

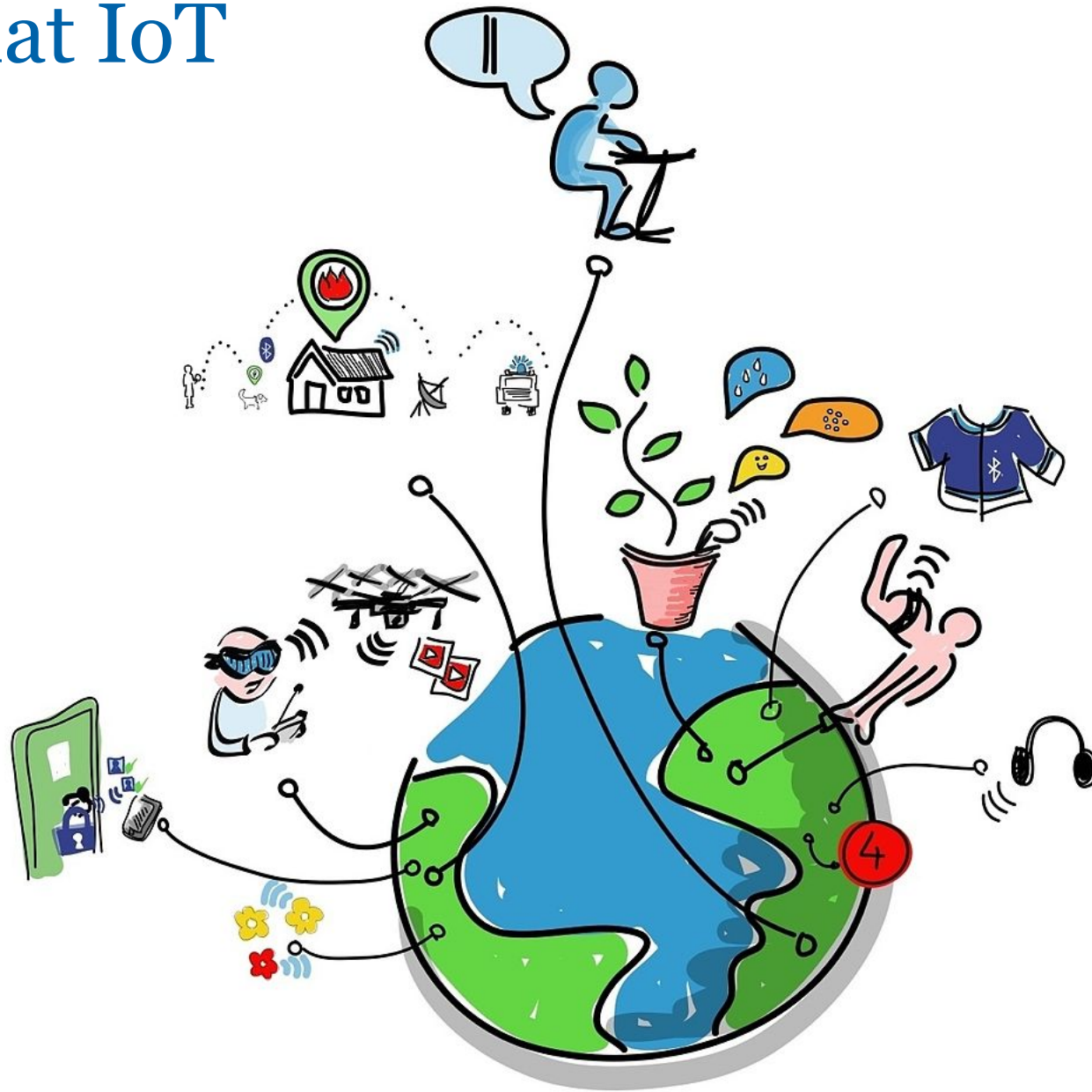
# Your Things Are Shouting At Me

The evolving security landscape of the IoT

Jelte Jansen | SIDN Connect 2019



# So, about that IoT



# 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



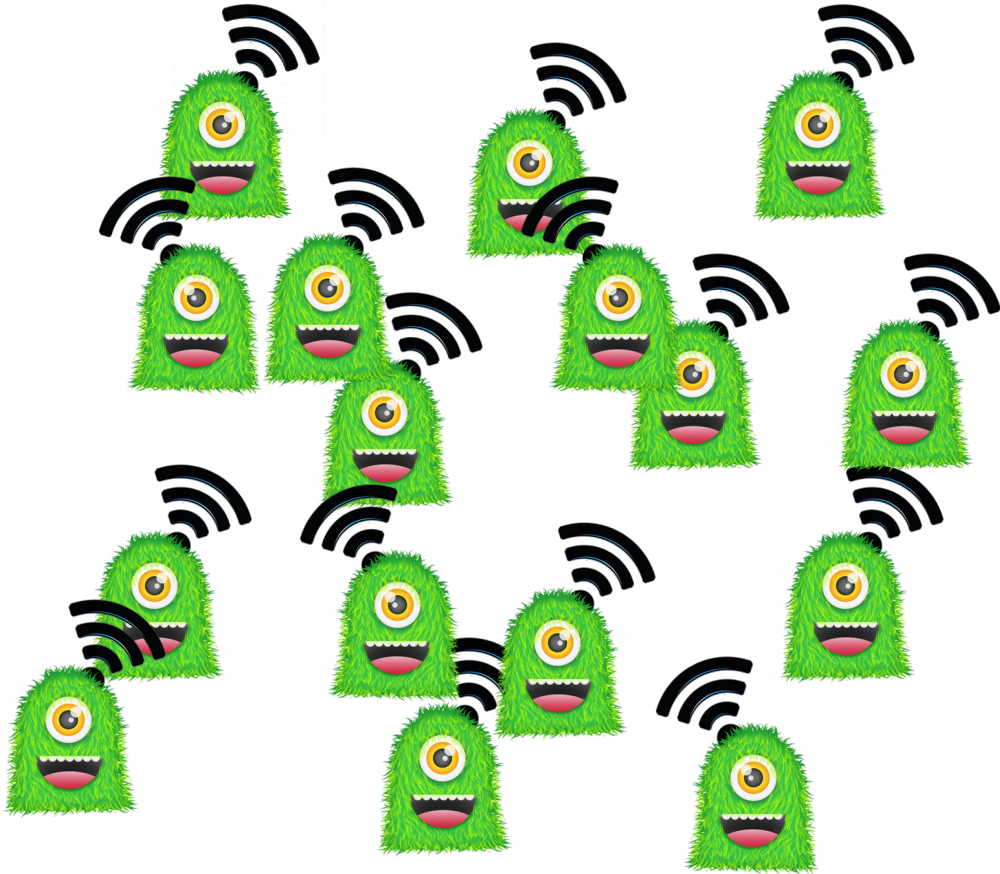
# Dumb to smart, separate to connected



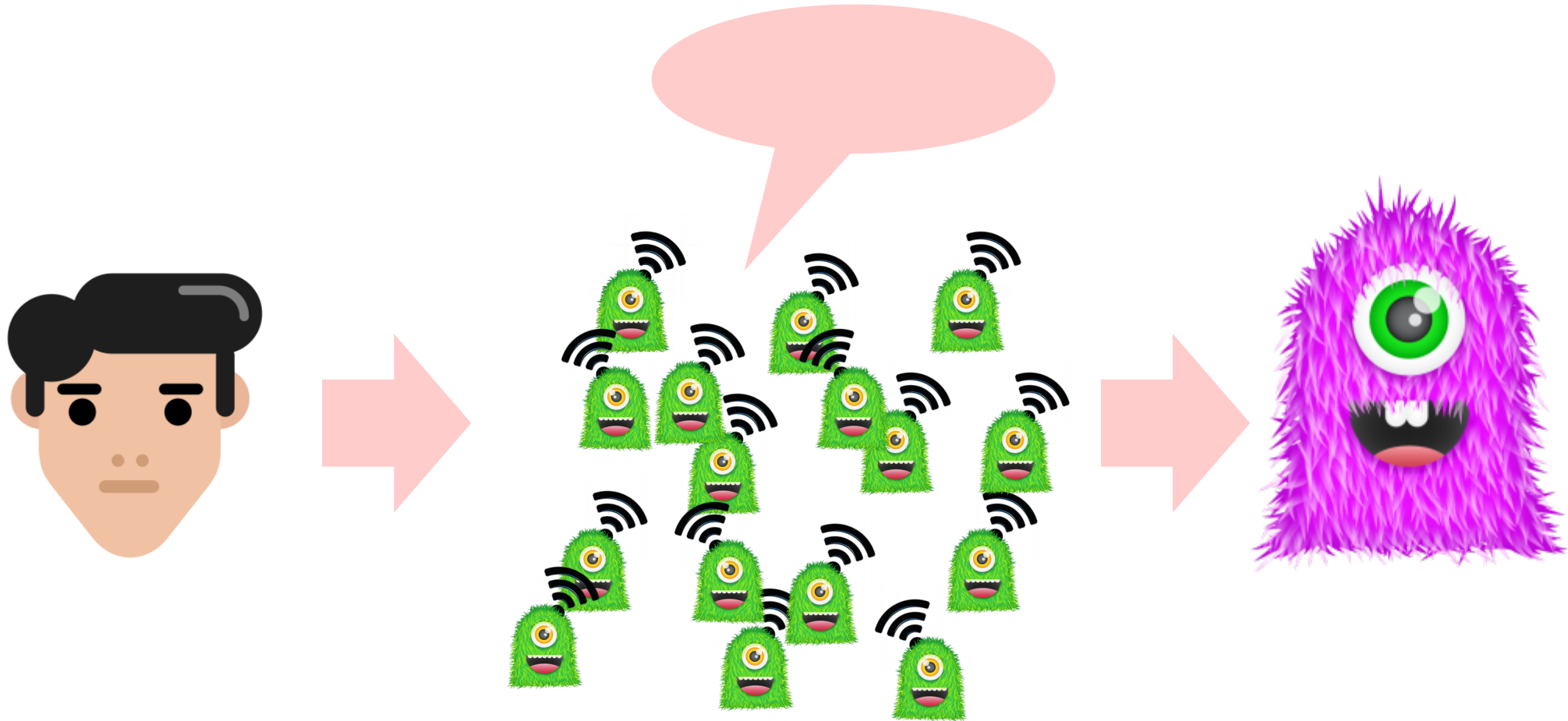
# Dumb to smart, separate to connected



# Dumb to smart, separate to connected



# Let's think about privacy



Print

Email

Facebook

Twitter

More

## 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.

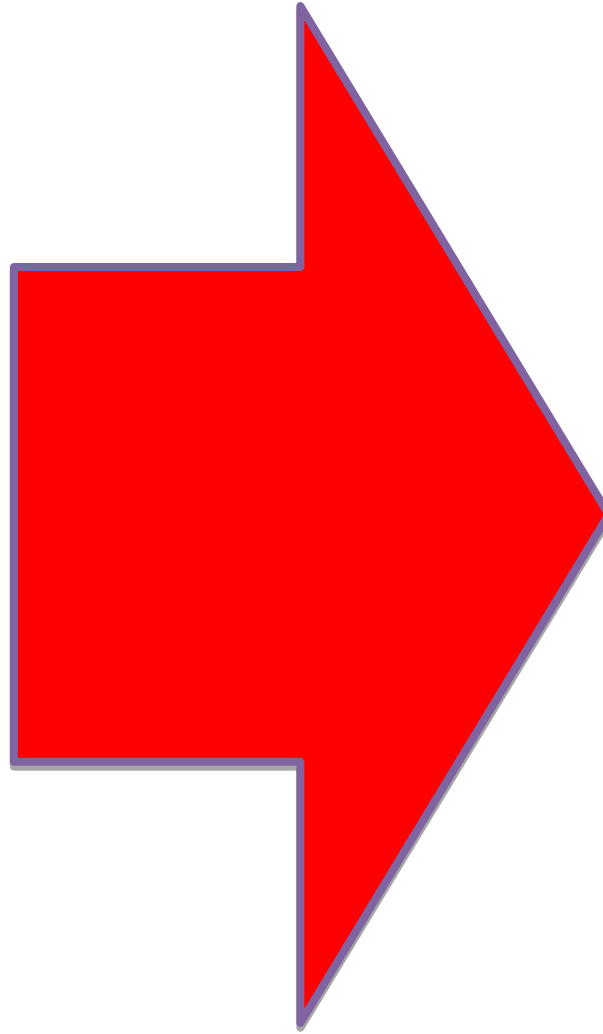
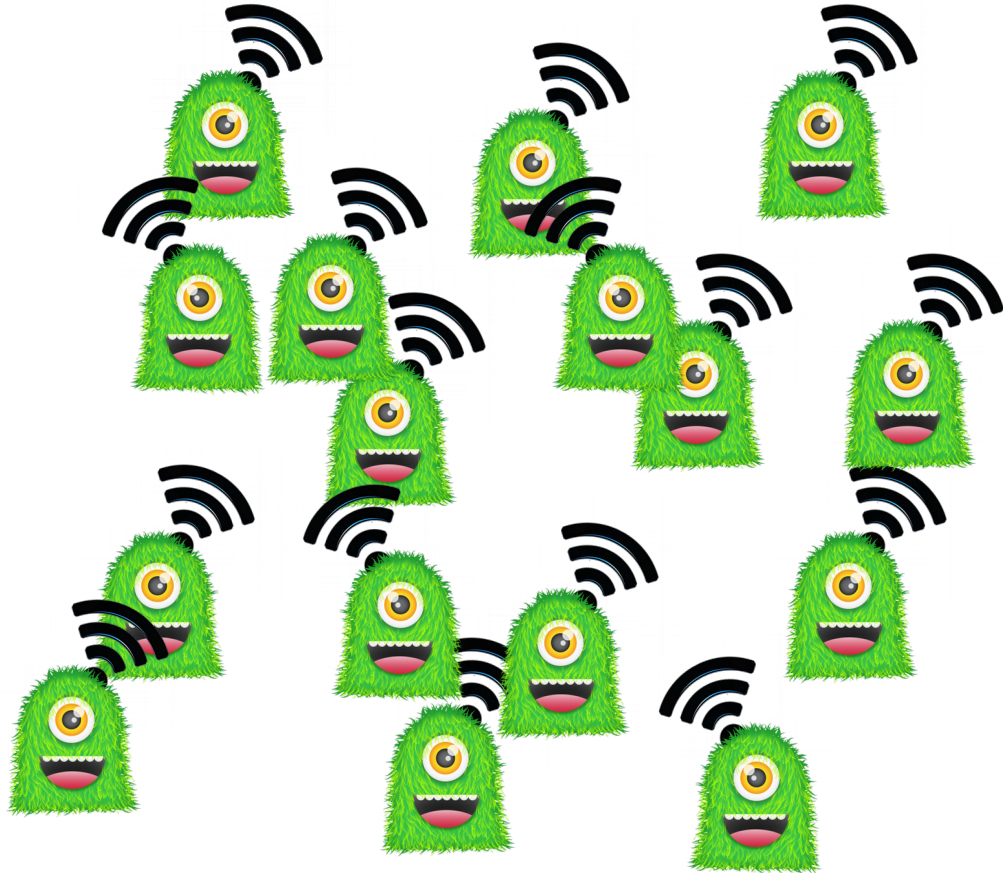
In this instalment of the [#DataLife project](#) I'm going to take a broad look at what all those requests are doing and break down some details about what I've found in the data so far.



**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)



# ...And about DDoS



# Hacked IoT Devices    Internet Services







# IoT Signals

---

SUMMARY OF RESEARCH LEARNINGS  
2019



# IoT Signals

---

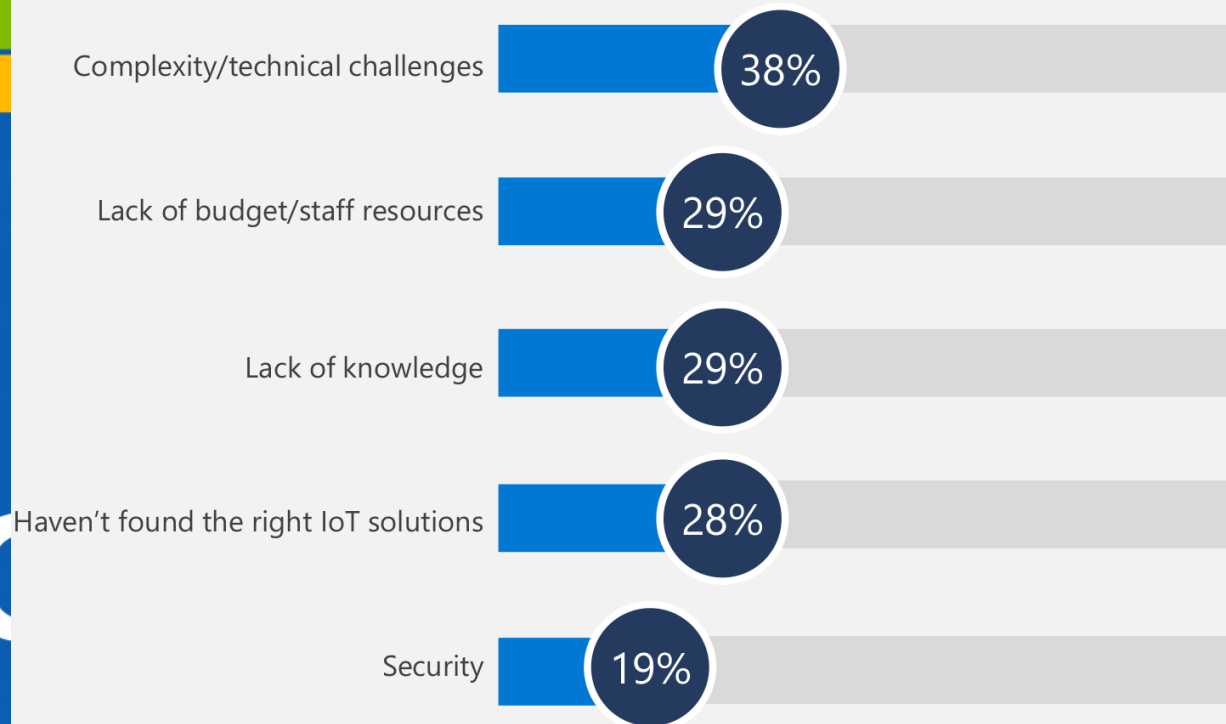
SUMMARY OF RESEARCH LEARNINGS  
2019

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



IoT

### TOP IOT CHALLENGES



## 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



NEWS

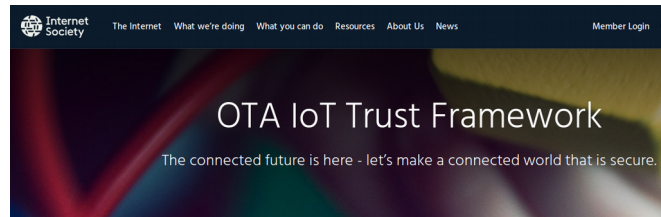
## More than two-thirds of consumers are concerned about IoT device security

By Sooraj Shah - April 27, 2017

Source: Internet of business



# Initiatives around the world, on many levels



The [Internet of Things \(IoT\)](#) offer consumers, businesses, and governments across the globe countless benefits. As is true with most emerging technology, however, there remain some significant challenges. [The Online Trust Alliance \(OTA\)](#), an Internet Society initiative, believes that through **leadership, innovation, and collaboration**, we can overcome these challenges and create a safer and more trustworthy connected world. This requires a shared responsibility including industry embracing security and privacy by design, and adopting responsible privacy practices.



## 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

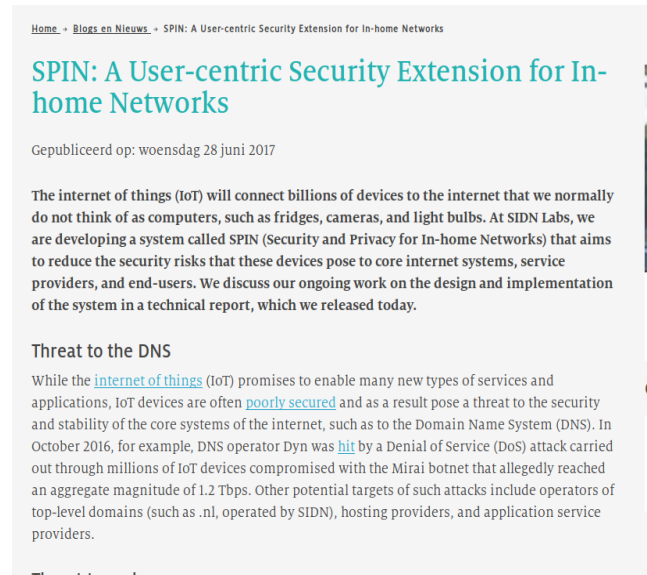
Jatinder Singh<sup>\*\*</sup>, Christopher Millard<sup>+</sup>, Chris Reed<sup>+</sup>, Jennifer Cobbe<sup>\*</sup>, Jon Crowcroft<sup>\*</sup>

<sup>\*</sup>Dept. of Computer Science & Technology (Computer Laboratory), University of Cambridge

<sup>+</sup>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.*



# Adviesraad kabinet: verbod op onveilige 'slimme' apparaten



**Joost Schellevis**

redacteur Tech · [Twitter](#) [Email](#)



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](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

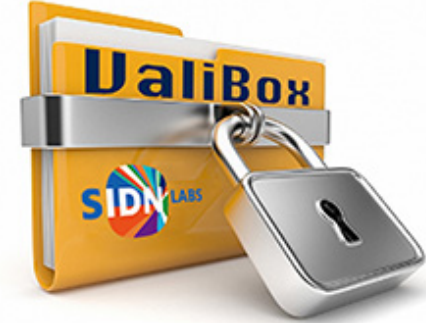
- Security and Privacy for In-home Networks
- Research and prototype of SPIN functionality:
  - Visualising network traffic
  - (Automatic) blocking of 'bad' traffic
  - Allow 'good' traffic

# The SPIN project at SIDN Labs

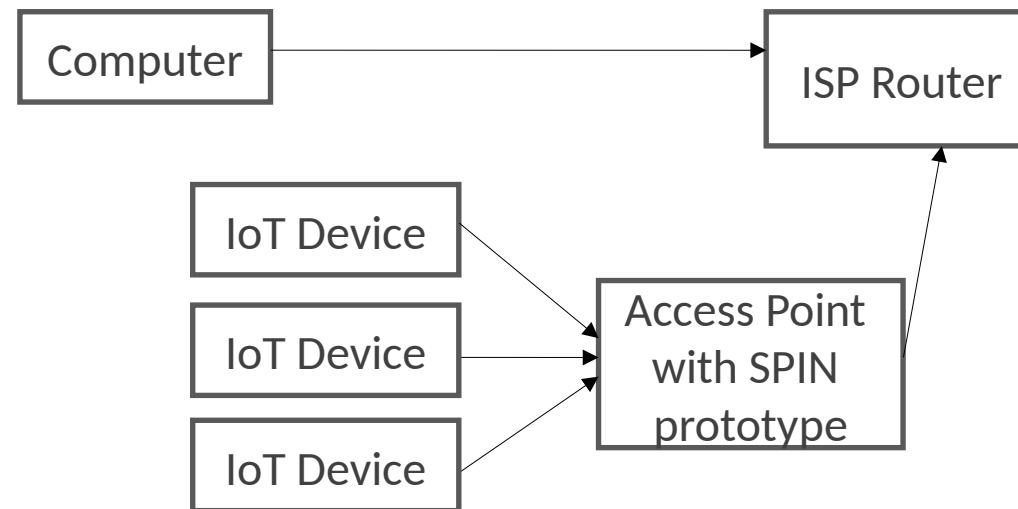
- Open source in-home router/AP software that
- Helps protect DNS operators (like SIDN!) and other service providers against IoT-powered DDoS attacks
- Helps end-users controls the security of their home networks

# Prototype built on OpenWRT

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



prototype 2, GL-Inet hardware

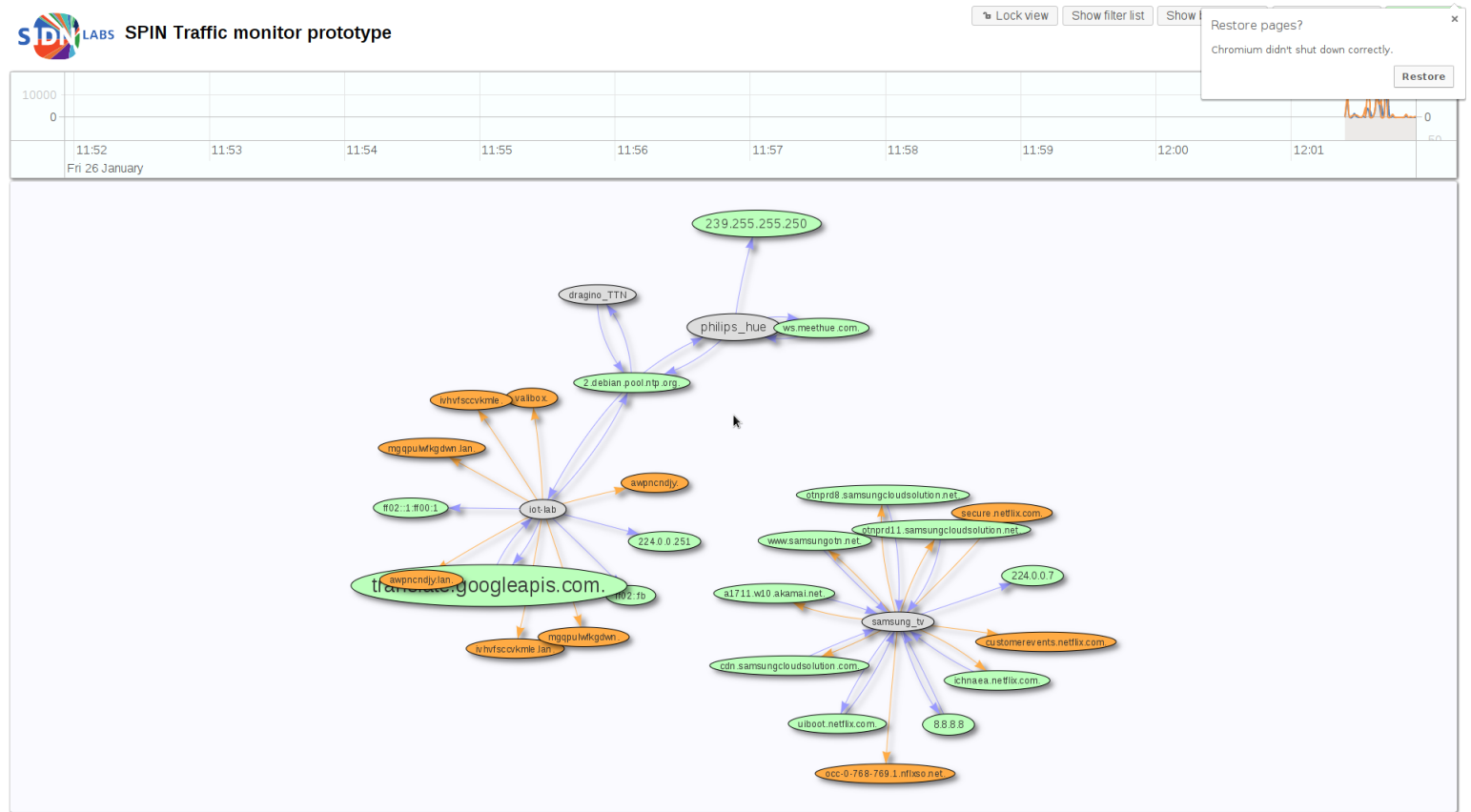


# SPIN project focus change

- 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



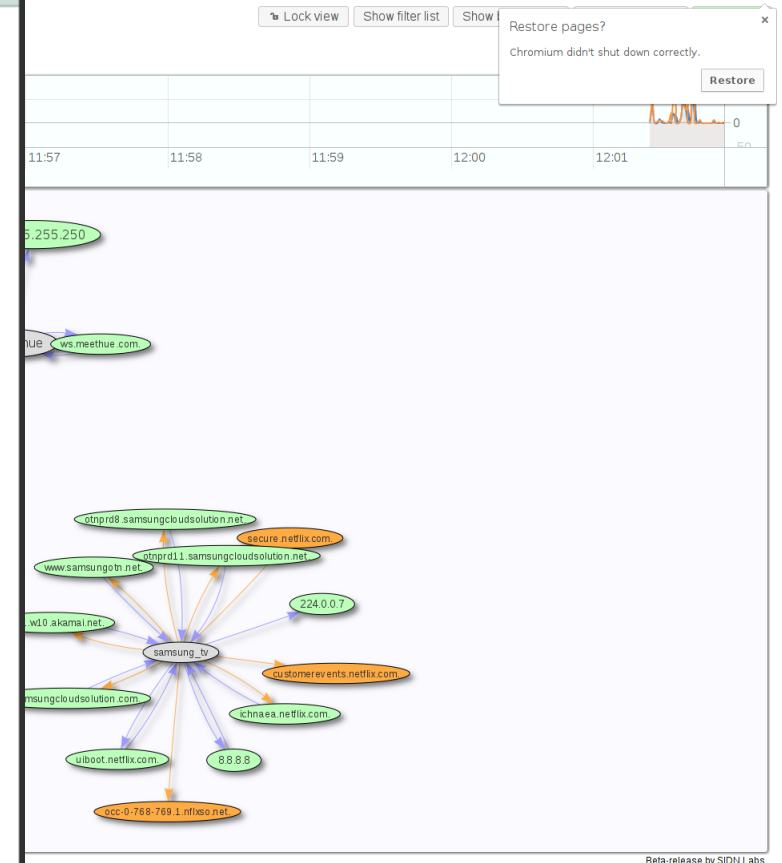
Beta-release by SIDN Labs.



# Running prototype visualizer

- 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

The screenshot shows a web browser window titled "Mozilla Firefox" with the address bar displaying "192.168.8.1/spin\_api/capture?device={". The main content area is titled "Device traffic capture" and includes a "Close window" button. Below this, there is a section for "Device information" with the following details: Name: unknown, Mac: 84:cf:bf:8f:03:12, and IP(s): 192.168.8.158, fd48:430c:f4bc::30e3:a414:1cbe:c9fa. A "Stop capture" button is located to the right of the device information. Below this, the "Capture status" is shown as "Running" in a green box, with "Bytes received: 15077", "Capture start time: 2019-11-26 14:50:13", and "Last data seen at: 2019-11-26 14:50:36". A "Download captured data" button is at the bottom of this section. The bottom part of the interface is titled "Additional functions" and contains an "Upload captured data to SIDN" button. At the very bottom, a message says "Not working? Try the [old download method](#)."



# 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 seen: 2019-09-08 22:55:47

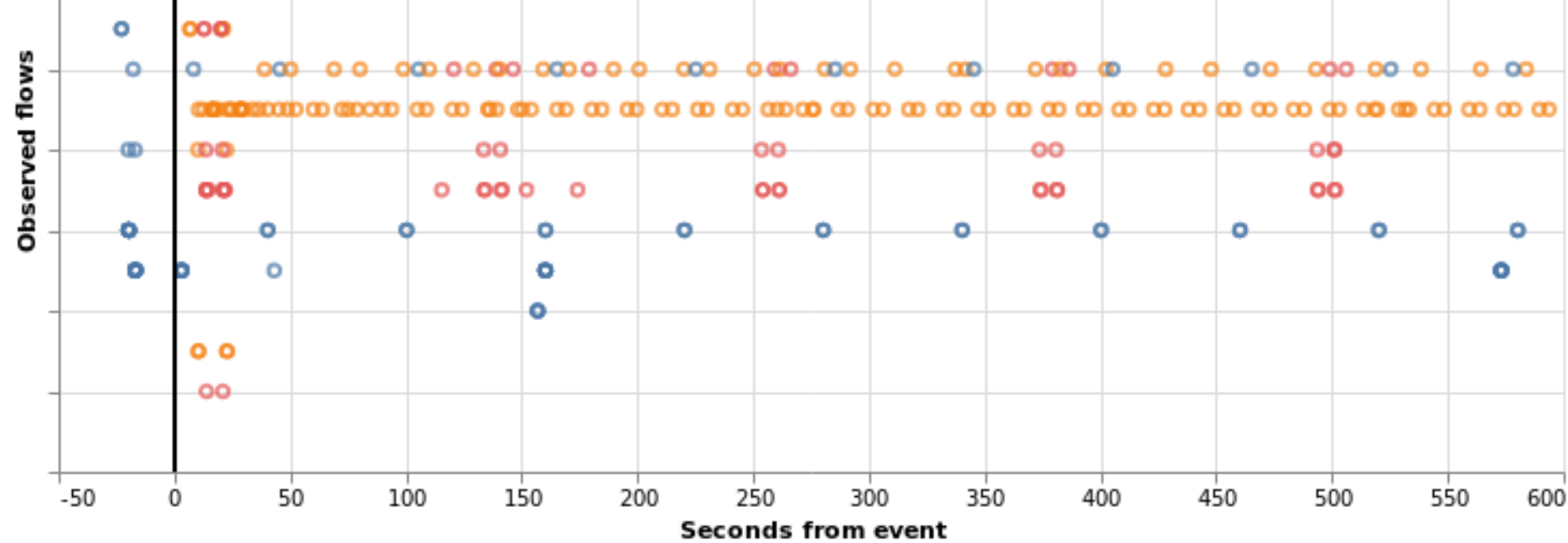
Last packet seen: 2019-09-09 22:58:47

Duration of trace: 24:02:59

~~~~~

IP Packet summary:

| source        | destination     | proto | port  | #sent_packets | #sent_bytes | #recv_packets | #recv_bytes |
|---------------|-----------------|-------|-------|---------------|-------------|---------------|-------------|
| 0.0.0.0       | 255.255.255.255 | UDP   | 67    | 2             | 700         | 0             | 0           |
| 192.168.8.1   | 192.168.8.211   | UDP   | 68    | 6             | 2088        | 4             | 1400        |
| 192.168.8.211 | 255.255.255.255 | UDP   | 6666  | 28859         | 6262403     | 0             | 0           |
| 192.168.8.211 | 52.58.217.66    | TCP   | 1883  | 2915          | 161970      | 1470          | 83267       |
| 192.168.8.211 | 18.194.70.37    | TCP   | 80    | 46            | 5356        | 30            | 3726        |
| 192.168.8.211 | 192.168.8.1     | UDP   | 53    | 2             | 148         | 2             | 228         |
| 192.168.8.211 | 224.0.0.1       | IGMP  | 0     | 1             | 46          | 0             | 0           |
| 52.29.251.104 | 192.168.8.211   | TCP   | 15257 | 1             | 54          | 1             | 54          |



Filter\_event

power\_on

power\_on

switch\_off

switch\_on

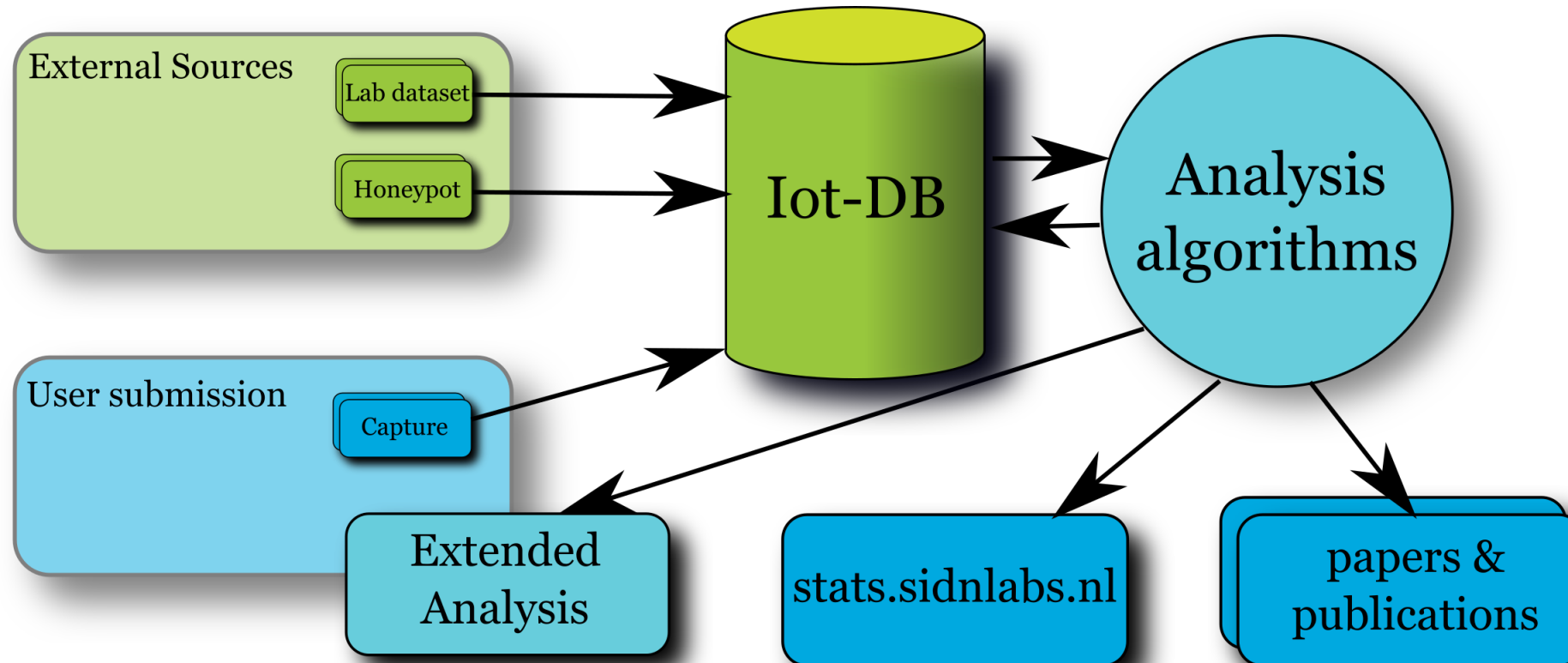
download\_stop

power\_off

turned\_off

WIP: Time-series analysis

# Potential goal: “IoT-DB”



Thank you for your attention!

Any questions?

*Follow us*



sidnlabs.nl



@SIDN @sidnlabs @twitjeb



SIDN

