of mere humans to manage

Potential for multiple points of failure. Requires:

- →Redundancy
- →Fault awareness
- →Fault tolerance

Billions of objects (and more!)

Crazy amounts of data

Dynamicity

- → Objects need to interact with many different things at different times
- → Able to respond to changing conditions
- → Problems and processes are distributed
- → NOT connection-oriented
- → Security approaches don’t parallel the IoT conceptually

Heterogeneity

- → Lots of different technologies cobbled together
- → Rush to market and pressure to keep costs down
- → Data leakage – or worse (ew!)
- → Transparency
- → Some objects likely to remain vulnerable indefinitely

Privacy

- → Omnipresent sensors and data gathering
- → Data collected is often sensitive (and even more so in aggregate)
- → There’s no escape

There's a **lot of talk…**

Alert I-091015-PSA

"Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices."

But not a great deal of **action**

Current approaches:

- → Standards
- → Cryptographic mechanisms
- → Embedded security
- → Secure applications
- → Novel frameworks
- → DTLS

What’s needed?

Due to the functions of the IoT and its related constraints, solutions need to be:

Lightweight and dynamic

Able to provide assurance for the confidentiality and integrity of data

‘Things-centric’ (as opposed to ‘Internet-centric’)

Scalable (yet fine-grained enough to deal with heterogeneity)

Robust

Largely automated

Self-aware and context-aware (for example, able to recognize the state of the systems it interacts with)

Considerate of privacy

Able to adapt to changing data streams and future uses

Fail safe

But what's **likely?**

- → The market is leading the charge - security is in the rear
- → True change is likely to occur when something actually goes wrong
- → Economic factors likely to drive security development

So with **that** in mind…

- → What *might* an attack look like?
- → What *might* a compromise look like?
- → PoC, PoC, PoC, PoC, PoC…

Read all about it!

→ *"Bizarre attack infects Linksys routers with self-replicating malware!"*
arstechnica.com, Dan Goodin - February 14, 2014

→ *"The Internet Of Things Has Been Hacked, And It's Turning Nasty!"*
content-loop.com, Selena Larson - January 17, 2014

→ *"IoT malware and ransomware attacks on the incline!"*
zdnet.com, Asha Barbaschow - September 2, 2015

→ *"Internet of Things is the new Windows XP—malware's favorite target!"*
apssites.com, "admin" - April 2, 2014

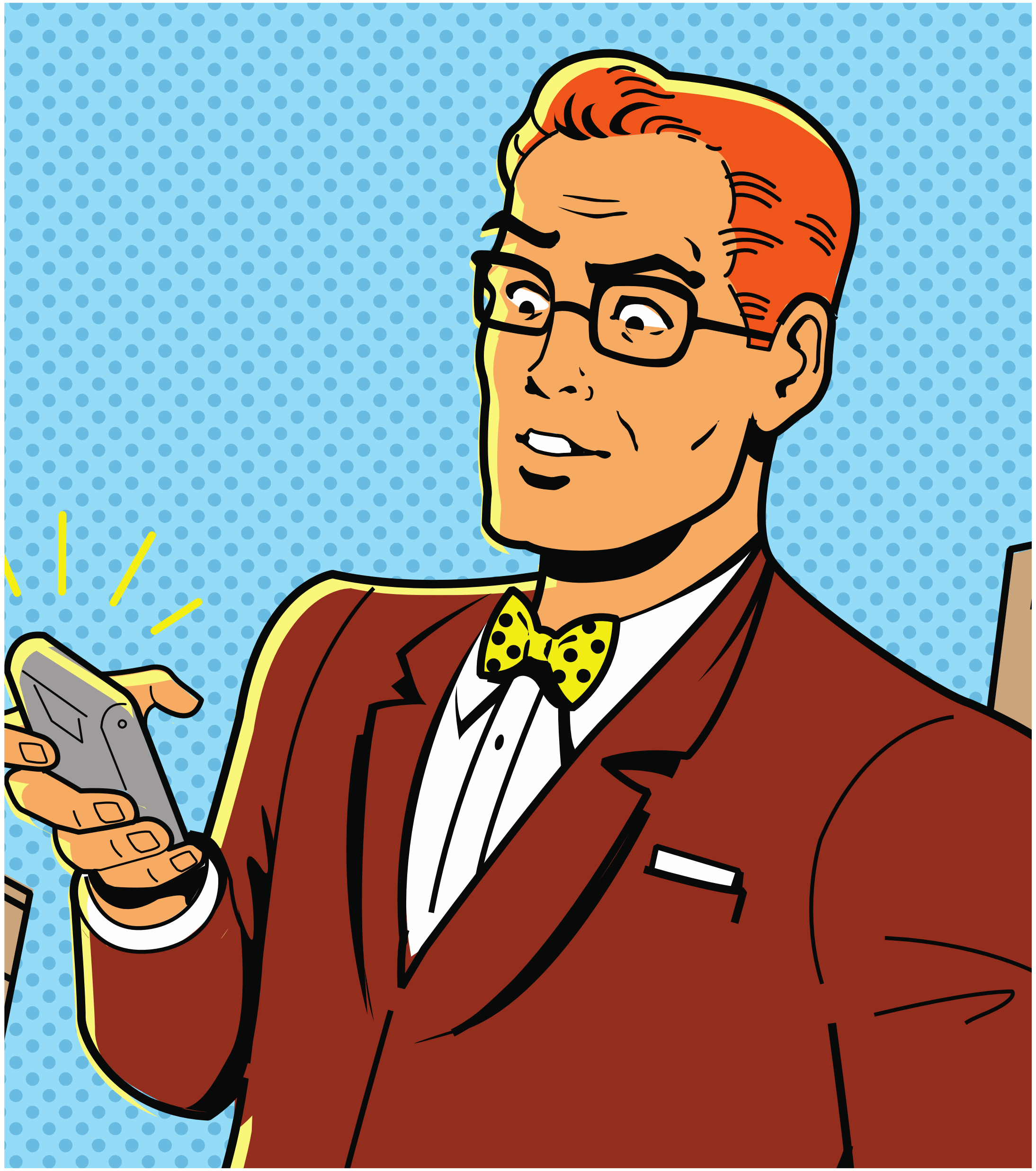
From PoC **to** attacks in the wild

→ What *does* an attack look like?

→ What *does* a compromise look like?

IoT by the **numbers**

- → What's most vulnerable?
- → What's being targeted/affected?
- → What patterns are emerging, if any?
- → What do we think might happen next?



Who’s doing what?

Many Big Names are working on embedded security products

- → In AV, one company is working on securing medical devices and another is offering IoT devices protection
- → Organizations, agencies and consortia are collaborating and devising recommendations – people are talking!

The IoT brings new opportunities

For doing good…

Questions?

Thank you!