### Are your devices talking behind your back?

Some thoughts on privacy and the IoT

Jelte Jansen | IDnext 2019





## So, about that 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."



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"."



IEEE published a document: *"Towards a definition of the IoT"* 

Only 86 pages!



A simpler definition:



"Stuff that was not networked before"



An even simpler definition:

"One big mess"





# Smart Devices

"A smart device is an electronic device, [snip], that can operate to some extent interactively and autonomously."

• Source: Wikipedia



# Smart Devices



"A smart device is an electronic device, [snip], that can operate to some extent interactively and autonomously."

• Source: Wikipedia



## 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





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





∬ ♀ ☆ 28.3K 17 2

Image: Hari Mari









Measures speed, duration, velocity, calory use, etc.

The beta-version has a positions counter!





#### What does i.Con do with its data? Can I use it anonymously?

Absolutely! All data will be kept anonymous but users will have the option to share their recent data with friends, or, indeed the world. You will be able to anonymously access stats that you can compare with i.Con users worldwide.





### Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny

This is the third time news has circulated about some jerk hijacking a wireless Foscam camera/baby monitor and made his virtual intrusion known by talking. Please change the default password!

**MORE LIKE THIS** 

#### 💙 🗗 🛅 🚭 🌚 🖸 🕞



🎒 🛛 Is You	ur TV Watching You? Latest Models Raise Concerns - Techlicious - Mozilla Firefox	×
T Is Your TV Watching You? Late	× +	
← → & ⊄ @	🛈 🛈 🔒 https://www.techlicio 📄 🔛 🐷 🏠 👱 🔍 Search 🍰 🦑	
	Techlicious	TECH
	HOME NEWS REVIEWS HOW-TOS DEALS	SIMPLE
	search our advice search	
HOT TOPICS: How to Fix Spam Calls	Bluetooth Problems   Browse the Web Anonymously   Complete Guide to Facebook Privacy   How t	to Block
TOP NEWS STO	ORIES	
<b>HD</b> <b>GURU</b> <b>IS Yo</b> by Gary M in TVs & V Security, E Techlic	Arson on March 20, 2012 Video Players, News, Music and Video, Health and Home, Home Safety & Blog :: 6 comments cious editors independently review products. To help support our mission, we may earn affiliate commissions from line contained on this page.	<b>AddThis</b>



### **SLIMME METERS**

### **MIJN BROERTJE GAAT** LANGER DOUCHEN IN DE HOOP **DAT DE CONTROLEURS DENKEN DAT HIJ** EEN VRIENDINNETJE HEEFT





6801 BA Arnhem www.loesje.nl

Translation:

**Smart meters** 

My little brother is going to take longer showers, hoping that the inspectors think he has a girlfriend.





0	Amazon Alexa - Mozilla Firefox 🗕 🛛	, c
오 Amazon Alexa	× +	
$\leftarrow$ $\rightarrow$ C $\textcircled{a}$	D 🔒 https://alexa.amazon.com/spa/index.html# 🛛 💀 🏠 🔍 Search 🚽 🛝 🗊 🍲 🥺 💩 🚿 🕨 📡 🙁 🚿	≡
Home	Home	
Now Playing	This website does not currently support all Amazon devices and Alexa features. For full functionality, please download the latest version of the Alexa at	× pp.
Music, Video, & Books		
Lists	Weather in Singapore AccuWeather.com	
Reminders & Alarms	Tuesday, November 7, 2017 Mostly cloudy with a couple of showers and a thunderstorm	
Contacts	Hi 30° / Lo 25° RealFeel: 33°	
Skills	Wind: ENE 1.9 km/h Precipitation: 70%	
Smart Home	Voice feedback	
Things to Try	Alexa heard: "what's the weather in singapore"	
Settings	Did Alexa do what you wanted? Yes No	
Help & Feedback	Remove card Learn more	
Not Jelte? Sign out	Less ^	•
	Make me a sandwich	
	Ok, you're a sandwich.	
	Voice feedback	
	Alexa heard: "alexa make me a sandwich"	
	Did Alexa do what you wanted? Yes No	
	Remove card Learn more	
	Less A	·



1	Amazon Alexa - Mozilla Firefox 💷 🗆 🗙
오 Amazon Alexa	× +
(←) → C (a)	🔒 https://alexa.amazon.com/spa/index.html#a 🚥 🛛 🏠 🔍 Search 🚽 🛝 🗊 🚳 🚳 🖉 🥓 🖤 🕨 🕲 » 😑
Home	Home
Now Playing	× This website does not currently support all Amazon devices and Alexa features. For full functionality, please download the latest version of the Alexa app.
Music, Video, & Books	
Lists	Weather in Singapore AccuWeather.com
Reminders & Alarms	Tuesday, November 7, 2017 Mostly cloudy with a couple of showers and a thunderstorm
Contacts	Hi 30° / Lo 25° RealFeel: 33°
Skills	Wind: ENE 1.9 km/h Precipitation: 70%
Smart Home	Voice feedback
Things to Try	Alexa heard: "what's the weather in singapore"
Settings	Did Alexa do what you wanted? Yes No
Help & Feedback	Remove card Learn more
Not Jelte? Sign out	Less ^
	Make me a sandwich
	Ok, you're a sandwich.
	Voice feedback
	Alexa heard: "alexa make me a sandwich"
	Did Alexa do what you wanted? Yes No
	Remove card Learn more
	Less ^



### What about a more meta-level?











### And what about the manufacturer itself?



### And what about the manufacturer itself?

- Even secure devices may send a lot of data home
  - Where 'home' is not your home
- Even if your device is not hacked, the manufacturer can be
- Or it can just sell your data
  - At least the GDPR should help there
    - (in some cases)



#### Orvibo data leak puts security spotlight on IoT back end

The security of devices that make up the internet of things (IoT) is a top concern for many in the industry, but leaks from an IoT database highlights the importance of backend security too

Warwick Ashford Senior analyst

Published: 02 Jul 2019 12:15





"Don't think of it as breaking up, I'm just updating my privacy settings."



### 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



#### IoT Trust by Design

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

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 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 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 nog niet klaar voor gebruik en dus nog nergens geïmnlementeerd. Om MUD-profielen te



obligations of manufacturers, importers and distributors, It has improved market surveillance instruments. One example is the possibility for required preregistration of radio equipment in categories with low compliance level

The RED was published in the OJELL on 22 May 2014, entered into force on 11 June 2014 and is applicable as of 13 June 2016. It included a one-year transitional period, which ended on 12 June 2017 (Article 48). 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. R&TTED)

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

Ma

Ge

Bl

Be

het

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 (ICAM), a committee related to Regulation (EU) No 1822011. TCAM gives its opinion on proposed implementing act under the PET. It also discusses the annihilation of the Diractive when because are structure and the annihilation of the Diractive when because are structure.

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

links

Events

Tools and Databases

Contracts and grants

Public consultations

Publications

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 <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.



# Initiative at SIDN: the SPIN project

- Security and Privacy for In-home Networks
- Research and prototype of SPIN functionality:
  - Visualising network traffic
  - (Automatic) blocking of 'bad' traffic
  - Traffic capture & analysis research
  - Platform for prototyping things as DOTS (or potenitally MUD)



# Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination
- Select device and capture (live) traffic for selected
- device
- Optional and WIP: upload
- captures for more in-depth analysis





# WIP: Initial high-over analysis

Collected data Total number o Packet types: ip: 33339 icmp: 3 arp: 2887 wauth: 4 unknown: 0	for Tuya_2019-09-	08_22-55-4	40.pcap	~~~~~		
First packet s Last packet se	een: 2019-09- en: 2019-09- 2019-09-	08 22:55:4 09 22:58:4	47 47			
TD Dackot summ	ace. 24.02.39	~~~~~~~~	~~~~~~	~~~~~		
SOURCE	destination	proto	nort	#sent nackets	#sent hytes	#recy packets
0 0 0 0	255 255 255 255	IIDP	p010 67	* bene_pacheeb 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	52.58.217.66	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





## Prototype built on OpenWRT

- Currently bundled with Valibox: http://valibox.sidnlabs.nl
- Source at https://github.com/SIDN/spin









prototype 2, GL-Inet hardware

# So what can you do?

A friend built his own home IoT network

From scratch...





Might be asking a bit much

# So what can you do?

- 'Be smart' (your devices are not!)
- Ask (around) for security status
- 'Can it run offline?'
  - Step-up to blocking internet access for (specific) devices by default
- Monitor, update, maintain
  - (yes that still asking a lot)



Your computer and phone leave your fingerprint

## And now, so do your devices

What do you want that fingerprint to be?



## Demo!

• Depending on time and local availability



# Thank you for your attention! Any questions?

Follow us



@SIDN @sidnlabs @twitjeb

in SIDN



### Are your devices talking behind your back?

Some thoughts on privacy and the IoT

Jelte Jansen | IDnext 2019



### 

### 

# Smart Devices

"A smart device is an electronic device, [snip], that can operate to some extent interactively and autonomously."

• Source: Wikipedia



# Smart Devices



"A smart device is an electronic device, [snip], that can operate to some extent interactively and autonomously."

• Source: Wikipedia





## Dumb to smart, separate to connected







## Dumb to smart, separate to connected







## Dumb to smart, separate to connected



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





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

## Let's think about privacy



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





Measures speed, duration, velocity, calory use, etc.

The beta-version has a positions counter!





#### What does i.Con do with its data? Can I use it anonymously?

Absolutely! All data will be kept anonymous but users will have the option to share their recent data with friends, or, indeed the world. You will be able to anonymously access stats that you can compare with i.Con users worldwide.



## IoT: Cool or Chilling?





## IoT: Cool or Chilling?



### IoT: Cool or Chilling?

**Translation:** 

**Smart meters** 

My little brother is going to take longer showers, hoping that the inspectors think he has a girlfriend.

### **SLIMME METERS**

MIJN BROERTJE GAAT LANGER DOUCHEN IN DE HOOP DAT DE CONTROLEURS DENKEN DAT HIJ EEN VRIENDINNETJE HEEFT

Postbus 1045 6801 BA Arnhem www.loesje.nl










What about a more meta-level?





•			SPI	N Traffic monitor protot	ype - Mozilla Firefox						
오 Amazon Alexa 🛛 🗙	SPIN Traffic monitor proto ×	< +							1		
← → ♂ ŵ	🕈 🏠 🕕 Ūturris/spin_graph/graph.html				🚥 🗵 🔂 🔍 Search				👱 III\ 🖸 🏟 🔩 💷 🥓 🕷 🔭		
	Traffic monitor pro	ototype				Unlock view	Show ignore list	Show blocked list	Show allowed list		
6000000 4000000 2000000											
20:11 Mon 16 Sentem	20:12	20:13	20:14	20:15	20:16	20:17	20:18	20:19	20:20		
com. otnprd9.sa	ingcloudedn com i.ytimg.c	idsolution.	net.	www.ecdint	diagn	ostics.meet	hue.com				
		fds.dc1.philips	s.com.								
(ads sar	www.samsung	otn.net.			Device A	cs.dcs.dc	21.philips.co	om.			
-	illounguus				1 total						
ution of	om			Beta-rele							







#### And what about the manufacturer itself?

- Even secure devices may send a lot of data home
  - Where 'home' is not your home
- Even if your device is not hacked, the manufacturer can be
- Or it can just sell your data
  - At least the GDPR should help there
    - (in some cases)



#### Orvibo data leak puts security spotlight on IoT back end

The security of devices that make up the internet of things (IoT) is a top concern for many in the industry, but leaks from an IoT database highlights the importance of ba end security too

Warwick Ashford Senior analyst Published: 02 Jul 2019 12:15





### 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?





### 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?



## We need to do it all



#### Initiatives around the world, on many levels



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

#### Initiative at SIDN: the SPIN project

- Security and Privacy for In-home Networks
- Research and prototype of SPIN functionality:
  - Visualising network traffic
  - (Automatic) blocking of 'bad' traffic
  - Traffic capture & analysis research
  - Platform for prototyping things as DOTS (or potenitally MUD)

# - research and developt IoT home network behaviour and security.

S DN LABS

Initial analysis: basic aggregation of traffic totals to destination and ports.

For example: this devices uses MQTT (port 1883)

Time-series analysis, very early work: can we tell from traffic that an event happened (such as turning on the light)

## So what can you do?

A friend built his own home IoT network

From scratch...



Might be asking a bit much



## So what can you do?

- 'Be smart' (your devices are not!)
- Ask (around) for security status
- 'Can it run offline?'
- Step-up to blocking internet access for (specific) devices by default
- Monitor, update, maintain
- (yes that still asking a lot)



Your computer and phone leave your fingerprint

And now, so do your devices

What do you want that fingerprint to be?



#### Demo!

• Depending on time and local availability



