IoT

Yeah, you know me

Hi!

> I’m Matt Lehman

> I focus on security for Ring

> Opinions expressed are my own

> Ask questions as we go

IoT 101

> The Internet has things

> We used to call them devices

> Both have been around for a while

> What’s new is the economics

Economics of Things

> The flipside of Moore’s law is that if we hold compute density even, prices have been dropping steadily and by large multiples for a while

> It causes us to ask fun questions like:

> What is the average cost per IP on the Internet?

> At what cost per IP does a device become truly disposable?

> Who would bother to secure something that is disposable and almost free?

Characteristics of Things

> Support: Managed, Manageable, **Unmanageable**

> Movement: Fixed, Mobile, **Wearable**, **Injectable/Ingestible**

> Reachability: **Global**, Local, Personal, Physical

> Resilience: Compensating, **Hopeful**, **Alone in the Wilderness**

> Purpose: **General** to Specific

> Price: Expensive to **Disposable**

Sidebar: Profiling Purpose Built Things

Fun experiment: Take a wifi camera and grab some traffic off the ethernet port of your AP

Extra credit: You can use a raspberry PI 3 and the hostAP package to turn it into a AP and just use tcpdump and ssh to grab the traffic

The traffic is super predictable - video/audio streams use common packet sizes/protocols, control plane and streaming also use the same sequencing, control plane is a small number of predictable API calls, and it always talks to the same small number of endpoints

You can use this to your advantage in your security tools - if the device has been owned it won’t act react anything like it normally does and it’s very hard to hide the IoC

IoT Contexts

> Things you own

> Things other people own

> Things that have been owned

> This influences almost all of our approaches to IoT security

Systemic Strategies

> Register everything

> Control the Internet (it’s worked so well in the past…)

> Legal/Regulatory (see Control the Internet)

> Educate

> Problems: Not much works except education

Larger scale strategies

> Manage your things

> Keep other people’s things away from you

> Pre-built containment/mitigation for owned things

> Monitor behavior

> Problems: Scale works against you for containment

Small Scale Strategies

> Manage your things

> Filter out the “bad things”

> Hide out in a Faraday Cage

> Problems: It’s hard to keep other people’s things away from you and consequently owned things away from you

Sidebar: Billions of little bots

> Most of the high profile IoT hacks involved exploiting very simple threats - common private keys and common default passwords

> This is what makes the unmanaged and unmanageable devices such a persistent threat

> Then there’s the problem that they outnumber you 1000 to 1

> Take away: Manage your devices/things

Closing up

> Things are just devices with some new obnoxious qualities

> Most of our strategies for securing devices also work well on things

> Purpose built things are very easy to profile and behavior anomalies are usually easy to see

Fin

> Thanks for your time and attention!

> Places you can find me:

> Twitter: @dmlehman

> Linkedin: https://www.linkedin.com/in/dmlehman