Sentinels was pionieren

13 augustus 2012

Van mobiele telefoons en RFID-chips tot grootschalige bedrijfsnetwerken: prof. dr. Sandro Etalle richt zich met zijn Sentinels-onderzoek aan de Technische Universiteit Eindhoven en de Universiteit Twente en met zijn spin-off bedrijf SecurityMatters op beveiliging van allerlei soortige digitale omgevingen. Van theoretisch tot zeer praktisch: 'Want afwisseling is leuk en leerzaam.'

Hoogleraar computerveiligheid Sandro Etalle is een bezig baasje. Alleen al binnen Sentinels is hij betrokken bij 5 van de 18 projecten. Binnen het project PEARL keek Etalle met zijn groep naar RFID-chips. 'Daar liggen voor ons als beveiligingsexperts nog heel veel uitdagingen. Bepaalde fundamentele vragen zijn nog niet beantwoord. Twee belangrijke aspecten waar wij vanuit de theoriegroep in Eindhoven naar gekeken hebben zijn anonimity en unlinkablility. Je wilt gebruikers kunnen garanderen dat een aanvaller niet kan ontdekken wanneer ze waar zijn geweest. Wij hebben ons afgevraagd wat er precies nodig is om die eisen te definiëren.'

prof. dr. Sandro Etalle, projectleider van MobileIDM en PEARL en betrokken bij IPID, S-Mobile en VRIEND

Alhoewel het logisch klinkt om met zo'n vraag te beginnen, is de volgorde in de praktijk vaak anders, zegt Etalle. 'Meestal wordt er eerst een protocol gemaakt. Daarna wordt pas gekwalificeerd in welke mate dat protocol bepaalde eisen garandeert. Dat zou eigenlijk andersom moeten. Maar daarvoor moet je eerst helder hebben wat die begrippen nu precies inhouden en welke eisen je daarmee aan zo'n protocol moet stellen. Op dit moment is er nog geen grote expertise in deze definities.'

Drie terreinen

Maar PEARL is veel breder dan Eindhoven alleen, en niet alleen op theorie gericht zegt Etalle. ‘Feitelijk hebben we samen met onze collega’s van Delft en Nijmegen op drie terreinen resultaten geboekt. We hebben algoritmen ontwikkeld die kunnen bepalen hoe gevoelig een RFID-architectuur is voor aanvallen. Vervolgens hebben we nieuwe algoritmen opgesteld om die aanvallen af te weren. En we hebben laten zien dat de bestaande theorieën over anonimity en unlinkablility niet in tegenspraak zijn met elkaar, maar elkaar juist aanvullen.’

RFID-chips dringen steeds verder door in het dagelijks leven. Ze zouden op termijn streepjescodes moeten gaan vervangen. Dat stelt hoge eisen aan de veiligheid ervan. ‘Je wilt die chips op verschillende manieren kunnen beveiligen. Als iemand zo'n chip uitleest, moet hij niet kunnen zien wat er daarvoor mee gebeurd is. En hij moet ook niet kunnen ontdekken welke sleutels in de toekomst gebruikt worden om data mee te coderen. Dat noemen we backward en forward privacy: de gegevens van de gebruiker moeten zowel in het verleden als in de toekomst veilig worden gesteld.’

Deur op een kier

Ook binnen het project S-Mobile waren kleine mobiele apparaten het onderwerp van studie. ‘Iedereen loopt tegenwoordig rond met kleine apparaatjes op zak waarmee je programma's kunt downloaden. Die apparaatjes hebben een open verbinding met de buitenwereld, maar ze bevatten meestal ook gegevens die de gebruiker liever geheim wil houden. Denk aan contactpersonen op je smartphone, inloggegevens van bijvoorbeeld banksites, maar ook de inhoud van eerder verstuurde berichten via sms of whatsapp. Sommige van die programma's moeten geheime informatie gebruiken, bijvoorbeeld een telefoonnummer uit je contactenlijst, maar moeten die informatie niet verder kunnen verspreiden. Dat is een lastig probleem. Als je de deur naar die informatie helemaal op slot zou kunnen houden, is het niet zo moeilijk. Helemaal open is ook geen probleem. Maar zo op een kiertje... dan heb je een goede beveiliger nodig die precies weet wie er wel en wie er niet in mag. Daar hebben wij aan gewerkt.’

In Eindhoven wordt vooral aan de theoretische grondslagen van dit soort vraagstukken gewerkt, zegt Etalle. ‘Wij denken bijvoorbeeld na over vragen als "Wat is lekkage?" In eerste instantie denk je bij een telefoon aan het doorsturen van telefoonnummers, maar dat hoeft niet letterlijk zo te gebeuren. Soms wordt er informatie verstuurd waaruit zo'n telefoonnummer makkelijk af te leiden is. Maar dat is een stuk lastiger te detecteren, want waar moet je naar zoeken? Wij ontwikkelen technieken om ook die laatste gaatjes te kunnen detecteren en te dichten.’ S-Mobile heeft een eerste doorbraak bereikt, zegt de Eindhovense hoogleraar. ‘We zijn er als eersten in geslaagd om een klein beetje afgeleide info toe te staan, met beschikkingsrecht voor de gebruiker. Hij kan zelf aangeven of een programma bepaalde afgeleide informatie mag versturen of niet.’

Etalle waarschuwt voor te hooggespannen verwachtingen van dit soort oplossingen. ‘Let op: wij werken op een theoretisch dieper niveau, wij leveren geen kant-en-klare oplossingen voor de industrie. Dat is onze taak als universiteit ook meestal niet. Wij leveren een proof-of-concept, de industrie moet dat dan weer verder uitwerken.’

Van idee naar start-up

Dat was echter niet het geval bij het Sentinels-project IPID, waar Etalle ook bij betrokken was. Dat onderzoek leidde niet alleen tot de ontwikkeling van een product, maar ook tot een start-up die erg succesvol is. ‘Binnen IPID zoeken we naar een experimentele oplossing voor aanvallen op bedrijfsnetwerken. Daar doen we dus ook echt testen in de praktijk.’

SecurityMatters is als spin-off van de Universiteit Twente opgericht door Sandro Etalle en de iPID- en VRIEND-promovendi Damiano Bolzoni en Emmanuele Zambon. Dit bedrijf heeft een systeem ontwikkeld om aanvallen op netwerkprotocollen te detecteren. Omdat het gebaseerd is op afwijkend gedrag van het netwerk in kwestie, kan het ook compleet nieuwe zero-day aanvallen herkennen.

‘Het bedrijf gaat heel goed. We zijn nu klaar met het ontwerp en de ontwikkeling van de eerste producten, we hebben de eerste klanten. Het is een gezond bedrijf, een start-up met grote mogelijkheden.’ Etalle verklaart dat succes: ‘We hebben een universeel probleem te pakken, waar we een hele nieuwe oplossing voor hebben. Dat zie ik als een mooi succes voor de Nederlandse manier van financieren. Het Sentinels-project IPID heeft de basis gelegd. Twee briljante promovendi hebben een eerste aanzet gegeven, en de samenwerking met het bedrijfsleven vanuit de gebruikerscommissie heeft ons verder op weg geholpen. Voor ons is de steun van STW in de vorm van de Valorisation Grant heel bepalend geweest, om die fase van marktonderzoeken, productontwikkeling en dergelijke door te komen.’

Etalle is niet snel in een hokje te vangen. Van puur theoretisch academicus tot ondernemer in zijn eigen bedrijf, geïnteresseerd in alles tussen RFID-chips en complete netwerken... ‘Die afwisseling in onderwerpen en manieren van aanpak houdt je scherp. En alles vult elkaar aan. Een project als S-Mobile zal niet zo snel tot een spin-off leiden. Daarvoor is het te fundamenteel gericht. Maar die fundamenten moet je niet weggooien. Zij brengen juist de echte grote innovaties voort. IPID heeft uiteindelijk ook min of meer per ongeluk hele praktische oplossingen opgeleverd.’

Etalle kijkt met optimisme naar de toekomst. ‘Het Cyber Security research programma zie ik als een mooie opvolger van Sentinels. Toen Sentinels begon was het nog pionieren. Door Sentinels is er een gemeenschap gegroeid, de Nederlandse onderzoekers op dit terrein kennen elkaar allemaal. Er zijn nieuwe leerstoelen gekomen en we hebben een internationale naam gekregen. De maatschappij vraagt om oplossingen voor security problemen, en wij zijn er klaar voor om die aan te pakken.’

Foto: Sjoerd van der Hucht Fotografie
Tekst: Sonja Knols, IngenieuSe