

Securing the Internet of Things

Fred Baker

Agenda

- I'd like to look at problems reported with the Internet of Things, and potential solutions
 - Where do known issues come from?
 - Are there assumptions that would bear a challenge?
- What can we learn from the Internet that would help?
 - What issues and potential solutions are intrinsic?
 - Can network design help?
 - Can AAA solutions help?

Issues

- Recent reports include:
 - A failing light bulb that DOS'd a home
 - <http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/>
 - Attacks in which IOT devices were infected by Bots
 - <http://www.darkreading.com/endpoint/another-iot-dominated-botnet-rises-with-almost-1m-infected-devices/d/d-id/1326776>
 - http://news360.com/digestarticle/ukyHHhsarU6yLKZr_xIQ4Q
 - Attacks in which IOT devices are engaged in surveillance
 - <https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government>
- IOT devices/applications may be designed to engage in surveillance
 - Home health care devices and applications may log or export data for medical purposes
 - GPS apps often export location or activity information
 - *IOT information also in back end systems - “the cloud”; that has to be secured as well*

I proposed this talk before the
recent wave of Mirai attacks

Just for the record

I feel like we are fighting yesterday's battle

- We have had problems with “consumer-grade” products in the Internet for quite some time
- Often essentially issues with manufacturing and specification:
 - Off-the-shelf software that is not necessarily up to date
 - Best Engineering Practices
 - Applying patches as they come out,
 - Regular software updates
 - Continuity between software or hardware versions.
- *How many products did we just describe? How many do you own?*

Add to that:

- Major argument against state of the art security software in IOT:
 - “These machines may not have enough power to implement it”
 - “There is no market for security”

Effect:

Nations regulating IOT and Internet markets

- US Presidential Cybersecurity Directive
 - <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>
- EU Cybersecurity Directive
 - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
- More to come...

So - how best to secure the Internet of Things?

Lessons from the Internet of People...

Components

- Securing Communications
- Securing sites
- Manufacturing and Maintenance

Securing Communications

- What can be secured?
 - Data at rest (record encryption)
 - Data in flight (encrypted transfer, encrypted query/access)
 - Sessions (TLS, DTLS, IPsec, http/2)
 - http/2 allows secured encapsulation of multiple sessions
 - Peers (mutual authentication/authorization)
- Which is best?
 - All are needed, but maybe not all at the same time

Thinking about IOT data flows

- Many, especially in academia, look at IOT as a great source of data to study.
 - Lots of flows, lots of traffic, Big Data is all the rage.
- Think about this: if you suddenly have everyone else's data to look at and make inferences from, *they also have yours*.
 - *Is that what you intended?*

Site security

This is not a plug for perimeter security (firewalls)

- **However, it can have its uses...**

Three major ways IOT devices communicate:

- **Locally among peers or with a manager**
- **With a remote manager**
- **Among a set of peers managed remotely**

Site security: Local-only access

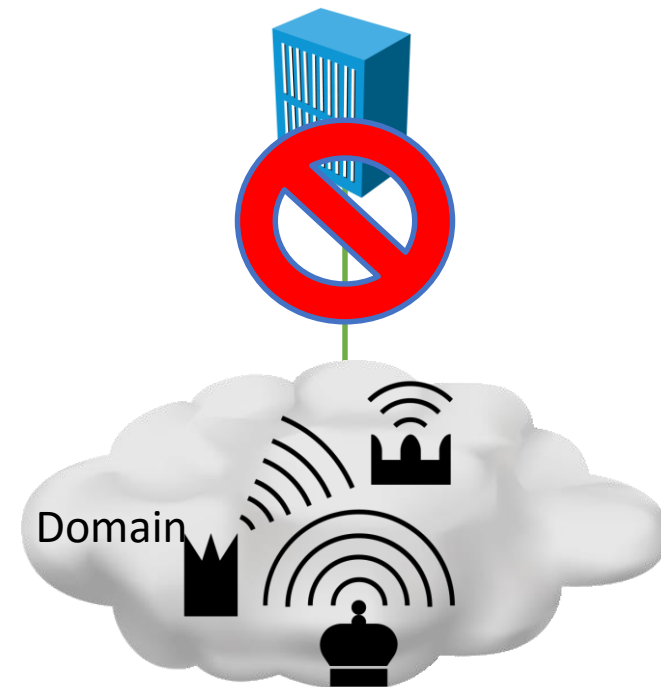
This is not a plug for perimeter security (firewalls)

- However, it can have its uses...

Three major ways IOT devices communicate:

- **Locally among peers or with a manager (air gap, addressing, or firewall)**
- With a remote manager
- Among a set of peers managed remotely

- Premise: if it has no route, it can't be attacked.
- But consider Stuxnet, and firewall-hopping viruses



Created by Michael Wohlwend
from Noun Project

Site security: Remote Manager

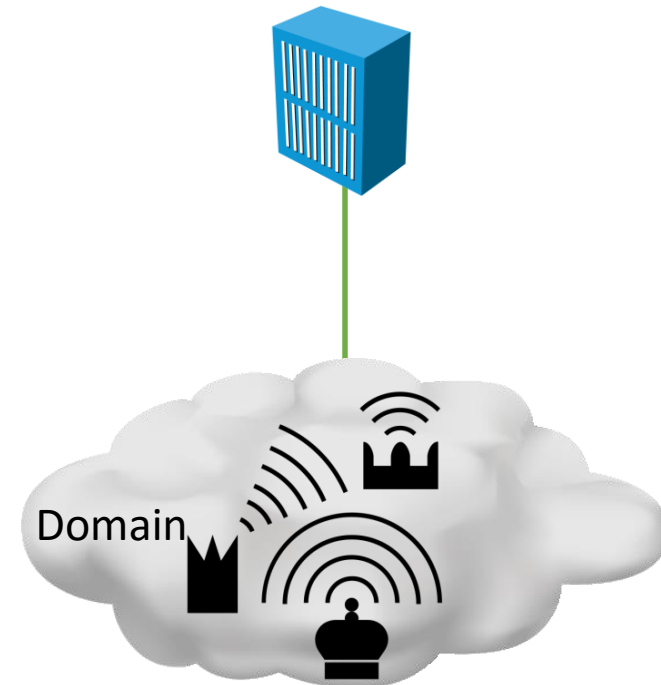
This is not a plug for perimeter security (firewalls)

- However, it can have its uses...

Three major ways IOT devices communicate:

- Locally among peers or with a manager
- **With a remote manager**
- Among a set of peers managed remotely

- Alexa, Siri, others
- Is your data visible to others? Recorded? Encrypted? Do you know?



Created by Michael Wohlwend
from Noun Project

Site security: Gateway plus Remote Manager

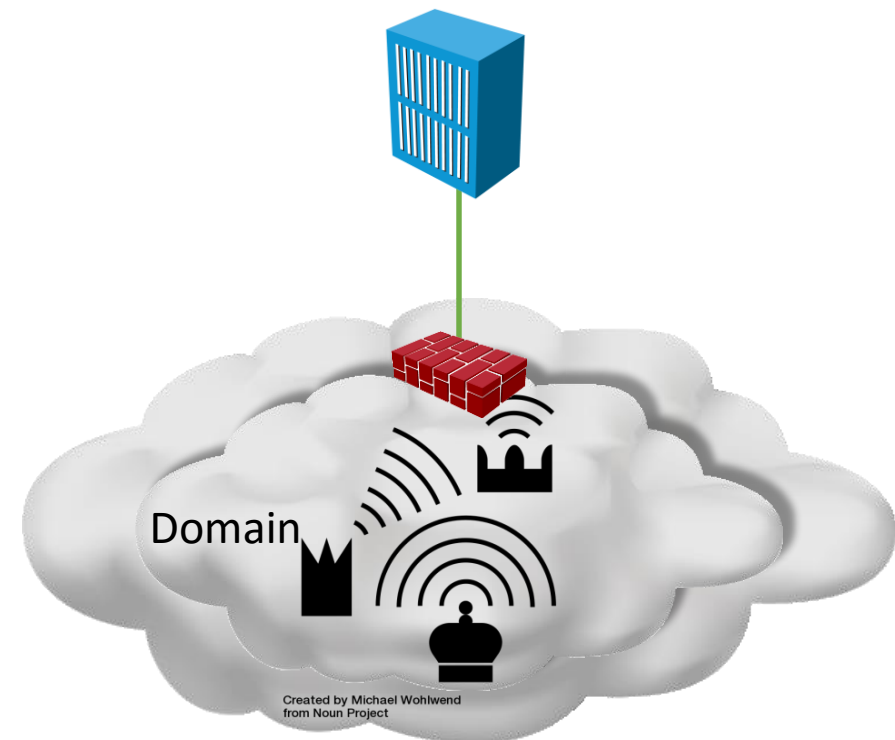
This is not a plug for perimeter security (firewalls)

- However, it can have its uses...

Three major ways IOT devices communicate:

- Locally among peers or with a manager
- With a remote manager
- **Among a set of peers managed remotely**

- AMQP, MQTT, and others
- Enables gateway function that limits access to the domain



Who is ultimately responsible for device security?

- We teach our children to not talk with strangers
 - Why do we let our computers talk with strangers?
- The network can provide a second layer of security
 - Defense in depth
- Ultimately, every device has to protect itself
 - Many attacks come from behind site security technologies
- How?
 - **Mutual authentication** – IOT devices have a small number of peers they are intended to communicate with, and those peers have specific things they can do.
 - Introduce them, and don't let others intrude.

Example: Home Health Care

- **Imagine you have a motion detector and bed monitor at your mother's house, so you can tell if she's OK**
 - You and her doctor know
 - Whether she got up today,
 - What part of the house she is in
 - You can measure her heartbeat and motion in bed
 - Intelligent alerts can get your attention if needed
- **Who needs to know?**
 - Her doctor, you,
 - not nosy neighbors or thieves
 - What if someone hacks the server?
 - is her data were encrypted?
 - Communications in flight –
 - Server identity can reveal information
 - And of course, what computers should the probes communicate with? Not just anybody...

Manufacturing and Maintenance

- Open Source software is often a good source of functionality
 - Even so, it is often not up to date, and needs to be updated as vulnerabilities are identified
 - This is an ongoing problem
- Testing:
 - Test the failure modes as well as the normal operation modes. You don't want to own the light bulb that DOS'd a house.
- When patches become available, you want them applied
 - Vendor should be maintaining/curating software
 - Device should update software from a provable source
 - On installation
 - On demand
 - Periodically

The lesson from Mirai

- Manufacturers are being forced to recall product
 - <http://www.welivesecurity.com/2016/10/24/webcam-firm-recalls-hackable-devices-mighty-mirai-botnet-attack/>
- Tell me about “shooting the messenger”?
 - <http://www.welivesecurity.com/2016/10/24/webcam-firm-recalls-hackable-devices-mighty-mirai-botnet-attack/>
- Wouldn't it be better if they could post a new software load and tell users to trigger a software update?
 - Or had updated the software before the attack was launched?
 - Or followed security 101 (not left a well known password open) before the product left the door?
- Come on, guys. We know this. It's not news. We can do better.