Cryptografie als privacybescherming

Drs. Wouter Teepe, promovendus bij de groep kunstmatige intelligentie aan de RUG

De veronderstelling dat privacy en terrorismebestrijding onverenigbare belangen zijn, is onjuist. Het is mogelijk de privacy van vliegtuigpassagiers te beschermen en tegelijk vluchtgegevens uit te wisselen met de Verenigde Staten om terroristen te weren.

Dit opinieartikel is eerder verschenen in het Financieele Dagblad (15 augustus 2005)

De mogelijkheid om de privacy van goedwillende burgers te waarborgen is te danken aan een nieuwe ontwikkeling binnen de vakgebieden van het geheimschrift —cryptografie — en de kunstmatige intelligentie. Neem de lijst met verdachten van terrorisme van de VS en een KLM-lijst van haar passagiers op een vlucht naar of over de VS. Met behulp van nieuwe cryptografische methoden kunnen zij achterhalen wat de overlap is tussen hun lijsten, waarbij de stukken van de lijsten die niet overlappen voor de andere partij geheim blijven. Dit is de oplossing voor het zogeheten lijst-intersectieprobleem.

Deze oplossing kan overal worden toegepast waar lijsten van gezochte personen (*watchlists*) worden gebruikt. Terwijl er politieke consensus is over het opsporen en ontmaskeren van terroristen, is er veel ontevredenheid over de praktijk waarin de privacy van goedwillende burgers evenveel wordt geschaad als die van gezochte terroristen. Deze nieuwe protocollen garanderen de privacy van de goedwillende burgers, terwijl de functionaliteit voor het vinden van gezochte personen gelijk blijft.

De situatie is nog het best te vergelijken met het roddelprobleem: twee mensen willen roddelen over een derde —'Geertje is zwanger'— maar willen niet degene zijn die de ander als eerste vertelt dat Geertje zwanger is. Als de twee roddelaars niet weten of de ander het weet, moeten ze elkaars voorkennis aftasten. Hengelen zonder door te laten schemeren waarin je geïnteresseerd bent is erg moeilijk, en zonder cryptografie leiden zulke aftastende gesprekken altijd tot het lekken van op zijn minst enige informatie, al is het maar dat er een roddel over iemand bestaat.

In veel meer situaties ligt het uitwisselen van informatie gevoelig, zoals tussen politiekorpsen en veiligheidsdiensten, of tussen medische hulpverleners voor het vinden van medische dossiers. Kenmerkend voor dit soort situaties is dat de partijen in principe coöperatief willen zijn, maar tegelijkertijd, om valide redenen, de wederpartij niet alle vertrouwelijke informatie kunnen geven.

De oplossing voor het lijst-intersectieprobleem maakt gebruik van cryptografische vingerafdrukken, waarmee van stukjes informatie zoals een naam een digitale vingerafdruk wordt gemaakt, die alleen maar voor de wederpartij herkenbaar is als de wederpartij de naam ook kent. Door op een slimme manier alleen maar vingerafdrukken van namen te communiceren, in plaats van de namen zelf, kan de veiligheid van de lijst gegarandeerd worden. Er is geen derde, alwetende en betrouwbare partij nodig. Zelfs voor partijen die elkaar slechts zeer beperkt vertrouwen biedt dit een oplossing zonder veel administratieve rompslomp.

Strijd tegen terreur en privacy gaan wél goed samen

In de discussie over de uitwisseling van passagiersgegevens gingen Europa en de VS er van uit dat er geen oplossing voor het lijst-intersectieprobleem bestaat, en dat dus een keuze tussen privacy en terrorismebestrijding gemaakt moet worden. Uiteindelijk hebben de partijen de privacy van goedwillende burgers geofferd. Maar dat hoeft niet. Omdat met deze nieuwe technieken terrorismeverdachten even makkelijk kunnen worden opgespoord, zijn er geen redenen om deze technieken niet toe te passen. ø