Baas in eigen box

8 augustus 2012

Hoe wissel je via een serviceprovider informatie uit met iemand anders, zonder dat die provider kan meelezen? Daar draaide het om in het Sentinels-project Kindred Spirits. Prof. dr. ir. Inald Lagendijk vertelt over de uitdagingen in het beschermen van de privacy in een digitaliserende wereld. Hoe ver moet je de deur openzetten, en hoe houd je die nieuwsgierige buurvrouw buiten?

'Als je op netwerksites als LinkedIn of Facebook zit, krijg je vaak aanbevelingen als “Wellicht kent je deze persoon ook?”. Of als je iets bestelt op een site als bol.com, krijg je een melding dat andere mensen die datzelfde boek bestelden, ook geïnteresseerd waren in boek X en Y en cd Z. Om die aanbevelingen te kunnen doen, moet een service provider zoals zo'n webwinkel behoorlijk veel van je weten. Zoals je aankoop- en zoekgeschiedenis. Maar daar geef je zelf eigenlijk niet expliciet toestemming voor, en daarmee is het gebruik van die gegevens feitelijk een inbreuk op je privacy. Wij hebben ons beziggehouden met de vraag hoe we ervoor kunnen zorgen dat zo'n serviceprovider die aanbevelingen kan doen, zonder dat hij zelf jouw gegevens kan lezen.’

Prof. dr. ir. Inald Lagendijk, projectleider van Kindred Spirits

In het project Kindred Spirits werkten de Technische Universiteit Delft en de Universiteit Twente samen met de bedrijven Irdeto, Philips en TNO aan oplossingen. Eindgebruikers Buurtlink, PAIQ, Waag Society en Bureau Promotie Podiumkunsten gaven al vroeg in het project aan waar voor hen de vragen lagen.

Veiligheidsgarantie

‘Oorspronkelijk hadden we een iets andere onderzoeksrichting voorzien,’ zegt Lagendijk, ‘maar in overleg met de eindgebruikers kwamen we al heel snel op deze lijn uit. In plaats van het ontwikkelen van een protocol waarmee je verschillende schillen van privacy rondom een netwerk kunt aanleggen, hebben

we ons meer gericht op het versleutelen van de informatie die gebruikers van zo'n netwerk uitwisselen. De eindgebruikers wilden vooral hun klanten kunnen garanderen dat hun persoonlijke informatie goed beschermd zou zijn en blijven.'

Binnen het project zijn twee concrete cases bestudeerd, die door de participerende bedrijven werden ingebracht. Een van de betrokken bedrijven was Irdeto. 'Zij werken onder andere aan de beveiliging voor set top boxen voor televisies. Dus van die kastjes waarmee je bijvoorbeeld betaald films kunt kijken bij je thuis. Op basis van films en programma's die je in het verleden hebt besteld, wil een provider als Ziggo of UPC je aanbevelingen kunnen doen van producten die je dan misschien ook wel interessant vindt. Het kijkgedrag en de interessen van de klant moet dus ergens bekend zijn. Maar dat hoeft die provider van diensten dan weer niet te weten. De centrale vraag voor ons was: hoe kunnen we een systeem maken dat werkelijk anoniem aanbevelingen kan maken, dus zonder dat het weet wat de klant in kwestie precies heeft gezien.'

Die anonimisering was voorheen nog niet zo goed geregeld, zegt de Delftse hoogleraar Multimedia Signal Processing. 'Vaak was informatie nog redelijk makkelijk te herleiden naar individuele bronnen.' Versleuteling bleek het toverwoord. 'We hebben een protocol ontwikkeld waarin bijvoorbeeld je voorkeur voor films versleuteld terechtkomt in een hele bak met films. Daarin wordt gezocht naar overeenkomsten, die ook weer versleuteld naar de consument thuis – bijvoorbeeld via zo'n set top box op de televisie – worden verstuurd. Pas als die informatie bij de ontvanger is aangekomen, wordt hij weer gedecodeerd. Dus alleen bij jou thuis is er daadwerkelijk inzicht in welke films jij al hebt gezien, en wat de inhoud van jouw aanbeveling is. In die hele weg daartussen kan niemand die informatie achterhalen.'

Medische gegevens

De andere case kwam uit de medische hoek. Aanjager daarvoor was Philips. 'Zij zijn geïnteresseerd in het aanbieden van platforms waarop medische informatie kan worden uitgewisseld en waarop gezondheidsaanbevelingen gedaan kunnen worden op basis van medische informatie. Tussen patiënten bijvoorbeeld, maar ook tussen arts en patiënt. Dat gaat over persoonlijke zaken: iemands medische gegevens. De intermediair – in dit geval apparatuur van Philips – wil helemaal niet weten wat de content is die hij verstuurt, maar moet er wel inhoudelijk iets mee kunnen doen.'

Aan hetzelfde bord

Om een goede samenwerking met de verschillende partners tot stand te brengen, zaten promovendi van de universiteit een aantal maanden intern bij de partners uit de industrie. Dat werkt goed, zegt Lagendijk. 'Dat heb ik jaren geleden al geleerd. Uiteindelijk kun je alleen maar echt samenwerken als je regelmatig in hetzelfde kantoor zit en voor hetzelfde bord staat om dingen te bespreken. De denkomgeving in een bedrijf is totaal anders dan op een universiteit, en dat ervaar je pas echt door er een tijdje in mee te draaien. Soms levert dat ook wel spanningen op. Een promotietraject stelt nu eenmaal andere eisen dan een productontwikkelingstraject. Maar als je op basis van

gelijkwaardigheid samenwerkt, kan elke partij zijn eigen doelstellingen daarin halen.’

Alhoewel er al een mooi resultaat ligt, is er nog genoeg werk te doen. ‘We hebben laten zien dat de technologie in principe werkt. Maar op dit moment vergt de versleuteling nog veel rekentijd. Dat betekent dat het bijvoorbeeld een minuut duurt voordat je een aanbeveling op je scherm krijgt. Dat is nog te lang. Daarnaast is er een belangrijke keerzijde aan het huidige protocol: we hebben het nu zo gemaakt dat de klant gegarandeerd een maximale privacy geniet, maar dat betekent dat de provider totaal geen toegang heeft. Hij kan dus ook geen extra services verlenen, wat de business case bemoeilijkt. We moeten nog zoeken naar een middenweg: hoe krijgt de provider wat hij nodig heeft om er geld mee te kunnen verdienen, zonder dat de privacy van de kant geschaad wordt? Een deel van deze vragen pakken we op in een vervolgproject binnen het COMMIT-programma, dat zich vooral op de medische toepassingen zal richten.’

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