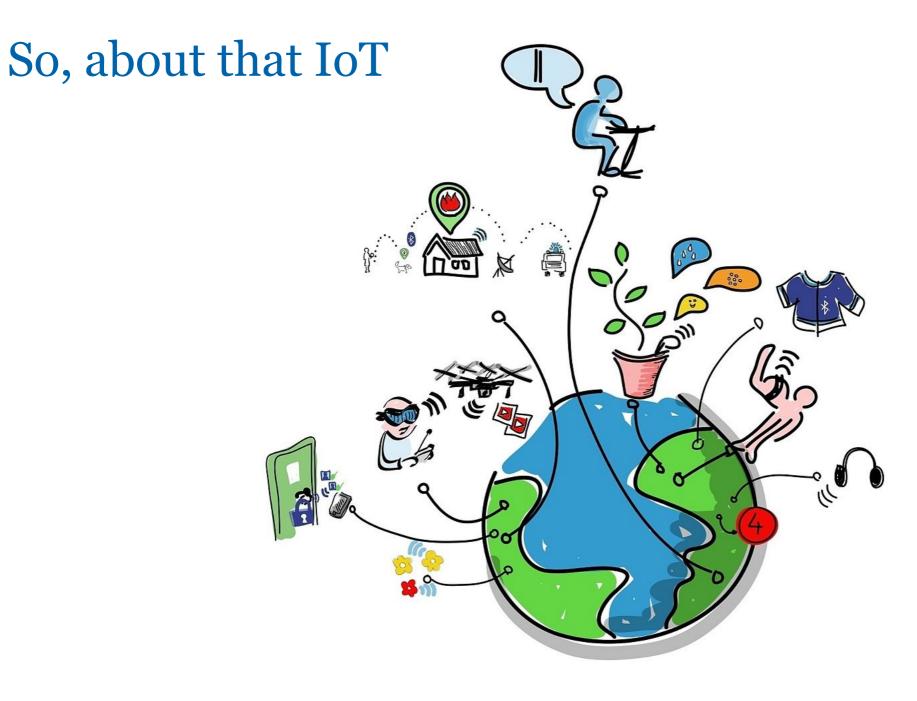
# Your Things Are Shouting At Me

The evolving security landscape of the IoT

Jelte Jansen | SIDN Connect 2019







# Should we even still be talking about 'the IoT'?

• It's really 'just' more computers

• A lot more...

• With dubious track-records, so far.....



# The future of the Internet (of Things)

- Prediction: 21 billion IoT devices in 2025
- source: IoT Analytics 2019

- Prediction: 42 billion IoT devices in 2025
- Source: International Data Corporation

- Prediction: lots and lots of devices in the future
- Source: me



# The "S" in IoT stands for SECURITY

Attributed to @tkadlec



## Dumb to smart, separate to connected





Image created by http://www.blog.spoongraphics.co.uk

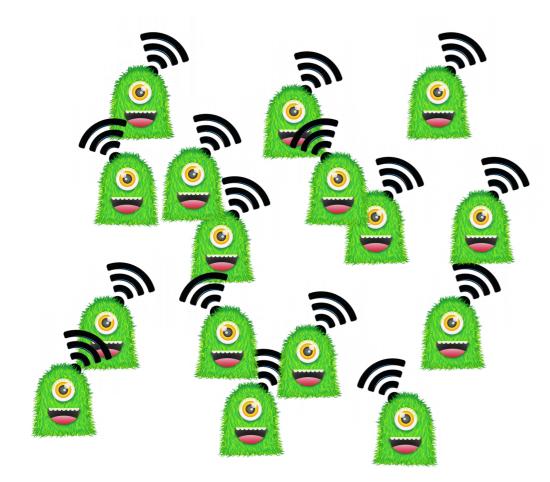
# Dumb to smart, separate to connected





Image created by http://www.blog.spoongraphics.co.uk

# Dumb to smart, separate to connected



SDILABS

Image created by http://www.blog.spoongraphics.co.uk

# Let's think about privacy

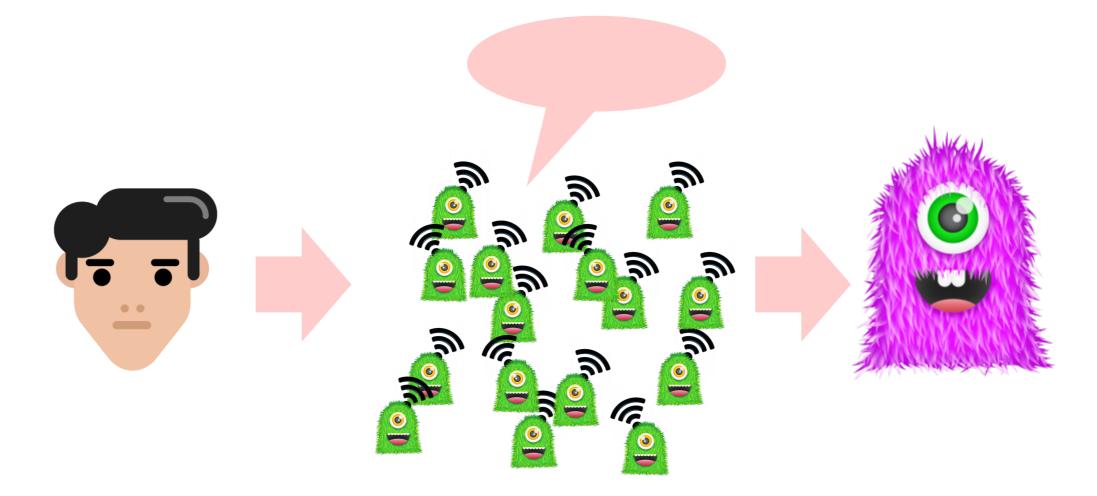
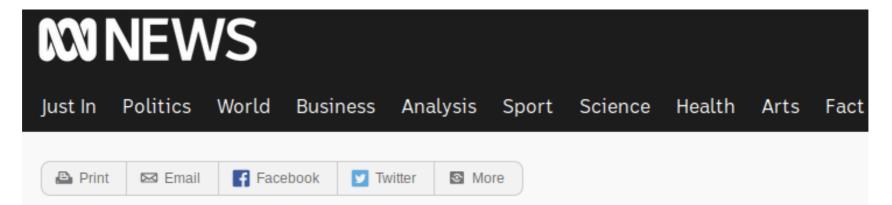




Image created by http://www.blog.spoongraphics.co.uk



# My devices are sending and receiving data every two seconds, sometimes even when I sleep

Story Lab By Simon Elvery

Updated 3 Dec 2018, 7:24am

When I decided to record every time my phone or laptop contacted a server on the internet, I knew I'd get a lot of data, but I honestly didn't think it would reveal nearly 300,000 requests in a single week.

On average, that's about one request every two seconds.

In this instalment of the **#DataLife project** I'm going to take a broad look at what all those requests are doing and break down some details about what I've found in the data so far.



**PHOTO:** For the #DataLife project, Simon Elvery intercepted and recorded every bit of data sent from his phone and laptop. (ABC News: Tim Leslie and Ben Spraggon)



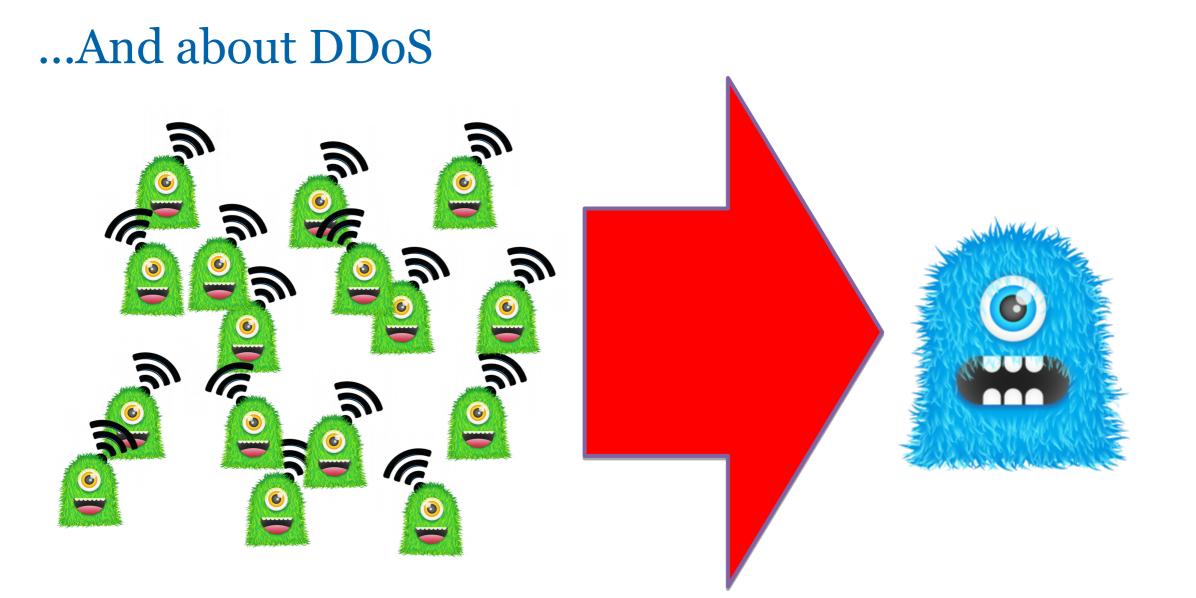




Image created by http://www.blog.spoongraphics.co.uk

# Hacked IoT Devices Internet Services







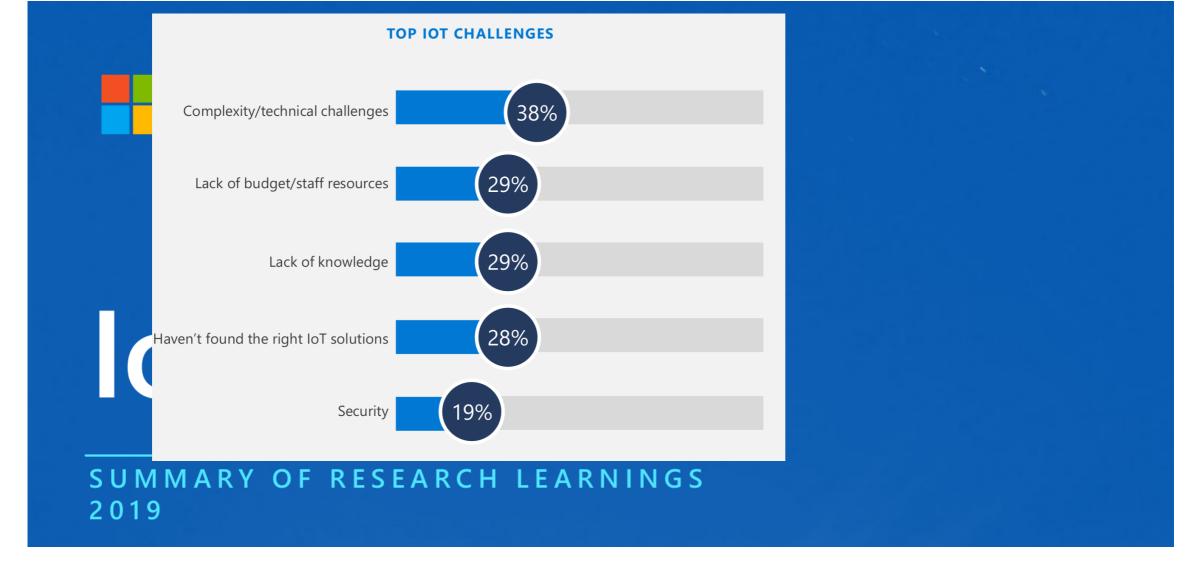
# loT Signals

SUMMARY OF RESEARCH LEARNINGS 2019



# **SUMMARY OF RESEARCH LEARNINGS** 2019

Security concerns around IoT adoption are universal: 97% of companies are concerned about security when implementing IoT (though this is not hindering adoption). Collectively, the top security priority is



Security concerns around IoT adoption are universal: 97% of companies are concerned about security when implementing IoT (though this is not hindering adoption). Collectively, the top security priority is



NEWS

### More than two-thirds of consumers are concerned about IoT device security

By Sooraj Shah - April 27, 2017

Source: Internet of business



# Initiatives around the world, on many levels



responsibility including industry embracing security and privacy by design, and adopting responsible privacy practices.

### IoT Trust by Design

The Internet Society's IoT Trust Framework identifies the core requirements manufacturers, service providers, distributors/purchasers and policymakers

Home + Blogs en Nieuws + Naar geautomatiseerde DDoS-bescherming met MUD

<u>ФТА</u>

### 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 Miraibotnet 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 <u>SPIN-project</u>. 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 IoTapparaten 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 noe niet klaar voor sebruik en dis nog nergens geïnnlementeerd. Om MID-specificatien te



Electrical and

What the C

EMC Directive

LVD Directive

links

Events

Electronic Engineering

Electrical engineering

Tools and Databases

Contracts and grants

Public consultations

Single Market and Single Market and Standards Standards SMEs SMEs SMEs

#### Radio Equipment Directive (RED)

The Radio Engineer Directive 2014/2014 [Direction] (Direction) and application of the placing radio engineers of the markst L sense as 2014 Boyle Markst for radio engineers by single sacredit requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for hume regulation governing is one additional aspects. These includes terrival features for the protection of privacy, personal data and against fraud. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination or addio equipment and software.

otice | Cookies | Contact | Search | English (en)

Ma

Ge

Bl

Be

het

The RED aligned the previous Directive, the Radio and Telecommunication Terminal Equipment Directive (<u>1999/5/FC</u> (R&TTED), with the <u>new legislative framework</u> for the marketing of products.

The revision also took account of the need for improved market surveillance. In particular, for the traceability obligations of manufacturers, importers and disbibutors. It has improved market surveillance instruments. One example is the possibility for required preventigistation of radio equipment in categories with low compliance levels.

The RED was published in the OLEU on 22 May 2014, entered into force on 11 June 2014 and is applicable as of 13 June 2016. Included a one-year transitional period, which ended on 12 June 2017 (Area 43), During the transitional phase, manufacturers were allowed to place on the market radio equipment compliant with either the RED or the EU legislation applicable before 13 June 2016 (e.g. RATTED).

For more details on the application of the RED, see the RED Guide under the Guidance section below.

#### Committee (TCAM)

Article 45 of the RED establishes the Telecommunication Conformity Assessment and Market Surveillance Committee (TCAM), a committee related to <u>Regulation (EU) No 182/2011</u> TCAM gives its opinion on proposed implementing acts under the BET) is its enforcement that and the Direction of the Direction when lesses are related alter but the chair or a

Home + Blogs en Nieuws + SPIN: A User-centric Security Extension for In-home Networks

#### SPIN: A User-centric Security Extension for Inhome 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 <u>internet of things</u> (IoT) promises to enable many new types of services and applications, IoT devices are often <u>poorly secured</u> 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 <u>hit</u> 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.

Threat to end-users



#### OPEN SECURITY KNOWLEDGE

#### FOR COMPLETE SOLUTIONS: END-TO-END

The IoT Security Initiative provides comprehensive guidance and tools for ensuring that the right levels of security and privacy are instilled into created and deployed products, systems, and services.

The security controls and guidelines recommended here are based upon an understanding of overall threat and risk to the technology asset, and how this risk can be mitigated in both the direct system and broader solution context. The IoT Security Initiative provides broad, high-level material

- that is at the same time direct, specific and actionable - to practitioners in various roles of solution development.

. management, IT, and information security.

#### AVAILABLE SECURITY GUIDANCE

Cybersecurity Principles of IoT Security Design Best Practices Device Security Level Agreement Privacy Design Best Practices Secure-Me: Digital-OPSEC \*\* Product Security Pre-Launch Checklist \*\* Cybersecurity Health-Check: Network & Cloud \*\* Cybersecurity Health-Check: Product Development

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

Jatinder Singh\*\*, Christopher Millard<sup>+</sup>, Chris Reed<sup>+</sup>, Jennifer Cobbe<sup>\*</sup>, Jon Crowcroft<sup>\*</sup>

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.





5

### Adviesraad kabinet: verbod op onveilige 'slimme' apparaten

Joost Schellevis redacteur Tech · y 🖂

Sport



ANP

Het kabinet moet onderzoeken of onveilige *internet of things*-apparaten geweerd kunnen worden van de markt. Daarvoor pleit de Cyber Security Raad, een adviesorgaan van het kabinet. In die raad zitten mensen uit het bedrijfsleven, de wetenschap en de overheid.



# But what WE like is research

# So let's focus on that!



# IoT (Collaboration) projects at SIDN

- **INTERSECT** An Internet of Secure Things
- **DINET** DNS-Based Trust, Security, Accountability, and Privacy for IoT

• MINIONS Mitigating IOT-Based DDoS Attacks via DNS



# Cleaning up the Internet of Evil things

https://www.ndss-symposium.org/wp-content/uploads/2019/02/ ndss2019\_02B-2\_Cetin\_paper.pdf

Paper by TUD, YNU, and NICT into the effectiveness of remediation strategies, such as notification and quarantining infected networks.

Tracked Mirai infections through several sources, and the rate of cleanup for several methods.



# Cleaning up the Internet of Evil things: Mirai

- 87% of infections in broadband access networks
- 58-74% natural cleanup rate (no action taken) over several control groups
- 77% cleanup on email notification
- 92% cleanup on quarantine
- Only 5% reinfection rate after 5 months



# Conclusion:

- Quarantining works best
- But please, do it right:
  - Specify issue and reason
  - Specify date and time
  - Specify what to do



# 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

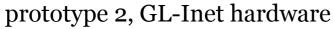


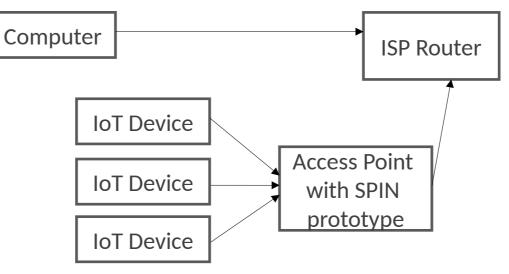
# Prototype built on OpenWRT

- https://spin.sidnlabs.nl
- https://github.com/SIDN/spin
- Currently working on better instructions for Raspberry Pi











# SPIN project focus change

• Renewed focus on research and analysis aspect

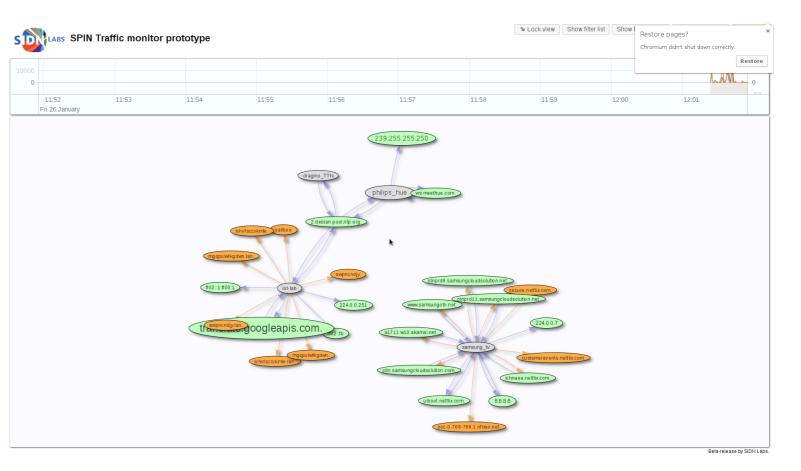
- Basic visualisation locally
- Sharing platform for further analysis (fully optional)

- Start out with other datasets:
  - Large dataset of honeypot data
  - Collected data from our lab devices



# 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





# Running prototyp

- Shows DNS queries
- Shows data traffic
- User can block traffic based source or destination, or bo
- Download traffic from speci
- devices
- Next research topics:
  - In-depth device traffic analy
  - Time-series based analysis

Mozilla Firefox _ D ×							
Ū 🔏 192.168.8.1/spin_api/capture?device={ 🗐 🦷 😎 🚖 😑					Charles Ether Ether	Charry	
Device traffic capture Close window				To Lock view	W Show filter list	Show I	Restore pages? Chromium didn't sl
Device information Name: unknown Mac: 84:cf:bf:8f:03:12 IP(s): 192.168.8.158, fd48:430c:f4bc::30e3:a414:1cbe:c9fa	11:57 5.255		11:58	11:5	59	12:00	1:
Stop captureCapture status:RunningBytes received:15077Capture start time:2019-11-26 14:50:13Last data seen at:2019-11-26 14:50:36Download captured data	w10.al	w.samsungotn.net	prd11.samsungclouds	aure netlix com olution net 2240 0 aea netlix com	nts.netflix.com		
Additional functions		000-768-7	769.1.nfixso.net.>				
Upload captured data to SIDN							
Not working? Try the <u>old download method</u> .							



Beta-release by SIDN Labs

Chromium didn't shut down correctly

12:01

Restore

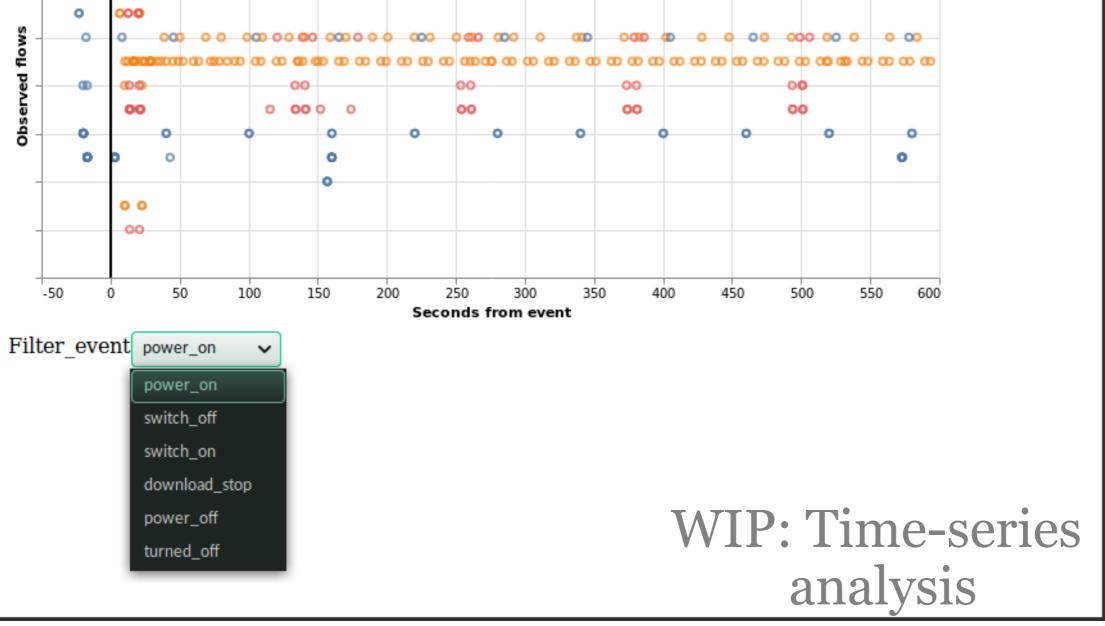
W

# WIP: Initial high-over analysis

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~														
Collected data for Tuya_2019-09-08_22-55-40.pcap Total number of packets in pcap: 36233														
Packet types:														
ip: 33339														
icmp: 3														
arp: 2887														
wauth: 4														
unknown: 0														
First packet s	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	2019-09-08	· ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	~~~~~~~~ 17	~~~~~									
Last packet se		2019-09-09												
Duration of tr		24:02:59		- /										
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~	~~~~~~~	~~~~~~	$\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$									
IP Packet summ	ary:													
source	destina	tion	proto	port	<pre>#sent_packets</pre>	#sent_bytes	<pre>#recv_packets</pre>							
0.0.0.0	255.255	.255.255	UDP	67	2	700	0							
192.168.8.1	192.168	.8.211	UDP	68	6	2088	4							
192.168.8.211	255.255	.255.255	UDP	6666	28859	6262403	0							
192.168.8.211	52.58.2	17.66	TCP	1883	2915	161970	1470							
192.168.8.211	18.194.	70.37	TCP	80	46	5356	30							
192.168.8.211	192.168	.8.1	UDP	53	2	148	2							
192.168.8.211	224.0.0	.1	IGMP	0	1	46	0							
52.29.251.104	192.168	.8.211	TCP	15257	1	54	1							

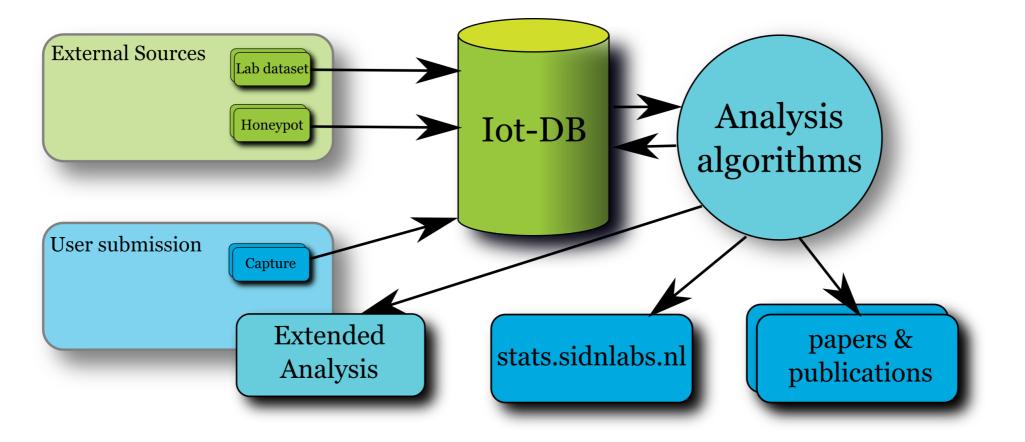


#revc bytes





# Potential goal: "IoT-DB"





# Thank you for your attention! Any questions?

Follow us



@SIDN @sidnlabs @twitjeb

in SIDN

