Samenvatting

Het thema van de bescherming van persoonsgegevens is actueler dan ooit. Een paradoxale eigenschap van persoonsgegevens is dat zowel het geheim houden, als het uitwisselen ervan gedaan kan worden onder het argument van 'veiligheid'. Het geheim houden van persoonsgegevens verhoogt veiligheid doordat deze gegevens niet misbruikt kunnen worden. Het uitwisselen van persoonsgegevens verhoogt veiligheid omdat het opsporingsdiensten helpt criminelen en terroristen te vangen. Zowel de argumenten voor het geheim houden van gegevens, als die voor het uitwisselen van gegevens zijn valide.

Het probleem is helder: het uitwisselen van gegevens en het geheim houden van gegevens lijkt niet, of althans moeilijk, samen te kunnen gaan.

Dit is niet alleen een probleem in de discussie tussen de voorvechters van privacy en de voorstanders van verregaande opsporingsbevoegdheden. Ook opsporingsdiensten zelf worstelen met het spanningsveld van uitwisseling versus geheimhouding: het is makkelijker een subject (bijvoorbeeld een verdachte) in de gaten te houden als hij of zij daar niet op beducht is. Wanneer het subject weet dat hij onderwerp van onderzoek is, kan hij of zij bijvoorbeeld mogelijk bezwarende bewijzen vernietigen. Hoe meer mensen binnen een opsporingsorganisatie weet hebben van een lopend onderzoek, hoe groter de kans is dat er gelekt wordt naar het subject. Aan de andere kant, hoe meer mensen binnen opsporingsdienst weet hebben van een lopend onderzoek, hoe meer mensen kunnen meehelpen met dat onderzoek.

Het hoofddoel van dit proefschift is om te onderzoeken of het mogelijk is om oplossingen voor dit spanningsveld te vinden. De resultaten van het onderzoek zijn van fundamentele en praktische waarde. Aan de fundamentele kant laten we zien, dat een een aantal problemen überhaupt oplosbaar is. Aan de praktische kant laten we zien dat deze oplossingen niet slechts theoretisch zijn, maar ook zonder al te veel problemen kunnen worden toegepast om bestaande, praktische problemen op te lossen. De oplossingen die gepresenteerd worden in dit proefschift bieden beleidsmakers de ruimte om de bescherming van privacy enerzijds, en het uitwisselen van persoonsgegevens voor terrorismebestrijding anderzijds, goed samen te laten gaan. In plaats van of/of, is er de mogelijkheid voor en/en, als de beleidsmakers het willen.

Enige relativering is hierbij wel op zijn plaats. Niet *alle* problemen rondom privacy en uitwisseling van persoonsgegevens kunnen worden opgelost, slechts *enkele*. Er is echter geen enkele reden om te veronderstellen dat dit proefschrift de mogelijkheden om dit type problemen op te lossen, heeft uitgeput. Dit proefschift is slechts een begin: we laten zien dat het überhaupt mogelijk is dit type problemen op te lossen; toekomstig onderzoek kan het palet van oplossingen verder uitbreiden.

In hoofdstuk 1 bespreken we de context van het onderzoek: welke maatschappelijke kwesties zijn er, waarbij zowel geheimhouding als uitwisseling van persoonsgegevens kan geschieden onder het motto van 'veiligheid'? Wat hebben deze kwesties gemeen? Ook wordt er van een praktijktoepassing uit de doeken gedaan hoe deze uitwisseling op het moment georganiseerd is. Deze toepassing is het uitwisselen van opsporingsinformatie tussen regiokorpsen van de Nederlandse politie. Verder besteden we aandacht aan de vraag of centrale opslag van persoonsgegevens wenselijk is. Uiteraard wordt in hoofdstuk 1 de structuur van dit proefschrift nader uitgelegd.

Omdat de lezer wellicht niet vertrouwd is met de theoretische achtergronden die te maken hebben met 'computerbeveiliging', bevat hoofdstuk 2 een bondige samenvatting en uitleg van veel begrippen en onderzoeksvelden waar dit proefschrift veelvuldig naar verwijst. Daaronder valt een aantal relatief brede onderwerpen, zoals encryptie, authorisatie, authenticatie, complexiteitstheorie en probabilistische algorithmen, maar ook een aantal vrij specialistische onderwerpen, zoals *oblivious transfer*, *secure multiparty computation* en *zero-knowledge proofs*.

De *cryptografische hashfunctie* heeft een dermate belangrijke rol in dit proefschrift, dat hoofdstuk 3 in zijn geheel gewijd is aan het bespreken van de eigenschappen van de cryptografische hashfunctie. Kort gezegd is een cryptografische hashfunctie een gereedschap om een soort vingerafdruk te maken van een blok gegevens. Deze vingerafdruk kan gebruikt worden om de informatie te identificeren of te herkennen, maar verklapt verder niets over die gegevens. Technisch gezien heeft het nogal wat voeten in de aarde om precies te definiëren wat een cryptografische hashfunctie is, en hoe je er eentje zou moeten maken. In dit kader bespreken we *niet-incrementaliteit*, een nieuwe, optionele eigenschap van cryptografische hashfuncties.

Een ander belangrijk gereedschap zijn *authenticatielogica's*, dat zijn logica's waarmee je *cryptografische protocollen* kunt analyseren. In hoofdstuk 4 wordt uitgelegd hoe authenticatielogica's in elkaar zitten en hoe je ze kunt gebruiken. De oudste authenticatielogica is BAN-logica, en andere authenticatielogica's, zoals GNY-logica, zijn afgeleid van BAN-logica.

In hoofdstuk 5 laten we zien dat BAN-logica een fout bevat. Deze fout in BAN-logica is dat cryptografische hashfuncties niet juist gemodelleerd worden. Dit demonstreren we aan de hand van een vrij eenvoudig protocol. Door deze fout blijkt het mogelijk om binnen BAN-logica om uit ware feiten onjuiste feiten af te leiden, wat natuurlijk zeer ongewenst is. Andere authenticatielogica's, zoals GNY-logica, bevatten deze fout niet.

Authenticatielogica's zijn niet altijd helemaal geschikt om bepaalde protocollen te analyseren. Ook de protocollen die in dit proefschrift worden geanalyseerd kunnen niet zonder meer geanalyseerd worden. Om een analyse toch mogelijk te maken, breiden we in hoofdstuk 6 de GNY-logica zó uit, dat het geschikt is voor onze doeleinden. De modellering van bepaalde eigenschappen van cryptografische hashfuncties wordt toegevoegd aan GNY-logica. Ook maken we een aantal zaken in GNY-logica preciezer, waardoor een nauwkeuriger analyse van protocollen mogelijk is.

Het daadwerkelijke beschermen van (persoons)gegevens is het onderwerp van hoofdstuk 7. Het beschermen van persoonsgegevens wordt moeilijk gemaakt door de wens vele informatiebronnen en databases aan elkaar te koppelen. Een gebruikelijke manier om die koppeling tot stand te brengen is het royaal toegang geven tot databases. Wij stellen een geheel andere aanpak voor, waarbij informatie juist zoveel mogelijk geïsoleerd wordt. Deze isolatie helpt bij de bescherming van de gegevens, maar óók bij het efficiënt koppelen van de databases. Centraal in onze aanpak staat de *information designator*, een soort pseudoniem voor informatie.

Kennisauthenticatie, het vergelijken van gegevens (geheimen) zonder deze te lekken is het onderwerp van hoofdstuk 8. Er wordt in kaart gebracht waaraan een communicatieprotocol moet voldoen om de vraag 'Ken jij de geheimen die ik ken?' correct te kunnen beantwoorden — zonder dat de geheimen zelf vrijgegeven worden, natuurlijk. Een aantal subtiele maar op essentiële punten verschillende variaties van dit probleem worden uitgelegd. Een belangrijke variatie is of *één* geheim wordt vergeleken met *vele* geheimen ('1-to-many'), of dat *vele* geheimen worden vergeleken met *vele* geheimen ('many-to-many').

In hoofdstuk 9 presenteren we het nieuwe T-1 protocol, dat op zeer efficiënte wijze 1-to-many kennisauthenticatie implementeert. Het T-1 protocol maakt intensief gebruik van cryptografische hashfuncties. Er is een variant waarin alleen maar cryptografische hashfuncties gebruikt worden, en een efficiëntere variant waarin ook encryptie gebruikt wordt als bouwsteen. Het T-1 protocol wordt geanalyseerd in de uitgebreide versie van GNY-logica.

Het T-2 protocol, dat we presenteren in hoofdstuk 10, is een nieuw en efficiënt protocol voor many-to-many kennisauthenticatie. Hiermee is het mogelijk de overlap tussen twee lijsten te bepalen, zonder dat bekend wordt wat er *buiten* het overlappende deel zit. Het T-2 protocol is een parallelle compositie van het T-1 protocol waarbij een aantal optimalisaties is toegepast. De belangrijkste optimalisatie is het gebruik van *prefix trees* om de hoeveelheid te communiceren bits te verkleinen.

Hoofdstuk 11 is de conclusie van dit proefschrift, waarin alle resultaten van het onderzoek netjes op een rij worden gezet, en aanbevelingen voor vervolgonderzoek worden gedaan.