Controle over onbeheerde apparaten thuis

Vermindering van IoT-veiligheidsrisico's met behulp van open source CPE software

SIDN Jouw wereld. Ons domein.

Introductie

Dit white paper bespreekt de veiligheids- en privacy-aspecten van het opkomende Internet of Things (IoT). De verwachting is dat een groot deel daarvan zal bestaan uit onbeheerde, onveilige apparaten en apparaatjes voor thuisgebruik. Als oplossing stellen we hier SPIN voor, kort voor Security and Privacy for In-home Networks. Deze open source software brengt IoT-beveiliging naar de gateway thuis in de vorm van nieuwe, waardevolle functionaliteit voor de eindgebruiker, terwijl access providers de IoT-apparaten en verkeersstromen op de locatie van hun klant onder direct centraal beheer kunnen brengen. Zo vermindert SPIN de veiligheidsrisico's verbonden aan het IoT-netwerk, terwijl privacy-gevoelige data in het gebruikersdomein blijft.

Inhoud

1 Management summary

Het opkomende Internet of Things (IoT) zal op korte termijn uit vele tientallen miljarden verbonden apparaten bestaan. Een groot deel daarvan betreft onbeheerde machine-to-machine (M2M)-apparaten voor thuisgebruik. De verwachting is dat een groot aantal van deze thuisapparaten helemaal nooit updates zal ontvangen, of dat updates zullen stoppen lang voordat deze apparaten van het netwerk worden losgekoppeld. Dit levert serieuze veiligheids- en privacy-risico's op voor zowel access providers als eindgebruikers.
Uitgaande grootschalige Distributed Denial-of-Service (DDoS)-aanvallen en IP-adresreeksen die worden opgenomen in zwarte lijsten kunnen de integriteit van het access-netwerk en de business continuity van de provider in gevaar brengen. Gebruikers kunnen te maken krijgen met allerlei vormen van privacy-schending, malware, de diefstal van identiteit, informatie, toegangsgegevens en eigendommen, en andere digitale misdaad.
De zwaarste last wat betreft de preventie en afhandeling van deze bedreigingen komt naar verwachting bij de access provider te liggen. Bovendien is hij ook het eerste aanspreekpunt voor onwetende en technisch niet onderlegde gebruikers.

SPIN is open source software waarmee access providers de IoT-apparaten en verkeersstromen op de locatie van hun klant onder direct centraal beheer kunnen brengen. Het biedt krachtige maar makkelijk te gebruiken firewall-functionaliteit en een gemeenschappelijk inzicht voor beide partijen, zonder dat de privacy van de klant daarbij in gevaar komt.
SPIN brengt IoT-beveiliging naar de gateway thuis in de vorm van nieuwe, waardevolle functionaliteit, die zowel als aantrekkelijk hebbeding als enabler fungeert voor de eindgebruiker.
Access providers kunnen de functionaliteit van SPIN integreren in hun bestaande security management-infrastructuur en zelfhulp-portals. Daarmee wordt geautomatiseerde interactie met eindgebruikers over veiligheidsaangelegenheden mogelijk en kunnen gebruikers zelf hun problemen verhelpen.
Fabrikanten van CPE-apparatuur kunnen de native interfaces van hun operating systems gebruiken om de software in hun gateways te integreren.
SPIN houdt zich strikt aan internationale, open standaarden voor IoT-beveiliging en privacy, waarmee de beste interoperabiliteit en juridische compliance verzekerd is.

SPIN is ontwikkeld door de Nederlandse domeinnaam-registry SIDN, een not-for-profit organisatie en voortrekker met een bewezen staat van dienst op gebied van Internet-veiligheid. Hun onderzoeksafdeling SIDN Labs zal SPIN blijven doorontwikkelen als onderzoeksplatform voor IoT-beveiliging.

SPIN is momenteel beschikbaar als een werkend prototype. De software werd gedemonsteerd als onderdeel van de TrustBox thuis-router op de laatste Consumer Electronics Show (CES) in Las Vegas, waar het apparaat de Best of Innovation Award in de categorie Cybersecurity & Personal Privacy won. De software is ook beschikbaar als integraal onderdeel van de build images voor Valibox, een andere innovatie in beveiliging ontwikkeld door SIDN Labs. Andere partijen die SPIN in hun projecten gebruiken zijn CZ.NIC (de Tsjechische registry voor de .cz-zone), CIRA (de Canadese registry voor de .ca-zone) en DistributIT (een Nederlandse startup).

SPIN bevindt zich momenteel in het stadium van first viable product, wat betekent dat het huidige prototype volledig functioneel is en klaar voor de eerste inzet in een pilot project.

2 Een zee van onbeheerde apparaten

Het opkomende Internet of Things (IoT) omvat nu al tientallen miljarden apparaten. Volgens Cisco's laatste Visual Networking Index [1] gaat het om 28,5 miljard aangesloten apparaten in 2022, ten opzichte van 18 miljard in 2017. Meer dan de helft hiervan – 14,6 miljard – betreft machine-to-machine (M2M)-apparaten, dat wil zeggen apparaten die alleen met andere systemen communiceren. En bijna de helft van die M2M-apparaten zal onderdeel uitmaken van connected home toepassingen zoals home automation, home security en videobewaking, aangesloten witgoed en volgsystemen. Het gemak waarmee consumenten allerlei goedkope apparaatjes direct aanschaffen via online marktplaatsen over de hele wereld om die vervolgens aan te sluiten op hun thuisnetwerk is zowel onthutsend als zorgwekkend.

Met een lage kostprijs als belangrijkste driver in deze markt en een gebrek aan veiligheidsbewustzijn als norm bij consumenten verwachten we dat een groot aantal van deze thuisapparaten helemaal nooit updates zal ontvangen, of dat updates zullen stoppen lang voordat deze apparaten van het netwerk worden losgekoppeld. De allergoedkoopste apparaatjes zullen niet eens het geheugen bevatten dat nodig is voor een software update en worden naar verwachting gewoon weggegooid nadat ze hun nut verloren hebben.

Al deze onbeheerde apparaten verbonden met thuis-routers en andere CPE's leveren in toenemende mate risico's op voor beide betrokken partijen. Verouderde apparaten bieden een attack surface aan de zijde van de eind-gebruiker. Zijn ze eenmaal gekraakt, dan fungeren deze apparaten als springplank voor de infectie van andere apparaten en systemen hogerop in het netwerk, of ze worden onderdeel van botnets die waardevolle informatie verzamelen, spam versturen en Distributed Denial-of-Service (DDoS)-aanvallen uitvoeren vanaf het access-netwerk.

3 Impact

Met een almaar groeiend aantal eindgebruikers achter een (CG)NAT gateway is een slechte reputatie of de opname van een grootschalig gedeeld IP-adres in een zwarte lijst iets dat access providers zich echt niet kunnen veroorloven vanwege de directe impact op een aanzienlijk aantal klanten. Tegelijkertijd vormen besmette apparaten een directe bedreiging voor de veiligheid en privacy van eindgebruikers, die te maken krijgen met verschillende vormen van afpersing, identiteitsdiefstal en andere digitale misdaad. Vanzelfsprekend zullen zij als eerste bij hun access provider aankloppen voor bescherming tegen dit soort ellende.

De uitdaging die voor ons ligt:

- eindgebruikers verbinden grote aantallen onveilige apparaten met hun gateway thuis
- ondanks de ontwikkeling van wetgeving is de verwachting dat noch eindgebruikers noch fabrikanten de veiligheid van deze thuisapparaten op orde zullen houden
- deze zee van onbeheerde apparaten vormt een bedreiging voor de integriteit van het access-netwerk, de continuïteit van de dienstverlening, en de veiligheid en privacy van de eindgebruikers
- helpdesk-medewerkers zullen een toenemend aantal veiligheids- en privacy-gerelateerde vragen en klachten ontvangen, terwijl ze geen inzicht hebben in de apparaten verbonden met het thuisnetwerk van de klant
- door de directe import van goedkope apparaatjes van online marktplaatsen over de hele wereld zal wetgeving de problematiek van onveilige apparaten slechts gedeeltelijk kunnen aanpakken

Directe en indirecte bedreigingen voor eindgebuikers:

- ransomware
- identiteitsdiefstal
- verlies van waardevolle informatie
- diefstal van paswoorden en andere toegangsgegevens
- verlies van geld en andere eigendommen
- verlies van resources, bijvoorbeeld door verborgen crypto-mining software
- publicatie van gevoelige en privé-informatie, bijvoorbeeld via leakware
- verlies van controle over hun thuisnetwerk, mogelijk zelfs van bedrijfsnetwerken en -systemen

4 Veiligheidsrisico's

Het is duidelijk dat access providers nieuwe mogelijkheden nodig hebben om de veiligheidsrisico's van deze stortvloed aan onbeheerde thuisapparaten te beperken. Dit wordt bemoeilijkt door het grote aantal van deze apparaten en de grote heterogeniteit ervan. Daarbij maakt wetgeving ter bescherming van de privacy van de klanten – die verbiedt bijvoorbeeld deep inspection van hun verkeer – het moeilijker om deze apparaten en hun netwerkverkeer onder direct centraal beheer te brengen.

Een extra complicatie ligt in het veellagige karakter van de IoT-infrastructuur: sommige apparaten verbinden direct met de CPE, andere bieden Internet-toegang aan weer andere apparaten door het opzetten van een eigen Wi-Fi-netwerk, en weer andere fungeren als gateway voor een lagergelegen niveau van apparaatjes via een IoT-specifieke of proprietary netwerktechnologie. In sommige gevallen heeft een gebruiker zelfs helemaal geen weet van de aanwezigheid van bepaalde apparaten – denk bijvoorbeeld aan het management-systeem voor zonnepanelen dat door de installateur aan een open poort van de router is verbonden. Al deze verschillende lagen hebben hun eigen, specifieke beveiligingsbehoeften.

5 Een gezamenlijk verbindingspunt

Als verbindingspunt gelegen tussen access provider en eindgebruiker is de gateway thuis de beste locatie om de veiligheid en privacy van de gebruiker te beschermen en inzicht te geven in al het netwerkverkeer. Omdat de gateway toegankelijk is voor beide partijen, krijgen provider en gebruiker een gemeenschappelijk inzicht in de aangesloten apparaten en hun verkeersstromen. Zo kan de een de acties van de ander (zoals het blokkeren van een apparaat of verkeersstroom) altijd zien en eventueel ongedaan maken. Wat precies zichtbaar is voor de provider en de acties die hij kan uitvoeren worden vanzelfsprekend beperkt door de juridische overeenkomst met de gebruiker en door locale wetgeving. Dat kan zelfs betekenen dat een eindgebruiker de toegang tot "zijn" CPE helemaal kan blokkeren voor de provider.

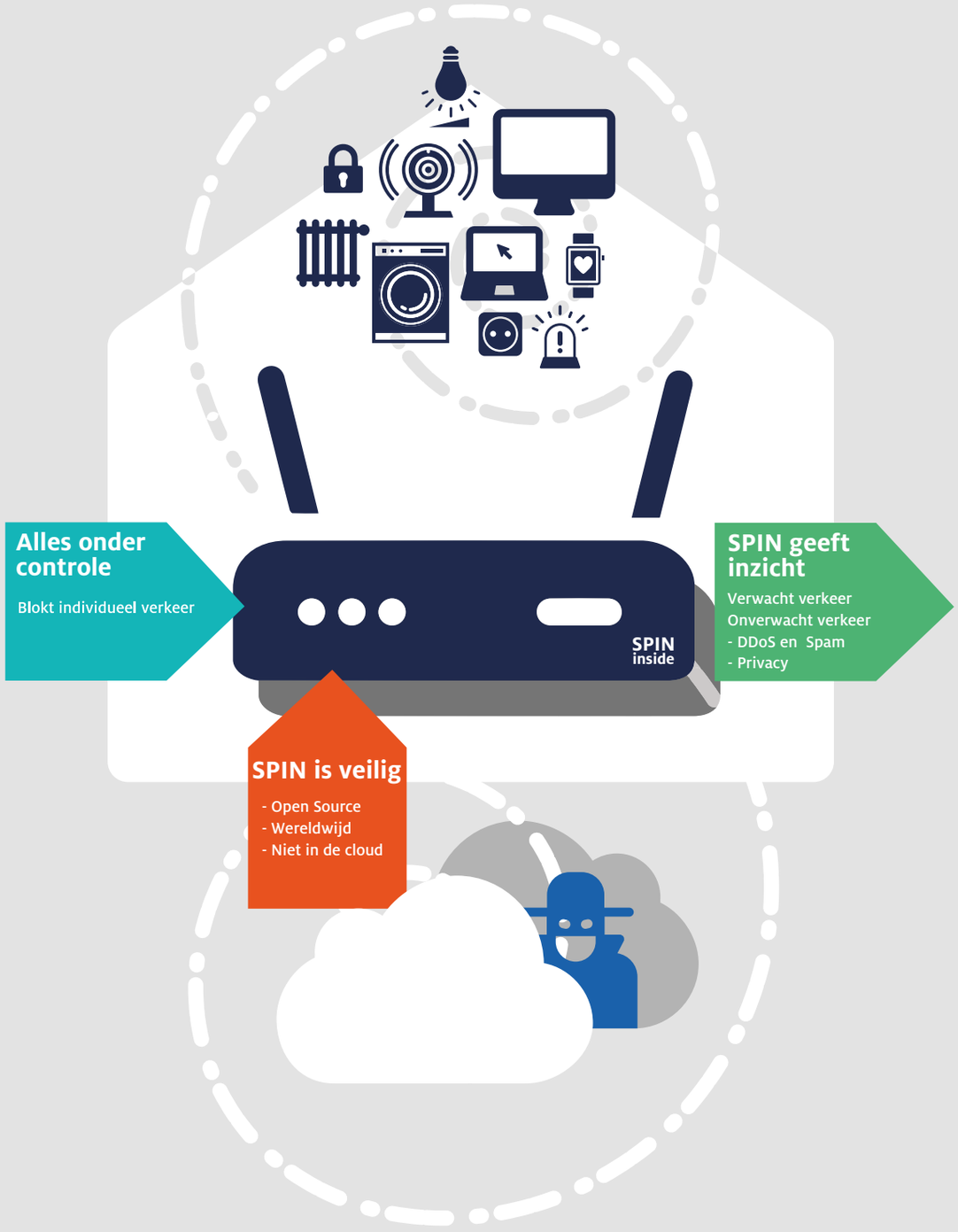
Wat dit alles zowel haalbaar als aantrekkelijk maakt is de mogelijkheid om nieuwe functionaliteit in de bestaande, web-gebaseerde configuratie-interface van de thuis-router op te nemen. Mocht wetgeving de verplichting opleggen om eindgebruikers de vrije keus van gateway-apparatuur te geven, dan zou deze toegevoegde waarde gebruikers wellicht kunnen overhalen om hun originele CPE te blijven gebruiken.

6 Propositie

De oplossing die we hier aandragen is open source software genaamd SPIN: Security and Privacy for In-home Networks. Daarmee kunnen CPE-fabrikanten en access providers firewall-achtige technologie toevoegen aan de gateway thuis, wat meestal de enige ingang is die providers bij hun klanten hebben. Zo blijft privacy-gevoelige data in het gebruikersdomein, terwijl beide partijen inzicht hebben in het verkeer dat door de gateway loopt.

Access providers kunnen SPIN-functionaliteit integreren in hun bestaande security management-infrastructuur en zelfhulp-portals. Daarmee wordt geautomatiseerde interactie met eindgebruikers over veiligheidsaangelegenheden mogelijk en kunnen gebruikers zelf hun problemen verhelpen. In ingewikkelder gevallen kunnen helpdesk-medewerkers samen met de gebruiker werken aan het oplossen van problemen veroorzaakt door aangesloten apparaten, op basis van een eenduidig inzicht in apparaten en verkeersstromen.

Op een hoger niveau kunnen access providers SPIN gebruiken om statistieken te verzamelen over het gebruik van thuisapparaten en het beveiligingsniveau bij hun klanten. Eindgebruikers kunnen het verkeersgedrag van hun apparatuur in de gaten houden en ongewenste verkeersstromen blokkeren via een makkelijk te gebruiken interface, waarmee zij aan hun kant de controle blijven houden. Ondertussen helpt de technologie eindgebruikers om hun kennis van privacy- en veiligheidsgerelateerde zaken te verbeteren en hun begrip voor beveiligingsmaatregelen te verhogen.

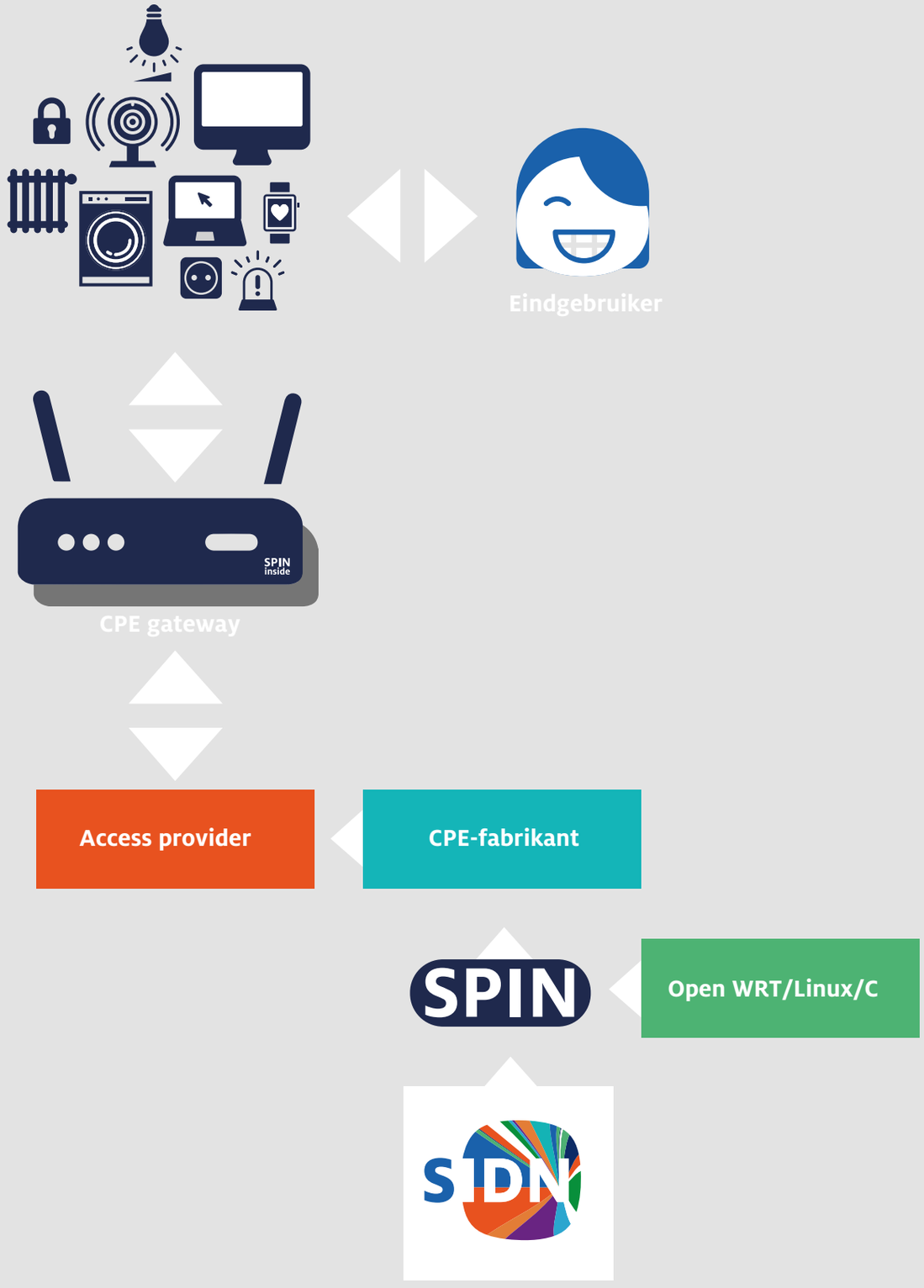


7 SPIN: een overzicht

SPIN is open source software voor CPE's die Linux draaien, waarmee het bijvoorbeeld kan worden opgenomen in een software image gebaseerd op OpenWrt. Als onderdeel van de gateway houdt SPIN de verkeersstromen tussen apparaten op het locale netwerk en het Internet in de gaten. Verkeersstromen naar specifieke nodes kunnen direct door de gebruiker geblokkeerd worden via de GUI van de CPE, of op afstand door de access provider via een web API die aan de software kan worden toegevoegd.

SPIN is geschreven in de programeertaal C voor maximale prestaties en portabiliteit. Daarmee kan de software ook worden ingebouwd in CPE-platformen gebaseerd op andere systemen dan Linux. De software is beschikbaar in zijn originele vorm van broncode in SIDN's GitHub repository, maar bijvoorbeeld ook als integraal onderdeel van een direct te gebruiken Valibox image voor de Raspberry Pi.

Andere uitgangspunten bij de ontwikkeling van SPIN zijn het strikt volgen van open standaarden, het bieden van inzicht en de controle aan eindgebruikers, en het bepalen van de koers voor doorontwikkeling en adoptie in samenwerking met andere belanghebbenden, zowel op technisch als strategisch vlak.



8 Voordelen van SPIN

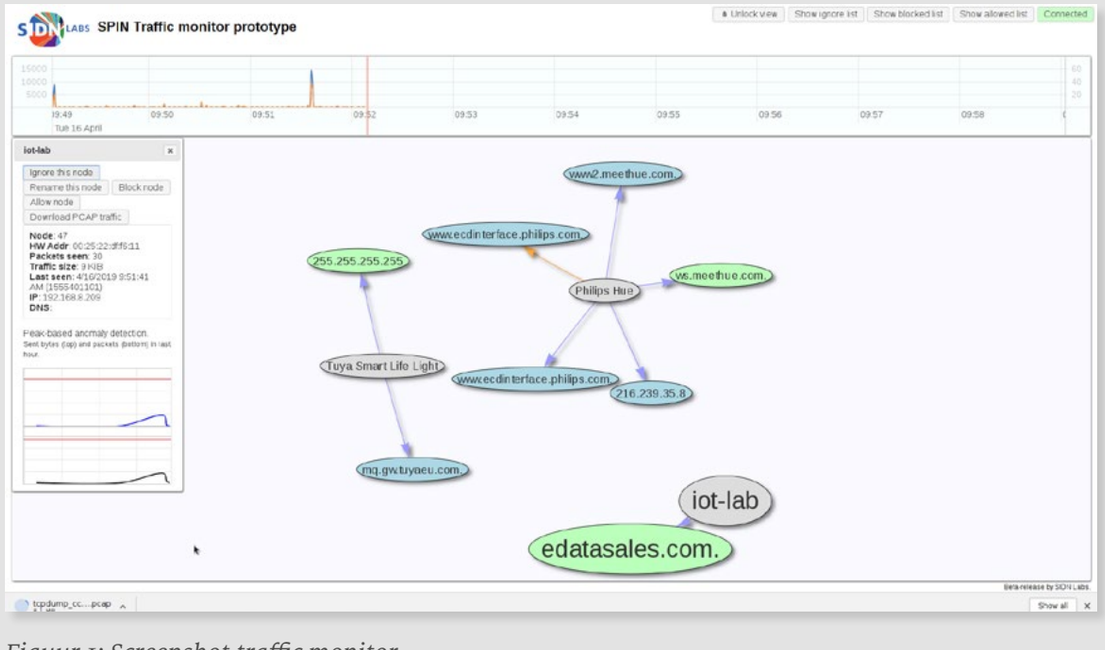
SPIN heeft diverse voordelen ten opzichte van bestaande firewalls en traffic analyzers:

- het is toegesneden op de thuis- en SOHO-omgeving
- een web-gebaseerde, interactieve GUI is beschikbaar als voorbeeld en ter inspiratie voor het bouwen van intuïtieve gebruikersinterfaces voor access providers en eindgebruikers
- het geeft eindgebruikers inzicht in veiligheids- en privacy-gerelateerde zaken op individueel niveau
- aan de software kan een API worden toegevoegd om access providers hetzelfde inzicht en dezelfde functionaliteit te geven die voor de gebruikers beschikbaar is
- door de native ubus en UCI interfaces te gebruiken kunnen CPE-fabrikanten de software makkelijk in hun gateways integreren
- voor webverkeer worden de domeinnamen van de originele bestemmingen gebundeld en weergegeven als een enkele node, in plaats van de individuele hostnamen van de servers

9 De Traffic Monitor

Het huidige prototype van de software is voorzien van een grafische (web-gebaseerde) interface die fungeert als voorbeeld hoe de functionaliteit van SPIN voor de eindgebruiker beschikbaar kan worden gemaakt. De Traffic Monitor (zie het screenshot hiernaast) laat alle verkeersstromen van de laatste tien minuten zien als een dynamische graaf van eindpunten en verbindingen. Interne apparaten zijn weergegeven in grijs, recente verbindingen in groen, en oudere verbindingen in blauw. Door op een node te klikken kan de gebruiker meer informatie opvragen. In het pop-up informatieblok kan de gebruiker de betreffende node laten negeren, hernoemen, verkeer blokkeren of juist toestaan.

Daarnaast is er de mogelijkheid om een traffic dump in PCAP-formaat te downloaden voor geavanceerde analyse met behulp van tools als tcpdump en Wireshark. Een van de ideeën waar SIDN op moment aan werkt is een web-portaal waar gebruikers deze dumps kunnen uploaden voor verdere analyse.



Figuur 1: Screenshot traffic monitor

10 Track record

SPIN is momenteel beschikbaar als een werkend prototype. De software werd gedemonsteerd als onderdeel van de TrustBox thuis-router [2] op de laatste Consumer Electronics Show (CES) in Las Vegas, waar het apparaat de Best of Innovation Award in de categorie Cybersecurity & Personal Privacy won. De software is ook beschikbaar als integraal onderdeel van Valibox [3], een OpenWrt software image voorzien van DNSSEC-validatie, en ook weer een innovatie in beveiliging ontwikkeld door SIDN Labs.

Andere partijen die SPIN in hun projecten gebruiken zijn CZ.NIC (de Tsjechische registry voor de .cz-zone), CIRA (de Canadese registry voor de .ca-zone) en DistributIT. Die laatste is een Nederlandse startup die SPIN heeft opgenomen in Holmes [4], een veiligheids- en privacy-gerichte gateway uitgebreid met een mobiele app.

CIRA heeft SPIN verwerkt in een gateway voor thuis met de naam Secure Home Gateway [5]. Het systeem is gebaseerd op de Turris Omnia [6], een high-end router ontwikkeld als een open hardware project door de Tsjechische registry CZ.NIC. Ook bij de Turris Omnia zelf is SPIN in de software opgenomen.

De Secure Home Gateway is door CIRA bedacht om consumenten en het Internet te beschermen tegen IoT-gebaseerde cyber-aanvallen, vergelijkbaar met de missie van SIDN bij de ontwikkkeling van de SPIN software. De gateway is door CIRA ingebracht in het ‘Canadian Multistakeholder Process – Enhancing IoT Security’ [7], waarin verschillende partners samenwerken om het opkomende IoT te beveiligen. Dit samenwerkingsmodel fungeert ook als een blauwdruk voor de Nederlandse IoT Privacy & Security multi-stakeholder werkgroep die binnenkort gelanceerd wordt. Verderop [op pagina xx] kun je meer lezen over dit inititatief’.

11 Conclusie

SPIN laat access providers de IoT-apparaten en verkeersstromen op de locatie van hun klant onder direct centraal beheer brengen. Het biedt krachtige maar makkelijk te gebruiken firewall-functionaliteit en een gemeenschappelijk inzicht voor beide partijen, zonder dat de privacy van de klant daarbij in gevaar komt.

SPIN houdt zich strikt aan internationale, open standaarden voor IoT-beveiliging en privacy. De software is ontwikkeld door de Nederlandse domeinnaam-registry SIDN, een not-for-profit organisatie en voortrekker met een bewezen staat van dienst op gebied van Internet-veiligheid.

De SPIN software is beschikbaar als open source en kan makkelijk door access providers en CPE-fabrikanten worden geïntegreerd in hun producten en diensten. SIDN Labs zal SPIN blijven doorontwikkelen als onderzoeksplatform voor IoT-beveiliging.

Het laatste Valibox image is de beste manier om snel een indruk te krijgen van de SPIN-functionaliteit zoals hierboven beschreven . Binaire images zijn kant-en-klaar beschikbaar voor verschillende Single-Board Computers, waaronder de Raspberry Pi.

12 Over SIDN

SIDN is een not-for-profit organisatie en verantwoordelijk voor het Nederlandse top-level domein. Als operator van de .nl-zone onderhoudt SIDN de kritieke DNS-infrastructuur voor 5.8 miljoen domeinnamen en verwerkt zij 1.3 miljard DNS queries per dag.

Het hogere doel van SIDN is om mensen en organisaties via een veilig en robuust Internet met elkaar te verbinden. Daarmee is SIDN met haar onderzoekstak SIDN Labs een wereldwijde pionier en voortrekker geworden in de ontwikkeling en standaardisatie van beveiligingstechnologie voor de Internet-infrastructuur.

SIDN is de ontwikkeling van SPIN begonnen naar aanleiding van de Mirai DDoS-aanvallen in 2016, welke werden uitgevoerd door een botnet bestaande uit besmette IP-camera's en thuis-routers gebaseerd op Linux.

13 Iedereen profiteert

Eindgebruikers
- inzicht op individueel niveau: waarheen lopen de verbindingen vanuit thuisapparatuur
- controle: blokkeer individuele bestemmingen direct of op basis van profielen
- privacy: verzameling en verwerking van data binnen het netwerk (geen cloud)
- makkelijk te begrijpen inzicht in privacy en veiligheidsgerelateerde zaken
- geavanceerder analyse mogelijk via een traffic dump

Access providers
- alle IoT-apparaten onder centraal beveiligingsbeheer
- hechte integratie in hun bestaande security management-infrastructuur
- geautomatiseerde interactie met eindgebruikers aangaande beveiligingskwesties
- helpdesk-medewerkers en eindgebruikers krijgen een eenduidig inzicht
- aanvullende functionaliteit voor analyse, interactie en interventie
- statistieken over het gebruik van thuisapparaten en het beveiligingsniveau thuis
- meer begrip voor beveiligingsmaatregelen bij eindgebruikers

SPIN
- krachtige firewall-functionaliteit en inzicht op het verbindingspunt thuis
- een eenduidig, gemeenschappelijk inzicht in aangesloten apparaten en verkeersstromen
- strikte volging van internationale, open standaarden
- open source software
- geproduceerd door SIDN, een wereldwijde pionier en voortrekker met een bewezen track record in Internet-beveiliging

CPE-fabrikanten
- IoT-beveiliging als nieuwe, waardevolle functionaliteit voor hun CPE's
- makkelijke integratie in hun bestaande OpenWrt/Linux-systemen
- integratie via OpenWrt's native interface (ubus en UCI)
- eenvoudige ontwikkeling van maatwerk beveiligingstoepassingen bovenop SPIN

SIDN
- een veiliger Internet
- impact: het bereiken van zo veel mogelijk consumenten

Internet-gemeenschap
- minder DDoS-aanvallen, spam en andere ellende vanaf thuisapparatuur
- een hoger bewustzijn van en inzicht in privacy- en veiligheidsgerelateerde zaken

14 SPIN features

- krachtige firewall-functionaliteit en inzicht op het verbindingspunt thuis:
  - monitoring en visualisatie van IoT-verkeersstromen in real-time (inzicht)
  - detectie en blokkering van kwestbare IoT-apparaten (veiligheid)
  - blokkering van ongewenste verbindingen (privacy)
- toegesneden op de thuis- en SOHO-omgeving, waarbij de eindgebruiker de controle houdt
- alle apparaten verbonden met de gateway onder centraal beheer gebracht, zonder daarbij de privacy van de gebruiker aan te tasten
- een eenduidig inzicht in de verkeersstromen die door de gateway lopen
- open source software geschreven in C, zodat SPIN makkelijk door de CPE-fabrikanten kan worden ingebouwd in hun gateways, bijvoorbeeld als onderdeel van een software image gebaseerd op OpenWrt/Linux
- volledige ondersteuning voor IPv6, zowel voor verbindingen als voor analyse
- grijpt aan op het niveau van IP-pakketten, waarmee TCP-, UDP- en ICMP-verkeer ondersteund worden
- functionaliteit beschikbaar via een native interface (OpenWrt ubus en UCI)
- een web-gebaseerde, interactieve GUI beschikbaar als voorbeeld en ter inspiratie
- levert makkelijk te begrijpen inzicht in privacy- en veiligheidsgerelateerde zaken, en maakt direct ingrijpen (bijvoorbeeld blokkeren) mogelijk
- meer informatie over een specifieke node kan worden opgevraagd, waarna de gebruiker de betreffende node kan laten negeren, hernoemen, verkeer blokkeren of juist toestaan
- geavanceerde analyse is mogelijk via een traffic dump in PCAP-formaat
- een web API gebaseerd op REST en JSON, waarvan de functionaliteit op dit moment wordt uitgebreid
- hooks in de software voor de implementatie voor nog een API die access providers kunnen gebruiken om op afstand verbinding te maken; zodat zij bijvoorbeeld:
  - een tcpdump-sessie op de CPE uit kunnen laten voeren (voor hulp of probleemoplossing)
  - statistieken kunnen verzamelen over het gebruik van thuisapparaten en het beveiligingsniveau bij de eindgebruiker

  waarmee een hechte integratie in de security management-infrastructuur van de provider mogelijk wordt (wel afhankelijk van juridische beperkingen en contractuele afspraken tussen klant, provider en fabrikant), net als geautomatiseerde, doelgerichte interactie met eindgebruikers aangaande specifieke beveiligingskwesties
- het gebruik van OpenWrt's native ubus en UCI interfaces maakt dat CPE-fabrikanten de software makkelijk in hun gateways kunnen integreren
- integrators kunnen MQTT inzetten om verkeersinformatie van de SPIN agents te ontvangen
- strikte volging van internationale, open standaarden voor IoT-beveiliging en privacy

15 Meer informatie

- Meer informatie over SPIN is beschikbaar op de project-pagina: https://www.spin4home.nl/
- De beste manier om de functionaliteit van SPIN beter te bekijken en zelf ervaring met de software op te doen is hier een van de voorgebakken Valibox images te downloaden en te installeren: https://valibox.sidnlabs.nl
- SPIN software beschikbaar als open source on GitHub: https://github.com/SIDN/spin
- specificatie van de 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 thuis router

[3] Valibox

[4] Holmes router en app, bij DistributIT

[5] CIRA Secure Home Gateway

[6] Turris Omnia router

[7] Canadian Multistakeholder Process – Enhancing IoT Security

[8] IoT Privacy & Security multi-stakeholder WG

Colofon

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

Wil je hier meer over weten of heb je andere vragen? Mail dan naar
communicatie@sidn.nl

SIDN
Postbus 5022
6802 EA Arnhem
Meander 501
6825 MD Arnhem
T +31 (0)26 352 5
www.sidn.nl