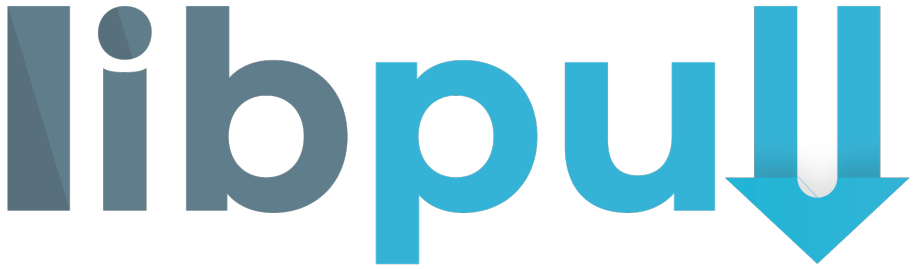


The Portable Updates Lightweight Library

Antonio Langiu

Outline

- Introduction to the Internet of Things;
- Internet of Things Security;
- Software Updates;
- Software Updates for Constrained Devices;

What is the IoT?

- The network of identifiable actuators and sensors connected to the Internet with the goal to create a connected and fluid world;
- Every object could becoming smart and connected;
- Expected 26 Billion Units By 2020;

https://www.gartner.com/newsroom/id/2636073

Where is the IoT?

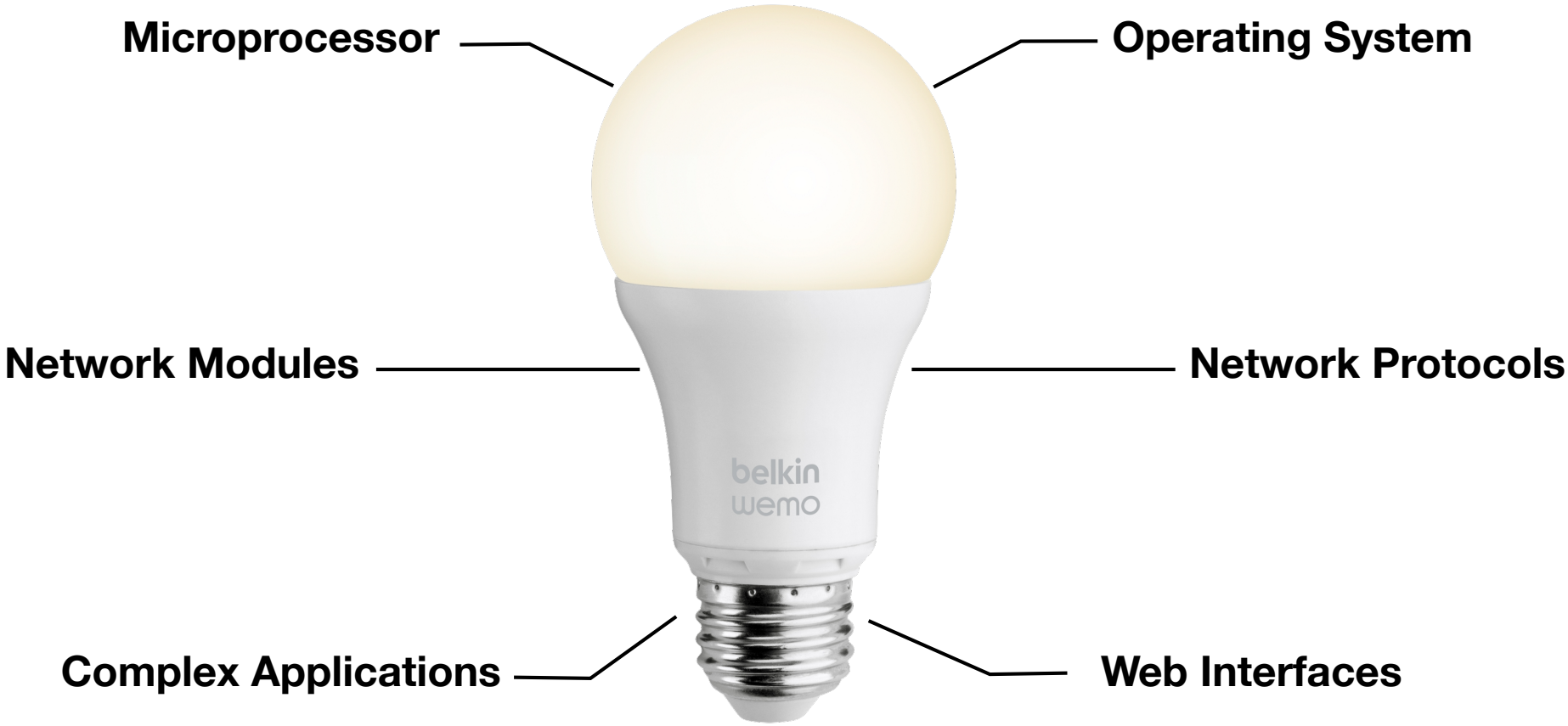
- Wearable;
- Smart cities;
- Smart homes;
- Transports;
- Health care;
- …

What is the IoT, really?

A computer included into an object.

User’s Perception

User’s Perception



Vendor’s Perception

Vendor’s Perception

How does the IoT perception impact security?

The S in IoT stands for Security

Attacks to IoT

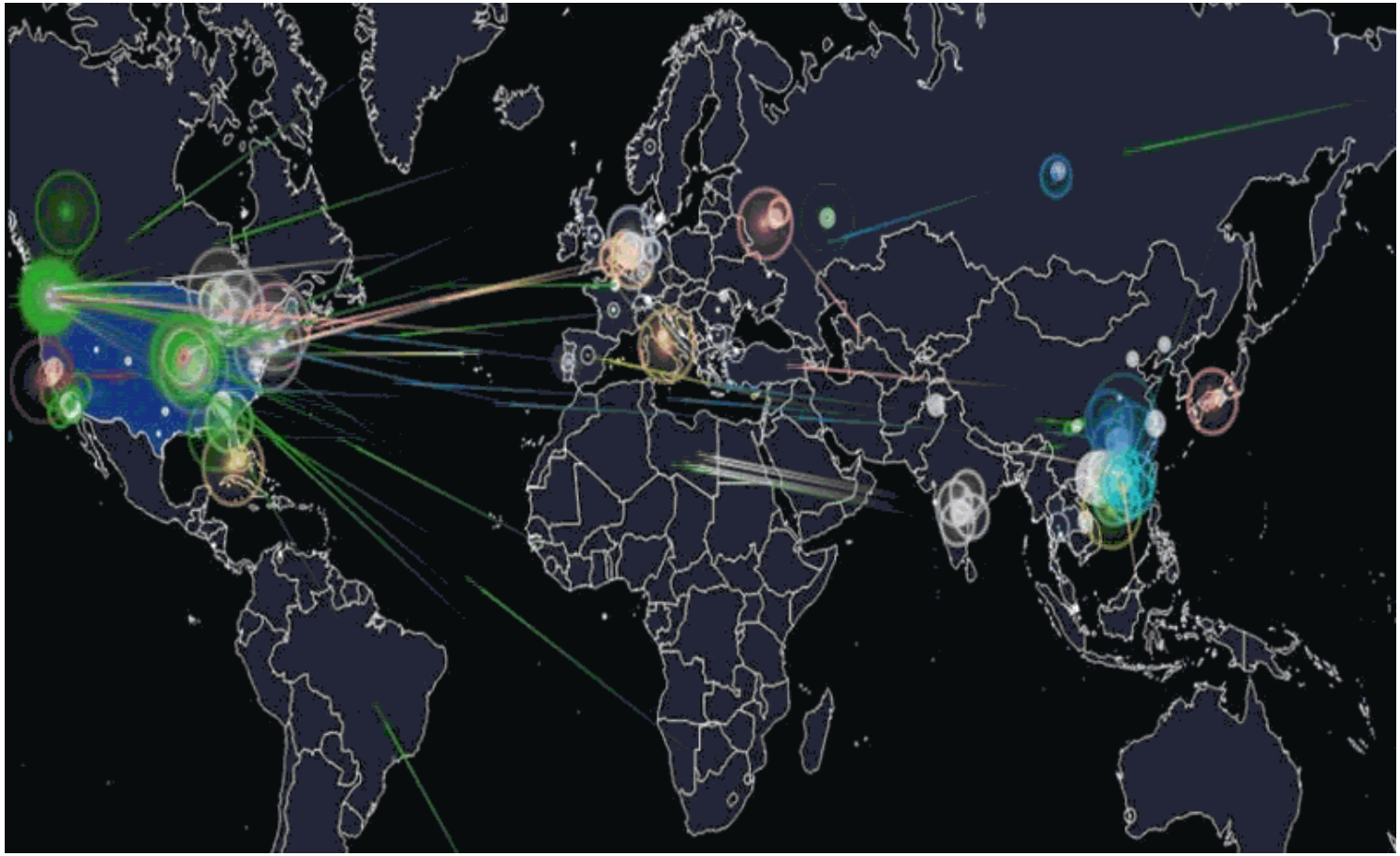
July 2017, Attacker Uses Smart Fish Tank to Steal Casino Data

https://goo.gl/aQPN49

https://github.com/nebgnahz/awesome-iot-hacks

Attacks from IoT

October 2016: Mirai botnet performed huge DDoS



Many others:

- Persirai;
- Imeij;
- Amnesia;
- Reaper;
- …
- BrickerBot

https://www.theguardian.com/technology/2016/oct/ 26/ddos-attack-dyn-mirai-botnet

Change of Perspective

We need to rethink the current IoT paradigm, shifting from considering IoT devices as simple objects with some integrated smart feature to treat them as computers which do specific jobs.

IoT security

- Many challenges to solve IoT security. One of them is software updates.
- Many IoT devices have unpatched vulnerabilities;
  - Vendors did not included an update system;
  - Vendors included an update system but did not send software updates;
  - Users do not secured or updated them correctly;

Software Updates

Why?

Introduce new features

Fix implementation bugs

Fix security vulnerabilities

How?

Locally

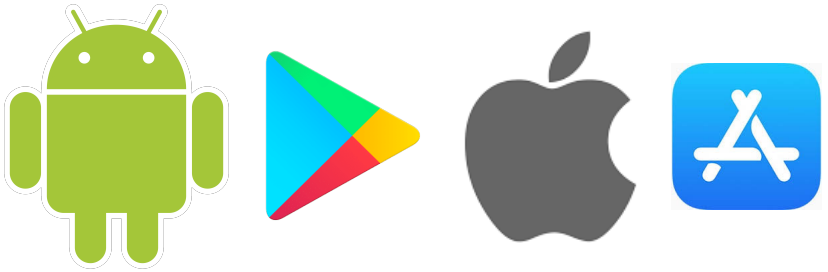
Over the Air

Software Updates System

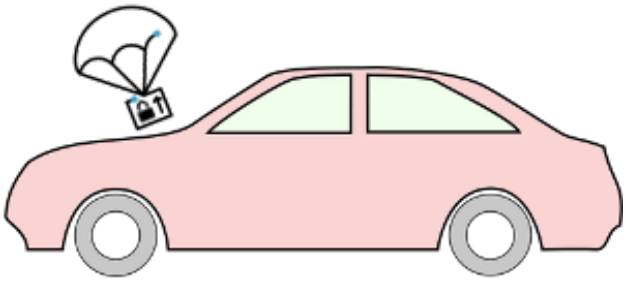
Not a new challenge...

Computer

Smartphones



Automotive



Internet of Things

Fiat Chrysler recalls 1.4 million cars after Jeep hack
http://www.bbc.com/news/technology-33650491

Constrained or not?

Constrained Devices

Non Constrained Device

Constrained Devices

- Devices with very limited:
  - Memory;
  - Energy;
  - Network bandwidth;
- Standardized in RFC 7228.

Portable Updates Ligthweight Library

github.com/libpull/libpull

README.md

The Portable Updates Lightweight Library

build passing

libpull is a C library to implement secure and portable updates on IoT devices. It targets Class 1 constrained devices, characterized by ~10 kB of RAM and ~100 kB of ROM. However, its lightweight and modular approach can be beneficial also for bigger devices.

The library can be included into MCU firmware to perform Over The Air updates. It is composed of many high-level modules that interact with the low-level interfaces, implemented for the specific platform. This is needed since accessing the memory and the network on embedded systems is a complex task and each platform and architecture uses its own primitive.

The goal of the library is to be a portable and secure solution to reduce the costs of securing IoT devices, allowing an easy device update and management also for very constrained applications.

Libpull

- Library for performing updates for Class 1 constrained devices, with ~100 kB of ROM and ~10 kB of RAM;
- It is not an update system, but provides all the functions to create an update system;
- Very different from standard updates. The need to have:
  - Very small memory footprint;
  - Very low energy consumption;
  - Interact with low level details (no OS abstractions);

Libpull

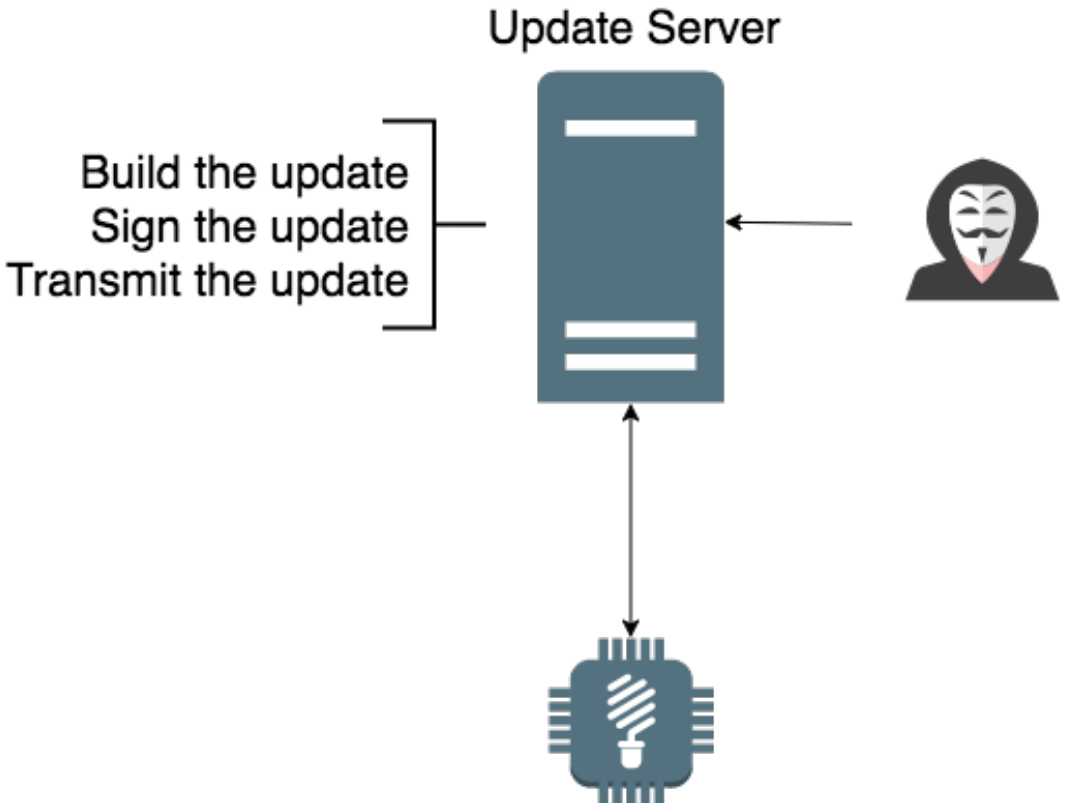
- It is designed to solve three main requirements:
  - Security requirements;
  - Portability requirements;
  - Platform constraints requirements.

Security Requirements

The update system can easily move from being a security feature to a security vulnerability if not designed and implemented correctly

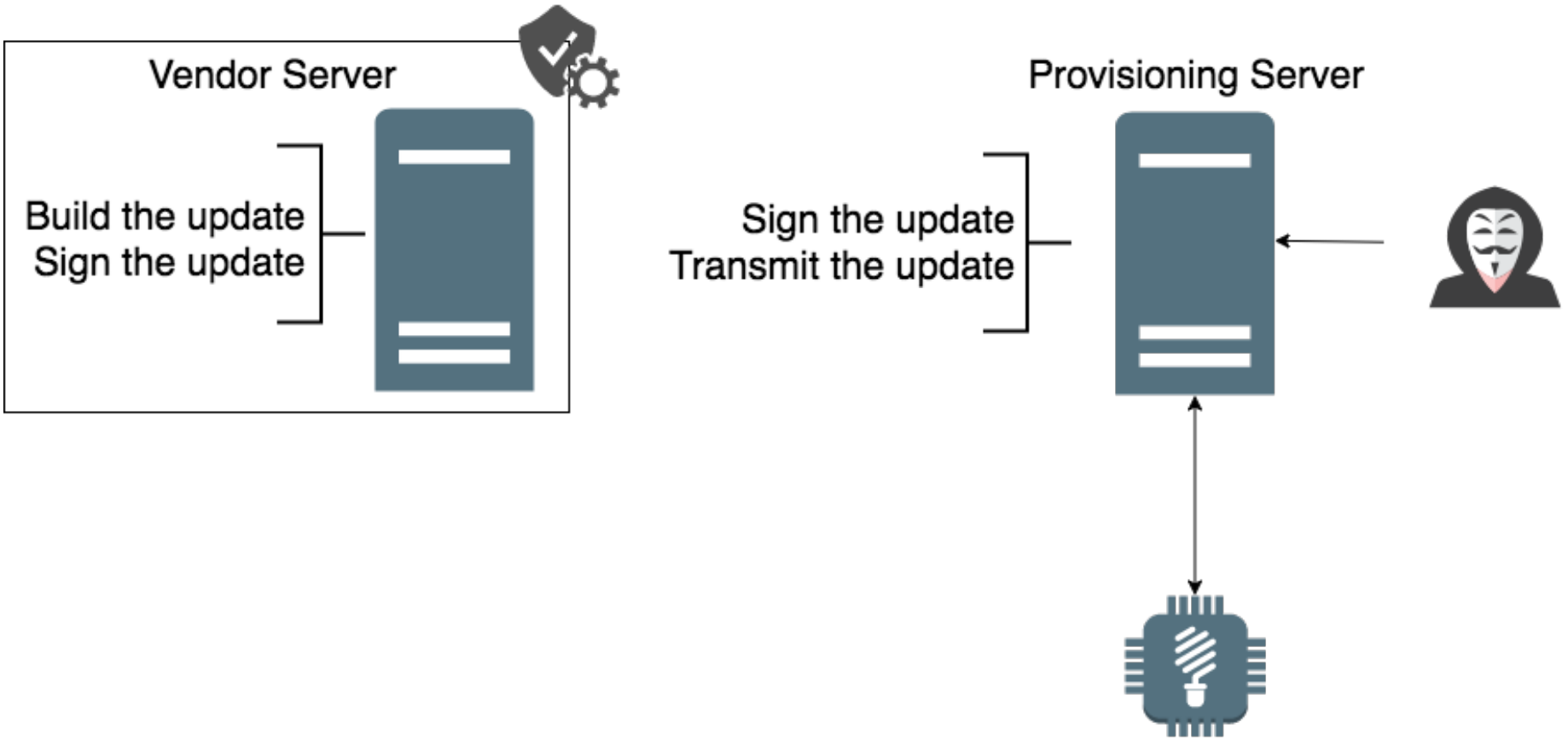
Security Requirements

- Double Server Architecture & Signature;



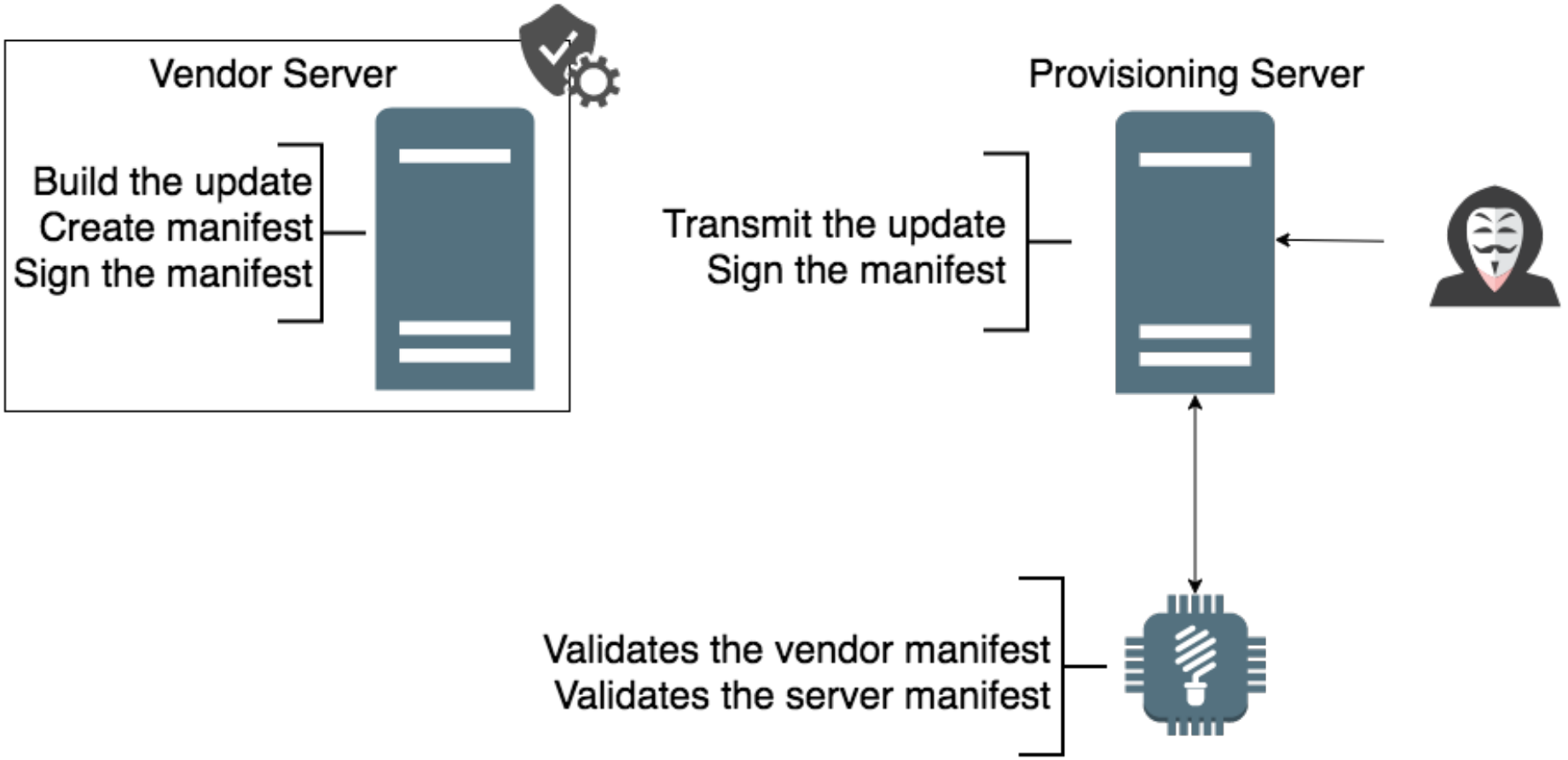
Security Requirements

- Double Server Architecture & Signature;



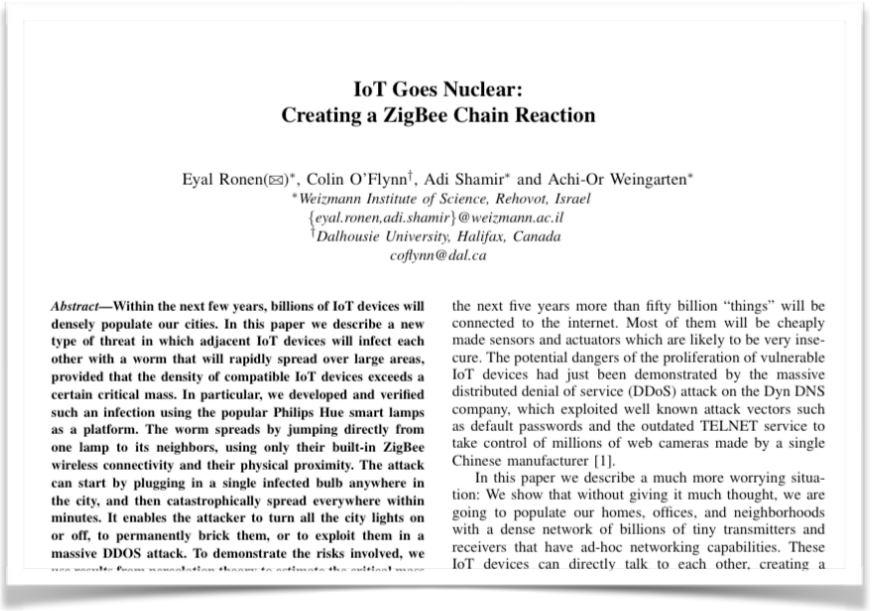
Security Requirements

- Double Server Architecture & Signature;
- Device manifest validation;



Security Requirements

- Double Server Architecture & Signature;
- Device manifest validation;
- Digital signature;



IoT Goes Nuclear:
Creating a ZigBee Chain Reaction

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*
*Weizmann Institute of Science, Rehovot, Israel
{eyal.ronen,adi.shamir}@weizmann.ac.il
†Dalhousie University, Halifax, Canada
coflynn@dal.ca

***Abstract*—Within the next few years, billions of IoT devices will densely populate our cities. In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will rapidly spread over large areas, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform. The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes. It enables the attacker to turn all the city lights on or off, to permanently brick them, or to exploit them in a massive DDOS attack. To demonstrate the risks involved, we**

the next five years more than fifty billion "things" will be connected to the internet. Most of them will be cheaply made sensors and actuators which are likely to be very insecure. The potential dangers of the proliferation of vulnerable IoT devices had just been demonstrated by the massive distributed denial of service (DDoS) attack on the Dyn DNS company, which exploited well known attack vectors such as default passwords and the outdated TELNET service to take control of millions of web cameras made by a single Chinese manufacturer [1].

In this paper we describe a much more worrying situation: We show that without giving it much thought, we are going to populate our homes, offices, and neighborhoods with a dense network of billions of tiny transmitters and receivers that have ad-hoc networking capabilities. These IoT devices can directly talk to each other, creating a

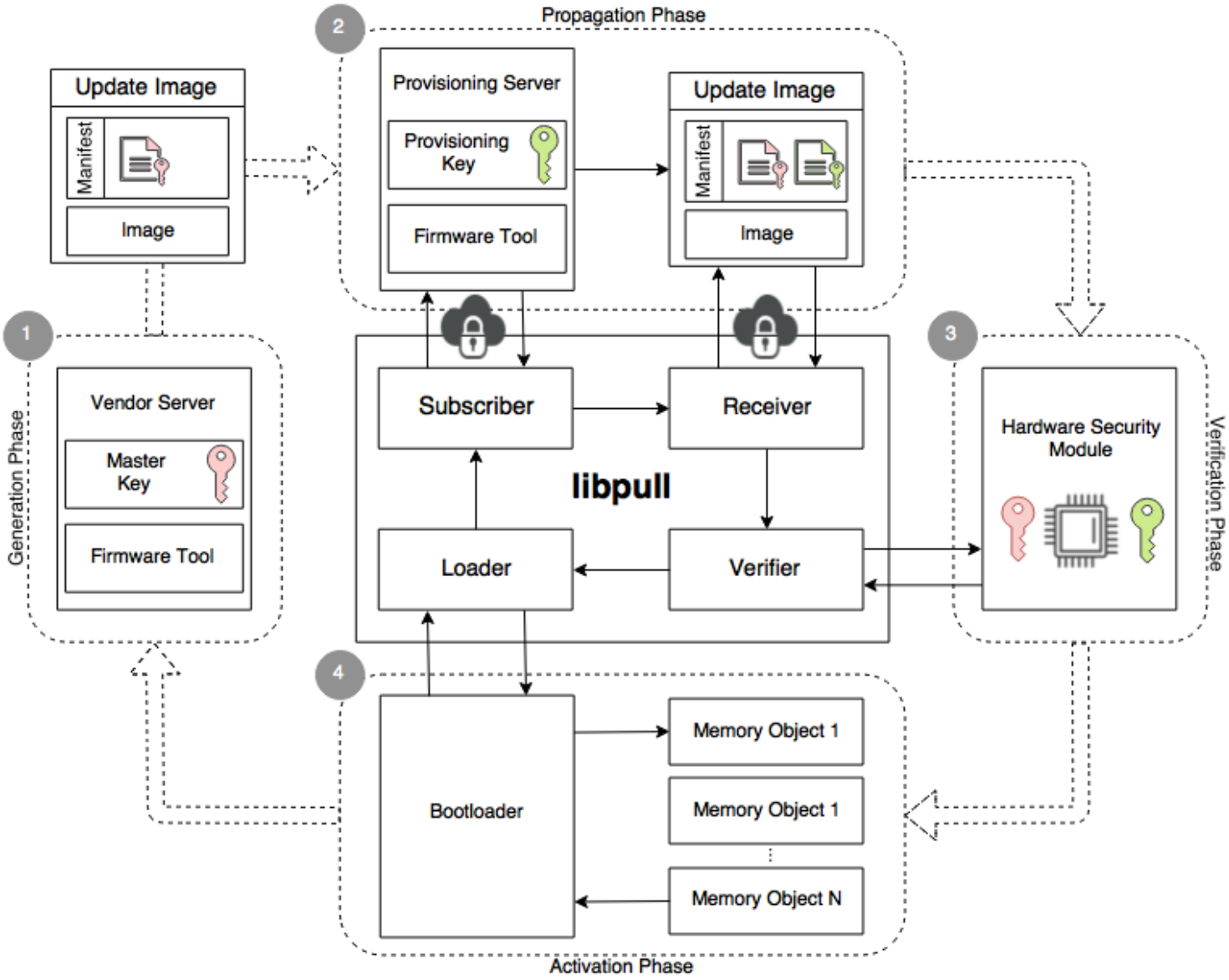
http://iotworm.eyalro.net

Security Requirements

- Double Server Architecture & Signature;
- Device manifest validation;
- Digital signature;
- Safe Key Storage;

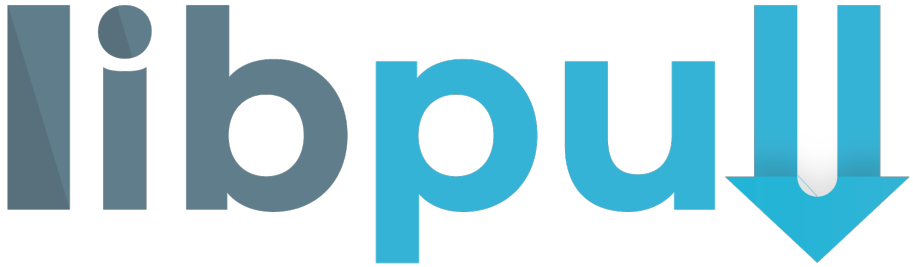
Hardware Security Modules

Libpull General Architecture



Goals of the Project

- Reduce costs of including an update system into constrained devices;
- Being a portable and suitable solution for Class 1 devices, but usable also on more powerful devices;
- Supporting standards targeting constrained devices;



Future Works

- Support other hardware and software platforms;
- Support OMA LWM2M for device management;
- Integrate delta updates to improve energy efficiency;



github.com/AntonioLangiu **@antonio_langiu** **linkedin.com/in/antoniolangiu/**