The SPIN project

Jelte Jansen – SIDN Labs

20 april 2018
So, about that IoT
What **is** the IoT?

Wikipedia definition:

“The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.”
What **is** the IoT?

Global Standards Initiative definition:

“a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[3] and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks".”
What **is** the IoT?

- IEEE published a document: “Towards a definition of the IoT”

- Only 86 pages!
What **is** the IoT?

A simpler definition:

“Stuff that was not networked before”
What **is** the IoT?

An even simpler definition:

“One big mess”
So, about that IoT

The internet of insecure things: Thousands of internet-connected devices are a security disaster in the making

By Josh Fruhlinger, CSO | Oct 12, 2016 4:00 AM PT
So, about that IoT

NEW MIRAI VARIANT CARRIES OUT 54-HOUR DDoS ATTACKS

by Tom Spring
March 30, 2017, 2:50 pm
So, what to do about this?

- Better practices for manufacturers?
- Better (free) standard software libraries?
- International policy, regulation, and certification?
- Generate market demand for secure products?
- Quarantine bad actors at ISP level?
- Educate users?
- Empower users?
So, what to do about this?

• Better practices for manufacturers?
• Better (free) standard software libraries?
• International policy, regulation, and certification?
• Generate market demand for secure products?
• Quarantine bad actors at ISP level?
• Educate users?
• Empower users?

“Yes”
So, what to do about this?

- Better practices for manufacturers?
- Better (free) standard software libraries?
- International policy, regulation, and certification?
- Generate market demand for secure products?
- Quarantine bad actors at ISP level?
- Educate users?
- **Empower users: SPIN**
The SPIN project at SIDN Labs

• Security and Privacy for In-home Networks

• Research and prototype of SPIN functionality:
  • Visualising network traffic
  • (Automatic) blocking of 'bad' traffic
  • Allow 'good' traffic
The SPIN project at SIDN Labs

• Open source in-home router/AP software that

• Helps protect DNS operators (like SIDN!) and other service providers against IoT-powered DDoS attacks

• Helps end-users controls the security of their home networks
Architecture

traffic capture
router
traffic block

MQTT

visualiser
stats MUD test policy enforcer
Prototype built on OpenWRT

- Currently bundled with Valibox: http://valibox.sidnlabs.nl
- Source at https://github.com/SIDN/spin
Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination

In beta:
- Select device and download (live) pcap for selected device
Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination

In beta:
- Select device and download (live) pcap for selected device
Core components

Currently:

- **OpenWRT/Linux kernel module (C)**
  - Captures and blocks traffic
  - Initial aggregation

- **User-space daemon (C)**
  - Further aggregation and enrichment of data
  - Sends to MQTT daemon

- **MQTT Daemon (Mosquitto)**
  - Distributes traffic data to clients (mqtt/websockets)
  - Sends commands back to router

- **Several Clients**
  - Visualiser (Javascript)
  - Statistics tool (Lua)
  - PoC MUD tool (Lua)
  - PoC (hardcoded) 'bad behaviour' tool (Lua)
  - Recent history storage (currently 10 minutes) (Lua)
Current research/prototype topics:

- Profiles concept
- Profiles implementation (MUD)
- Anomaly Detection
- Incident Report System
Profiles: Conceptual

• Still very much in the 'idea forming' stage

Base profiles

- Social networks
- Streaming sites
- Order new milk
- Download updates
- Don't spread Mirai
Profiles: Conceptual

• Still very much in the 'idea forming' stage

Base profiles

- Social networks
- Streaming sites
- Order new milk
- Download updates
- Don't spread Mirai

Television profile

- Streaming sites
- Download Updates
- Don't spread Mirai

Don't spread Mirai
Profiles: Conceptual

- Still very much in the 'idea forming' stage

Base profiles

- Social networks
- Streaming sites
- Order new milk
- Download updates
- Don't spread Mirai

Television profile

- Streaming sites
- Download Updates
- Don't spread Mirai

Refrigerator profile

- Order new milk
- Download Updates
- No virussy stuff
Profiles: Implementation: MUD?

Manufacturer Usage Description (MUD)
• Draft at IETF
• JSON description of internet traffic that is or is not allowed from and to the device
• Translates almost directly to firewall rules

Our work:
• Provide (additional) early implementation for testing
• Looking into automatic generation of basic profiles
• Looking into extending it (e.g. to add a bandwidth limitation)
• Looking into 'reverse' profiles (any device that matches profile X is infected with Y, think IDS rules)

And more wildly:
• A way for users and companies to create and share device profiles (that improve manufacturer-provided ones)
Profiles: Implementation: MUD

Subproject: Lua-MUD
- Small MUD library for Lua
- Tiny subset for now (and pretty much hardcoded)
- Lua-mud-0.1 (on luarocks and github)
- Working on ‘full’ version.

Master student working on traffic analysis for MUD
- And generation of profiles like mudgee
- Research question: how much can you deduce from observation?
Incident report system

Problem:

If ISP’s do anything about bad traffic from their customers in the first place, it’s generally a full quarantine of the customer.
Incident report system

AbuseHub

ISP1

home network 1

ISP2

home network 2
(192.0.2.123)

ISP3

home network 3

ISP4
Incident report system

AbuseHub

ISP1
Abuse 192.0.2.123

ISP2
Abuse 192.0.2.123

ISP3

ISP4

home network 1

home network 2 (192.0.2.123)

home network 3

Quarantined!!1!
Incident report system

AbuseHub

ISP1
Abuse 192.0.2.123
home network 1

ISP2
Abuse 192.0.2.123
Please reinstall windows
home network 2 (192.0.2.123)

ISP3

ISP4
home network 3
Incident report system

AbuseHub

- ISP1
  - Abuse 192.0.2.123
- ISP2
  - Abuse 192.0.2.123
- ISP3
- ISP4

Abuse to 192.0.2.1 at <time>

- home network 1
  - device1
- home network 2 (192.0.2.123)
  - device2
  - device3
- home network 3
  - device4
Incident report system

AbuseHub

ISP1
Abuse 192.0.2.123

ISP2
Abuse 192.0.2.123

ISP3

ISP4

home network 1

home network 2
(192.0.2.123)

home network 3

device1

device2

device3

device4

Abuse to 192.0.2.1 at <time>
Running prototype

Small (Django) web application for reports

Notification to router (poll or push)

Router finds device in history

Router blocks device
General research topic:
• Can 'bad' behaviour be recognized?
• Perhaps by looking at historic behaviour of device?

Since we keep a (short) history of device traffic, we are looking into extending that into a framework for researchers to do anomaly detection

Currently nothing to show yet, though.
Discussion/questions/cheers/tomatoes

- Try it out!
  https://valibox.sidnlabs.nl
  https://github.com/SIDN/spin

- Make/use SOHO routers, want to set up PoC?

- Missing something?

- Any other questions or comments

Jelte Jansen
jelte.jansen@sidn.nl
@twitjeb

sidn.nl | sidnlabs.nl
@sidnlabs