IoT research at SIDN Labs

Elmer Lastdrager | NCSC 14 april 2020

Operator van het .nl top-level domein (TLD)

- Stichting Internet Domeinregistratie Nederland (SIDN)

- Kritische infrastructuur (‘aanbieder van essentiële diensten’)
  - Opzoeken van IP-adres van een domeinnaam (bijna elke interactie)
  - Registratie van alle .nl-domeinnamen
  - Beheren van een fouttolerante en gedistribueerde infrastructuur

- Waarde van het Internet voor Nederland en daarbuiten vergroten
  - Veilig en nieuw gebruik van het Internet mogelijk maken
  - Veiligheid en weerbaarheid van het Internet zelf verbeteren

.nl = the Netherlands
17M inhabitants
5.9M domain names
3.2M DNSSEC-signed
1.3B DNS queries/day

SIDN fonds

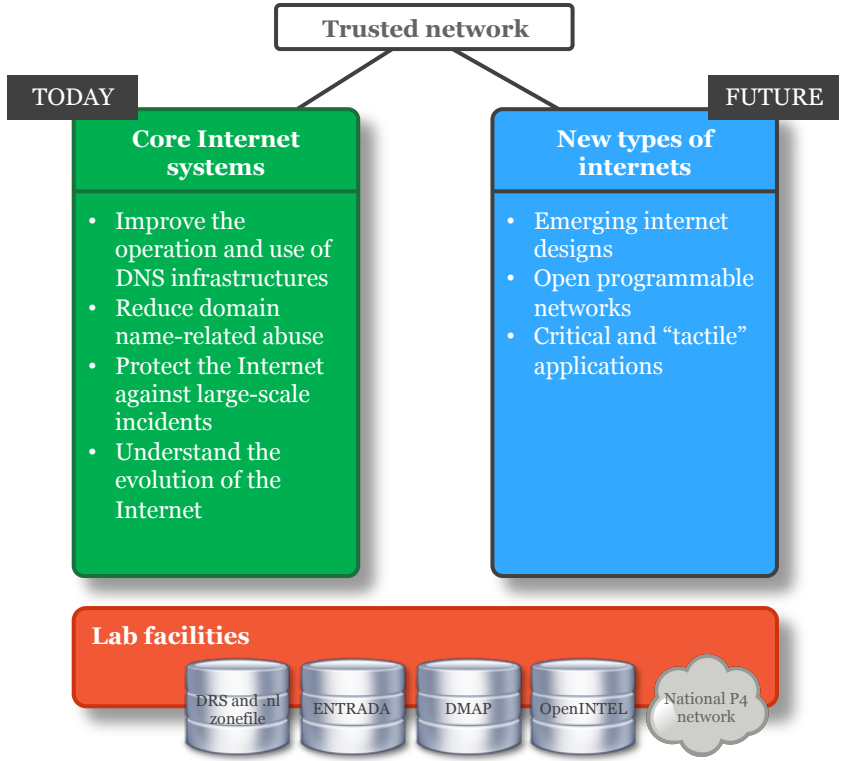
SIDN LABS

Doel SIDN Labs: verhogen van de betrouwbaarheid van de internetinfrastructuur van onze samenleving

- Betrouwbaar = veilig, stabiel, weerbaar en transparant, voor .nl en NL in het bijzonder

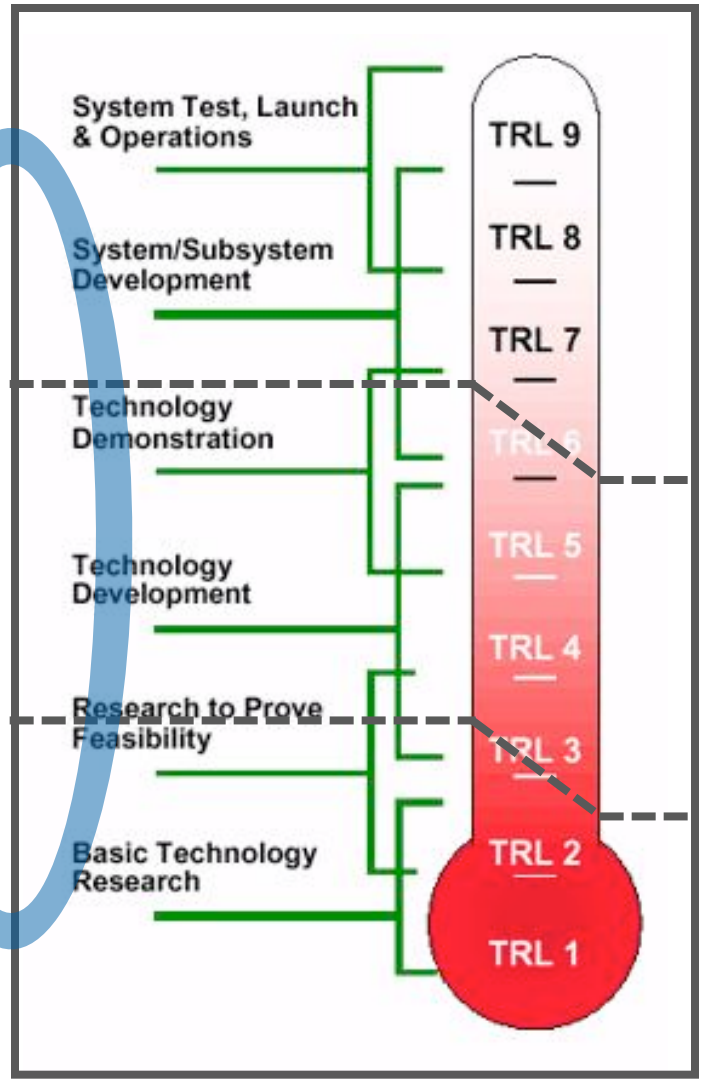
- Strategieën om dat te bereiken
  - Onderzoek naar mechanismen die betrouwbaarheid verder verhogen (meten, prototypen, evalueren)
  - Idem voor nieuwe soorten internetten die het Internet aanvullen
  - Versterken van de NL, Europese en mondiale onderzoek- en operationele gemeenschappen

- 2020's: grip op publieke waarden van NL en EU zoals privacy en safety ('digitale soevereiniteit')



Technology Readiness Levels

SIDN Labs
richt zich op
de **R** in R&D



Operations

Experimenteel

Fundamenteel onderzoek

https://en.wikipedia.org/wiki/Technology_readiness_level

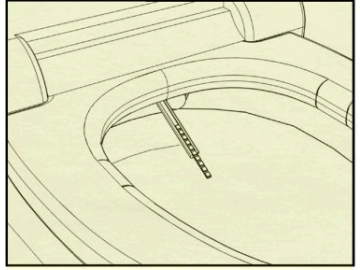
O'Reilly, C. A., & Tushman, M. L. (2013). Organizational ambidexterity: Past, present, and future. Academy of Management Perspectives, 27(4), 324-338

Voorbeelden van onderzoekpartners

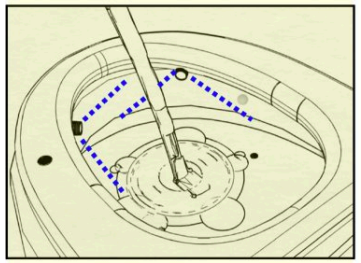
Dagelijks werk

- Operationele teams helpen
- Open source software schrijven
- Grote hoeveelheden data analyseren
- Experimenten draaien
- Academische paper en tech rapporten schrijven
- Samenwerken met universiteiten

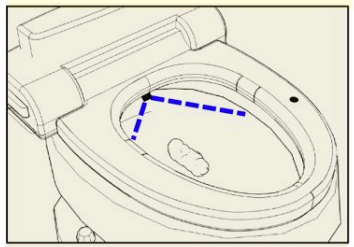
SIDN LABS



Urinalysis

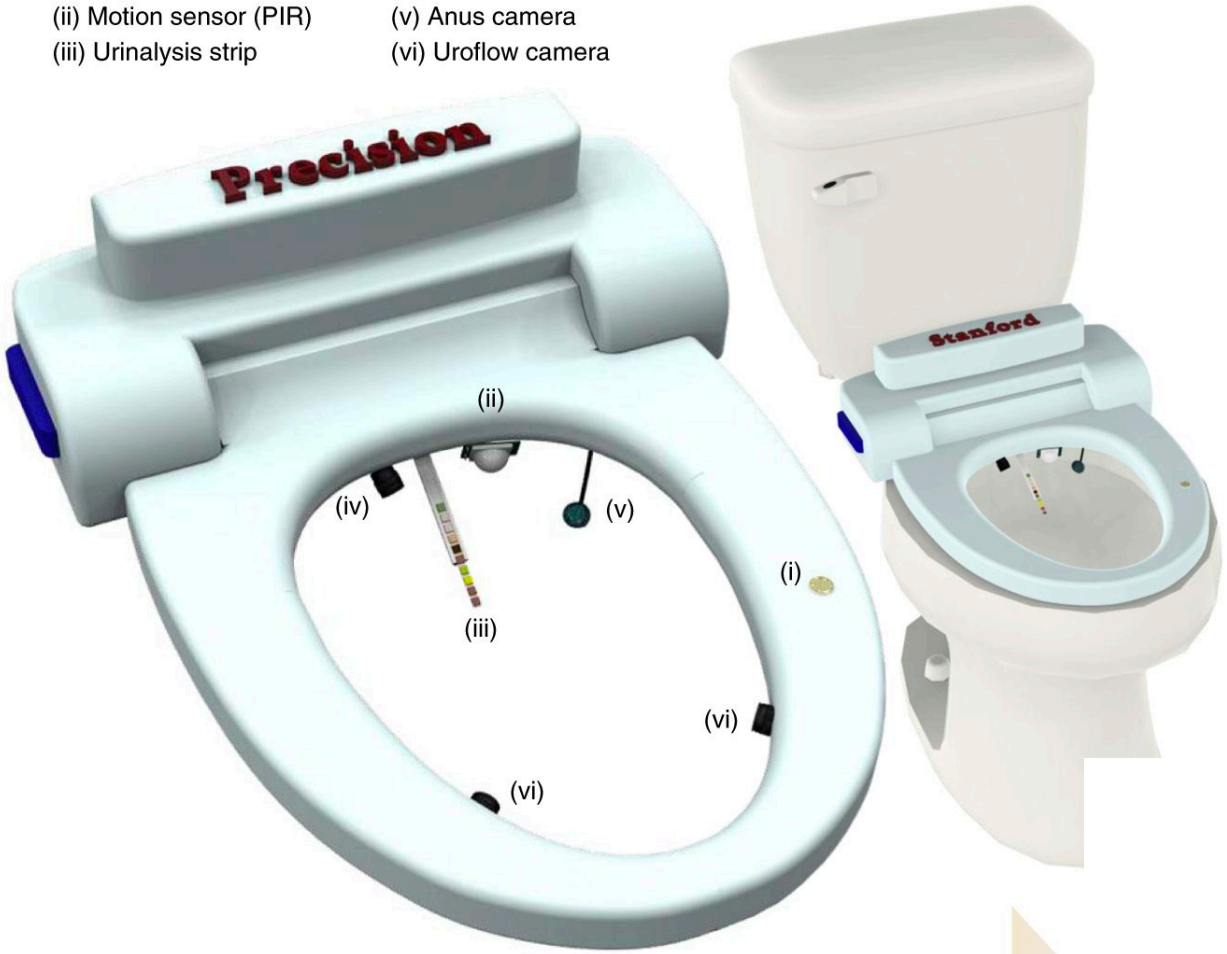


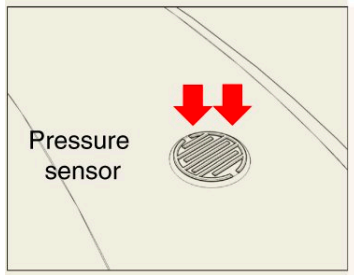
Uroflowmetry



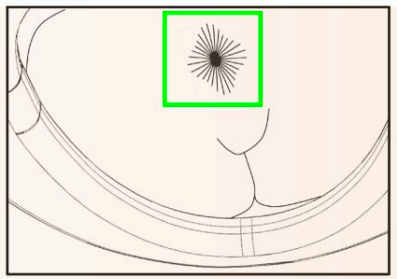
Bristol stool form scale

(i) Pressure sensor
(ii) Motion sensor (PIR)
(iii) Urinalysis strip
(iv) Stool camera
(v) Anus camera
(vi) Uroflow camera

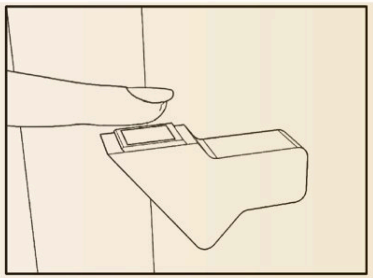




Seating time
defecation time



Analprint scan



Fingerprint scan

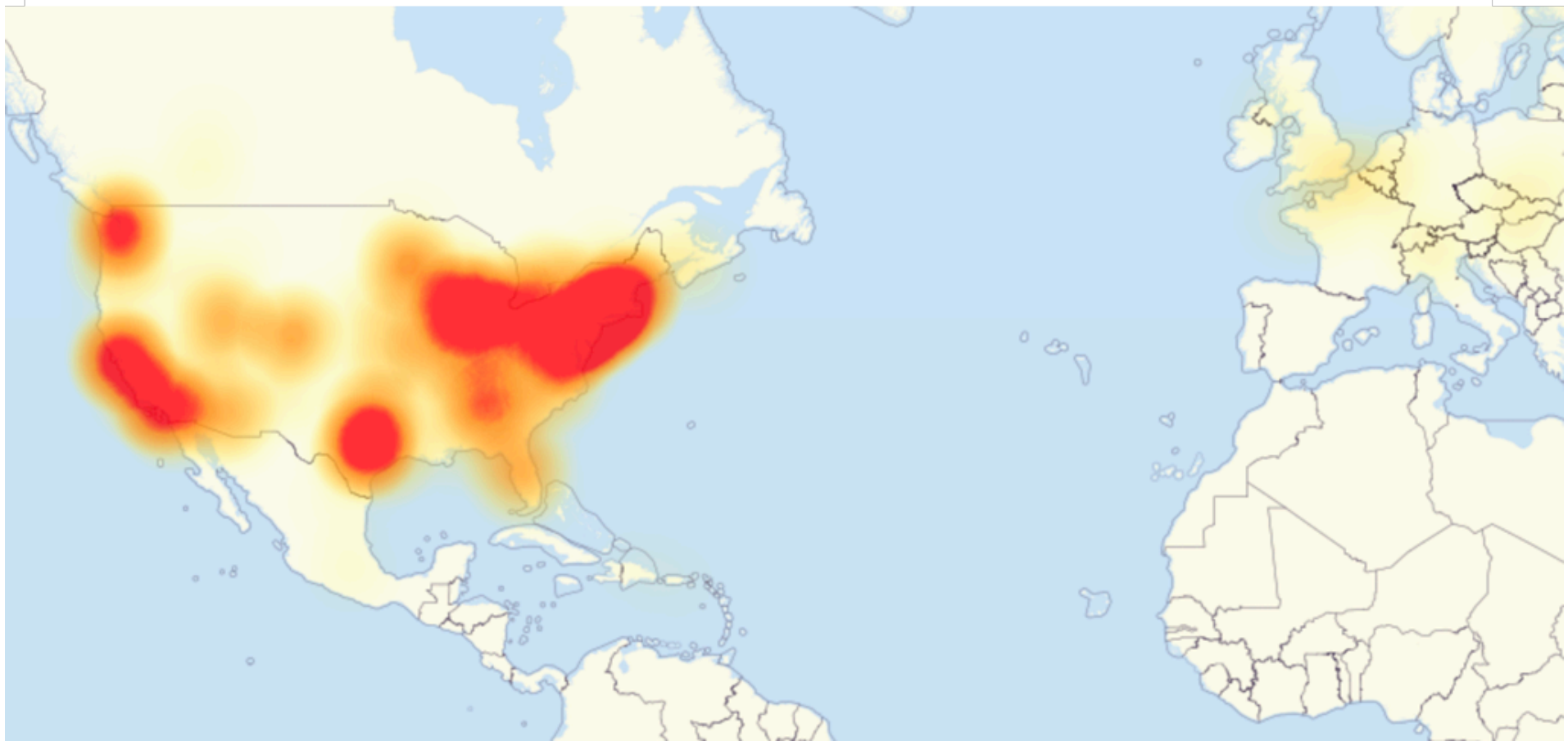
Cloud-based
health portal

SDN LABS

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



IoT projecten

MINIONS-NL *(extern: TU Delft)*

DAGOBERT *(extern: OU & Quarantainenet)*

SPIN *(intern)*

MINIONS

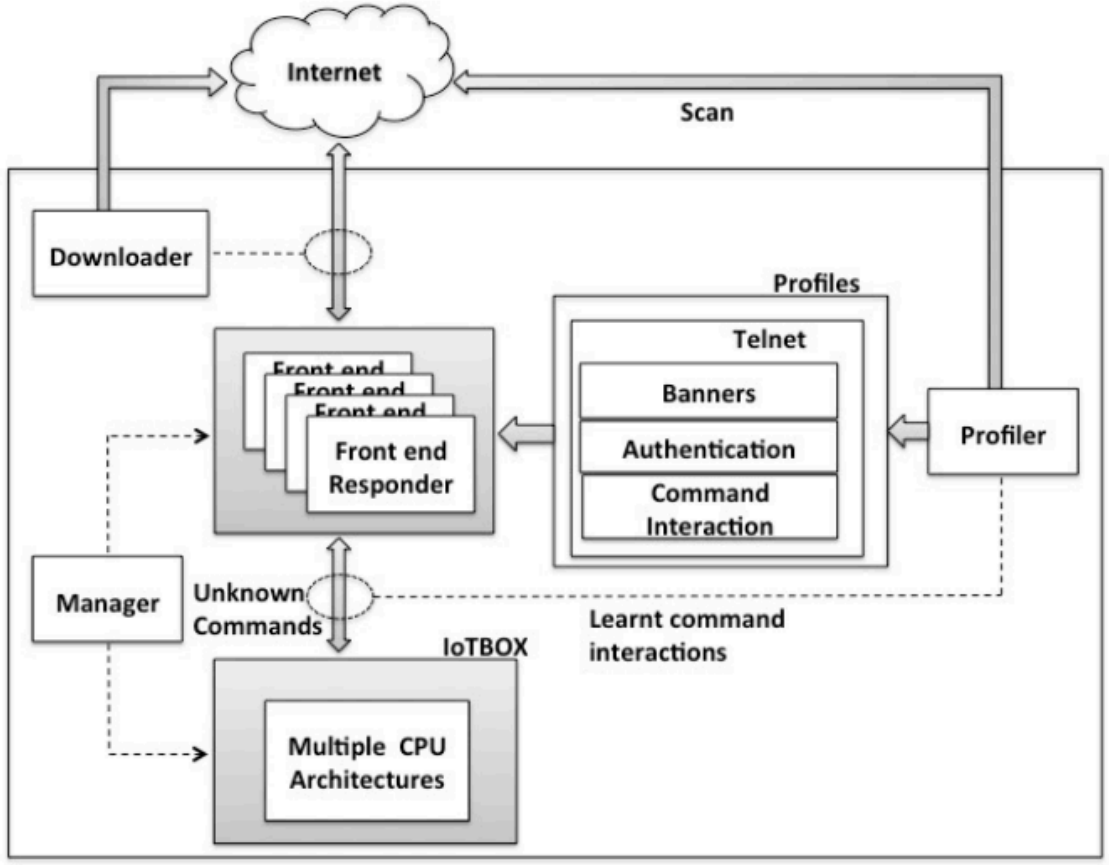
1. het verkrijgen van empirisch inzicht in het landschap van onveilige IoT-apparaten en de oorzakelijke factoren achter concentraties van geïnfecteerde apparaten
2. het ontwerpen van DNS-gebaseerde technieken voor de detectie van geïnfecteerde IoT-apparaten
3. het voorkomen van toenemend misbruik door IoT-botnets door geïnfecteerde apparaten en hun command-and-control infrastructuur te signaleren en geïnfecteerde apparaten op te schonen.

Economics of Cybersecurity. TU Delft.

SIDN LABS

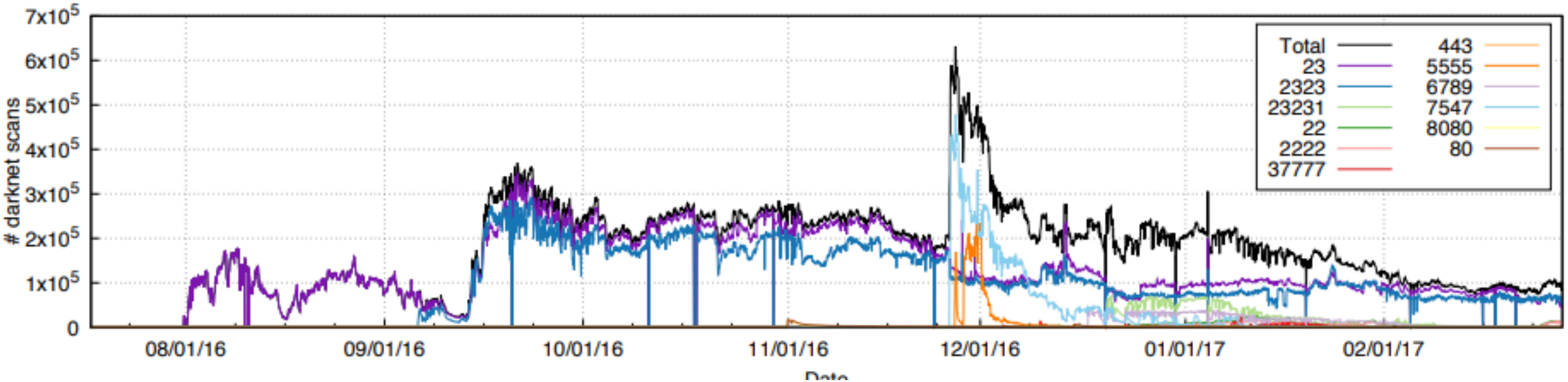
IoTPot

Honeypot door Yokohama National University



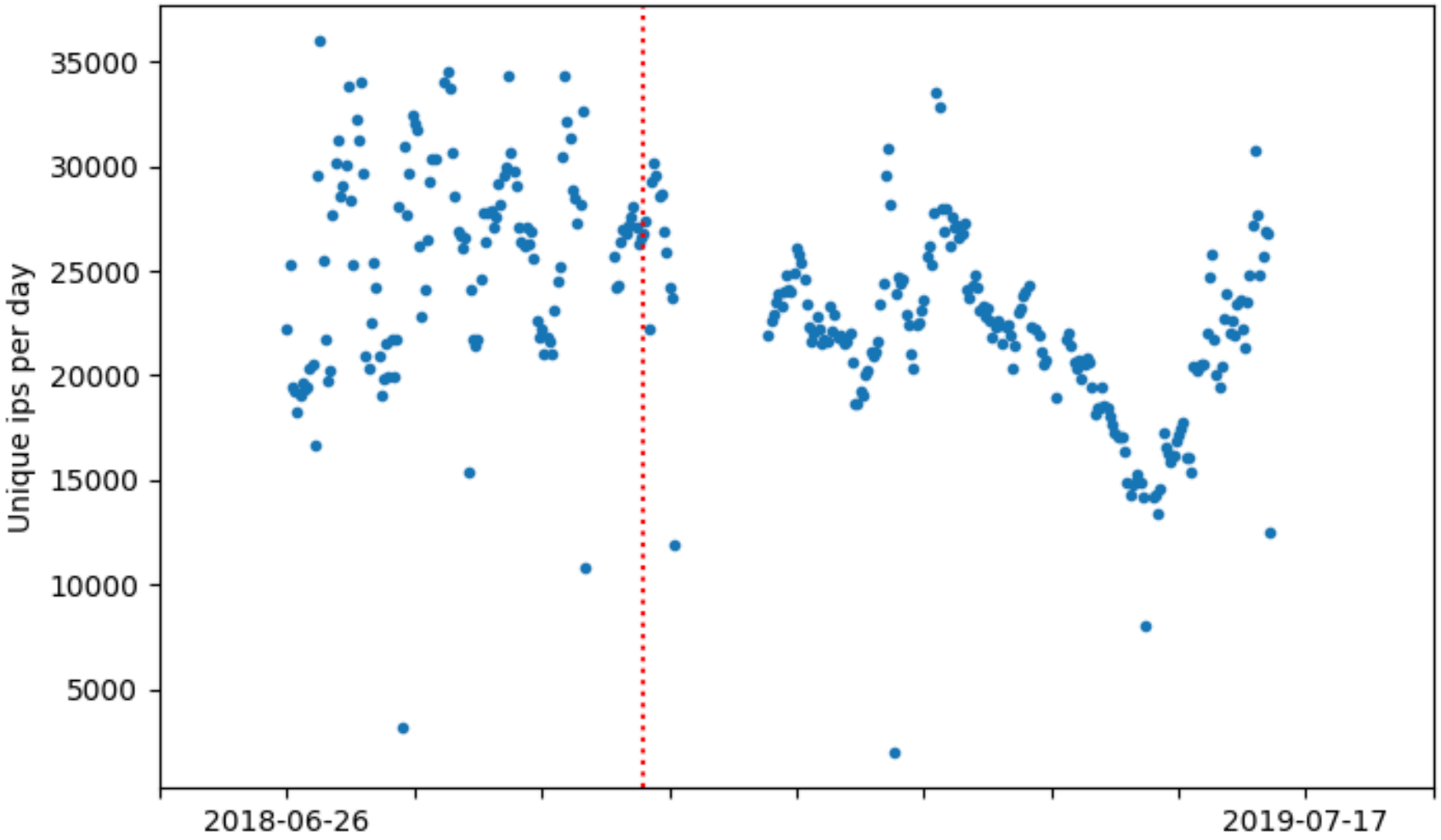
Pa, Yin Minn Pa, et al. "IoTPOT: analysing the rise of IoT compromises." *9th USENIX Workshop on Offensive Technologies*. 2015.

Mirai in 2016/2017



Bron: Antonakakis et al. “Understanding the Mirai Botnet” in USENIX Security 2017

Mirai in 2018/2019



MINIONS output

Paper: Infected IoT Device Cleanup Efforts (under review)

Paper: Longitudinal Mirai study

Study: Monetization of IoT botnets towards DDoS attacks

DAGOBERT: goals

Botnets detecteren in DNS verkeer

Profielen van (on)bekende botnets maken

Zowel recursive resolver (ISPs) als authoritative (.nl) data

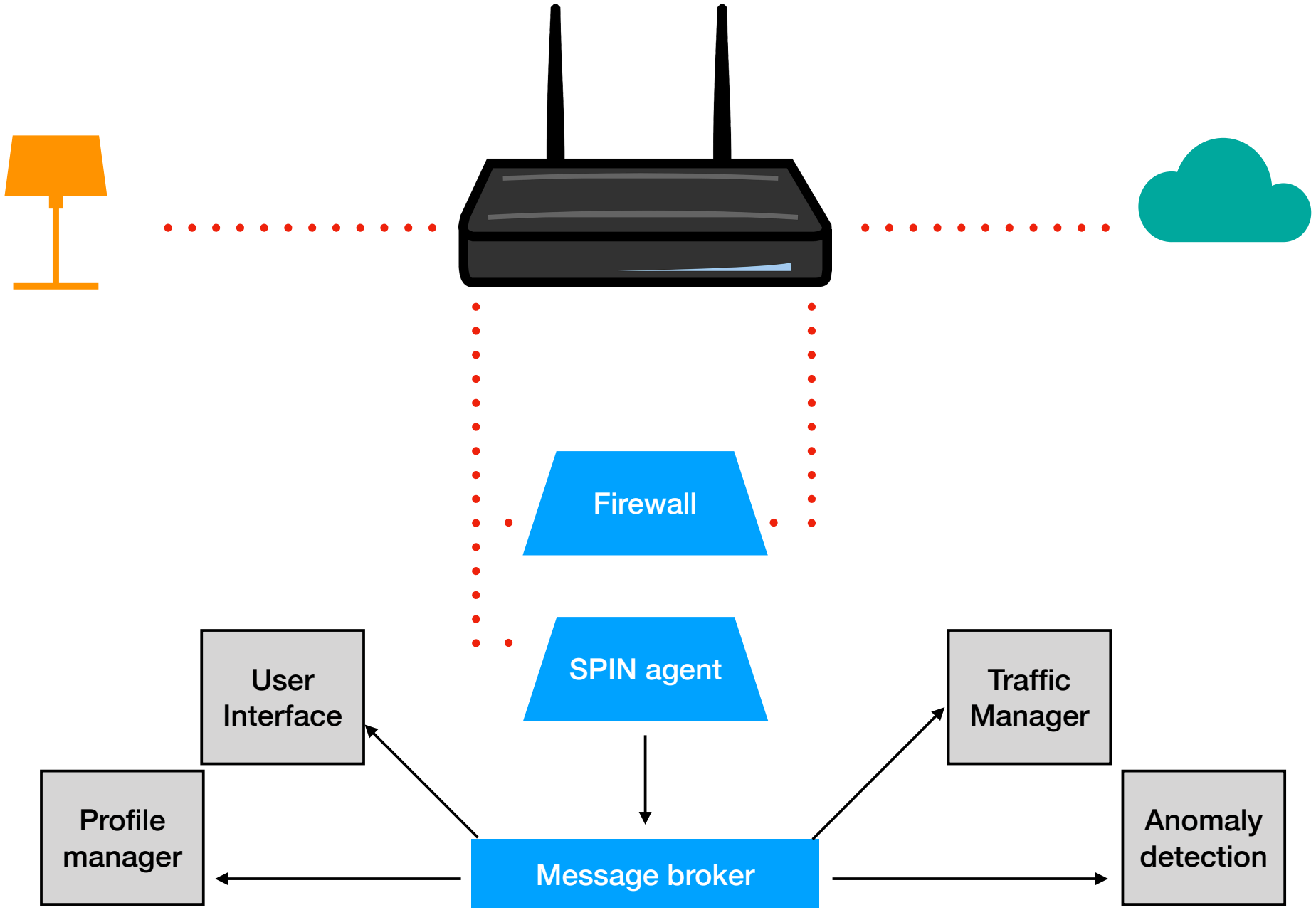
Gebruik machine learning om grote hoeveelheden data te analyseren. Onderzoeken effectiviteit.

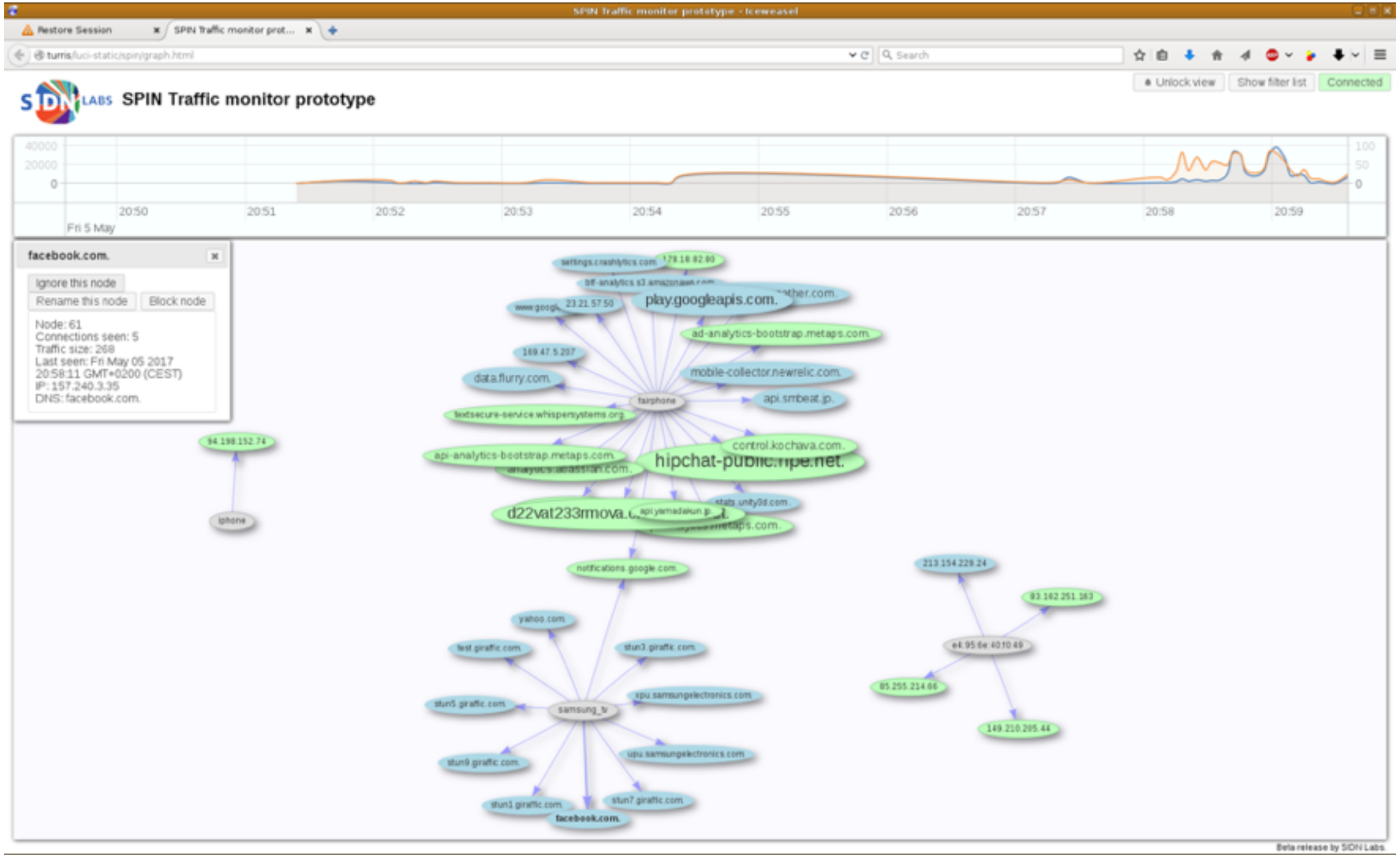
DAGOBERT

- Langdurige contractonderhandelingen
- Lastig om intentie te concretiseren
- ISP's zeer geïnteresseerd, operationeel lastiger.
- Te weinig databronnen.

- Maar: inmiddels wel ISP resolver data
  - Pseudonimised DNS data streams
- Detect DGA-domains 98.89% TP, 0.12% FP

Security and Privacy for In-home Networks (SPIN)


Firewall
SPIN agent
User Interface
Traffic Manager
Profile manager
Anomaly detection
Message broker
SDN LABS


SPIN Traffic monitor prototype - Iceweasel
Restore Session
SPIN Traffic monitor prot...
turris/luci-static/spin/graph.html
Search
SDN LABS
SPIN Traffic monitor prototype
Unlock view
Show filter list
Connected
40000
20000
0
100
50
0
20:50
20:51
20:52
20:53
20:54
20:55
20:56
20:57
20:58
20:59
Fri 5 May
facebook.com.
Ignore this node
Rename this node
Block node
Node: 61
Connections seen: 5
Traffic size: 268
Last seen: Fri May 05 2017 20:58:11 GMT+0200 (CEST)
IP: 157.240.3.35
DNS: facebook.com.
settings.crashlytics.com.
179.18.82.80
play.googleapis.com.
www.google.com.
23.21.57.50
ad-analytics-bootstrap.metaps.com.
169.47.5.237
data.flurry.com.
mobile-collector.newrelic.com.
fairphone
api.smbeat.jp.
textsecure-service.whispersystems.org.
94.198.152.74
iphone
api-analytics-bootstrap.metaps.com.
control.kochava.com.
hipchat-public.hpe.net.
stats.unity3d.com.
api.yamadakun.jp.
notifications.google.com.
yahoo.com.
test.giraffic.com.
stun3.giraffic.com.
stun5.giraffic.com.
samsung_tv
xpu.samsungelectronics.com.
stun9.giraffic.com.
upu.samsungelectronics.com.
stun1.giraffic.com.
stun7.giraffic.com.
facebook.com.
213.154.229.24
83.162.251.163
e4:95:6e:40:10:49
85.255.214.66
149.210.205.44
Beta release by SDN Labs.

PROPOSED STANDARD
Errata Exist

Internet Engineering Task Force (IETF)
Request for Comments: 8520
Category: Standards Track
ISSN: 2070-1721

E. Lear
Cisco Systems
R. Droms
Google
D. Romascanu

March 2019

Manufacturer Usage Description Specification

Abstract

This memo specifies a component-based architecture for Manufacturer Usage Descriptions (MUDs). 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.

This memo specifies two YANG modules, IPv4 and IPv6 DHCP options, a Link Layer Discovery Protocol (LLDP) TLV, a URL, an X.509 certificate extension, and a means to sign and verify the descriptions.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.


Max input: 230 V


WHICH ONE IS THE DEPLOY BUTTON?

Volg ons

SIDN.nl

@SIDN

SIDN

Vragen en discussie

www.sidnlabs.nl | stats.sidnlabs.nl

Elmer Lastdrager
Research Engineer
elmer.lastdrager@sidn.nl | @elmerlastdrager