Beyond The Toaster Oven

Building A Secure Future For The IoT

DR. PAUL VIXIE

Traditional Internet-Connected End-User Devices

- Short product lifetime (laptop: 3-5 yrs; phone: 2 yr contract)
- Small number of devices per home (1-2 per person)
- Abundant CPU, memory, storage + full display & keyboard I/O
- Full network connectivity
- Mature cryptographic support
- Well-defined (and user-expected) patching process

IoT By The Numbers

By 2020, there will be **38.5 billion IoT** devices
(Juniper Research)

Traditional connected devices like PCs, smartphones and tablets now **account for less than 1/3** of all connected devices. (Strategy Analytics)

Sensor market to grow to more than **$115 billion** by 2019
(*Automation World*)

90% of data generated by smart devices is never analyzed or acted on (IBM/*IndustryWeek*)

70% of smart gadgets have serious security flaws
(2014 HP Security Report)

The Internet of Things Defined

The current "Internet of Laptops" is more than JUST an Internet of laptops and smart phones, it also includes "things" such as:

-- Tablets
-- VoIP phones
-- Printers
-- Game consoles
-- TV set top boxes
-- Internet radios
-- Home surveillance cameras
-- Pacifiers

Etc., etc.

AND the home wireless "routers" that provides an RFC 1918 NAT'ed address environment connecting them all

IoT: Smart Baby Pacifier and Hapifork

The "Internet of Things" Is Not Like The "Internet of Laptops and Smart Phones"

The IoT is not a single **category** of device. Rather, it can be:

- Simple network-connected sensors (smoke detectors, etc)
- Numerous cheap/limited-lifetime network-controlled devices (such as programmable networked light bulbs)
- Expensive network-connected "durable" household goods (such as smart TV sets and smart kitchen appliances)
- Infrastructural items, such as smart meters adopted by a local utility company for differential billing purposes
- Networked mobile systems, including cars that monitor location, driving behavior, engine condition, etc.
- Biomedical devices (glucose monitors and insulin pumps, cardiac monitoring and pacing equipment, etc.)

IoT Challenges

Optimistic threat models: who'd even be interested in attacking "smart" utility meters? (no one, *no one at all*, *no....*)

Rapid time-to-market: entirely new classes of devices rapidly taken to market due to business pressures, without extensive hardening, or even much time for testing and bug elimination

Price points: inexpensive devices don't have much margin to cover the cost of security engineering and security operations

Long (or short!) product lifetimes: IoT devices may have a lifetime that's radically different than a laptop or smart phone

Limited man-machine interface capabilities: IoT devices may not have a dedicated display or a dedicated input device

Consumer willingness to maintain IoT devices may be low: are you really going to update your thermostat's firmware?

Some Similarities to the "Internet of Laptops"

While some IoT devices may run an actual real-time embedded operating system, most will just use a stripped down version of Linux or Microsoft Windows, just like traditional devices (obviously this is very familiar to hacker/crackers interested in *attacking* the IoT)

IoT devices will routinely use WiFi and the Internet for their local and wide area network connectivity, just like traditional devices (again, familiar/convenient territory for attackers)

Configuration and control may be via a dedicated handheld remote (crude and non-scalable), or via a web GUI (often w/o proper TLS protection and certificate validation) through the user's laptop or smart phone (have *those* control units ever been attacked?)

Authentication may be primitive (e.g., plain old passwords)

SCADA Problems Recapitulated?

Ten years ago Farsight Security staffer Joe St Sauver was invited to speak about security issues with SCADA systems by the FBI Infragard, see
https://www.stsauver.com/joe/scadaig/infraguard-scada.pdf

SCADA security is typically five to ten years behind typical information technology security (IoT: the same?)

Often SCADA devices are assumed not to be Internet accessible (implicitly true for IoT, where RFC1918 space is assumed to be the norm?)

Compromises=serious real-world impacts (people hurt/killed)

Crude protocols (no positive confirmation feedback loop)

Long lifecycle devices, etc., etc., etc.

Will we ever learn?

What Must We Do? Design Phase

First, and most critically, security cannot be "bolted-on" as an after thought. IoT devices need a *security architecture* as an integral part of their initial – and *final* – design:

-- Can the device survive exposure to the global Internet (rather than being sheltered behind a network firewall)? Has the device's attack surface been minimized? Or is "everything" enabled by default?
-- How will user access be enabled and controlled? (e.g., what's the plan for scalable identity management?)
-- How will any discovered software or firmware bugs be quickly and securely patched?
-- Will the hardware have the horsepower and memory it needs to run protocols protected by strong encryption?

Companies should conduct a privacy or security risk assessment as part of the design process; test security measures before a product is launched (FTC)

What Must We Do? Incident Management

Let's assume that a latent vulnerability is exploited and hundreds (or thousands) of IoT devices are compromised. How will we recover from that sort of attack?

Will we need to physically touch every device, and perform a hardware-reset-to-default-factory-configuration for each one? Pushing the hidden reset switch is fine for the onesie-twosie case, but impractical as the number of devices increases, and much of the value of the device comes from its saved state, accumulated over time.

Allowing network resets would be more convenient, but that also sounds like a terrific potential attack... and do we really think Joe or Jane Average User would know when they really need to pull the trigger on that sort of thing?

What Must We Do? Operational Lifetime

Fielding a hardware device is like deciding to start a family: you're making a long-term commitment to support what you create. In the case of hardware:

-- Are you ready to accept bug reports, and develop and distribute patches (and NOT just via download and tftp!)

-- Have you been clear about your expectations for product lifetimes? People may expect to rely on it for 2 or 3 times that period. Are you ready to provide support for that long a time, even far after revenue from active product sales have long stopped? Publish product lifecycle information!

-- What will happen to device software and firmware images if the company goes bankrupt? Will those be escrowed and eventually open-sourced or ?

What Must We Do? Long Term Success

Over the long term, the top challenge will be working to achieve *standardization* and *interoperability* (which will help greatly when it comes to delivering scalability).

We also need to work to obtain maximum value from the IoT by treating it as a *system* rather than scores of disjoint devices. That implies either:

-- a centralized controller-based architecture (with all the associated implications for single-points-of-failure) OR

-- devices that are able to securely and automatically peer with other authorized devices – but not random third-party devices controlled by a 3rd party attacker.

The Need To Protect Privacy

With IoT, manufacturers can give each of their physical assets a digital identity that enables them to know the exact location and condition of those assets in real time

IoT devices, if ubiquitous and pervasive, have the potential to totally undermine our privacy. This cannot be allowed to happen.

For example, users must be able to physically block cameras and disconnect microphones to block eavesdropping.

A more subtle privacy aspect of the IoT is the need to ensure that "innocuous" sensor data (such as electricity usage patterns) doesn't get uploaded and exploited by those who might seek to do so, without the knowledge and informed consent of those providing that data.

Partnerships Are Key To IoT Success

The IoT won't be able to successfully and securely be deployed unless partnerships are forged:

-- All IoT vendors need to work together for interoperability

-- Broadband ISPs providing wide area connectivity are the ones who are going to be best positioned to see (and to potentially be able to help deal with) IoT devices that are being attacked, or which have been compromised (and which may even be getting misused to attack other network-connected sites)

-- Suppliers of consumables (e.g., food for refrigerators, clothing manufacturers for washers and driers, etc.) need to be convinced to enable RFID/other sensor technologies

We Need to Stop Standing On Our Own Boot Laces

If the IoT has had a slow rate of uptake by rightfully skeptical consumers, it may be because we are holding ourselves back:

-- Consumers need a compelling value proposition for adding more complexity to their lives. WHY do users need smart light bulbs or a smart refrigerator? What **real** value will those devices deliver that dumb versions can't?
-- Consumers know that things connected to the Internet must be carefully secured, and they've seen what happens when their laptops and smartphones aren't. Those who field IoT devices need to convince consumers that their IoT devices are different, their IoT devices WILL be secure.

Ultimately, this will be the only path forward.

Recommendations

- Security cannot be an afterthought – instead, it must be "baked" in throughout the product lifecycle of the expected billions of **IoT** devices
- Device mfrs must be held accountable – Set a floor on quality and thus the QA budget
- A IoT device needs to ability to be patched throughout that product's expected lifetime.
- Consider Dan Geer's recent proposal – A non-patchable embedded device would expire
- Consumer privacy must be protected at all costs

Thank you!

For more information, contact:

Dr. Paul Vixie

CEO, Farsight Security, Inc.

vixie@fsi.io

https://www.farsightsecurity.com