SPIN:
Security and Privacy
in the Internet of Things

Marco Davids

IETF 99
NMRG (IRTF)
What *is* the IoT?

- Quite a few definitions of IoT
  - I like the approach of RFC7452

- We may not agree on a definition…

- But we know there will be plenty of ‘IoT’!

*Source: Gartner*
What **is** the IoT?

Actually it is (also):

- “One big mess”
- A security nightmare
The result...

So, what to do about this?

• No silver bullet
• We need to do it all
• But in our project we focus on:
  - *Empower users*
The SPIN project

• ‘Security and Privacy for In-home Networks’

• Research the user-empowerment part:
  - Detect anomalies in the home network
  - Automatically block suspicious traffic to/from IoT devices
  - Inform the end user about the system’s findings and actions
  - Allow the user to configure security and privacy parameters
Motivation

• Protect infrastructure operators (such as SIDN)
• Give users more control over their in-home IoT
• Preserve trust in the internet
User centric approach

• Allow users to easily deploy it
• Protect users’ privacy by keeping the intelligence within the home
• Allows users to configure the system with their security preferences

Also:
• Embrace collaborative ‘security by design’ security community
The SPIN concept

- **SPIN controller**
  - Visualize traffic
  - Monitor devices
  - Control traffic

- Processing is done locally
  - User in control
  - But largely automated

Inhoudsopgave

- The SPIN concept
  - SPIN controller
    - Visualize traffic
    - Monitor devices
    - Control traffic
  - Processing is done locally
    - User in control
    - But largely automated

**Diagram**

- **Device Scanner**
  - Topology Database
  - Traffic Capturer
  - Traffic Filter
  - Filtering DP
  - Policy Database
  - Applications (e.g., notifications, settings)
  - SPIN System

- **Traffic Filter**
  - Filtering decision
  - topology changes (SPIN protocol)

- **Threat Detector**
  - Event
  - Notifications
  - Manual override

- **Packet Forwarder**
  - Control
  - Packet forwarding path

- **Incoming traffic**
  - Outgoing traffic

- **Community of security researchers**
  - Generic device info

- **PCAP**
  - Import
  - Export

- **Topology Database**
  - Update
  - Topology changes

- **Policy Database**
  - Import
  - Import
  - Update
  - Filter decision

- **繁荣**
  - Topology changes
  - Notifications
  - Settings

- **Traffic Capturer**
  - Device info
  - Generic info

- **Other SPIN System**
  - SPIN policy community
  - Event
  - Notifications

- **Applications**
  - (e.g., notifications, settings)

- **Traffic Filter**
  - Filtering decision
  - topology changes (SPIN protocol)

- **Traffic Capturer**
  - Device info
  - Generic info

- **Packet Forwarder**
  - Control
  - Packet forwarding path
Prototype built on OpenWRT

• Currently bundled with our open source ‘Valibox’ software
• Working on a separate OpenWRT package feed
• Focus on IoT devices with ‘predictable behavior’

*Prototype built on OpenWRT*

*Currently bundled with our open source ‘Valibox’ software*

*Working on a separate OpenWRT package feed*

*Focus on IoT devices with ‘predictable behavior’*

*Prototype 2, GL-Inet hardware*
Ga naar de tab 'Start'.
Hier vind je 2 knopjes zoals onderstaande afbeelding.
D.m.v. deze knopjes kun je eenvoudig tussen tekstniveaus wisselen.
Current status

- Running prototype on our Valibox (OpenWRT) platform
  - Focus on privacy
  - ‘Vertical slice’ of the concept (modular deployment)
  - Visualize basic traffic (with DNS names, if known)
  - Block traffic to/from devices or external points
- Incremental updates deployed as features are implemented
- Software (free, go get it):
  - Open source: https://github.com/SIDN/spin
  - GL-inet images at: https://valibox.sidnlabs.nl/
Vision

• Get it into deployed devices
  • Bullguard Dojo seems similar, but is proprietary
  • So is the Bitdefender Box
  • NIC.CZ Turris router comes closer

• Become an open standard in/for home routers
  • We have it running on the Turris

• Work on interoperable ‘IoT security/privacy standards’
  • Protocols
  • Data formats (T2TRG WG?)
  • API’s
Future Work

• Refinements
• Research question: how to protect the protector
• (Collaborate on) a platform for sharing IoT device information
  - In a uniform, standardized way
  - Repositories for known bad devices/versions
  - Trusted traffic profiles
    - “My TV should stream the news and Netflix, but do nothing else”
    - Perhaps something like draft-ietf-opsawg-mud-08?
• Interested in collaboration? Come talk!
Questions/ideas/suggestions?

Tech-paper about this on:


Short URL:

http://tinyurl.com/SIDN-IoT