Software en hardware om auto-elektronica weer veilig te maken

In moderne voertuigen zit een uitgebreid netwerk van controleprocessoren. Die interpreteren informatie van sensoren en sturen actuatoren aan. Hoe een auto zich in bepaalde omstandigheden gedraagt, welke veiligheidsfuncties in actie komen, het wordt allemaal geregeld door deze processoren. Ze ondersteunen rem- en stuurmanoeuvres, bedienen de lichten, blazen de airbags op, optimaliseren het motorvermogen, enz. Pas sinds kort staan deze netwerken ook met de buitenwereld in contact. Maar daardoor worden ze kwetsbaar voor hackers, terwijl aan de beveiliging nog een en ander schort. Jan Tobias Mühlberg is onderzoeksmanager bij imec – DistriNet – KU Leuven. Hij legt uit hoe onderzoekers bij imec deze uitdaging aangaan. Zij ontwikkelden een nieuwe beveiligingsarchitectuur voor genetwerkte ingebedde apparaten en stemden die zorgvuldig af op de hedendaagse eisen. Hun gebruiksklare oplossing beveiligt niet alleen slimme voertuigen, maar ook andere kritische infrastructuur, zoals medische toestellen, slimme gebouwen of elektriciteitsnetwerken.

Eilandjes van slimme elektronica

“De complexe industriële machines van vandaag worden aangestuurd door elektronicanetwerken van sensoren, actuatoren en controleprocessoren die voortdurend informatie uitwisselen,” zegt Mühlberg. “In

bijvoorbeeld auto's speelt deze interactie zich af rond de zogeheten CAN-bus (Controller Area Network), een van oorsprong gesloten en bedraad netwerk dat moeilijk te kraken was voor indringers."

De CAN-specificaties werden zo'n 30 jaar geleden ontwikkeld. Voordien functioneerden voertuigen vrijwel volledig mechanisch. CAN werd ontworpen als standalone netwerk en die taak vervult het nog altijd perfect. Meer nog, vandaag zijn CAN-netwerken belangrijker dan ooit: er komen steeds meer heterogene sensoren en controleprocessoren in voertuigen die via de CAN-bus betrouwbaar en snel informatie versturen en ontvangen, zonder dat er een centrale computer aanwezig is. De CAN-bus verbindt bijvoorbeeld de rotatiesensoren in de wielen met het ABS-remsysteem en met de aandrijving.

Jan Tobias Mühlberg: "Je vindt vergelijkbare netwerken in de meeste industriële controlesystemen en gerobotiseerde assemblagelijnen. Ze werden stuk voor stuk zorgvuldig ontworpen en getest om met alle mogelijke uitzonderingstoestanden en fouten rekening te houden, waardoor ze heel veilig waren. Maar daar komt nu verandering in..."

Venster op de wereld

Moderne auto's en zeker topmodellen hebben allerlei infotainment- en navigatiesystemen aan boord die zowel met het CAN-netwerk als met de buitenwereld verbonden zijn. Via de verbinding met de CAN-sensoren is het zo mogelijk om zo de muziek automatisch luider af te spelen als je sneller of op een slecht wegdek rijdt. En via de buitenwereld ontvang je informatie over het verkeer, binnenkomende telefoons, en software-updates. Zelfrijdende auto's zullen nog verder gaan: ze communiceren met elkaar en de weginfrastructuur om zich veilig door het verkeer te bewegen.

"Dat alles betekent dat indringers nu plots wel over toegangen beschikken om het CAN-netwerk over te nemen. Alle communicatie met de buitenwereld gaat via Bluetooth of IP-netwerken die vaak met het internet zijn verbonden. En het internet is natuurlijk een hoogst onbetrouwbaar netwerk," zegt Mühlberg. "De hardware en software van de CAN-bus zijn helemaal niet ontworpen om in zo'n onveilige omgeving te functioneren. Authenticatie en autorisatie ontbreken bijvoorbeeld. Als het remsysteem van een auto een syntactisch correct CAN-bericht ontvangt, dan gaan de remmen er gewoon vanuit dat het bericht legitiem is en van een vertrouwde bron komt en niet van ergens anders."

Bovendien hebben de ontwerpers ervoor gezorgd dat CAN-processoren heel klein zijn, goedkoop en zo energiezuinig mogelijk. Ze zijn afgestemd op de taken die ze moeten uitvoeren, met lichte besturingssystemen en specifieke communicatie- en controletoepassingen. Maar in vergelijking met de processoren in een laptop of smartphone hebben ze geen beveiligd geheugen of een geïsoleerde 'sandbox' om processen in te draaien. Elke app die een CAN-processor aanspreekt, ook al hoort die daar niet thuis, heeft toegang tot het hele processorgeheugen en kan het overschrijven."

Welke risico's levert dit op? Mühlberg: "Onderzoekers hebben onlangs laten zien dat ze op afstand de besturing van een auto kunnen overnemen via de wifi- of Bluetooth-gateway. In Oekraïne is gebleken dat elektriciteitsnetwerken te hacken zijn, met mogelijk dramatische gevolgen. En onderzoekers bij imec – COSIC – KU Leuven hebben aangetoond dat ze zelfs pacemakers kunnen binnenkomen, waarbij het mogelijk is om die toestelletjes af te luisteren en zelfs potentieel fatale commando's te geven."

"Al betekent dit niet noodzakelijk dat dergelijke aanvallen gemakkelijk zijn. Een hacker moet heel slim, geraffineerd en geduldig te werk gaan. Maar omdat het aantal apparaten of voertuigen – bijvoorbeeld elektronisch identieke auto's – zo groot is, kan een hacker die erin slaagt om zich tot één zo'n systeem toegang te verschaffen een bedreiging vormen voor de veiligheid van heel veel identieke systemen."

Dataverwerking in geïsoleerde, veilige zones

In tegenstelling tot de duurdere processoren in bijvoorbeeld laptops en smartphones zijn controllerchips klein en beperkt in capaciteit. Ze beschikken niet over de beveiliging die standaard in andere processoren zit ingebouwd, zoals privilegeniveaus en geheugensegmentering. Maar het is onmogelijk om alle ingebedde processoren door high-end systemen te vervangen, omdat die voor deze toepassingen te duur en te complex zijn en te veel energie vragen.

“Daarom stelden wij ons tot doel om helemaal vanaf nul een veilige architectuur te ontwerpen,” zegt Jan Tobias Mühlberg. “Een architectuur die geschikt is om de ingebedde systemen van nu te beveiligen, zoals CAN-netwerken in auto’s, controlesystemen voor industriële productie of kleine IoT-componenten. Daarbij moeten we rekening houden met de vereisten van de industrie dat dergelijk systemen klein, goedkoop en uiterst zuinig moeten blijven.”

De onderzoekers vertrokken van een kleine microcontroller, representatief voor diegene die in auto’s worden gebruikt en breidden het ontwerp ervan uit. Ze voegden er naast veilig geheugenbeheer ook een encryptie-eenheid aan toe die is geoptimaliseerd voor een laag stroomverbruik. Het resultaat is een processor die niet veel groter is dan de huidige en maar weinig extra energie vraagt (ongeveer 6%).

Die processor is in staat om belangrijke software in een veilige zone te isoleren zodat die niet kan worden aangevallen. Bovendien zal de software enkel vertrouwen stellen in de hardware waar hij gebruik van maakt. Externe processen, maar zelfs software die op dezelfde processor draait, kan zo de beveiliging niet omzeilen om bv de runtime-toestand van het proces te lezen of te overschrijven.

Weten wie je kunt vertrouwen

“Maar zelfs als de processor die de remmen van je auto bedient niet langer te hacken is, dan luistert hij misschien wel nog naar een commando uit een kwaadwillige bron,” geeft Mühlberg toe. “Daarom hebben wij de vertrouwde berichtenbronnen beperkt tot bronnen die zichzelf als legitiem kunnen authentificeren. Een remcommando mag dus alleen maar van een vertrouwde processor komen die zelf niet kan worden gehackt, en van een geauthentificeerd stuk software op die processor. Het CAN-netwerk van een auto bestaat op die manier uit vele kleine, niet te hacken applicaties die elkaar wederzijds authentificeren en vertrouwen.”

Maar stel nu dat een ingebed systeem toch informatie met de buitenwereld moet uitwisselen, bijvoorbeeld met een softwareleverancier voor de installatie van updates of met de verkeersinfrastructuur? Voor die gevallen hebben de imec-specialisten veilige communicatie en attestering op afstand ingebouwd. Een externe partij kan dus berichten uitwisselen met een specifieke softwaremodule op een specifieke node, als het vaststaat dat het de correcte module is (authenticiteit), dat die niet werd gewijzigd (integriteit) en dat de status ervan correct is.

Demo op ITF Belgium en verdere stappen

Sancus, zoals de oplossing heet, is een beveiligingsarchitectuur voor schaalbaar-genetwerkte ingebedde systemen die voor geheugenbeveiliging, attestering op afstand, sterkte integriteit en authenticiteitsgaranties zorgt. Het systeem bestaat uit de uitgebreide microprocessor, specifieke software die in veilige zones draait en een C-compiler die beveiligde Sancus-code genereert.

Het Sancus-project is nog niet afgesloten: de onderzoekers van de imec-groepen DistriNet – KU Leuven en COSIC – KU Leuven willen nog enkele moeilijkheden uit de weg ruimen.

Eén ervan is ervoor zorgen dat het netwerk altijd beschikbaar is en in real time functioneert. “Wij kunnen met onze innovatie garanderen dat alle berichten die in de module aankomen legitiem zijn”, zegt Mühlberg. “Maar wij kunnen nog niet garanderen dat ze zullen aankomen. Een hacker zou nog altijd berichten kunnen tegenhouden. Dat levert normaal geen gevaarlijke situaties op, want de node zal dit detecteren en het systeem op een veilige manier tot stilstand brengen. Maar het blijft wel vervelend.”

Een andere vraag: hoe garandeer je 100% dat de softwaremodules geen interne fouten bevatten? Zonder een formele ontwerpmethodologie en inherent veilige programmeertalen kan dat niet en kunnen er altijd nog onveilige situaties ontstaan. Maar omdat de onderzoekers erin geslaagd zijn de modules klein te houden en isoleren, moet het ook doenbaar zijn om ze op een meer formele, foutenvrije manier te ontwerpen.

Het team van Mühlberg wil graag samenwerken met partners om hardware- en softwareoplossingen te ontwikkelen die aan hun behoeften zijn aangepast. “Wij zullen een Sancus-demo houden op het Imec Technology Forum in Antwerpen (ITF Belgium, May 16-17), hetzij in een autotoepassing, hetzij in een oplossing voor slimme energiemeters, want ook daarvoor heb je beveiligde ingebedde processoren nodig. Voor geïnteresseerde bedrijven is dit een buitenkans om alle technische details met ons te bespreken. Dit onderwerp wint immers snel aan belang nu slimme zelfrijdende auto’s met de omgeving beginnen te communiceren.”

Beschikbaarheid en dank

Voor de verifieerbaarheid en reproduceerbaarheid van de Sancus-resultaten werden het hardwareontwerp en de software van het prototype openbaar gemaakt. Zowel het hardwareontwerp als de bronbestanden, binaire pakketten en documentatie zijn hier te raadplegen.

Sancus werd ontwikkeld door imec – DistriNet – KU Leuven en imec – COSIC – KU Leuven, twee onderzoeksgroepen die een wereldfaam hebben opgebouwd met hun werk rond beveiliging. De ontwikkeling werd gedeeltelijk gesteund door het University Research Office van het Intel Lab, het onderzoeksfonds van de KU Leuven, het EU FP7-project NESSoS en het Belgian Cybercrime Centre of Excellence (B-CCENTRE).

Biografie

Jan Tobias Mühlberg is onderzoeksmanager bij imec – DistriNet – KU Leuven. Voordien deed hij onderzoek aan de universiteit van Bamberg (Duitsland, tot 2011), behaalde hij zijn doctoraat aan de University of York (UK, 2010) en werkte hij als onderzoeker aan de University of Applied Sciences in Brandenburg (Duitsland, tot 2005), waar hij zijn master behaalde. Tobias legt zich toe op softwarebeveiliging en formele verificatie en validatie van softwaresystemen, specifiek voor ingebedde systemen en componenten van low-level besturingssystemen. Tobias heeft vooral belangstelling voor beveiligingsarchitecturen voor ingebedde systemen met belangrijke veiligheidsrisico's en voor het IoT.