Analysis, Implications, and Challenges of an Evolving Consumer IoT Security Landscape

Christopher Bellman & Paul C. van Oorschot
Carleton University, Ottawa, Canada
PST2019, August 28, 2019

chris@ccsl.carleton.ca

Carleton
UNIVERSITY

The “Internet of Things”

“**Internet of Things**” (IoT)

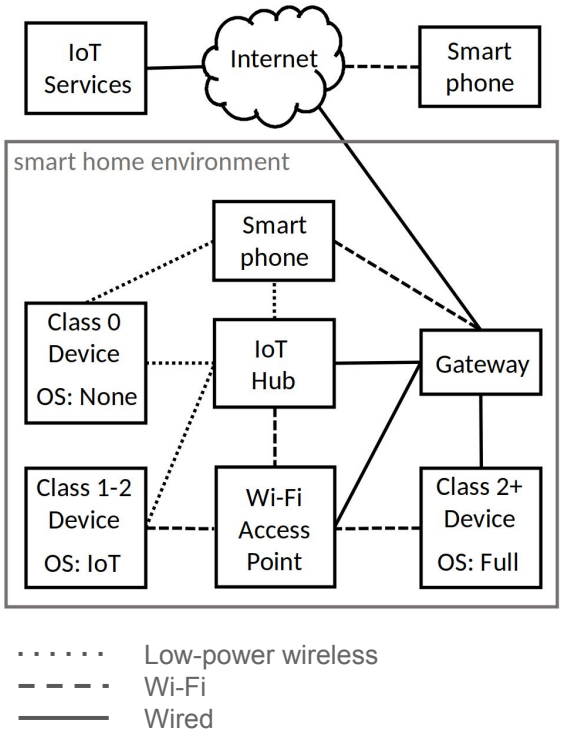
- Commonly, “**adding** network connectivity **to everyday objects**”
- E.g., toaster, TV, thermostat

Being added everywhere:

- **Critical infrastructure**: Power, water, telecom
- **Smart cities**: Road sensors, traffic lights, security cameras
- **Industrial**: Building lighting, automated factories, remote monitoring

Our focus: **Consumer-grade** devices

- Common to have many devices per house



Distinguishing Characteristics of IoT

Internet of Computers (IoC)

- Desktop/laptop computers, smart phones, servers, etc.

While similar in many ways, the **IoT differs** from the **IoC**

We highlight five **characteristics of IoT**

- These characteristics **distinguish IoT from IoC**

Each characteristic has **implications for IoT security**

- These **implications** present **unique issues** that will need to be addressed

1. Low-Cost (Section III-A)
   - Constrained resources
   - Smaller/no OS
   - Need for more efficient protocols
   - Need for lightweight crypto
   - Over-provisioned functionality (cost-friendly component re-use)
   - Manufacturer security inexperience (IoT sub-component)
2. Non-Standard Interfaces (Section III-B)
   - New attack surfaces
   - Greater physical access to devices
   - Complicates device management, configuration, updates; exacerbated by scale
3. Cyberphysical Interaction (Section III-C)
   - Successful network attack may affect physical world
   - Implied trust in manufacturer
4. Expectation of Long-Lived Devices (Section III-D)
   - Lack of software updates may leave vulnerabilities unpatched
   - Forgotten devices remain attractive targets
   - Device outliving manufacturer impacts software updates
   - Cryptographic algorithms and protocols must be future-proofed
5. "Many-User" Devices with Unclear Authority (III-E)
   - Home guests may be denied functionality of critical services
   - Rogue guests may retain remote access
   - Difficult to differentiate authorized and unauthorized users

1. Low-Cost

Everyday devices but with included **network connectivity**

- "**Low-cost"** referring to **IoT sub-component**
- E.g., adding communications to a toaster, TV, light bulb, door lock

Manufacturers may **favour low-cost** and **market presence** over security

- Investing in **security** generally costs **more money**
- Security often takes back-seat while establishing presence

Implications for security:

- Constrained **resources**
- **Small/no OS**
- Need for more **efficient protocols**
- Need for **lightweight crypto**
- **Over-provisioned** functionality (**cost-friendly** component reuse)
- **Manufacturer** security **inexperience** (for IoT sub-component)

2. Non-Standard Interfaces

Typical device **interfaces/interaction design**:

- IoC: **keyboard + mouse, touchscreen** ← **“standard”** interfaces
- IoT: **phone/hub, voice, cloud-based web** ← **not standard** interfaces

Device diversity is high

- Many different interfaces, interaction styles
- Possibly highly-constrained, some interfaces may not work

Implications for security:

- **New** attack **surfaces**
- Greater **physical access** to devices
- **Complicated** device **management, config., updates**; exacerbated by scale

3. Cyberphysical Interaction

Terms “Cyberphysical system” and “IoT device” have merged definitions over time

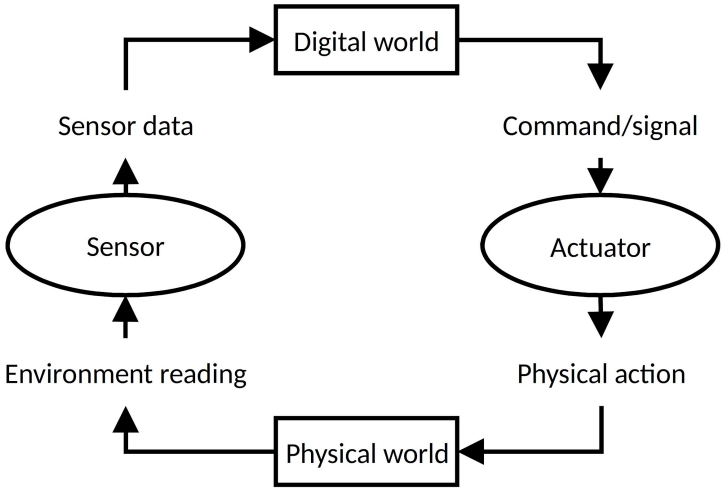
- For our purposes, simply “a device that **interacts with and affects its environment**”

Two basic types of **cyberphysical** device:

- **Sensor** (physical→digital)
- **Actuator** (digital→physical)

Implications for security:

- Successful **network attack** may **affect physical world**
- Implied **trust in manufacturer**



4. Expectation of Long-Lived Devices

Users expect their devices to last for a **long time**

Depending on the device, **interaction** may be kept at a **minimum**

- A “**set-and-forget**” device to function for a long time
- A smart motion sensor: set up, forgotten about until it stops working

Implications for security:

- **Lack of software updates** may leave vulnerabilities unpatched
- **Forgotten devices** remain attractive targets
- Device **outliving manufacturer** impacts software updates
- Cryptographic algorithms and protocols must be **future-proofed**

5. “Many-User” Devices with Unclear Authority

In **IoC**, devices are “**multi-user**” or “**single-user**” based on architecture and usage

- **IoT** devices often **belong to** an **environment** rather than a user
- **IoT**: may be used by **many users**, without identification → a “**many-user**” device
- E.g., Amazon Echo voice commands

Implications for security:

- Home **guests** may be **denied** functionality of **critical services**
- Rogue **guests** may **retain** remote **access**
- **Difficult to differentiate** authorized and unauthorized **users**

Common Themes

Two common **themes** visible in **IoT**:

1. Current/expected **scale**
    - The **scale** of IoT **exacerbates problems** associated with characteristics
    - Methods for **handling scale** will become **increasingly important**
2. **Lack of** standard **toolkits/software**
    - Generally acknowledged that **IoT** is **vulnerable** - what **tools** are available **for developers?**
    - Given **resource constraints**, we need:
        - **Lightweight** crypto toolkits
        - Common **algorithms updated** to meet **performance challenges**
        - **Securely-designed OSs** for Class 1+ devices (**common codebase**)

Analysis, Implications, and Challenges of an Evolving Consumer IoT Security Landscape

Christopher Bellman & Paul C. van Oorschot
Carleton University, Ottawa, Canada
PST2019, August 28, 2019

chris@ccsl.carleton.ca

Carleton
UNIVERSITY

Constrained IoT Devices

RFC 7228 Class	Volatile memory (KiB)	Non-volatile memory (KiB)	OS & Communications
Class 0	<<10	<<100	**OS:** Function-specific hardware, few IoT OSs **Comms:** Basic health indicators, keep-alive messages; requires intermediate node for further communication
Class 1	~10	~100	**OS:** IoT-specific OSs **Comms:** Lightweight wireless (e.g., BLE)/wired, UDP-based protocols
Class 2	~50	~250	**OS:** IoT-specific OS **Comms:** Lightweight wireless/wired, UDP-based protocols, commonly-used upper-layer protocols
Class 2+	>50	>250	**OS:** IoT-specific, full OS (e.g., Linux) **Comms:** Commonly-used communication protocols