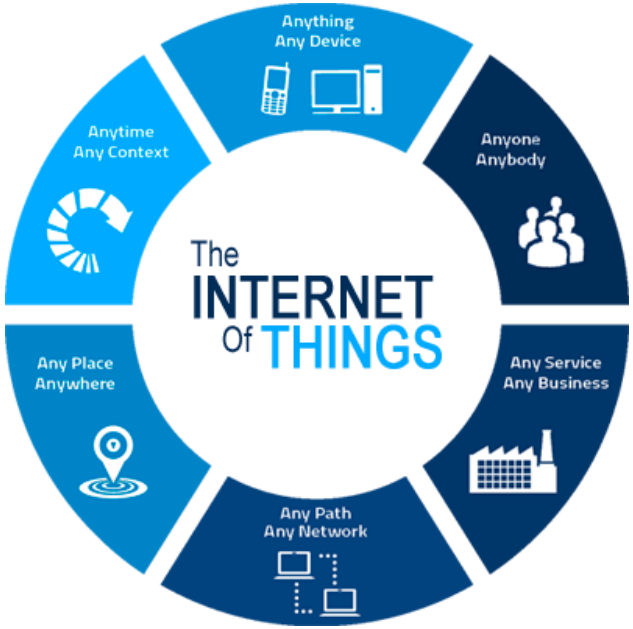
Sandia National Laboratories

Exceptional service in the national interest

IoT Security: The Internet of Other People's Things

Jack Wampler

Thanh Nguyen



U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2016-7001 PE

So what is IoT?

Sandia National Laboratories

At it's core, IoT devices are:

- Embedded systems
- With network connectivity
- And a physical component

None of these things are new!

The applications and ecosystems of these devices bring about new challenges

So what is IoT?

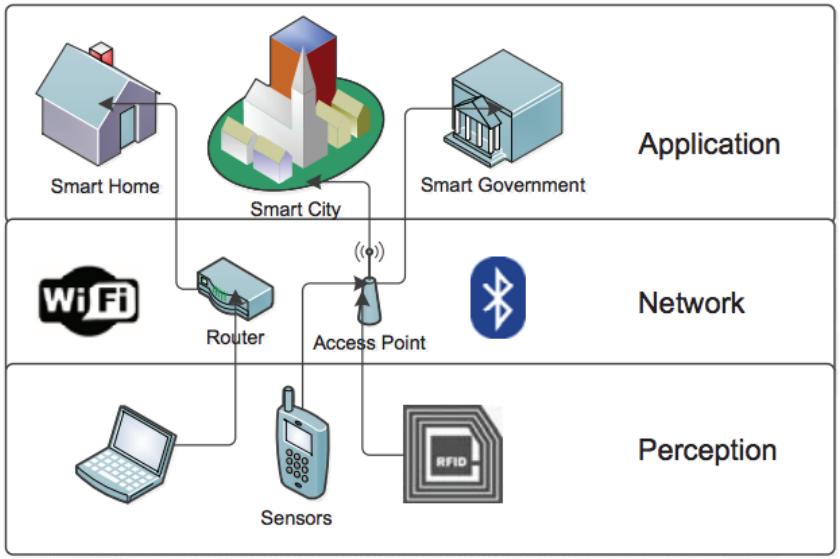


Figure 1. Three-layer IoT architecture.

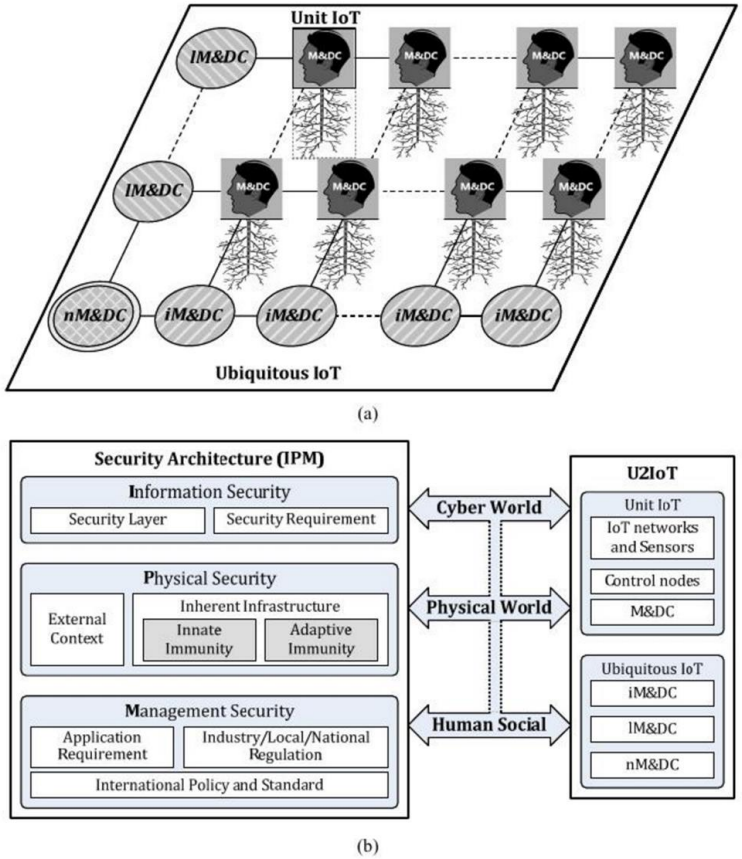
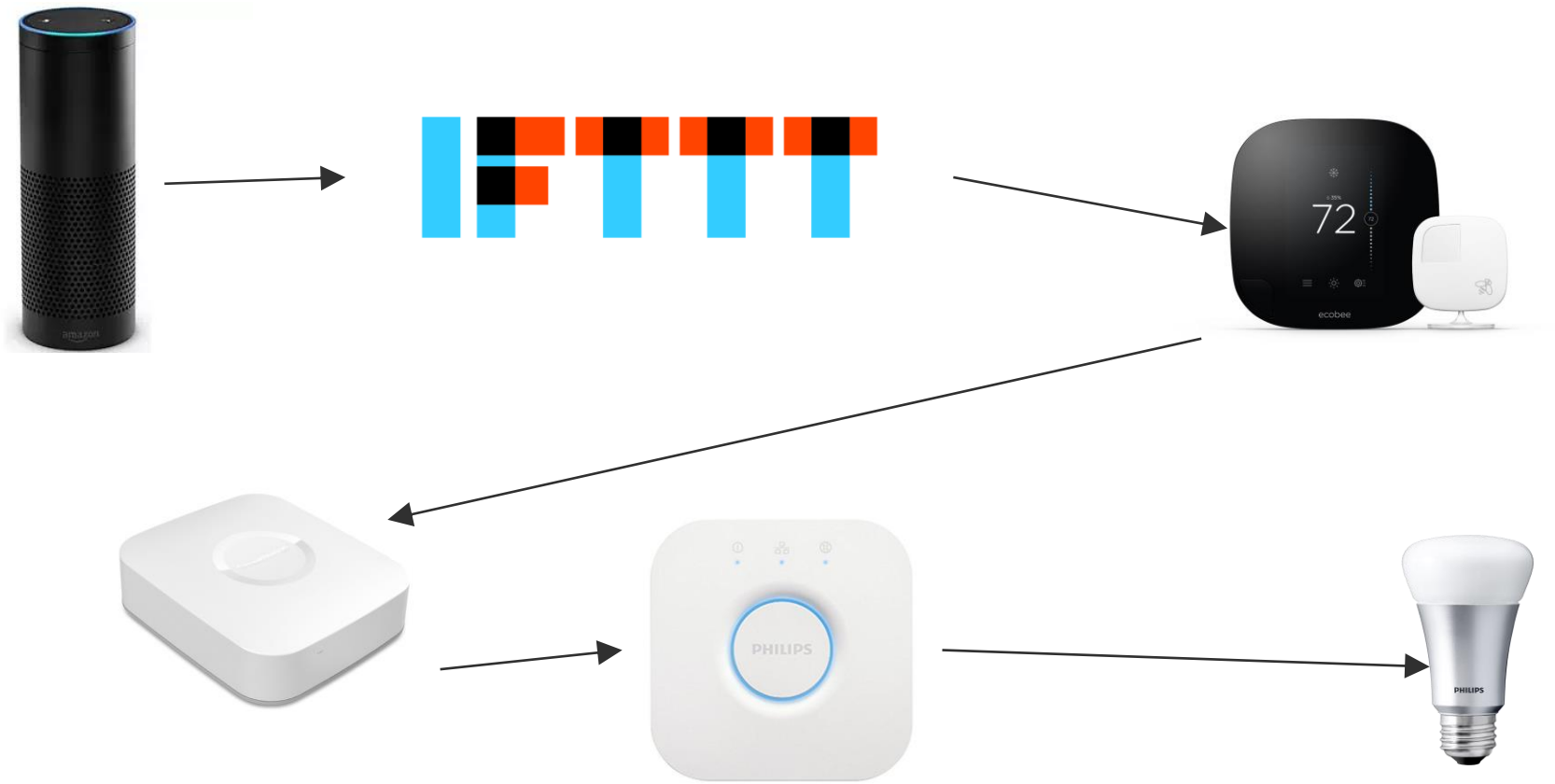


Figure 1. U2IoT model and its security architecture (IPM). (a) The U2IoT (Unit IoT and Ubiquitous IoT) model; (b) The proposed security architecture (IPM) based on U2IoT.

Today's IoT devices

The things must interact!



Risk

Sandia National Laboratories

- Encryption Vulnerabilities
- Complexity of Intertwining network technology
- Account and data management
- Cross platform capabilities & vulnerabilities
- Correlating human behaviors with cyber systems (Spying on someone)
- Human safety concerns with bridging the cyber and physical world

Project Goals

Sandia National Laboratories

- Define the “real” security model of IoT, as actually implemented by today’s IoT devices. Show how this clashes with previous work, and common security best-practice.
- Document the primary types of device and service interactions (Bootstrapping, Control, Sharing) in the modern IoT ecosystem.
- Propose a better solution for each that mitigates security concerns without sacrificing usability.
- Explore compromise scenarios
- Back the above with any vulnerabilities discovered during this work

Approach?

Sandia National Laboratories

- **Reverse Engineering:**
  - Android APK (Android Application)
  - Firmware
- **Pentesting**
  - Network
  - Web Service
  - Android APK
  - Bluetooth
  - Low frequency radio waves protocol(Zigbee, Z-Wave, etc)
- **Locate Encryption Vulnerabilities**
- **Accessing Data Leakage**
- **Documentation**
  - Vulnerabilities, protocols, and security architectures

Findings

- **Evaluated a number of consumer products**
  - Locks
  - Camera
  - Hubs
  - Sensors
  - Switches
- **Diverse Array of Security Models**
- **General Problems:**
  - Encryption Issue
  - Data Management
  - Authentication/Environment Assumption

Sandia National Laboratories

Questions, Comments, Concerns?!