Irma brengt persoonsgegevens efficiënt en privacyvriendelijk naar chipkaart

Onder leiding van de Radboud Universiteit Nijmegen werkt het Irma-project aan een privacyvriendelijke oplossing voor het beheer van persoonsgegevens op een chipkaart. Onderzoeker Jaap-Henk Hoepman vertelt hoe.

Jaap-Henk Hoepman

Als je drank of sigaretten wilt kopen, moet je aantonen dat je ouder bent dan achttien. In de winkel doe je dit simpelweg door je paspoort of identiteitskaart te laten zien. Tenzij de kassière een fotografisch geheugen heeft, zal ze je naam of adres niet onthouden. Op internet is dit lastiger. Van een digitaal paspoort kunnen webwinkels eenvoudig een kopie maken. Sterker nog: ze zullen moeite moeten doen om alle irrelevante informatie niet op te slaan. Toch is het ook online belangrijk dat je op een privacyvriendelijke manier kunt aantonen dat je ouder bent dan achttien.

Een belangrijke reden is het voorkomen van identiteitsfraude. Ook in het digitale domein kunnen criminelen een kopietje paspoort misbruiken om op jouw naam bijvoorbeeld een lening of een mobiel abonnement af te sluiten. Maar net zo belangrijk is bescherming van de privacy zelf. Zonder contextscheiding zou informatie over je privéleven (ziektes, je seksuele en politieke voorkeuren) zonder jouw medeweten haar weg kunnen vinden naar je werkgever, je collega's of je zorgverzekeraar. Zo zijn er nog veel meer redenen waarom adequate privacybescherming belangrijk is en ook bij wet is geregeld.

ABC's

Iedere persoon heeft een groot aantal kenmerken, zoals naam, adres, leeftijd, haarkleur, bloedgroep, allergieën, politieke overtuiging, lidmaatschap van de voetbalclub, abonnement op een tijdschrift, enzovoorts. Dit noemen we attributen. Sommige hangen af van de context. Mijn privételefoonnummer verschilt bijvoorbeeld van het nummer op mijn werk. Alle attributen die een persoon binnen een specifieke context beschrijven, noemen we zijn identiteit (binnen die context) en het technisch beheer van de attributen heet identiteitsmanagement.

Er zijn meerdere systemen voor identiteitsmanagement, die verschillen in de mate van veiligheid en privacybescherming die ze bieden. Een zeer veilige en privacyvriendelijke variant is gebaseerd op *attribute-based credentials* (ABC's). Zo'n credential is een veilige container die een aantal attributen bevat. Credentials worden uitgegeven door *issuers*, die instaan voor de waarde van de attributen. Zo zou de Gemeentelijke Basisadministratie een credential uit kunnen geven waarin mijn naam, adres en geboortedatum als attributen zijn opgeslagen.

ABC's hebben twee eigenschappen om de privacy van de houder te beschermen. De eerste, *selective disclosure*, maakt het mogelijk om slechts een selectie van de attributen in één credential daadwerkelijk te tonen. De webwinkel ziet alleen daarvan de waarde en komt over de andere attributen niets te weten. Vergelijk het met de kassière die alleen de leeftijd verifieert.

De tweede eigenschap, *unlinkability*, zorgt ervoor dat credentials onherkenbaar zijn iedere keer dat ze worden gebruikt. Als hetzelfde credential meerdere keren voorbijkomt bij een webwinkel, zal deze dit in principe telkens als een ander, nieuw, credential zien. Merk hierbij op dat deze bescherming teniet wordt gedaan als het attribuut dat je iedere keer toont je naam of telefoonnummer is.

Er zijn ruwweg twee concurrerende systemen voor ABC's die unlinkability ondersteunen: U-Prove (van Microsoft) en Idemix (van IBM). Het nadeel van U-Prove is dat een credential maar één keer kan worden gebruikt. Bij hergebruik is het credential alsnog *linkable*. De gebruiker moet dus iedere keer een nieuw credential aanvragen bij de issuer. Beiden moeten hiervoor on-

Op de buitenkant van de Irma-kaart staat slechts een pasfoto van de houder, voor offline gebruik, en retourinformatie.

line zijn. Idemix heeft dit nadeel niet, maar is als gevolg daarvan iets complexer.

Chipkaart

In het Irma-project (I Reveal My Attributes) werken de Radboud Universiteit Nijmegen, TNO en Surfnet aan een privacyvriendelijk systeem voor identiteitsmanagement op basis van ABC's. Daarbij hebben we gekozen voor een implementatie met Idemix omdat een deel van de oplossingen die wij voorzien offline is. Denk aan de vervanging van de *age coin* bij sigarettenautomaten of het gebruik van ABC's als privacyvriendelijk alternatief voor de ov-chipkaart.

Idemix gebruikt een zogeheten *zero-knowledge*-protocol. Dit stelt de houder in staat om aan een webwinkel te bewijzen dat hij een credential bezit, ondertekend door de issuer en met de aangegeven waardes voor de attributen, zonder het zelf te tonen. Het credential blijft dus geheim en kan opnieuw worden gebruikt.

Credentials zijn persoonsgebonden en alleen de houder moet ze kunnen gebruiken. Om eigendom binnen Idemix te bewijzen, is de bijbehorende privésleutel nodig. De meest veilige plek om die op te slaan, is op een chipkaart. In het Irma-project doen we dit daarom ook.

De Irma-kaart slaat de sleutel en de credentials veilig op op de chip. Op de buitenkant staat slechts een pasfoto van de houder, voor offline gebruik. Online is er een pincode die de binding van de kaart met de houder verzekert. Het extra voordeel van de chipkaart is dat het onmogelijk is om credentials van verschillende gebruikers samen te brengen. Dit voorkomt dat iemand kan bewijzen een dertigjarige Nederlander te zijn op basis van het credential van een minderjarige Nederlander en een dertigjarige Fransman.

NFC

De kern van het Irma-project is de efficiënte implementatie van ABC's op een chipkaart. Vanwege de complexe cryptografische berekeningen die nodig zijn en de beperkte beschikbaarheid van rekenkracht en Ramgeheugen op de kaart is dit een behoorlijke uitdaging. Eerdere pogingen maakten gebruik van shortcuts, door bijvoorbeeld een deel van de berekeningen op de kaartlezer of de pc uit te voeren, wat de veiligheid en privacy vermindert. Pim Vullers van de Radboud Universiteit is erin geslaagd alles volledig op de kaart te implementeren.

We gebruiken de SLE 78-chipkaart van Infineon met een MultOS-omgeving, waarvan de crypto-Api toegang geeft tot alle functionaliteit van de crypto-coprocessor. We hebben het in eerste instantie geprobeerd op NXP's SmartMX-chip met Javacard, maar dat mislukte omdat de cryptografische Api van Javacard beperkt is tot de standaard algoritmes. Een groot deel van de wiskundige berekeningen die de cryptografische coprocessor op de chipkaart supersnel kan uitvoeren, is daardoor niet toegankelijk voor applets die op de kaart draaien.

Onze implementaties zijn behoorlijk efficiënt: de tijd om een credential te tonen, ligt, afhankelijk van het aantal weergegeven attributen, tussen de negen- en vijftienhonderd milliseconden. Dat is wel een record te noemen. Het is echter nog niet snel genoeg voor commercieel gebruik binnen bijvoorbeeld het openbaar vervoer. Zo houdt Trans Link Systems, van de ov-chipkaart, een maximale kaarttransactietijd aan van 350 ms. We komen echter in de buurt en zijn zeker al snel genoeg voor webtransacties.

De Infineon-chipkaart heeft zowel een contact- als een contactloze interface. Dat maakt het mogelijk om gegevens uit te wisselen via NFC. Een steeds groter aantal mobiele apparaten heeft zo'n interface. Binnen Irma gebruiken we de Google Nexus-smartphone en de Google Nexus 7-tablet. Deze apparaten draaien stand-alone apps, maar kunnen ook fungeren als kaartlezer voor een pc.

QR

Zonder middleware en applicaties is een Irma-kaart met credentials niet in de praktijk te gebruiken. Daarom hebben we zelf ook een aantal toepassingen ontwikkeld. Met onze kaartmanagementapp kan een gebruiker de credentials op zijn kaart beheren. Hij kan zien welke credentials erop staan, en er eventueel een verwijderen. Daarnaast geeft de app een overzicht van de log die de kaart bijhoudt. Zo kan een gebruiker nagaan welke dienstenaanbieders toegang hebben gehad en welke attributen uit welke credentials zijn opgevraagd. Dit is een van de manieren waarop we het lastig maken om ongemerkt meer informatie te verzamelen dan nodig is.

Een van de *use cases* binnen Irma is het geven van korting op koffie in de kantine voor de studenten van het Kerckhoffs Instituut, onze masteropleiding security. Hiervoor hebben we de *card verifier*-app ontwikkeld. Deze draait op een tablet die naast de kassa van de kantine staat en kan via NFC het studentcredential op een Irma-kaart uitlezen en het resultaat van de controle duidelijk aangeven. De student hoeft enkel zijn kaart tegen de tablet aan te houden. In de toekomst kan deze functionaliteit ook in pinapparaten worden geïntegreerd, waardoor een apart kastje overbodig is.

Daarnaast hebben we een *card proxy*-app gemaakt. Die maakt het mogelijk om een smartphone te gebruiken als Irma-kaartlezer voor een willekeurig apparaat, bijvoorbeeld een pc. Voor de verbinding tussen computer en telefoon gebruiken we QR-codes. Als een gebruiker een attribuut wil laten verifiëren bij een website, scant hij de op de inlogpagina van die site getoonde QR-code. Hierin staan een sessie-*identifier* en een URL waarmee de smartphone contact moet opnemen. De telefoon vraagt vervolgens om de Irma-kaart en zet een verbinding op met de server in de URL. Die server kan nu direct met de kaart communiceren en het attribuut verifiëren alsof er een gewone kaartlezer aan de pc hangt. Wel heeft de smartphone hiervoor een internetverbinding nodig. De card proxy-app is op min of meer dezelfde manier ook te gebruiken om nieuwe credentials op een Irma-kaart te laden.

De keuze voor QR maakt dat het niet nodig is om speciale drivers te installeren op de pc. Het werkt dus vanaf een willekeurige computer. De gebruiker hoeft slechts eenmalig de card proxy-app op zijn smartphone te zetten. Overigens is het ook gewoon mogelijk om een kaartlezer aan te sluiten op de pc en via die weg de Irma-kaart op het web te gebruiken.

Jaap-Henk Hoepman is senior onderzoeker bij TNO en de Radboud Universiteit Nijmegen. Meer informatie over de ABC-implementatie binnen het Irma-project is te vinden op www.irmacard.org. *De broncode is openbaar en beschikbaar via* www.github.com/credentials.

Redactie Nieke Roos