**Fortinet en Renesas werken samen aan beveiliging van connected cars**

**10 januari 2018 -** [Fortinet](http://www.fortinet.com) (NASDAQ: FTNT), wereldwijd leider in uitgebreide, geïntegreerde en geautomatiseerde oplossingen voor cyberbeveiliging, werkt samen met [Renesas Electronics](https://www.renesas.com/en-us/) aan een oplossing voor de belangrijkste netwerk beveiligingsrisico’s van connected cars. De beide bedrijven lanceren een prototype, dat laat zien hoe Fortinet FortiOS, het besturingssysteem voor de beveiliging, kan worden geïntegreerd met de R-Car H3 system-on-chip (SoC) van Renesas voor het beschermen van netwerkdomeinen, cloud-diensten en applicaties.

Een demonstratie van de oplossing vindt plaats op [CES 2018](https://www.ces.tech) tijdens de Renesas Advanced & Autonomous Test Track en Future Ready Solutions Showcase (9 t/m 12 januari in Las Vegas, Nevada.) Fortinet en Renesas zullen tijdens de CES cyberaanvallen op een prototype van een connected car simuleren, zoals pogingen om een intrusion prevention system (IPS) onklaar te maken en een DDoS (distributed denial of service)-aanval uit te voeren. Het doel is om te laten zien hoe effectief deze geautomatiseerde en geïntegreerde beveiligingsoplossing bestuurders beschermt tegen hackers die de controle over hun voertuig of applicaties willen overnemen.

Fortinet en Renesas zullen tijdens CES laten zien hoe de integratie van de Fortinet Security Fabric-technologie met de R-Car H3 SoC het mogelijk maakt om beveiligingsregels te beheren en toe te passen en geautomatiseerde beveiliging biedt van de aandrijvings- en communicatiecomponenten van het voertuig. Dat geldt onder meer voor de LTE-module, de module voor de communicatie tussen voertuigen, het draadloze access point en de module voor motorbesturing. Gebruikmakend van de beveiligingsfuncties op de chip van de Renesas R-Car H3 beschermt Fortinet het communicatieverkeer en past het beveiligingsregels toe om de toegang tussen bepaalde domeinen in te perken om grip te krijgen op potentiële cyberbedreigingen. Fortinet en Renesas laten aan de hand van simulaties van pogingen tot het hacken van het intrusion prevention system (IPS) en DDoS-aanvallen zien hoe het FortiOS automatische beveiliging biedt van de data die van een publieke cloud-dienst naar het entertainmentsysteem binnen de auto wordt overgedragen.

Recente incidenten wijzen op de prangende noodzaak van geïntegreerde beveiliging voor de steeds geavanceerdere autonetwerken. Voorbeelden zijn de hack van de 2015 Jeep Cherokee, waarbij een groep hackers erin slaagde om via een draadloze verbinding in te breken in het voertuigsysteem en de controle over essentiële functies over te nemen, en de meer recente hack van de CAN-bus van Tesla’s Model S, die het mogelijk maakte om op 19 kilometer afstand te knoeien met de remmen, deursloten en dashboardcomputer van het voertuig.

**Geautomatiseerde beveiliging**

In 2025 zullen er volgens de prognoses 300 miljoen connected cars in gebruik zijn. In 2016 bedroeg dit aantal nog 37 miljoen. De jaarlijkse omzet voor apparatuur en diensten voor connected cars zal naar verwachting boven de 250 miljard dollar uitkomen.[[1]](#endnote-1) Belangrijke factoren die bijdragen aan de groei van de wereldwijde markt voor connected cars, jagen tevens de vraag aan naar zelfrijdende functionaliteit, datagestuurde beslissingen en connectiviteit binnen het voertuig, zoals toegang tot smartphone-functies, het on demand afspelen van muziek, internetverbindingen en infotainment.

Een connected car is voorzien van internettoegang en een wireless local area network (WLAN). Bestuurders kunnen de internetverbinding delen met andere apparaten binnen en buiten het voertuig. Om passende beveiliging te bieden en het vertrouwen van consumenten te winnen, moeten autofabrikanten de beveiliging vooropstellen bij het ontwerp en de implementatie van connected car-technologie. Beveiligingssystemen moeten communicatieprotocollen, apparaten en netwerken omspannen. Daarnaast moeten ze het overzicht, de integratie en het beheer uitbreiden van individuele voertuigen naar het bredere vervoersecosysteem, zoals systemen voor het beheer van wegen en verkeersstromen.

Connected cars vragen om het gebruik van verschillende beveiligingsoplossingen die als één systeem werken. Dit vereist strategische segmentatie van belangrijke functionele domeinen, zoals de aandrijving, telematica en infotainment. Deze segmentatie maakt het mogelijk om bedreigingen automatisch in te dammen en te elimineren. Een andere belangrijke vereiste is het gebruik van een real-time systeem voor bedreigingsinformatie, zoals [FortiGuard Labs](https://fortiguard.com) van Fortinet. Dit systeem moet actuele informatie over kwetsbaarheden en bedreigingen aan het voertuig aanleveren ter ondersteuning van effectieve en geautomatiseerde beveiliging. Dit moet ook een terugkoppeling naar een cloud-netwerk omvatten, zodat beveiligingsgebeurtenissen kunnen worden gedeeld en met elkaar in verband worden gebracht en updates en patches tijdig kunnen worden aangeleverd.

Meer informatie over de demo van Fortinet en Renesas, de Renesas Advanced & Autonomous Test Track en de Future Ready Solutions Showcase is te vinden op <http://renesasatces.com>.

Michael Xie, oprichter, bestuursvoorzitter en chief technology officer bij Fortinet: “Connected cars zijn de volgende grote technologische innovatie die voor disruptie binnen de auto-industrie zorgt. Driedimensionale kaarten, de verwerking van sensordata, de integratie van slimme apparatuur, cloud-diensten, geavanceerde LAN-/CAN-netwerken en zelfrijdende systemen staan aan de basis van de connected car van de toekomst, maar brengen ook serieuze beveiligingsrisico’s met zich mee. En nu allerhande IoT-apparaten een verbinding maken met het netwerk binnen connected cars om toegang te krijgen tot content en applicaties, wordt het aanvalsoppervlak alleen maar groter. Geïntegreerde beveiliging is van cruciaal belang voor de veiligheid van consumenten en hun vertrouwen in connected cars. Fortinet breidt zijn leiderschapspositie in netwerkbeveiliging uit naar de auto-industrie nu fabrikanten voertuigen beginnen te ontwikkelen die vragen om geautomatiseerde beveiliging, real-time bedreigingsinformatie en strategische segmentatie. Dit is nodig om de complexe architectuur van de auto optimaal te beschermen. We zijn verheugd om met Renesas samen te werken en tijdens CES veilige netwerkoplossingen te demonstreren die tegemoetkomen aan de unieke eisen van de veranderende besturingsomgeving van auto’s.”

Amrit Vivekanand, vice president Automotive Systems Business Division bij Renesas: *“*Autotechnici binnen de complete toevoerketen doen een beroep op Renesas voor uitgebreide oplossingen die de ontwikkelingscycli en time-to-market verkorten. Renesas heeft zijn krachten met Fortinet gebundeld om uiterst geavanceerde beveiligingsoplossingen te ontwikkelen die de geïntegreerde bescherming bieden die nodig is om de connected cars van morgen veilig te houden. We zien Fortinet als een betrouwbare adviseur die met zijn toonaangevende kennis van netwerkbeveiliging kan voldoen aan de unieke behoeften en infrastructuurvereisten van beveiligingssystemen voor de autonetwerken van de toekomst*.*

1. [ON World Connected Car Markets Report](https://www.onworld.com/connectedcar/), april 2017 [↑](#endnote-ref-1)