Security and Privacy for In-home Networks

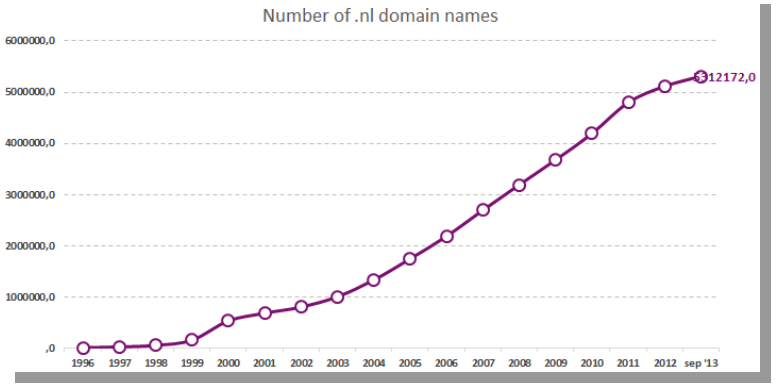
The SPIN project at SIDN

Jelte Jansen | Sensemakers meetup

SIDN LABS

Introduction: SIDN

- Domain name registry for .nl ccTLD
- 5.8 million domain names
- 3 million domain names signed with DNSSEC



Introduction: SIDN Labs

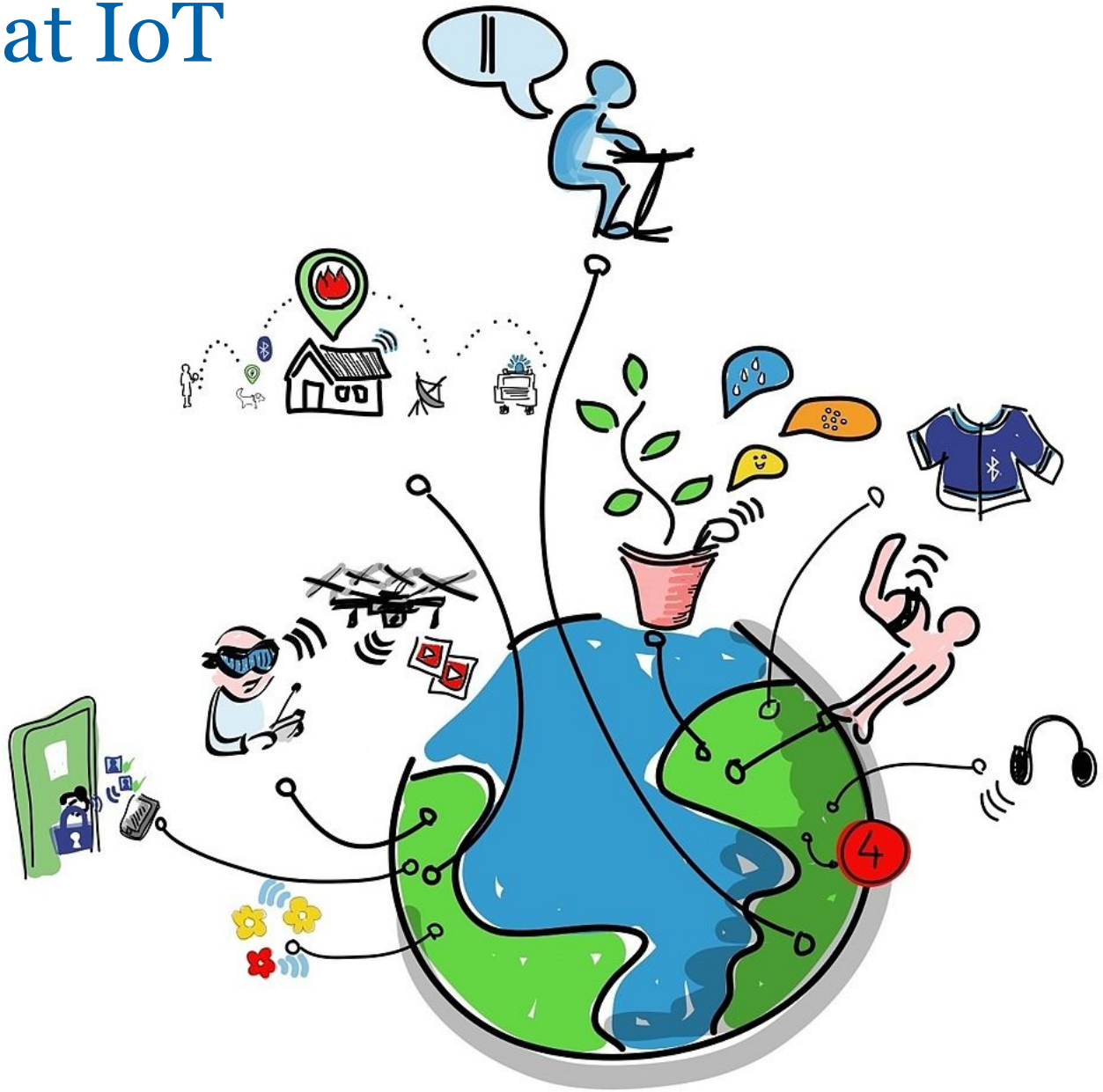
- R&D team of SIDN
- Improve services of SIDN
- Center of expertise
- Increase security of the Internet
- Facilitate external research

Introduction: Me

- Research Engineer at SIDN
  https://sidnlabs.nl
- Independent consultant on eInvoicing
  https://ionite.net
- Board of advisors at SIDN Fund
  https://sidnfonds.nl
- Programme committee for RIPE meetings
  https://ripe79.ripe.net

- But mainly just a tech geek
  https://tjeb.nl

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".”

SDN LABS

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*"

(from a security standpoint)

Attributed to @tkadlec

SDN LABS

These Flip Flops Are 'Smart' for the Dumbest Possible Reason

Christina Warren
3/28/17 5:58pm • Filed to: WHO NEEDS THIS?

28.3K 17 2

Image: Hari Mari

SDN LABS

So, about that IoT

Home > Data Protection > Internet of Things

SLIDESHOW

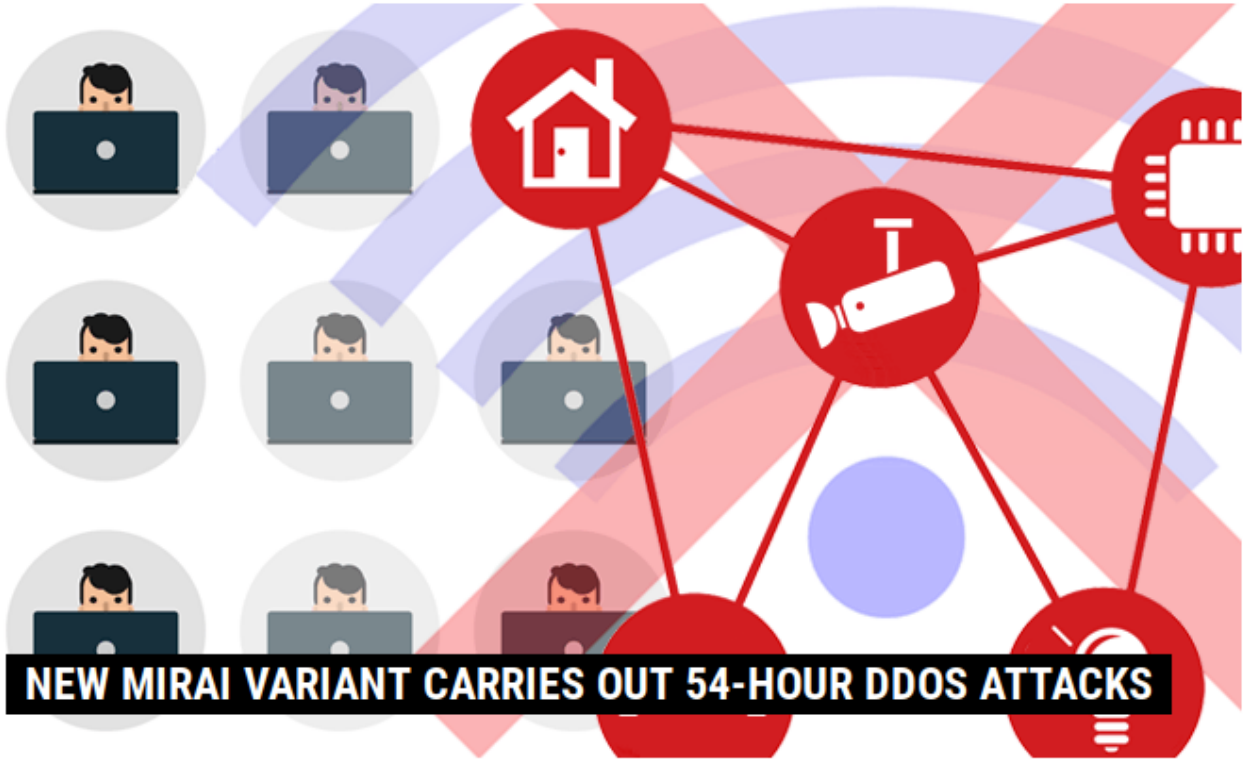
The internet of insecure things: Thousands of internet-connected devices are a security disaster in the making

By Josh Fruhlinger, CSO | Oct 12, 2016 4:00 AM PT

So, about that IoT

threatpost CATEGORIES FEATURED PODCASTS VIDEOS

Welcome > Blog Home > Hacks > New Mirai Variant Carries Out 54-Hour DDoS Attacks



by Tom Spring March 30, 2017 , 2:50 pm

SDN LABS

What should we do?

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

What should we do?

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

“Yes”

What should we do?

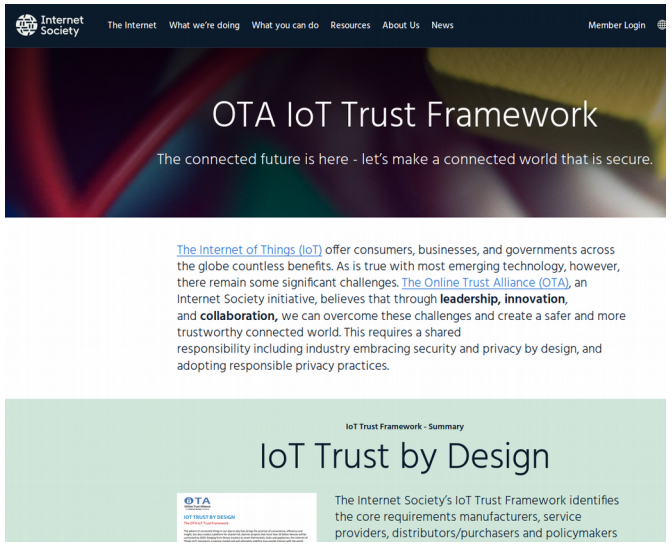
- Better practices for manufacturers?
- Free **secure** software stacks?
- International policy, regulation, certificiation?
- Clear up accountability issues?
- Generate market demand for secure products?
- Quarantine bad actors (e.g. at ISP)?
- Educate users?
- Empower users?

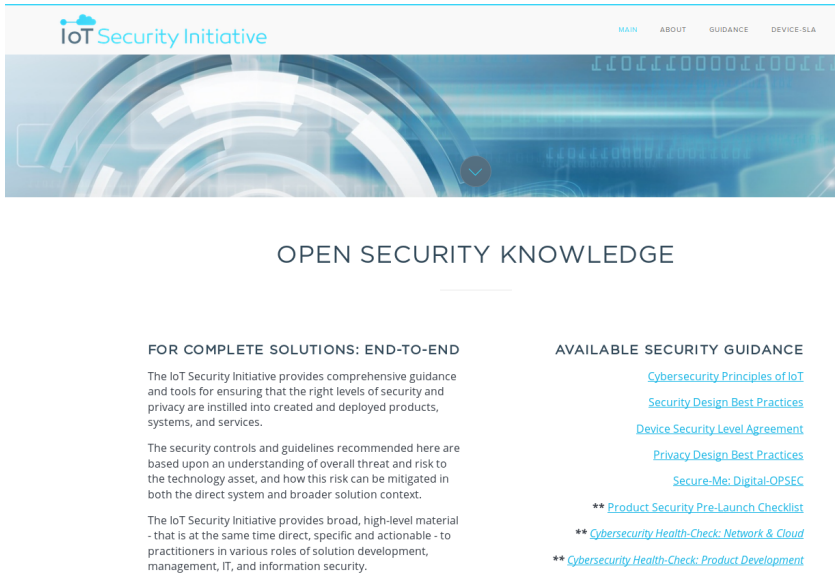
“Yes”

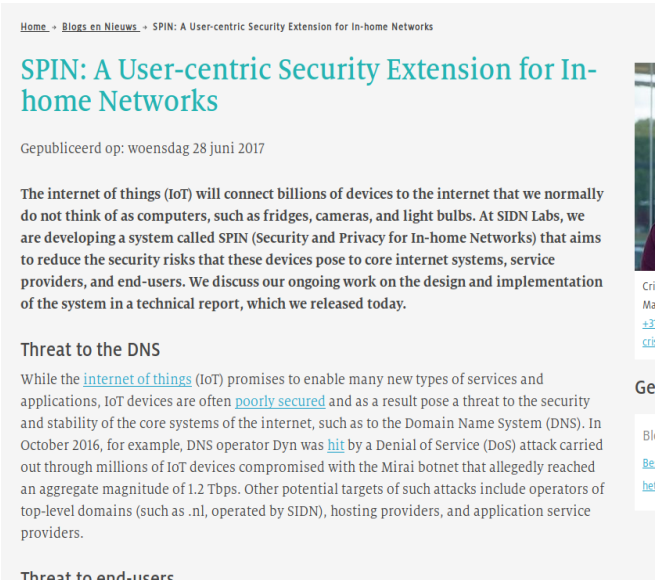
We need to do it all

SIDN LABS

Initiatives around the world, on many levels







SIDN LABS

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

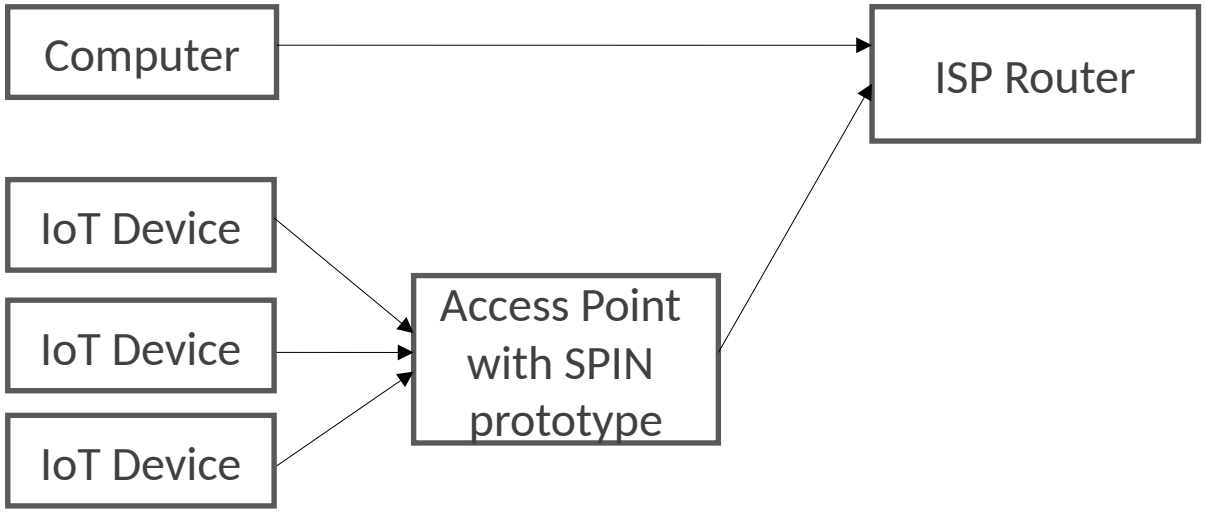
The SPIN project at SIDN Labs

- 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

Prototype built on OpenWRT

- Currently bundled with Valibox: http://valibox.sidnlabs.nl
- Source at https://github.com/SIDN/spin
- Currently working on instructions for Raspberry Pi

prototype 2, GL-Inet hardware

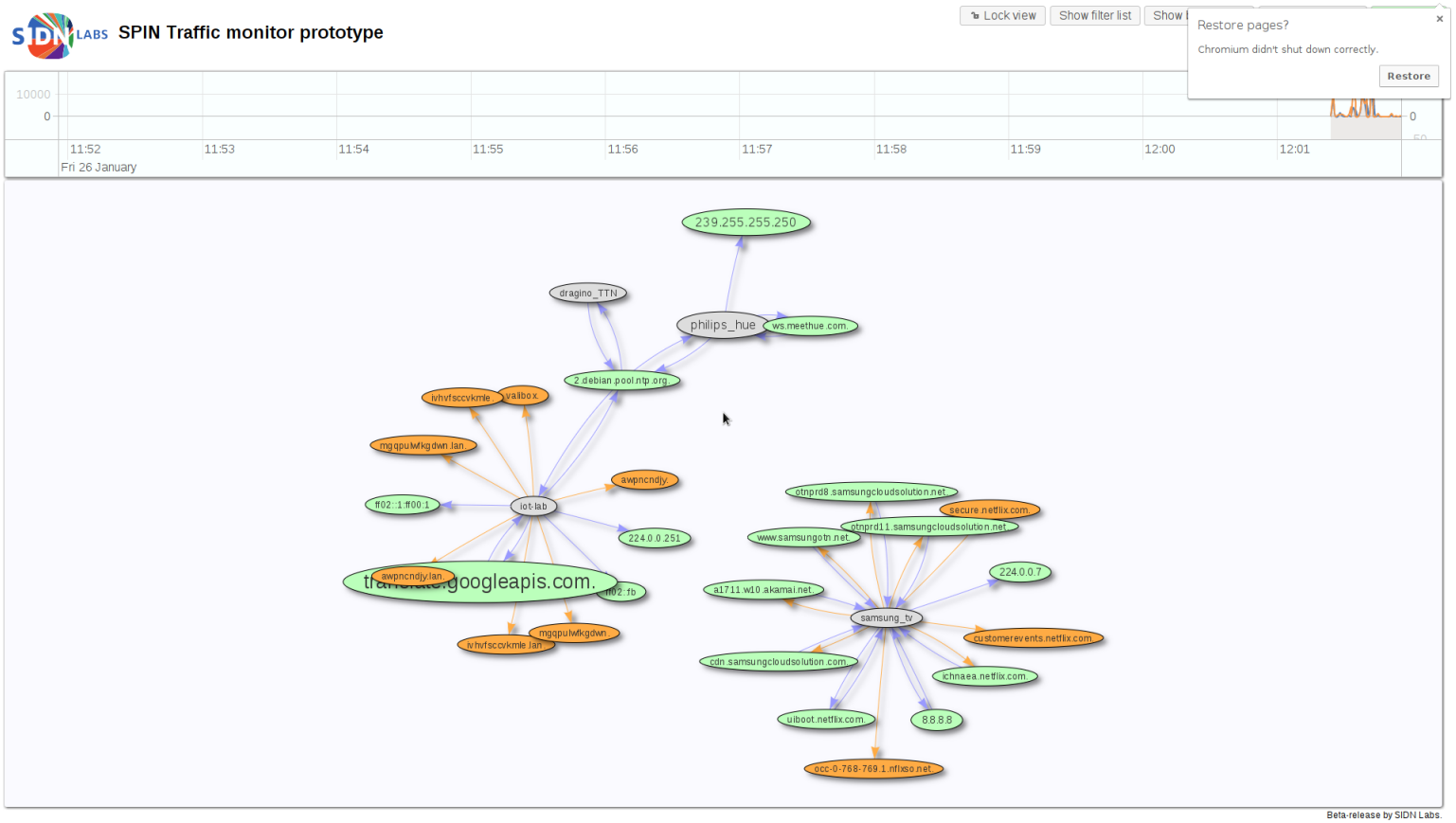


Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination, or both
- Download traffic from specific devices

Next research topics:

- In-depth device traffic analysis
- Time-series based analysis



DEMO TIME!

Please please please please please
Please please please please work

So what can you do?

A friend built his own

from scratch…

Might be asking a bit much

So what can you do?

- 'Be smart'
- Ask (around) for security status
- 'Can it run offline?'
  - Step-up to blocking internet access for (specific) devices
- Monitor, update, maintain
  - (yes that still asking a lot)

Thank you for your attention!

Any questions?

Follow us

sidnlabs.nl


@SIDN @sidnlabs @twitjeb


SIDN

SIDN LABS

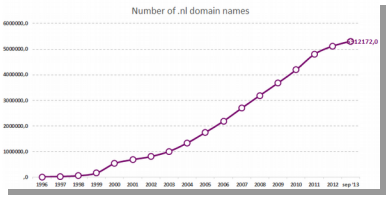
Security and Privacy for In-home Networks

The SPIN project at SIDN

Jelte Jansen | Sensemakers meetup

Introduction: SIDN

- Domain name registry for .nl ccTLD
- 5.8 million domain names
- 3 million domain names signed with DNSSEC



Introduction: SIDN Labs

- R&D team of SIDN
- Improve services of SIDN
- Center of expertise
- Increase security of the Internet
- Facilitate external research

Introduction: Me

- Research Engineer at SIDN
  https://sidnlabs.nl
- Independent consultant on eInvoicing
  https://ionite.net
- Board of advisors at SIDN Fund
  https://sidnfonds.nl
- Programme committee for RIPE meetings
  https://ripe79.ripe.net

- But mainly just a tech geek
  https://tjeb.nl

- This screenshot shows the impact of a phish on the DNS traffic of a compromised domain name.

- Top bar shows the number of queries for each day, the red bar is the day the phish was reported.
- Before the red bar there is a visible ramp up in traffic.
- This could be used as an indicator for automatic detection.
- The same is true for the number of unique networks (ASN) query the domain name.
- The geographical distribution of clients (resolvers) also changes when there is a phish.

This screenshot shows the impact of a phish on the DNS traffic of a compromised domain name.

Top bar shows the number of queries for each day, the red bar is the day the phish was reported.

Before the red bar there is a visible ramp up in traffic.

This could be used as an indicator for automatic detection.

The same is true for the number of unique networks (ASN) query the domain name.

The geographical distribution of clients (resolvers) also changes when there is a phish.

This screenshot shows the impact of a phish on the DNS traffic of a compromised domain name.

Top bar shows the number of queries for each day, the red bar is the day the phish was reported.

Before the red bar there is a visible ramp up in traffic.

This could be used as an indicator for automatic detection.

The same is true for the number of unique networks (ASN) query the domain name.

The geographical distribution of clients (resolvers) also changes when there is a phish.

This screenshot shows the impact of a phish on the DNS traffic of a compromised domain name.

Top bar shows the number of queries for each day, the red bar is the day the phish was reported.

Before the red bar there is a visible ramp up in traffic.

This could be used as an indicator for automatic detection.

The same is true for the number of unique networks (ASN) query the domain name.

The geographical distribution of clients (resolvers) also changes when there is a phish.

This screenshot shows the impact of a phish on the DNS traffic of a compromised domain name.

Top bar shows the number of queries for each day, the red bar is the day the phish was reported.

Before the red bar there is a visible ramp up in traffic.

This could be used as an indicator for automatic detection.

The same is true for the number of unique networks (ASN) query the domain name.

The geographical distribution of clients (resolvers) also changes when there is a phish.

Attributed to @tkadlec

SDN LABS

Dyn attack; issues with paypal, netflix, twitter, reddit, xbox Live, airbnb, amazon, github, spotify, the guardian, and many, many more

What should we do?

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

What should we do?

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

"Yes"

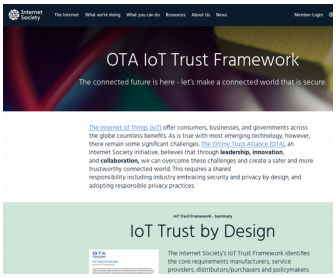
What should we do?

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

"Yes"

We need to do it all

Initiatives around the world, on many levels



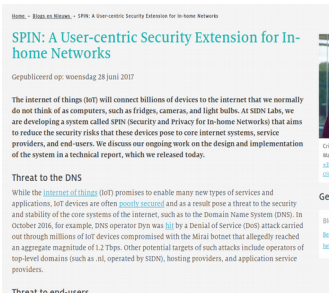

Naar geautomatiseerde DDoS-bescherming met MUD

Gepubliceerd op: maandag 29 oktober 2018

Onveilige Internet of Things apparaten (IoT-apparaten) worden gebruikt om Distributed Denial of Service (DDoS) aanvallen uit te voeren. Een bekend voorbeeld hiervan is de Mirai-botnet aanval op DNS-operator Dyn, die leidde tot grootschalige uitval van DNS-diensten. Om het schaderisico van onveilige IoT-apparaten te beperken, lanceerde SIDN Labs het SPIN-project. Hierbij evalueerden we de bruikbaarheid van de Manufacturer Usage Description (MUD) specificatie, die momenteel wordt ontwikkeld door de Operations and Management Area Working Group (OPSAWG) binnen de Internet Engineering Task Force (IETF).

De achterliggende gedachte hierbij is dat wanneer een IoT-apparaat verbinding zoekt met een netwerk, het apparaat doorgeeft welke resources het nodig heeft om goed te kunnen functioneren. Deze informatie wordt vastgelegd in een *MUD-profiel*, dat het beoogde netwerkgedrag van het apparaat beschrijft op basis van een 'whitelist'. Deze whitelist zou compleet moeten zijn en dus kan de toegang tot andere netwerkresources worden geweigerd zonder dat dit de goede werking van het apparaat belemmert.

In dit onderzoek bestudeerden we de toepasbaarheid van MUD voor het beveiligen van IoT-apparaten tegen hackpogingen. Ook onderzochten we of de bruikbaarheid van IoT-apparaten voor DDoS-aanvallen afneemt door een profiel te handhaven. De MUD-specificatie is echter

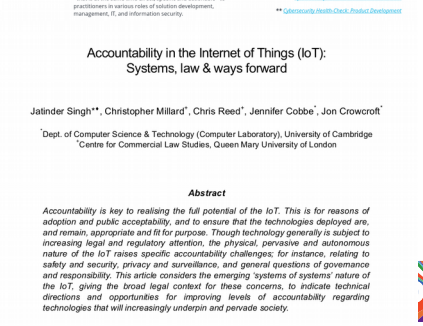

SPIN: A User-centric Security Extension for In-home Networks

Gepubliceerd op: woensdag 28 juni 2017

The internet of things (IoT) will connect billions of devices to the internet that we normally do not think of as computers, such as fridges, cameras, and light bulbs. At SIDN Labs, we are developing a system called SPIN (Security and Privacy for In-home Networks) that aims to reduce the security risks that these devices pose to core internet systems, service providers, and end-users. We discuss our ongoing work on the design and implementation of the system in a technical report, which we released today.

Threat to the DNS

While the internet of things (IoT) promises to enable many new types of services and applications, IoT devices are often poorly secured and as a result pose a threat to the security and stability of the core systems of the internet, such as to the Domain Name System (DNS). In October 2016, for example, DNS operator Dyn was hit by a Denial of Service (DoS) attack carried out through millions of IoT devices compromised with the Mirai botnet that allegedly reached an aggregate magnitude of 1.2 Tbps. Other potential targets of such attacks include operators of top-level domains (such as .nl, operated by SIDN), hosting providers, and application service providers.


Accountability in the Internet of Things (IoT): Systems, law & ways forward

Jatinder Singh**, Christopher Millard*, Chris Reed*, Jennifer Cobbe*, Jon Crowcroft*

*Dept. of Computer Science & Technology (Computer Laboratory), University of Cambridge
*Centre for Commercial Law Studies, Queen Mary University of London

Abstract

Accountability is key to realising the full potential of the IoT. This is for reasons of adoption and public acceptability, and to ensure that the technologies deployed are, and remain, appropriate and fit for purpose. Though technology generally is subject to increasing legal and regulatory attention, the physical, pervasive and autonomous nature of the IoT raises specific accountability challenges; for instance, relating to safety and security, privacy and surveillance, and general questions of governance and responsibility. This article considers the emerging 'systems of systems' nature of the IoT, giving the broad legal context for these concerns, to indicate technical directions and opportunities for improving levels of accountability regarding technologies that will increasingly underpin and pervade society.

- IoT Trust framework (ISOC)
- RED directive (EU)
- GDPR even (EU)
- Accountability (law scholars)
- IETF: MUD/DOTS/etc.

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

DEMO TIME!

Please please please please please
Please please please please work

So what can you do?

A friend built his own

from scratch…

Might be asking a bit much

SDN LABS

So what can you do?

- 'Be smart'
- Ask (around) for security status
- 'Can it run offline?'
  - Step-up to blocking internet access for (specific) devices
- Monitor, update, maintain
  - (yes that still asking a lot)

SIDN LABS

Thank you for your attention!

Any questions?

Follow us


sidnlabs.nl


@SIDN @sidnlabs @twitjeb


SIDN