Managing unmanaged home devices

Reducing IoT security risks with open source CPE software

SIDN Your world. Our domain.

Introduction

This white paper explores the security and privacy issues involved with the evolving Internet of Things (IoT), which is expected to comprise a large portion of unmanaged, insecure home devices. The solution presented here is SPIN, short for Security and Privacy for In-home Networks. It is open-source software that brings IoT security to the residential gateway as new added-value functionality for the end user, and allows access providers to bring IoT devices and traffic flows at their customers' premises under direct central management. SPIN mitigates security risks related to the IoT network, while keeping privacy-sensitive data in the user domain.

Contents

1 Management summary

The evolving Internet of Things (IoT) will soon comprise many tens of billions of networked devices, of which a large portion will be unmanaged machine-to-machine (M2M) home devices.
It is expected that a large number of these home devices either will never be updated at all, or will stop receiving software updates long before they are disconnected from the network. This poses serious security and privacy risks to both access providers and end users.

Outgoing massive Distributed Denial-of-Service (DDoS) attacks and blacklisted IP address ranges may threaten the integrity of the access network and the business continuity of the provider, while users may be confronted with all sorts of privacy infringements, malware, theft of identity, information, credentials and assets, and other digital crimes.
Most of the burden of preventing and dealing with these threats is expected to fall on the access provider, who is also the first contact for uninformed and technically incapable users

SPIN is open-source software that allows access providers to bring IoT devices and traffic flows at their customers' premises under direct central management. It provides powerful yet easy-to-use firewall functionality and insight based on a view that is common to both parties, without invading customers' privacy.
SPIN brings IoT security to the residential gateway as new added-value functionality, serving both as an attractive goodie and an enabler to the end user.
Access providers can integrate SPIN functionality into their existing security management infrastructure and self-help portals, allowing for automated interaction with end users on security issues and helping users to solve problems on their own.
CPE manufacturers can use the native interfaces of their operating systems to easily integrate the software into their gateways.
SPIN adheres strongly to international, open standards for IoT security and privacy, so as to ensure the highest level of interoperability and regulatory compliance.

SPIN is produced by the Dutch domain name registry SIDN, a not-for-profit organization and thought leader with a proven track record in Internet security. Its research branch SIDN Labs will continue to develop SPIN as a research platform for IoT security.

SPIN is currently available as a working prototype. It was demonstrated as part of the TrustBox home router at the last Consumer Electronics Show (CES) in Las Vegas, where the device won the Best of Innovation Award in the Cybersecurity & Personal Privacy category. It is also available as an integral part of the build images for Valibox, which is another security innovation created by SIDN Labs. Other parties using SPIN in their projects are CZ.NIC (the Czech registry for the .cz zone), CIRA (the Canadian registry for the .ca zone) and DistributIT (a Dutch startup company).

SPIN is currently at the stage of a first viable product, meaning that the prototype is now fully functional and ready for initial deployment in a pilot project.

2 A sea of unmanaged devices

The evolving Internet of Things (IoT) already comprises tens of billions of devices. According to Cisco's latest Visual Networking Index [1] there will be 28.5 billion networked devices by 2022, up from 18 billion in 2017. More than half this number – 14.6 billion – will be machine-to-machine (M2M) devices, i.e. devices communicating only with other devices. And nearly half of these M2M devices will be in 'connected home' applications such as home automation, home security and video surveillance, connected white goods and tracking systems. Moreover, the ease with which consumers buy all sorts of cheap devices directly from online marketplaces all over the world and connect these to their home networks is staggering as well as worrying.

Low cost being the main driver in this market, and a lack of security awareness being the norm with consumers, we expect a large number of these home devices either to be never updated at all, or for their software updates to stop long before the device is disconnected from the network. The cheapest devices will not even have the memory required to perform a software update and are simply expected to be thrown away once their useful life is over.

All these unmanaged devices connected to residential gateways and other CPEs pose an increasing risk to parties at both ends. Obsolescent devices provide an attack surface at the end user's premises. Once hacked, these devices then serve as springboards to infect other devices and upstream systems, or become part of botnets collecting valuable data, sending spam, and launching Distributed Denial-of-Service (DDoS) attacks.

3 Impact

With ever-increasing numbers of end users behind (CG)NAT gateways, a bad reputation or the blacklisting of a (massively) shared IP address is something access providers can ill afford, as it immediately impacts a substantial number of customers. At the same time, affected home devices pose a direct thread to the security and privacy of end users, who will be confronted with extortion schemes, identity theft and other digital crimes. Naturally, they will look first to their access providers for protection against such harms.

The challenge we are facing:

- end users are connecting huge numbers of insecure devices to their residential gateways;
- despite legislation currently being developed, neither end users nor manufacturers are expected to keep the security of these home devices up to par;
- this sea of unmanaged devices is threatening the integrity of the access network, the continuity of the service, and the security and privacy of end users;
- helpdesk agents will receive an increasing number of questions and complaints on security- and privacy-related issues, while having no overview of the devices connected to the customer's home network; and
- due to the direct import by consumers of cheap devices from online marketplaces all over the world, legislation could only ever partly address the issue of insecure devices.

Direct and indirect threats to end users:

- ransomware,
- identity theft,
- loss of valuable information,
- theft of passwords and other credentials,
- loss of money and other assets,
- loss of resources, e.g. by rogue cryptomining software,
- publication of sensitive and private information, e.g. through leakware,
- loss of control over their home networks, e.g. by botnets, and
- infection spreading to other home networks, and maybe even to company networks and systems.

4 Security risks

Access providers clearly need new ways to limit the security risks of this abundance of unmanaged home devices. What makes this hard is the sheer volume of these appliances and their huge heterogeneity. In addition, legislation to protect customers' privacy – for instance by prohibiting deep inspection of their traffic – makes it harder to bring these devices and their network traffic under direct central management.

An additional complication lies in the multi-layered nature of IoT infrastructures: some appliances connect directly to the CPE, others provide Internet connectivity to even more devices by setting up another Wi-Fi network, and still others provide gateway functionality to their downstream devices using an IoT-specific or even proprietary networking technology. Even the very existence of some devices may be unknown to the user – an example might be a solar panel management system that an installer has connected to an open router port, for instance. All these various, cascaded layers have their own, specific security needs.

5 A shared choke point

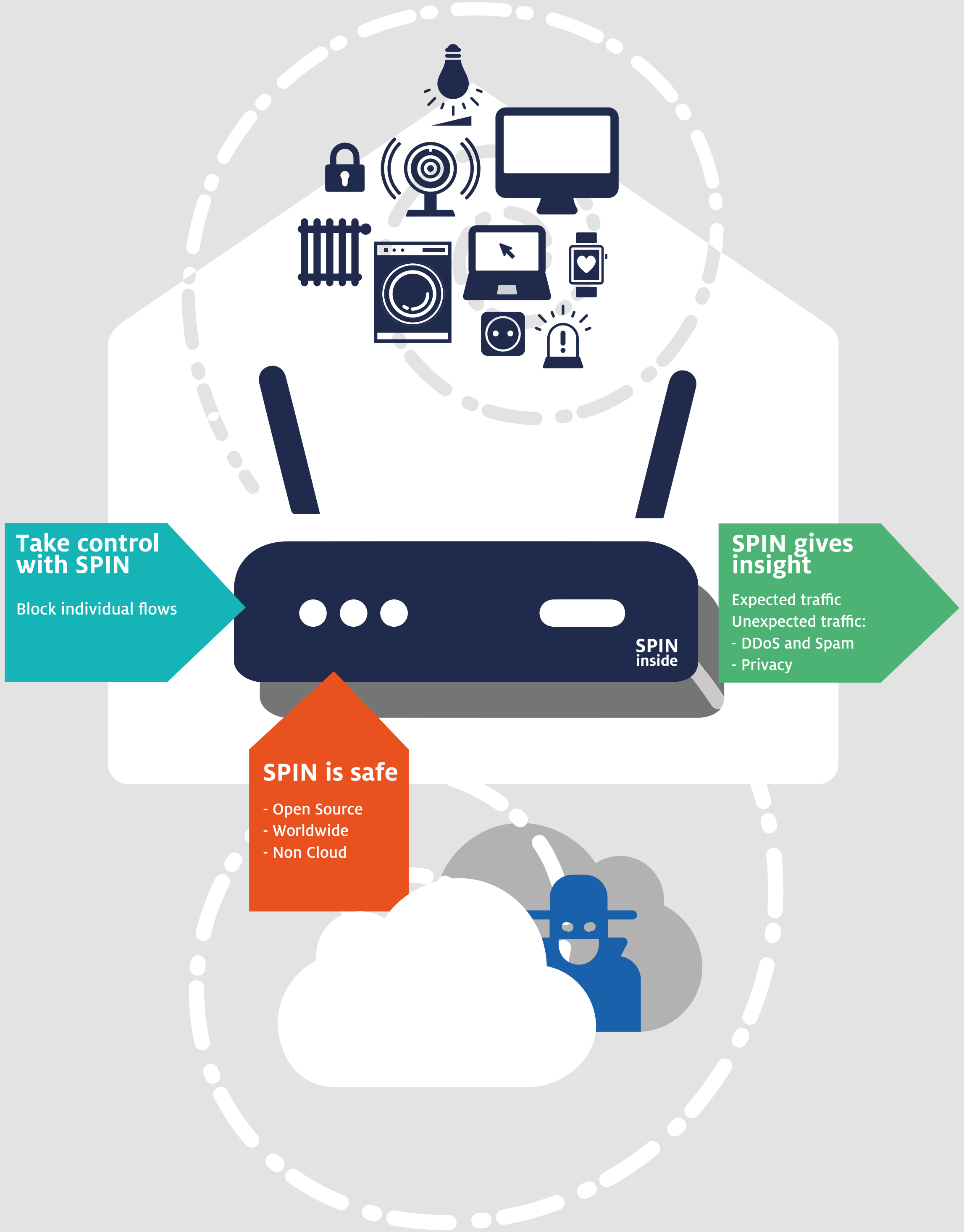
As a choke point situated between access provider and end user, the residential gateway turns out to be the best location for protecting the security and privacy of the user while providing insight into all network traffic. Since the gateway is accessible to both parties, it allows provider and user to share a common view of connected devices and their traffic flows. That way, the one can always see or undo actions (e.g. blocking of a specific device or flow) performed by the other. Of course, exactly what can be seen and done by the provider is limited by the legal contract with the user and by local legislation, to the extent that the end user might even have the option to completely block the provider from accessing 'his' CPE.

6 Proposition

The solution we offer here is open-source software called SPIN: Security and Privacy for In-home Networks. It allows CPE manufacturers and access providers to add firewall-like technology to the residential gateway, which is generally the only presence providers have at their customers' premises. This keeps privacy-sensitive data in the user domain, while giving both parties insight into the traffic running through the gateway.

Access providers can integrate SPIN functionality into their existing security management infrastructure and self-help portals, allowing automated interaction with end users on security issues and helping users to solve problems on their own. In more difficult cases, helpdesk agents can work with users to resolve issues caused by connected appliances, while sharing a common view of devices and traffic flows.

On a more generic level, access providers can use SPIN to collect statistics on the use of home devices and the state of security at their customers. End users can keep an eye on the traffic behavior of their appliances through an easy-to-use interface and block any unwanted flows, keeping them in control at their end. Meanwhile, the technology helps end users improve their knowledge of privacy- and security-related issues and better understand security measures.



Take control with SPIN

Block individual flows

SPIN gives insight

Expected traffic
Unexpected traffic:
- DDoS and Spam
- Privacy

SPIN is safe

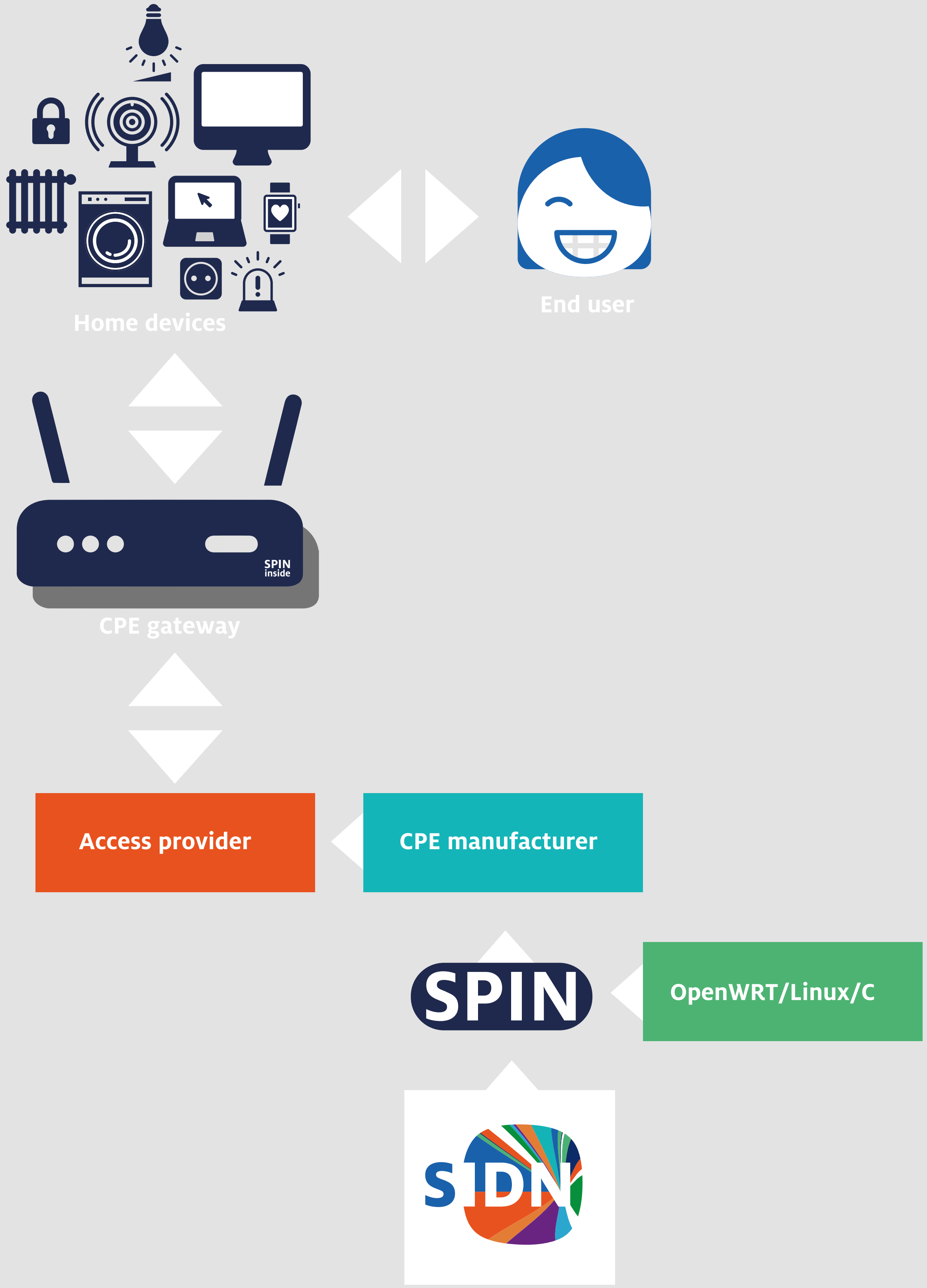
- Open Source
- Worldwide
- Non Cloud

7 SPIN: an overview

SPIN is open-source software for CPEs running on Linux, so for instance it can be part of a software image based on OpenWrt. As part of the gateway it keeps an eye on traffic flows between devices on the local network and the Internet. Flows to specific nodes can be blocked directly by the user via the CPE's GUI, or remotely by the access provider through an API that can be added to the software.

SPIN is written in the C programming language for maximum performance and portability. This also allows the software to be incorporated into CPE platforms based on systems other than Linux.
The software is available in its original (source) form from SIDN's GitHub repository, but also for instance as an integral part of a ready-for-use Valibox image for the Raspberry Pi.

Other principles for the development of SPIN are adherence to open standards, providing insight and control to end user. And managing further development and the push for adoption in cooperation with other stakeholders, technically as well as strategically.



8 SPIN advantages

Until now, it's been impossible for end users to see what data is flowing to and from the devices connected to their home networks. SPIN changes that by providing end users with a picture of the internet traffic associated with their connected devices. So they're able to manage their devices and get notifications whenever anything unusual shows up.

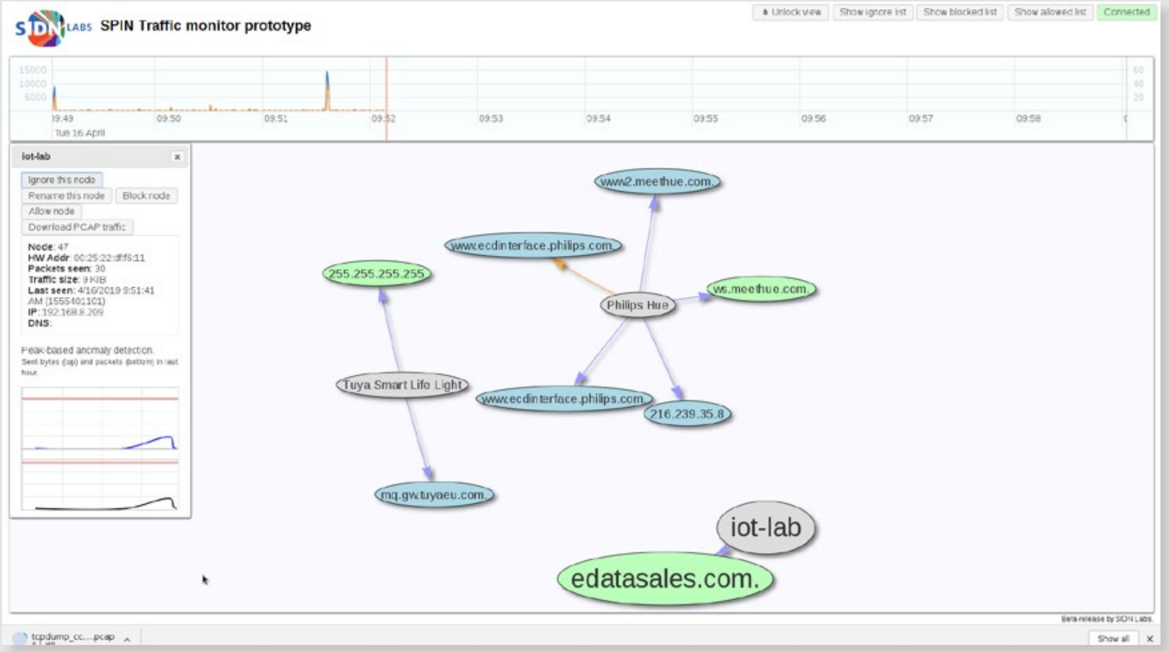
SPIN has several advantages over existing firewalls and traffic analyzers:

- it is tailored to the home and SOHO environment;
- a web-based, interactive GUI is provided as an example and as inspiration to build intuitive user interfaces for access providers and end users;
- it gives end users insight into security- and privacy-related matters on an individual level;
- an API can be added to the software to give access providers the same view and functionality that is available to users;
- the use of OpenWrt's native ubus and UCI interfaces allows CPE manufacturers to easily integrate the software into their gateways; and
- for web traffic, the domain names of the original destinations are bundled and shown as a single logical node, instead of the individual hostnames of the servers.

9 The Traffic Monitor

The current prototype of the software comes with a graphical (web-based) interface that serves as an example of how SPIN's functionality can be made available to the end user. The Traffic Monitor (see screenshot) shows all flows in the last ten minutes as a dynamic graph of endpoints and connections. Internal devices are marked in grey, recent connections in green, and older connections in blue. Clicking on a node allows the user to drill down for more information. The pop-up information block allows the user to ignore, rename, block, or whitelist this node.

Another option is to download a traffic dump in PCAP format, ready for advanced analysis using tools like tcpdump and Wireshark. One of the ideas SIDN is currently working on is to provide a web portal where users can upload these dump files and have them further analyzed.



Node: 47
HW Addr: 00:25:22:df:f6:11
Packets seen: 30
Traffic size: 9 KiB
Last seen: 4/16/2019 9:51:41 AM (1555401101)
IP: 192.168.8.209
DNS:

Peak-based anomaly detection.
Sent bytes (top) and packets (bottom) in last hour.

Figure 1: Screenshot traffic monitor

10 Track record

While the first GUI provides a native interface to SPIN's functionality, the second demonstrates the use of the web API, which access providers will use to connect remotely to their customers' SPIN agents. In addition to the functionality just described. This allows SPIN to be closely integrated into the provider's security management infrastructure and facilitates automated, targeted interaction with end users on specific security issues.

CPE manufacturers and system integrators who want to incorporate SPIN into their products and management solutions can use the built-in MQTT mechanism to receive traffic information from the SPIN agents.

You can find a more detailed list of SPIN's features and capabilities in the appendix.

SPIN is currently available as a working prototype. It was demonstrated as part of the TrustBox home router [2] at the last Consumer Electronics Show (CES) in Las Vegas, where the device won the Best of Innovation Award in the Cybersecurity & Personal Privacy category. It is also available as an integral part of Valibox [3], an OpenWrt software image including DNSSEC validation, which is another security innovation created by SIDN Labs.

Other parties using SPIN in their projects are CZ.NIC (the Czech registry for the .cz zone), CIRA (the Canadian registry for the .ca zone) and DistributIT. The latter is a Dutch startup company that has incorporated SPIN into Holmes [4], a security- and privacy-focused gateway that extends its features to a mobile app.

CIRA has worked SPIN into a residential gateway named the Secure Home Gateway [5]. The system is based on the Turris Omnia [6], a high-end router developed by the Czech registry CZ.NIC as an open-source hardware project. The Turris Omnia itself also includes SPIN in its software.

The Secure Home Gateway project was initiated by CIRA to protect consumers and the Internet from IoT-based cyber attacks, a mission very similar to what drove SIDN to develop the SPIN software. The gateway was brought in by CIRA in the 'Canadian Multistakeholder Process – Enhancing IoT Security' [7], in which various partners work together to secure the evolving IoT. This collaboration model also serves as a blueprint for the soon-to-be-launched Dutch 'IoT Security & Privacy multi-stakeholder WG'.

11 Conclusion

SPIN allows access providers to bring IoT devices and traffic flows at their customers' premises under direct central management. It provides powerful yet easy-to-use firewall functionality and insight to both parties, without invading customers' privacy.

SPIN adheres strongly to international, open standards for IoT security and privacy. It is produced by the Dutch domain name registry SIDN, a not-for-profit organization and thought leader with a proven track record in Internet security.

The SPIN software is available as open source and is easy for access providers and CPE manufacturers to integrate into their products and services. SIDN Labs will continue to develop SPIN as a research platform for IoT security.

The latest Valibox image is the best way to get a quick impression of the SPIN functionality described above. Binary images are readily available for download for various Single-Board Computers, including the Raspberry Pi.

12 About SIDN

SIDN is a not-for-profit organization responsible for the Dutch top-level domain. As the registry and operator of the .nl zone, SIDN maintains the critical DNS infrastructure service for 5.8 million domain names, processing 1.3 billion DNS queries per day.

The higher-level mission of SIDN is to connect people and organizations through a safe and resilient Internet. This has made SIDN and its research branch SIDN Labs a worldwide pioneer and thought leader in the development and standardization of Internet infrastructure security technology.

SIDN started the development of SPIN after the 2016 Mirai DDoS attacks, which were initiated by a botnet consisting of infected Linux-based IP cameras and home routers.

13 We all win

End users

- insight on an individual level: where are home devices connecting to?
- control: directly block destinations individually or based on profiles
- privacy: in-network collection and processing of data (no cloud)
- easy-to-understand insight into privacy- and security-related issues
- more advanced analysis possible using a traffic dump

Access providers

- all IoT devices under central security management
- close integration into their existing security management infrastructure
- automated interaction with end users on security issues
- helpdesk agents and end users share a common view
- additional functionality for analysis, interaction and intervention
- statistics on the use of home devices and the state of residential security
- better understanding of security measures at end users

SPIN

- powerful firewall functionality and insight at the home choke point
- a single, shared view of connected devices and traffic flows
- strong adherence to international, open standards
- open source software
- produced by SIDN, a worldwide pioneer and thought leader with a proven track record in Internet security

CPE manufacturers

- IoT security as a new value-add feature for their CPEs
- easy integration into their existing OpenWrt/Linux systems
- integration using OpenWrt's native interface (ubus and UCI)
- easy development of custom security applications on top of SPIN

SIDN

- a more secure Internet
- impact: reaching as many consumers as possible

Internet community

- fewer DDoS attacks, less spam and other abuse from home devices
- increased awareness of and insight into privacy- and security-related issues

14 SPIN features

- powerful firewall functionality and insight at the residential gateway:
  - monitoring and visualizing IoT internet traffic flows in real time (insight)
  - detecting and blocking vulnerable IoT devices (security)
  - blocking unwanted connections (privacy)
- tailored to suit the home and SOHO environment, keeping the end user in control
- bringing all devices connected to the gateway under central security management, without invading the user's privacy
- providing a common view of the traffic flows running through the gateway
- open-source software written in C, allowing CPE manufacturers to easily integrate SPIN into their gateways, for instance as part of a software image based on OpenWrt/Linux
- full IPv6 support, for connectivity as well as analysis
- engages at the IP packet level, supporting TCP, UDP and ICMP traffic
- functionality available through a native interface (OpenWrt ubus and UCI)
- a web-based, interactive GUI provided as an example and for inspiration
- provides easily-understandable insight into privacy- and security-related issues, and allows direct intervention (e.g. blocking)
- first drill-down provides information on specific devices, allowing a user to ignore, rename, block, or whitelist a specific node
- more advanced analysis can be done after downloading a traffic dump in PCAP format
- web API based on REST and JSON, the functionality of which is currently being extended
- hooks in the software allow for the addition of another API providing an entrance for access providers to connect remotely, so they can for example:
  - run a tcpdump session on the CPE (for help or troubleshooting)
  - collect statistics on the use of home devices and the state of end users' security

  allowing close integration with the provider's security management infrastructure (all depending on legal limitations and contractual arrangements between customer, provider and manufacturer);
  this in turn facilitates automated, targeted interaction with end users on specific security issues
- the use of OpenWrt's native ubus and UCI interfaces allows CPE manufacturers to easily integrate the software into their gateways
- integrators can deploy MQTT to receive traffic information from the SPIN agents
- adheres strongly to international, open standards for IoT security and privacy

15 More information

More information on SPIN is available through its project page:
https://spin.sidnlabs.nl/

The best way to take a better look at SPIN's functionality and get hands-on experience is to download and install one of the premade Valibox images available here:
https://valibox.sidnlabs.nl

SPIN software available as open source on GitHub:
https://github.com/SIDN/spin

Specification of the web API:
https://github.com/SIDN/spin/blob/master/doc/web_api.md

SIDN Labs Technical Report SIDN-TR-2017-002 'SPIN: a User-centric Security Extension for In-home Networks':
https://www.sidnlabs.nl/downloads/papers-reports/SIDN-TR-2017-002.pdf

16 Footnotes

[1] Cisco Visual Networking Index: Forecast and Trends, 2017–2022

[2] TrustBox home router

[3] Valibox

[4] Holmes router and app, by DistributIT

[5] CIRA Secure Home Gateway

[6] Turris Omnia router

[7] Canadian Multistakeholder Process – Enhancing IoT Security

[8] IoT Privacy & Security multi-stakeholder WG

Colophon

SIDN
Christiene Bouwens - Marketing Manager
Ad Bresser - SPIN Propositie Manager
Ir. drs. Adrian Offerman - Tech Journalist
Jelte Jansen - SIDN Labs

Questions about the whitepaper may be mailed to
communicatie@sidn.nl

SIDN
PO Box 5022
6802 EA Arnhem, The Netherlands
Meander 501
6825 MD Arnhem, The Netherlands
T +31 (0)26 352 55 00
www.sidn.nl