Door Robert Fransen

Identity-metasystem, de missing link op internet

INTERVIEW MET RAFAL LUKAWIECKI

Een van de keynote-sprekers op de Microsoft DevDays 2006 was Rafal Lukawiecki, strategic consultant bij Project Botticelli. Tijdens zijn keynote gaf Rafal zijn visie op de huidige trends in de ICT. Zo besprak hij onder andere team-development, MSF versie 4 en domain specific languages, maar zijn interessegebied ligt voornamelijk bij alles wat met security te maken heeft. Een hobby van Rafal - voor zover je over hobby kan spreken - is cryptografie.

De DevDays 2006 was groter opgezet dan voorgaande jaren. Meer dan 2500 ontwikkelaars hebben de DevDays bezocht. Dit jaar waren er zes parallelle tracks met meer dan 50 indepth sessies. De sessies werden verzorgd door nationale en internationale sprekers. Terwijl de DevDays volop aan de gang waren, had Rafel tussen alle bedrijven door even tijd voor een kort interview, hoewel hij ook nog een sessie moest geven over WinFX security.

Je bent een veelgevraagde spreker. Je komt op de TechEd, de PDC, vandaag in Nederland en morgen weer op de DevDays in België. Is dit waar jij je brood mee verdient?

"Nee en ja", antwoordt Rafal, "ik ben er laatst achter gekomen dat mijn inkomsten uit trainingen en presentaties gegroeid zijn en nu meer dan 50% van mijn inkomsten uitmaken. Het geven van presentaties is ooit begonnen om de naamsbekendheid van onze security-practice en consultancyservice te verhogen. Het is nu een bijna een dayjob geworden. Ik geef veel presentaties en trainingen in Europa en daarbuiten, en daarvoor maak ik nu ongeveer 150 vluchten per jaar. Toch is het nog steeds de fun-part van mijn job."

Wat direct opvalt, is dat er in bijna al je presentaties een security-component zit, hoe komt dat?

"I just like security", zegt Rafal. "In mijn opinie is beveiliging de underdog in de ICT. Zelfs mensen die niets van beveiliging afweten hebben er een hekel aan. Beveiliging is moeilijk, saai, wazig en veel werk. Noem een negatief woord en mensen associëren het met beveiliging. Tijdens een presentatie voor een zaal van 170 ontwikkelaars vroeg ik laatst wie data-protection-API's (DPAPI) gebruikt om connection strings en passwords te beschermen. Tot mijn grote verbazing stak slechts één persoon zijn hand op. Hier schrok ik van. Beveiliging op de applicatielaag is namelijk belangrijker dan ooit tevoren. Zowel op het besturingsysteem als op netwerkniveau is de beveiliging de laatste jaren ingrijpend verbeterd. Het zal niet lang duren voordat de hackers zich gaan richten op applicaties. Beveiliging is niet erg geliefd bij ontwikkelaars; zelfs de ontwikkelaars bij Microsoft zijn pas vanaf 2000 serieus aan de slag gegaan en bij Apple eigenlijk pas vanaf OS X. Beveiliging heeft helaas toch nog steeds een 'uncool' imago, het is niet zichtbaar. Maar let op, dit gaat binnenkort veranderen."

Waar zit de zwakke schakel op het gebied van beveiliging? Zijn het de ontwikkelaars, de eindgebruikers, of wie?

"In het perspectief van beveiliging is iedereen een zwakke schakel. Neem het voorbeeld van een luchthaven: niemand wil dat zijn vlucht gekaapt wordt, maar ik ken ook niemand die veel plezier ondervindt van alle beveiligingsmaatregelen. We willen veiligheid, maar we hebben een hekel alle extra procedures en handelingen die nodig zijn voor een goede beveiliging. En daar zit nu juist het probleem. De uitdaging is om het heel eenvoudig te maken. Microsoft InfoCard is zo'n initiatief om het voor ontwikkelaars eenvoudig te maken. Vanuit een technologisch standpunt is InfoCard een prima technologie, maar bij acceptatie is er ook een beetje geluk nodig. Ik wens Microsoft heel veel succes en hoop van harte dat het breed geaccepteerd wordt. Zelf ben ik er erg positief over. Ik denk dat InfoCard en de onderliggende technologie de juiste weg is. Voor het eerst in de computerindustrie – en als je het breder bekijkt zelfs in mensenheugenis – is er één systeem en interface om je te identificeren bij een bank, winkel, instelling, bedrijfsnetwerk of wat dan ook."

Eén identity-system voor alles en iedereen, is dat niet de rol van de overheid?

"Nee" reageert Rafal snel. "InfoCard is een identity-metasysteem. Een identity-metasysteem bestaat uit drie componenten, te weten: 1) Subjects, mensen jij en ik; 2) Relying parties, websites, shops, banken, instanties en wie nog meer onze identity nodig heeft; en 3) Identity-providers, bedrijven en instanties die identity uitgeven en controleren.
De overheid kan optreden als een identity-provider. Als je vraagt of de overheid dé enige identity-provider moet zijn, dan is het antwoord nee. De overheid moet er één van zijn. Net zoals het niet wenselijk is dat je bij de bakker je paspoort nodig hebt om een brood te kopen, is het niet wenselijk dat je een elektronisch ID van de overheid nodig hebt als je iets wil kopen bij een willekeurige internetshop. Er is een misconceptie dat je alles met een overheids-ID moet doen. Het overheids-ID gebruik je alleen als de overheid een te rechtvaardigen partij is, bijvoorbeeld bij het doen van je belastingaangifte. Een identity-provider kan het bedrijf zijn waar je werkt, een bank, enzovoort. Of je maakt zelf een identity aan. InfoCard ondersteunt dus twee soorten identities, 'self-issued' en 'managed'. Wat betreft managed identities, is het wenselijk dat er verschillende identity-providers komen. Als ik mijn bankrekening wil bekijken zou ik een overheids-ID kunnen gebruiken, maar ik kan er ook voor kiezen om deze juist niet te gebruiken en een andere identity-provider te kiezen. Wat Microsoft tegenwoordig predikt is puurheid van technologie en provider. En dat niemand de fout maakt zoals bij Passport. Laten we eerlijk zijn, Passport is een mislukking en tegelijk een succes. Microsoft Passport is het enige systeem op de wereld dat meer dan 1 miljard authenticaties

per dag verricht. Maar tegelijk mist het de grootschalige adoptie als het universal identity-system zoals het ooit bedoeld was. Geen enkel systeem zal op deze manier succesvol zijn, ook niet Liberty van Sun Microsystems of iets dat de overheid opzet. Het zullen dus niet één identity-providers zijn, maar een veelvoud van ID's die het identity-metasystem moet ondersteunen."
Rafal gaat verder: "Kijk, in het dagelijkse leven hebben we dit systeem al in gebruik en het heeft zich in de praktijk bewezen. Als je bijvoorbeeld een huurcontract voor een woning wilt afsluiten, moet je verschillende ID's tonen. De combinatie van bijvoorbeeld je paspoort, werkgeversverklaring en bankpas moet de nieuwe huurbaas genoeg vertrouwen bieden. Tot op heden misten we een dergelijk systeem op het internet. Dit wordt ook wel de 'missing layer' van het internet genoemd. Het mooie van een identity-metasystem is dat een 'relying' party geen 100% trust/no trust-relatie nodig heeft met een identity-provider. Net zoals de huurbaas geen 1-op-1 relatie heeft met de bank of je werkgever. Het identity-metasystem biedt ook de mogelijkheid voor een relying party om bijvoorbeeld drie identities te vragen (lees te vertrouwen) van een bepaalde groep identity-providers of bijvoorbeeld twee: één van de overheid en één van een andere partij. Belangrijk is dat het voor gebruikers gemakkelijker wordt en dat ontwikkelaars niet voor elke toepassing een authenticatiesysteem hoeven te bouwen."

Hoe zit het met concurrerende technologie? Zijn er andere partijen?

"Ja, Sun Microsystems is zeker bezig, maar misschien is het beter om in plaats van Sun over OASIS te praten, waarbij aangetekend dient te worden dat Sun wel een zeer actief lid is. OASIS en Sun zijn onderdeel van een grote groep bedrijven die sponsor zijn van een verzameling security interoperability protocols WS-Security. Wat vandaag de dag het dichtst bij een identity-metasystem in de buurt komt, zijn de WS-Security guidelines. Dus per definitie ondersteunt OASIS het identity-metasystem en indirect dus InfoCard. Natuurlijk zijn er in de toekomst bedrijven die denken geld te kunnen verdienen aan het opzetten van een identity-system, maar ik denk niet op basis van het principe van een identity-metasystem. Bovendien heeft Microsoft het open opgezet. Er is geen security-standaard gekozen, maar in plaats hiervan is er een metastandaard gebruikt; een niveau hoger dus. Hierdoor heb je de vrije keuze om zelf de protocollen te kiezen. Op dit niveau zal en kan niemand er tegen zijn. Wel verwacht ik tegenwerking ten aanzien van de user-interface van InfoCard. De InfoCard identity-selector is namelijk een specifieke implementatie. Er zullen vast andere komen - en dat is naar mijn mening niet verkeerd - maar Microsoft loopt duidelijk voorop met InfoCard."

Wordt dat niet verwarrend voor de eindgebruiker als er verschillende interfaces komen?

"Ja, dat wel, maar het is interessant om te zien hoe dit zich gaat ontwikkelen. Ik maak me er geen zorgen om, want de onderliggende protocollen zijn uniform. Eigenlijk ben ik best blij dat Microsoft zo'n grote installed base heeft, want brede acceptatie is wat de wereld nu nodig heeft. Je mag me quoten, want er zijn situaties wanneer een monopoliepositie negatief kan uitpakken. In dit geval zijn we allemaal gebaat bij grootschalige acceptatie. InfoCard is iets waar Microsoft de wereld een dienst mee kan bewijzen. Neem nu het voorbeeld GSM. Het slaagde alleen in Europa, in Amerika is het er nog steeds niet en het is een zooitje. Trouwens een erg duur zooitje. Zo'n bende is het nu ook op het internet met allerlei verschillen inlog- en autenticatiesystemen. Daar moet eenheid in komen, zodat gebruikers niet allerlei lijsten moeten bijhouden met gebruikersnaam en wachtwoord voor elke website die ze willen bezoeken. Voor het eerst stagneert de groei wat betreft het aantal online aankopen in de USA. Het vertrouwen van gebruikers neemt af. Gebruikers zijn voorzichtig geworden met het doorgeven van creditcardgegevens. En terecht. Kijk maar eens op www.antiphishing.org. Het aantal phishing attacks neemt almaar toe met een nieuw record in maart 2006. We moeten het vertrouwen terug brengen met een solide identity-metasystem."

Rafal Lukawiecki tijdens de keynote op de DevDays 2006.

Waarom is InfoCard interessant voor ontwikkelaars?

"Je moet het bekijken vanuit het perspectief van de ontwikkelaar, de gebruiker en de community", zegt Rafal. "Het grote voordeel voor ontwikkelaars is dat ze met InfoCard een duidelijke en gemakkelijke interface krijgen voor iets dat normaal erg moeilijk is. Een identity-selector bouwen is niet eenvoudig en je kunt er snel de fout mee ingaan. Met InfoCard wordt het heel simpel om een identity-selector te implementeren. Wat eindgebruikers betreft, daar ligt het grootste voordeel. Gebruikers krijgen namelijk een eenvoudige en eenduidige interface voor alle identity-processen. Bovendien is het voor de thuisgebruiker helder of ze kritische data doorgeven of slechts een gebruikersnaam en wachtwoord-combinatie. De metafoor die getoond wordt, is een paspoort, geld en een portefeuille (wallet). Erg gaaf en allemaal heel herkenbaar voor de gebruiker."

Al vanaf IE3 is een wallet onderdeel van de browser, dit is toch niet weer een wallet die niemand gebruikt?

"Nee, dit is geen nieuwe wallet zoals we die kennen in browsers. Elke browser heeft een eigen wallet, Firefox heeft een wallet, ook Internet Explorer, Safari van Apple, Opera weer eentje, noem maar op en ze zijn allemaal mislukt wat betreft adoptie. Dat komt omdat ze niet gebaseerd zijn op de 'seven laws van identity metasystems'. Eén van die wetten zegt namelijk dat de wallet - of hoe je ze ook noemt - open en puur moet zijn qua technologie. Dat zijn de wallets in de browsers niet. De wallet in Opera kun je namelijk alleen in Opera gebruiken en nergens anders. Deze wallets zijn niet door andere applicaties te gebruiken, de gebruiker moet altijd in controle zijn en de identity moet een directed identity zijn die niet reusable is. Kortom, wallets in browsers zijn niet de oplossing. Als je meer wilt weten over de seven laws van identity-metasystems is er een goede blog van Kim Cameron op www.identityblog.com.

Waar komt de beveiligingsfascinatie eigenlijk vandaan?

"Ik weet nog dat ik als negenjarige jongen het boek van Silverman over security aan het lezen was. Dat was natuurlijk vrij ongewoon voor een jongen op de basisschool in Polen. Security was vooral het domein van de mainframes. Ik las het boek van voor naar achter en er was één puzzel die ik niet kon oplossen. Hoe verberg je de key die je bij cryptografie gebruikt in je software? Eigenlijk is dit nog steeds een heel lastig."

Referenties

http://msdn.microsoft.com/winfx/reference/infocard

Online security training van Rafal Lukawiecki op ITs Showtime:

www.microsoft.com/netherlands/technet/itsshowtime/result_search.aspx?speaker=16