

Securing the IoT using SPIN

Elmer Lastdrager

13 september 2018



YOU GET CONNECTED!

AND YOU GET CONNECTED!

EVERYTHING GETS CONNECTED!

[Home](#) > [Data Protection](#) > [Internet of Things](#)

SLIDESHOW

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





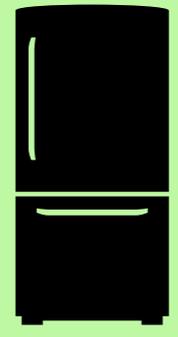
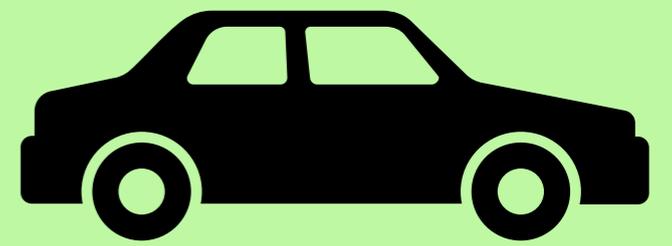
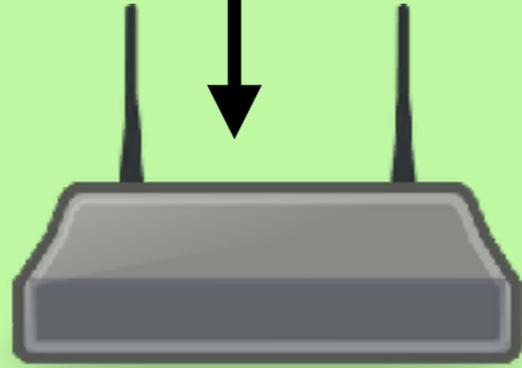
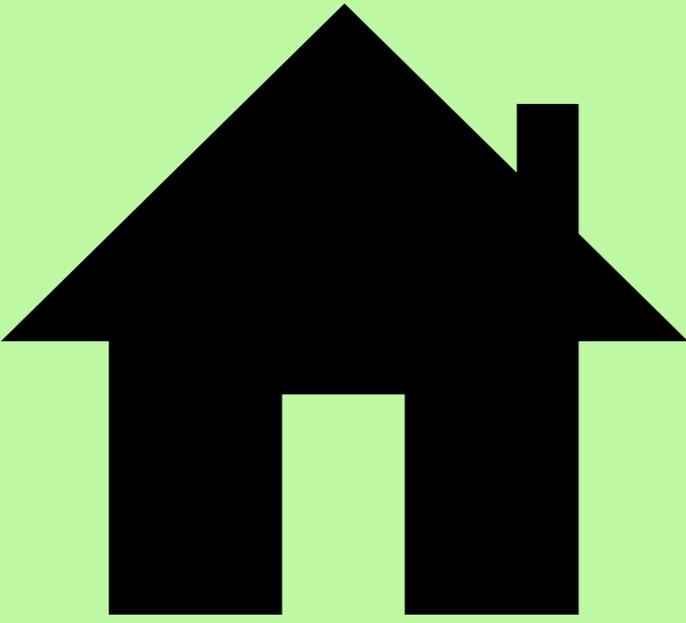
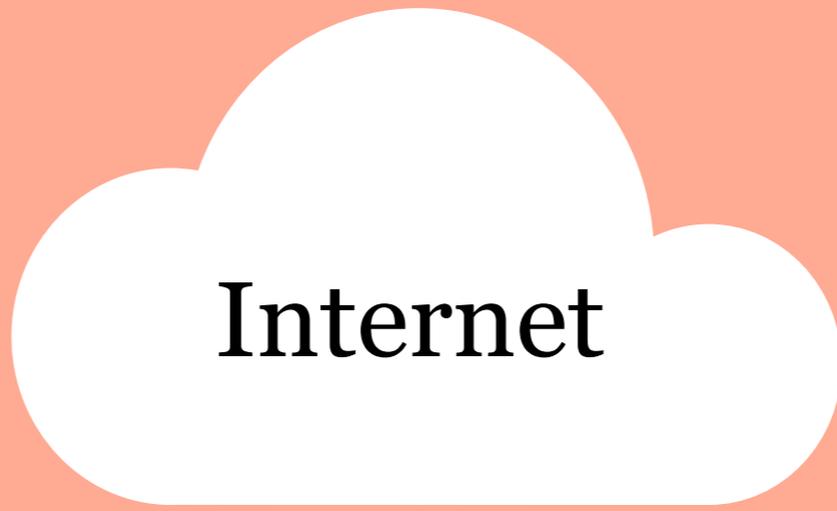
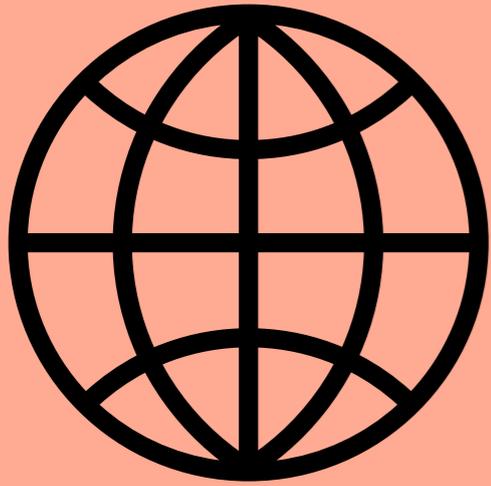
The "S" in IoT
stands for
SECURITY



What to do?

- ▶ Better practices for manufacturers?
- ▶ Free **secure** software stacks? ← 
- ▶ International policy, regulation, certification?
- ▶ Clear up accountability issues?
- ▶ Generate market demand for secure products?
- ▶ Quarantine bad actors (e.g. at ISP)?
- ▶ Educate users?
- ▶ Empower users?

“Yes”



Stichting Internet Domeinregistratie Nederland (SIDN)

Critical Internet services

- ▶ Lookup IP address of a domain name (almost every interaction)
- ▶ Domain name registration
- ▶ Manage fault-tolerant and distributed infrastructure

“Catalyst” of the Internet in the Netherlands

- ▶ Enable safe and novel use of the Internet
- ▶ Improve the security and resilience of the Internet itself



.nl = the Netherlands
17M inhabitants
5.8M domain names
2.8M DNSSEC-signed
1.3B DNS queries/day



SIDN Labs

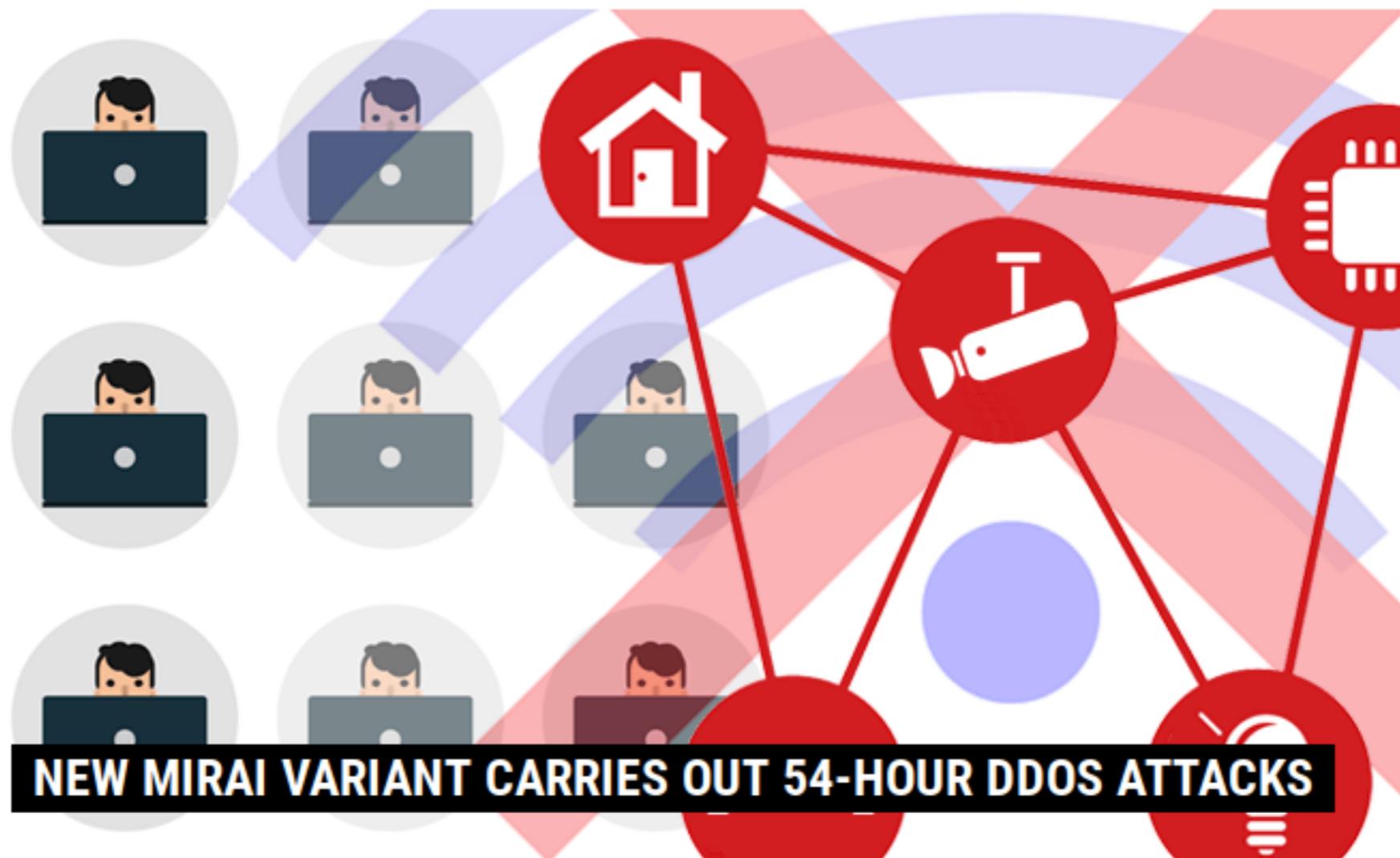
Goal: thrust operational security and resilience of the Internet through world-class measurement-based research and technology development

Challenges: DNS and Internet security and resilience, Internet evolution, inter-domain AAA infrastructures

Daily work: help operational teams, write open source software, analyze vast amounts of data, run experiments, write academic papers, work with universities



[Welcome](#) > [Blog Home](#) > [Hacks](#) > [New Mirai Variant Carries Out 54-Hour DDoS Attacks](#)



by [Tom Spring](#)

March 30, 2017 , 2:50 pm

A variant of the Mirai malware pummeled a U.S. college last month with a marathon 54-hour long attack. Researchers say this latest Mirai variant is a more potent version of the notorious Mirai malware that made headlines in [October](#), targeting DNS provider [Dyn](#) and the [Krebs on Security](#) website.

NETFLIX



WIRED

amazon.com



BBC

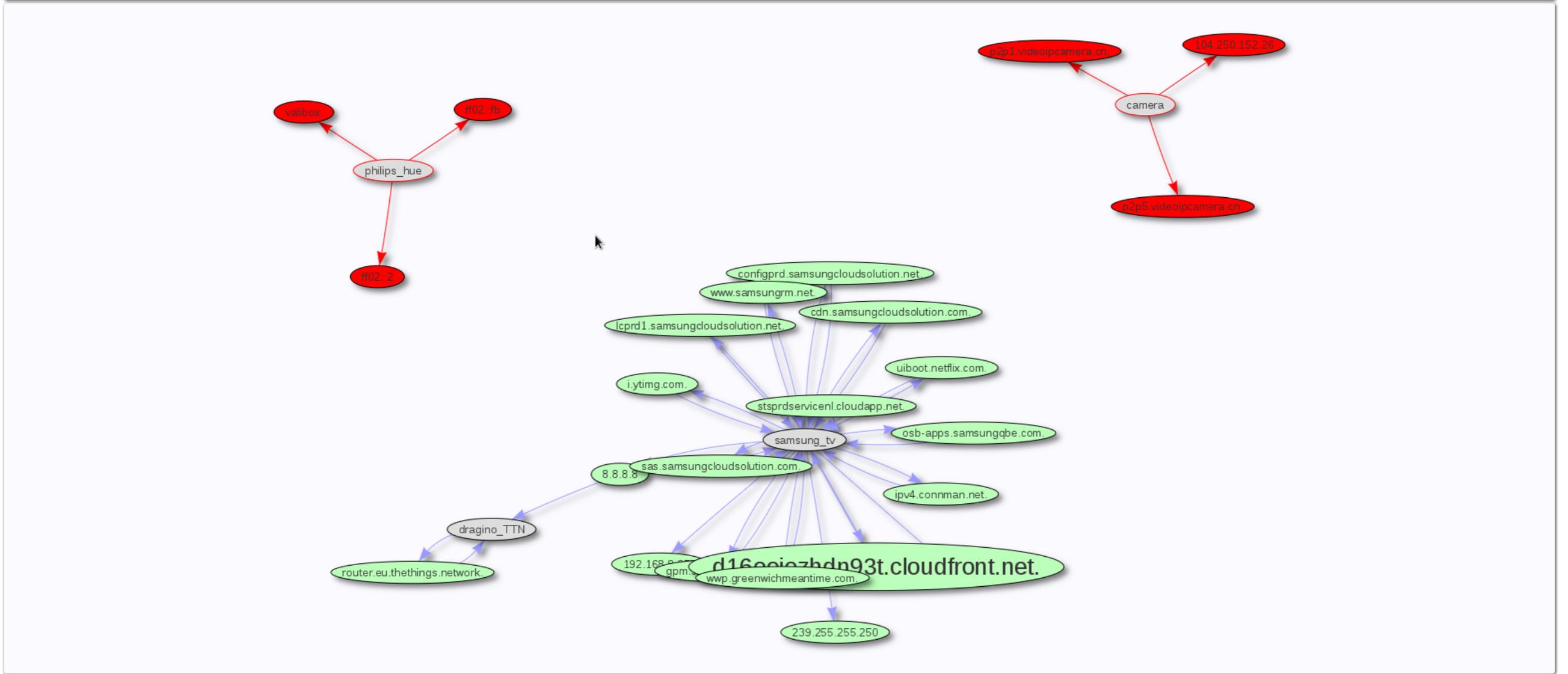
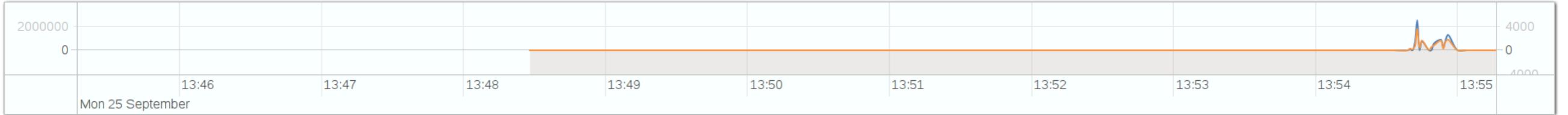
CNN

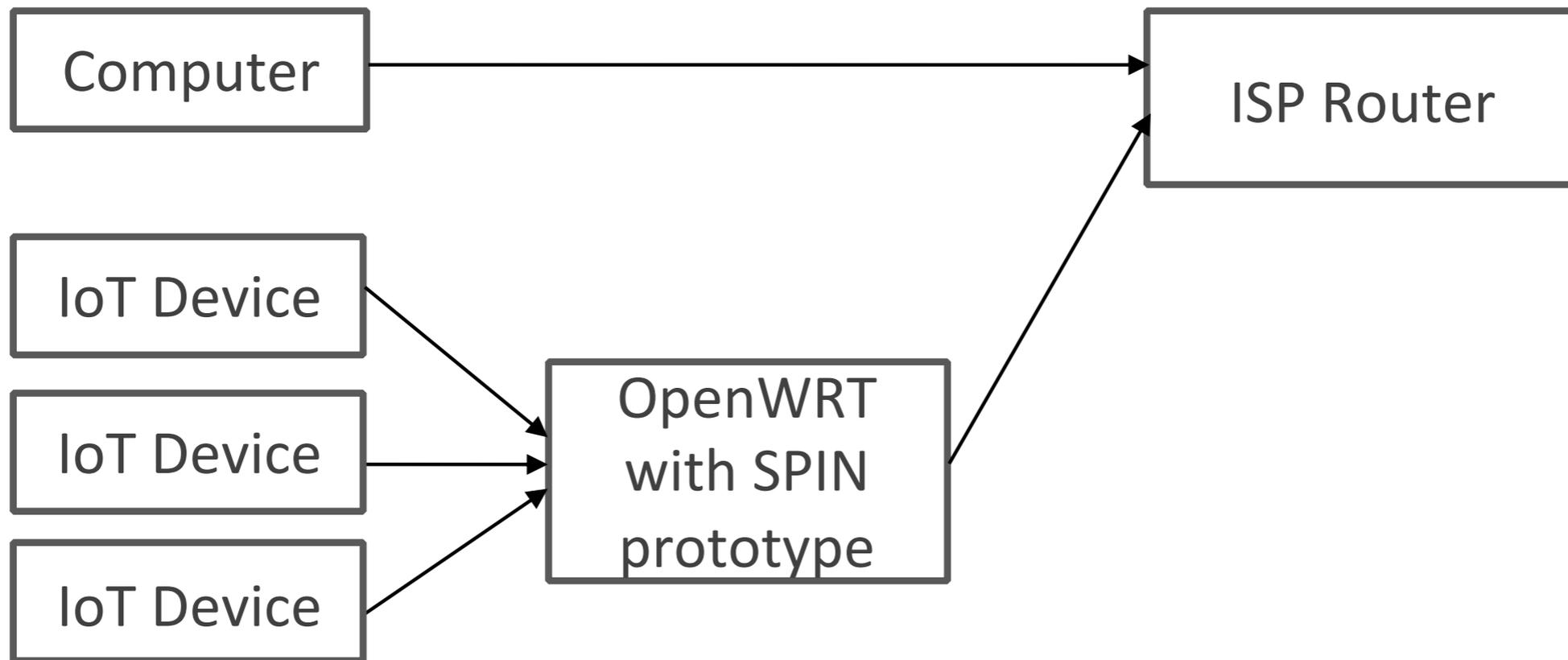


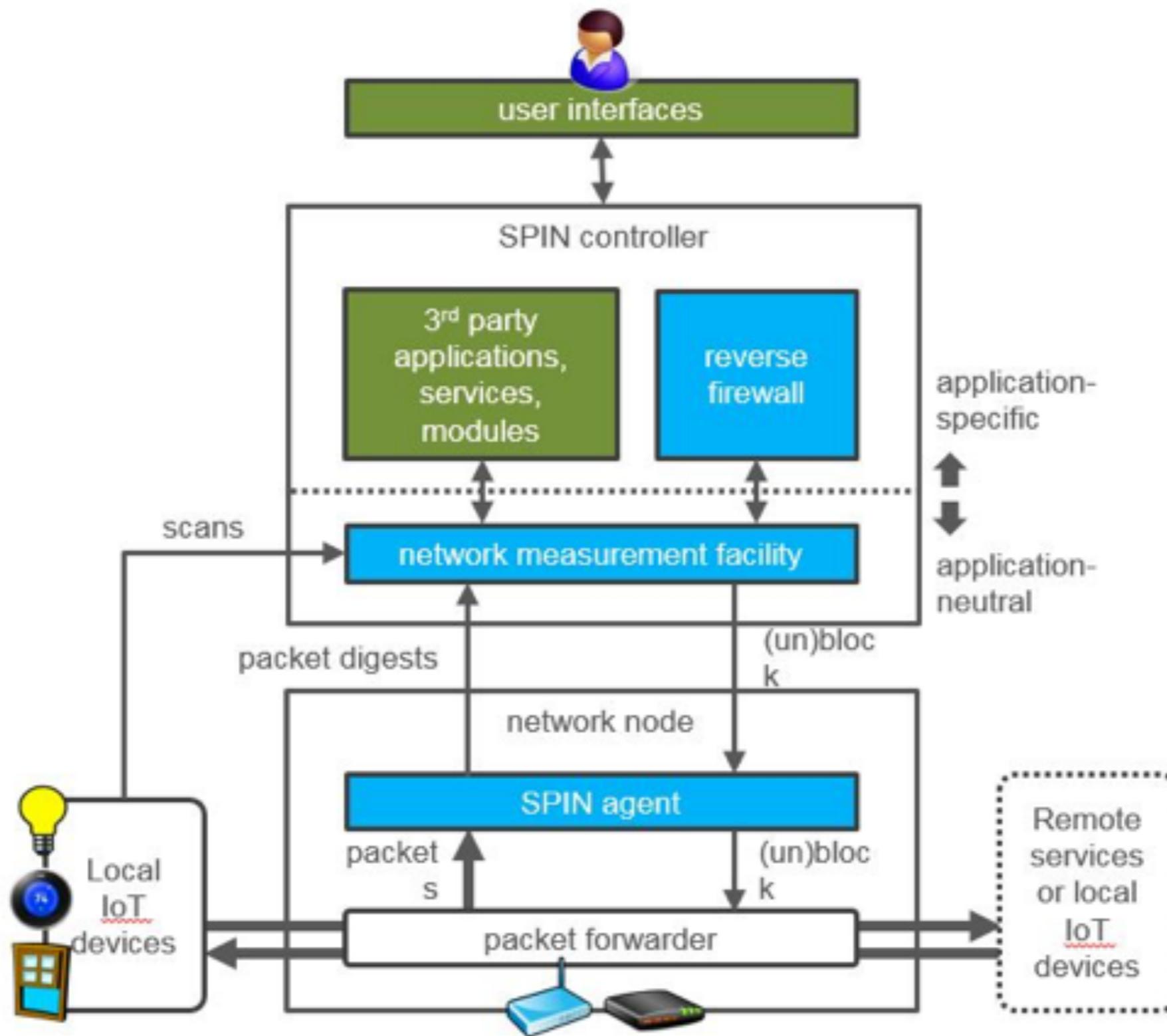
HBO

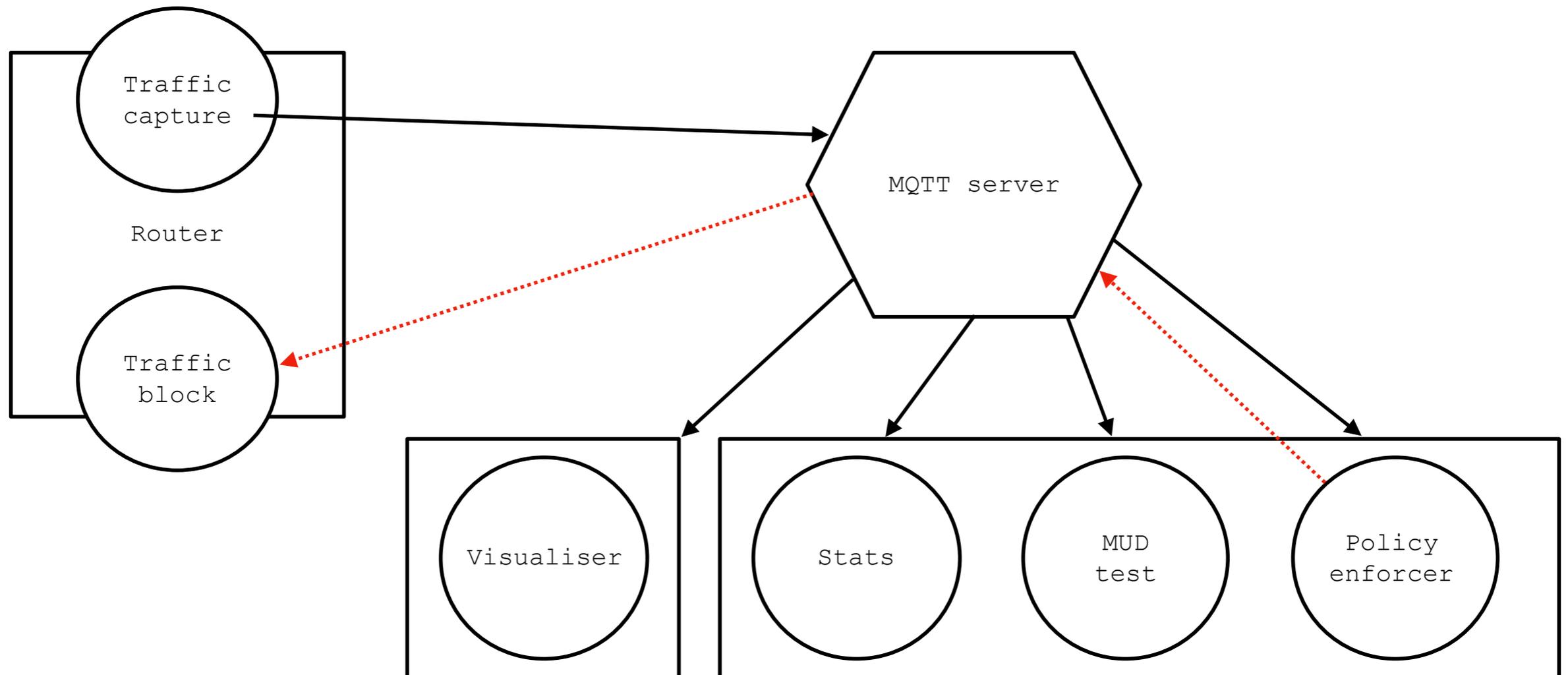
Security and Privacy for In-home Networks (SPIN)











[\[Docs \]](#) [\[txt \]](#) [\[pdf \]](#) [\[xml \]](#) [\[html \]](#) [\[Tracker \]](#) [\[WG \]](#) [\[Email \]](#) [\[Diff1 \]](#) [\[Diff2 \]](#) [\[Nits \]](#)

Versions: ([draft-lear-ietf-netmod-mud](#)) [00](#) [01](#)
[02](#) [03](#) [04](#) [05](#) [06](#) [07](#) [08](#) [09](#) [10](#) [11](#) [12](#) [13](#)
[14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#)

Network Working Group

Internet-Draft

Intended status: Standards Track

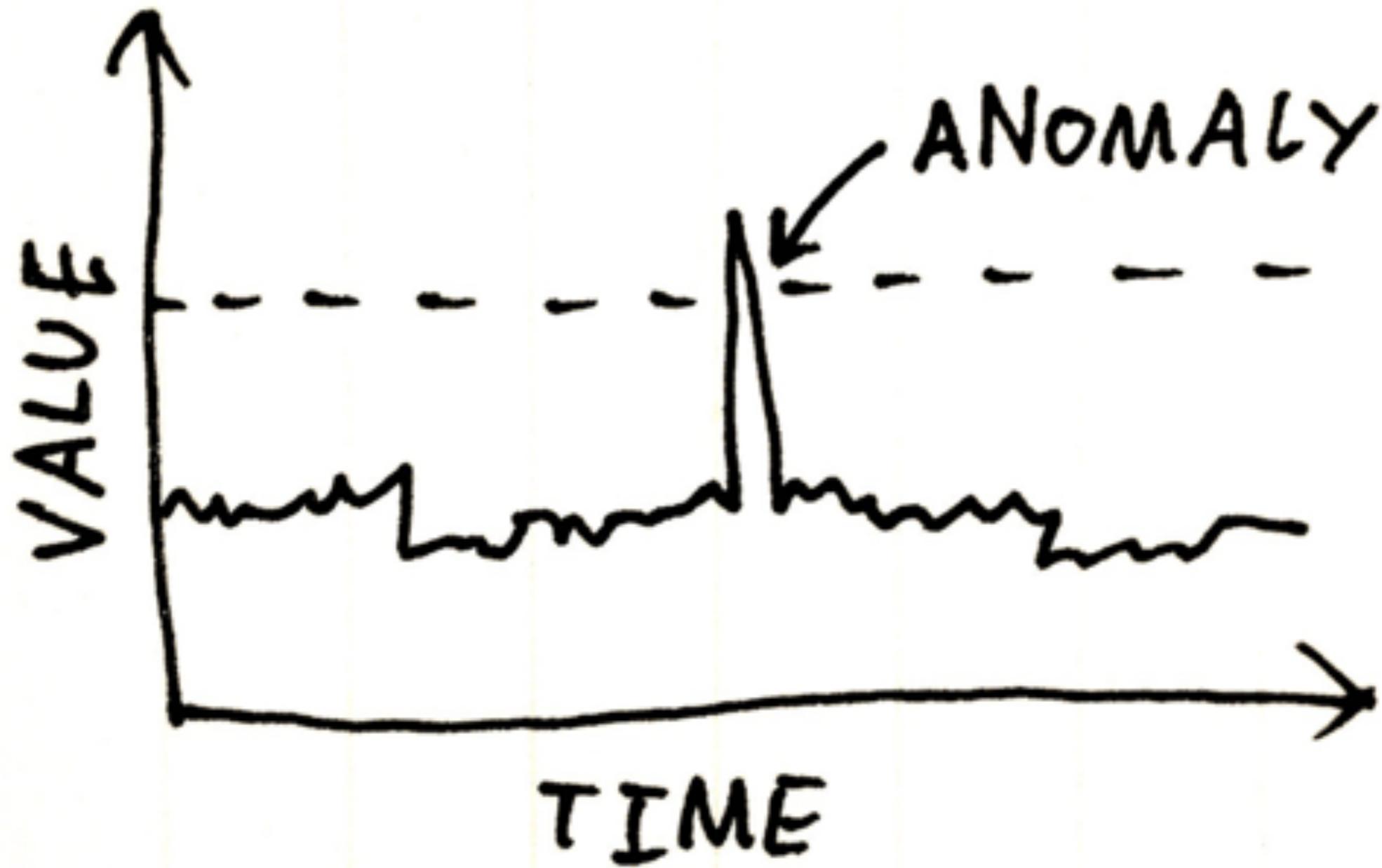
Expires: December 17, 2018

E. Lear
Cisco Systems
R. Droms
Google
D. Romascanu
June 15, 2018

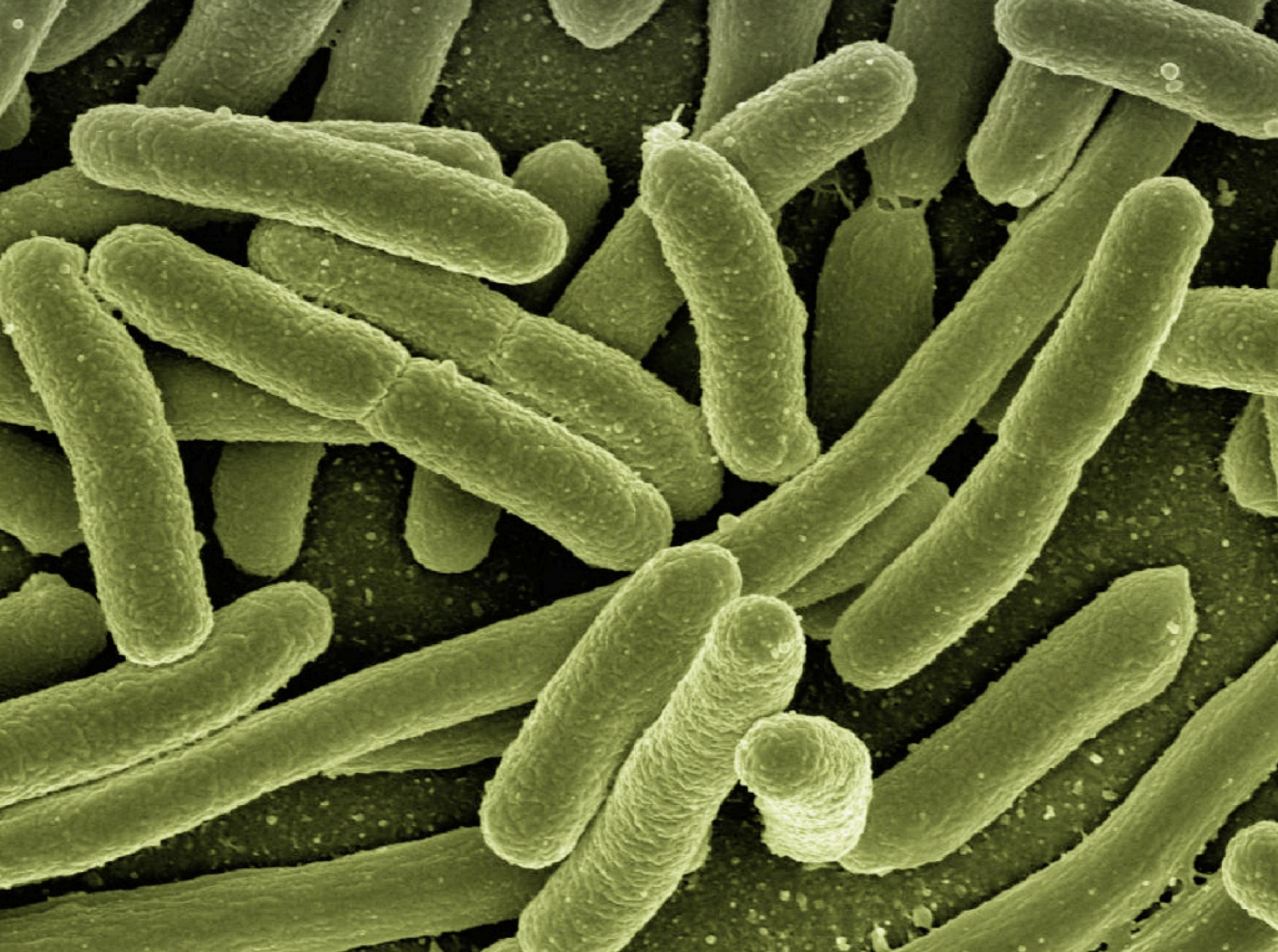
Manufacturer Usage Description Specification
draft-ietf-opsawg-mud-25

Abstract

This memo specifies a component-based architecture for manufacturer usage descriptions (MUD). The goal of MUD is to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function. The initial focus is on access control. Later work can delve into other aspects.

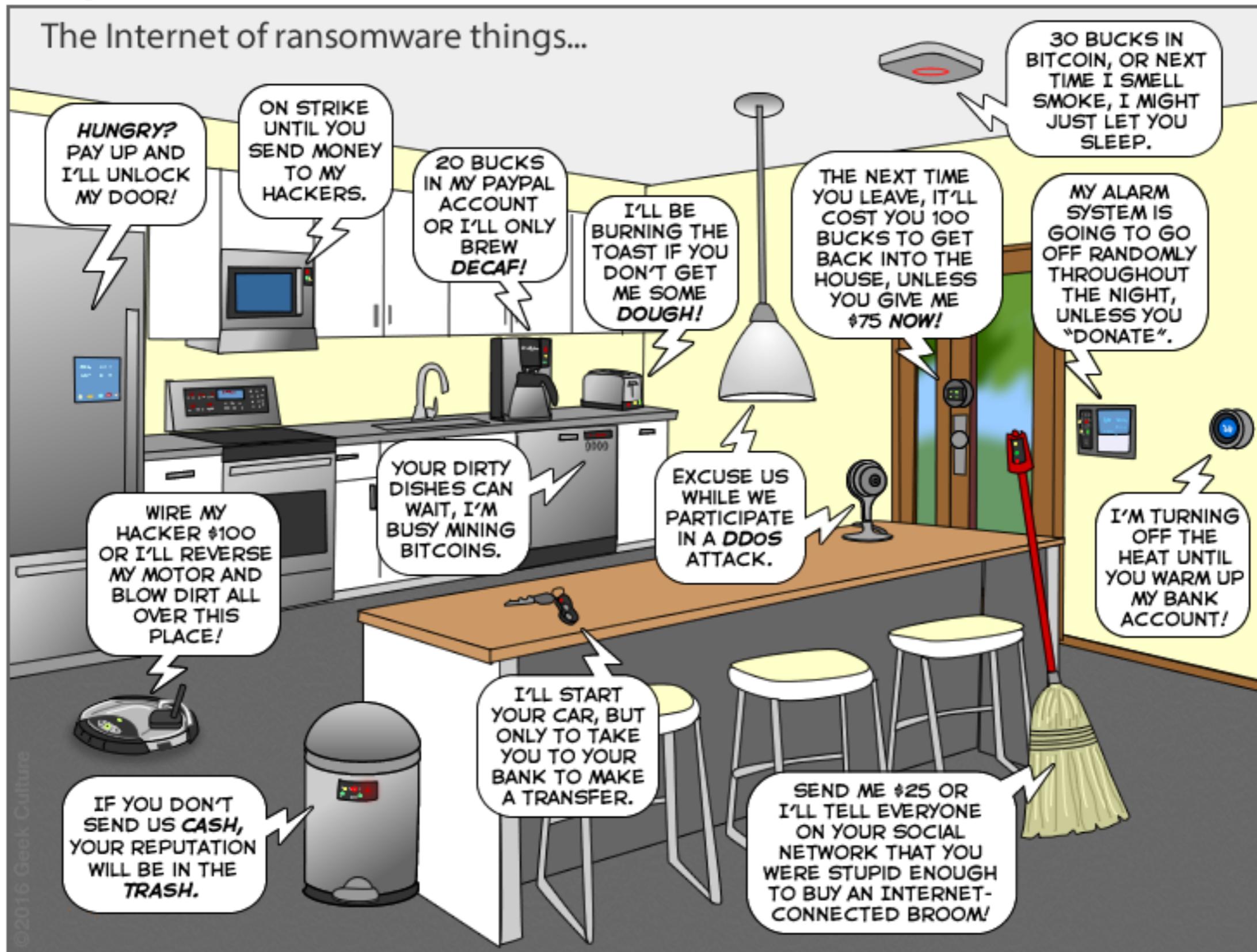








Max input: 230 V
- 60/50 Hz



elmer.lastdrager@sidn.nl
<https://spin.sidnlabs.nl>