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
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".”
• **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)
The “S” in IoT stands for SECURITY

Attributed to @tkadlec
So, about that IoT

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

By Josh Fruhlinger, C90 | Oct 12, 2016 4:00 AM PT
So, about that IoT

NEW MIRAI VARIANT CARRIES OUT 54-HOUR DDoS ATTACKS

by Tom Spring
March 30, 2017, 2:50 pm
What should we do?

• Better practices for manufacturers?
• Free **secure** software stacks?
• International policy, regulation, certification?
• 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, certification?
• 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, certification?
- 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
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
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
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.
The “S” in IoT stands for **SECURITY**

Attributed to @tkadlec
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, certification?
- 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, certification?
• 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, certification?
• 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 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 control the security of their home networks
DEMO TIME!

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

.nl sidnlabs.nl
@SIDN @sidnlabs @twitjeb
SIDN