Cryptologie : theorie en praktijk van de moderne informatiebeveiliging

Cryptologie, Theorie en Praktijk van de Moderne Informatie-beveiliging

INTREEREDE

Prof.dr.ir. C.J.A. Jansen

Technische Universiteit Eindhoven

INTREEREDE

Uitgesproken op 30 oktober 1998
aan de
Technische Universiteit Eindhoven

Prof.dr.ir. C.J.A. Jansen

Mijnheer de Rector Magnificus, dames en heren,

Steeds vaker krijgt de consument te maken met producten en diensten waarin cryptografie toegepast wordt. Voorbeelden hiervan die bijna iedereen kent, zijn: de GSM telefoon en de draadloze (DECT) telefoon in de huiskamer, de elektronische betaalpas en het telebankieren. Het merendeel van de gebruikers van deze toepassingen realiseert zich echter niet dat hier sprake is van elektronische informatie die kwetsbaar is en dat er risico's verbonden zijn aan het gebruik. Men weet in het algemeen niet dat er cryptografische technieken toegepast worden om belangrijke informatie te beveiligen, laat staan dat men weet wat cryptografie is.

In mijn betoog wil ik een aantal aspecten belichten van de praktijk van de moderne informatiebeveiliging. Cryptografie speelt hierbij een belangrijke rol. Ik zal u iets vertellen over de relatie tussen cryptografie en informatiebeveiliging, de kenmerken van klassieke en moderne cryptografische systemen en me wagen aan een blik in de toekomst van de cryptologie. Vervolgens zal ik de situatie op de Information Super Highway, het internet, nader beschouwen. Tenslotte zal ik wat dieper ingaan op het belang van sleutelbeheer en symmetrische cryptografische bouwstenen voor de moderne informatiebeveiliging.

Cryptografie en awareness

Dames en Heren,

De afgelopen jaren heb ik voor diverse gehoren de vraag gesteld: "Wat is cryptografie?", met als bedoeling een introductie te geven op de voor velen zo abstracte en complexe materie van de cryptografische informatiebeveiliging. Ik heb het vervolgens trachten uit te leggen aan de hand van voorbeelden van cryptografische systemen, met behulp van formele definities zoals gehanteerd door Shannon in zijn publicatie uit 1949 [1], of op een meer technische manier door blokschematische voorstellingen van zogenaamde vercijfersystemen. De technisch opgeleide toehoorder is hier duidelijk in het voordeel: hij of zij heeft geleerd te denken in modulaire concepten en interfaces tussen de verschillende modules of blokjes. Het is mij daarbij mogelijk gebleken om een vrij volledige introductie cryptologie te verzorgen gebruik makend van slechts twee à drie ovehead sheets, waarbij de wiskundige diepgang redelijk nauwkeurig af te stemmen was op het niveau van het gehoor.

Deze ervaringen van mij zijn echter geenszins representatief voor de situatie in het algemeen, waarbij vrijwel niemand weet wat cryptografie is, wat je ermee kunt, laat staan dat je het wel eens nodig zou kunnen hebben voor de beveiliging

van informatie. Veruit de meeste mensen associëren cryptografie met cryptogrammen uit puzzelboekjes of kranten of menen dat het iets geheimzinnigs is wat gebruikt wordt door geheime diensten en dus geheim is. Een beeld dat niet in de laatste plaats opgeroepen wordt door de Nederlandstalige termen als geheim en geheimhouding.

Het is in het algemeen droevig gesteld met de 'awareness', het bewustzijn van dreigingen en beschermingsmaatregelen met betrekking tot (elektronische) informatieverwerkende systemen. Mijn introductie vervolgend, kan ik stellen dat het meeste resultaat bij het beantwoorden van de vraag wat cryptografie is, verkregen wordt door cryptografie te definiëren als het omzetten van betekenisvolle gegevens (informatiebevattende gegevens) in wartaal, ogenschijnlijk willekeurige, geen zinvolle informatie bevattende gegevens. Essentieel in het verhaal is verder ook dat de omzetting van gegevens in wartaal op een (vaak groot) aantal manieren gerealiseerd kan worden aan de hand van een veelal geheime sleutel.

Ook door aan te geven wat cryptografie beslist niet is: codering, scrambling, versluiering, steganografie, kan de definitie verder aangescherpt worden. Met name het laatstgenoemde begrip steganografie is vaak nog minder bekend, maar na uitleg dat het hierbij gaat om het verbergen van zinvolle informatie in andere op zich ook zinvolle informatie, begrijpt eenieder waar het om gaat: je zegt gewoon iets anders dan wat je bedoelt; een situatie die menigeen onmiddellijk herkent.

Cryptologie

Het begrip cryptologie heb ik al een paar maal gebruikt zonder daarbij een expliciete definitie te geven. Onder wat we zouden kunnen omschrijven als "leer der geheimschriften" worden vandaag de dag alle deelgebieden van de wiskunde, informatica, elektrotechniek en andere wetenschappen gevat, die zich bezighouden met alle aspecten van de cryptografische beveiliging van informatie. Hierbij ligt de nadruk niet zo zeer op de betekenis van het woord cryptografisch als wel op het doel van beveiliging dat nagestreefd wordt. Het begrip geheim vindt men vooral terug in de zogenaamde geheime sleutel: een hoeveelheid geheime informatie welke uitsluitend en alleen aan de eigenaar bekend is en dient te blijven. In het algemeen zal men ook willen kunnen vaststellen of de verschillende beveiligingsdoelen gehaald worden door toepassing van een cryptografisch systeem; anders gezegd: hoe is de mate van beveiliging die het cryptografisch

systeem verschaft, hoe sterk is het. Een antwoord op deze vraag is niet altijd even gemakkelijk te geven, maar door intensieve pogingen het systeem te kraken, d.w.z. een methode te vinden om uit het cryptogram de boodschap of zelfs de geheime sleutel te halen zonder dat men over andere (geheime) informatie beschikt, kan er vaak een bruikbaar beeld verkregen worden van de sterkte van het systeem. Een nette term hiervoor is cryptoanalyse. In de literatuur worden crypto-analisten vaak afgebeeld als de aanvallers van het systeem met minder goede bedoelingen. Ofschoon dit zeker vaak voorkomt, dient de crypto-analist niet verward te worden met de hacker. Deze laatste vindt cryptografie eenvoudigweg te moeilijk en probeert er omheen te komen in plaats van er doorheen, en niet altijd zonder succes.

Cryptografie en Beveiliging

In tegenstelling tot vroeger, toen cryptografie synoniem was voor geheimhouding, onderscheiden we vandaag de dag verschillende beveiligingsdoelen. Men spreekt in dit verband vaak over de zg. Security Services, zoals daar zijn:

- confidentialiteit (vertrouwelijkheid), de bescherming van gegevens tegen ongeoorloofde kennisname;
- integriteit, de bescherming tegen ongeoorloofde modificatie van gegevens;
- authenticiteit, de garantie dat de gegevens van de juiste bron afkomstig zijn;
- onweerlegbaarheid (non-repudiation), de garantie dat niet ontkend kan worden dat de gegevens verstuurd dan wel ontvangen zijn.

De moderne informatieverwerkende systemen zijn ook zeer complex wat betreft hun opbouw, werking en soms ook beheer. Men kan hierbij denken aan gedistribueerde systemen met gegevensbestanden (databases) van enorme afmetingen, waarin verschillende soorten informatie opgeslagen en bewerkt worden en welke toegankelijk zijn voor grote groepen gebruikers. Welhaast vanzelfsprekend heeft niet iedere gebruiker dezelfde rechten op het verkrijgen en omgaan met de opgeslagen informatie, maar dienen de gegevens integer en authentiek opgeslagen en bewaard te worden. Ook kan er sprake zijn van vertrouwelijke gegevens die niet iedereen mag inzien, laat staan modificeren of vernietigen. Het feit dat dergelijke systemen gedistribueerd zijn, betekent dat de verschillende componenten van een systeem via communicatienetwerken met elkaar verbonden zijn. De verscheidenheid aan communicatienetwerken wat betreft de infrastructuur (koper, glas, draadloos), de manier van schakelen (circuit-, pakket- of berichtgeschakeld) en de protocolstandaard (ISDN, PSTN,

X.25, TCP/IP) dragen in belangrijke mate bij aan de complexiteit van het moderne informatieverwerkende systeem.

Dergelijke systemen berusten voor de goede werking mede op regels en procedures, waarin idealiter vastgelegd is wie onder welke voorwaarden met wat voor informatie mag omgaan en met name hoe de beveiliging hiervan geregeld is. Men noemt dit laatste dan ook vaak Security Policy ofwel beveiligingsbeleid.

Het is met name de complexiteit van de hiervoor genoemde informatieverwerkende systemen welke aanleiding heeft gegeven tot het aanbrengen van meer structuur in de aard van beveiliging. Deze structuur vindt men terug in de hiërarchie van services, mechanismen en bouwstenen die men de afgelopen 10 jaar steeds meer is gaan gebruiken. Zo kunnen de policy maker en de systeemarchitect in overleg met de risicoanalist bepalen welke security services aanwezig dienen te zijn, de ontwerpers van apparatuur en netwerken zich verdiepen in de toe te passen mechanismen en kan de cryptograaf de meest geschikte bouwstenen specificeren.

Het zijn voornamelijk de bouwstenen welke enorm veel aandacht krijgen in de crypto-literatuur: de protocollen, hashfuncties en vercijferalgoritmen, hoewel dit slechts enkele schakels zijn in de lange keten van informatiebeveiliging. Zo is het niet ongebruikelijk dat gebruikers alles willen weten over de toegepaste algoritmen, maar zich absoluut niet afvragen hoe het met het beheer van de geheime sleutels gesteld is. Het begrip Crypto-Algoritme heeft voor velen iets geheimzinnigs, soms zelfs iets magisch en oefent een enorme aantrekkingskracht uit. Ik wil hier niets aan toevoegen of op afdingen, maar voor de wiskundige is een crypto-algoritme slechts een voorschrift hoe men de boodschap met behulp van de sleutel dient om te zetten in een cryptogram en omgekeerd; als een recept uit een kookboek waaruit je kunt lezen hoe je uit de ingrediënten een gerecht moet bereiden.

Klassieke en Moderne Cryptosystemen

Terugkerend naar de cryptografische bouwstenen kunnen we een nog duidelijker verschil tussen vroeger en nu onderscheiden, namelijk het bestaan van symmetrische en asymmetrische bouwstenen, ook wel geheime-sleutel- en publieke-sleutelbouwstenen genoemd. Men spreekt in dit verband ook wel van klassieke en moderne cryptosystemen. Deze aanduiding kan echter tot verwarring leiden. Klassieke systemen worden reeds enkele duizenden jaren toegepast, ook nu nog,

daarentegen is het concept van asymmetrie in cryptografie voor het eerst in 1976 in een publicatie in de openbare literatuur verschenen. Ik doel op het belangrijke artikel van Diffie en Hellman: "New Directions in Cryptology" [2]. Er zijn echter nog vele nieuwe klassieke systemen beschreven na 1976, hetgeen een indicatie is van het belang van deze systemen in de moderne cryptografische informatiebeveiliging. Dit belang ligt voor een aanzienlijk gedeelte in de complexiteit van de implementatie in concrete hardware en software en de daarmee gepaard gaande kosten: de efficiëntie van de verkregen oplossing.

Er is naar mijn mening een duidelijke rol weggelegd voor onderwijs, onderzoek en ontwikkeling op het gebied van symmetrische cryptografische bouwstenen, welke zo efficiënt mogelijk zijn. Ik doel hier op de moeilijkheidsgraad van de implementatie in relatie tot de cryptografische sterkte en de prestatie van de bouwstenen. De moeilijkheidsgraad zou je kunnen uitdrukken in de gebruikte chip oppervlakte of het aantal regels softwarecode; de prestatie heeft meestal betrekking op de snelheid van vercijferen. Van de sterkte zeggen we vaak dat die adequaat moet zijn en we bedoelen dan dat de moeite van het kraken in balans moet zijn met de waarde van de te beveiligen informatie of applicatie. Een in dit opzicht bijzonder relevante klasse van symmetrische bouwstenen wordt gevormd door de stream-cipher (stroomvercijfer) systemen. Dit zijn vercijfersystemen met een interne toestand ofwel geheugeninhoud, waardoor vercijfering van steeds dezelfde boodschap resulteert in een steeds ander cryptogram.

De genoemde combinatie van adequate sterkte, implementatiecomplexiteit en prestatie is zeer belangrijk in de praktijk van het ontwerpen van cryptografische systemen. Men dient hierbij wel een juist gevoel voor de state-of-the-art van cryptologie en technologie te hebben. Ik zie het als een van mijn taken om aandacht te besteden aan deze onderwerpen.

Ook op het gebied van sleutelbeheer en protocollen is er een duidelijk verschil tussen het toepassen van klassieke en moderne cryptografische bouwstenen. Een klassieker onder de moderne systemen is wel het RSA [3] systeem, dat een echte digitale handtekening mogelijk maakt en zijn gelijke onder de symmetrische bouwstenen niet kent. In de hedendaagse praktijk van cryptografische informatiebeveiliging wordt in toenemende mate belang toegekend aan gebruikersvriendelijke sleutelbeheersystemen. Het lijkt mij ondenkbaar, dat dit gerealiseerd kan worden zonder gebruikmaking van asymmetrische

bouwstenen. De stellingname dat asymmetrische bouwstenen het sleutelbeheerprobleem geheel oplossen gaat mij echter te ver. Het is derhalve zeer aannemelijk dat er ook in de nabije toekomst een rol is weggelegd voor zowel symmetrische als asymmetrische cryptografische bouwstenen.

Verleden, heden en toekomst van de cryptologie

Interessant is het om wat verder in de toekomst van de cryptologie kijken. Wat staat de cryptograaf, de crypto-analist, maar ook de gebruiker, beheerder en beleidsmaker te wachten? Om deze vraag enigszins te kunnen beantwoorden is het verstandig de evolutie van de cryptologie tot nu toe te beschouwen. Geheimschriftsystemen bestonden in het verleden voornamelijk uit pen-en-papier (misschien wel hamer-en-beitel); de cryptograaf cryptografeerde letterlijk. Pas in de vorige eeuw ([4]) is daar echt verandering in gekomen. De industriële en technologische evoluties gingen ook aan de cryptograaf niet voorbij. Achtereenvolgens werden technieken uit de mechanica, elektromechanica en elektronica toegepast in cryptosystemen. Vandaag de dag worden technieken uit verschillende gebieden toegepast zoals elektronica en informatica en er is een grote belangstelling voor het toepassen van theorieën uit de quantumfysica.

Met name de quantumfysica lijkt een ultieme uitdaging voor de cryptograaf, aangezien volgens de huidige inzichten systemen gebaseerd op deze theorie superieur zouden zijn aan de hedendaagse systemen. Eigenschappen als bewijsbare veiligheid en enorm hoge snelheden zouden voor deze systemen gelden. Er is weer een beetje magie terug, veroorzaakt door de theorie van de quantumfysica die door velen als lastig en tegenstrijdig ervaren wordt. Nog onlangs las ik over de quantum-informatie-eenheid de 'qubit'. Probeert u zich eens voor te stellen: de qubit is een superpositie van de waarden 0 en 1 met een zekere amplitude, representerend de kansverdeling van een 1- en 0-toestand, niet te verwarren met een waarde tussen 0 en 1 in. Voor de cryptoloog betekent deze evolutie op termijn een uitbreiding van de relevante vakgebieden als elektronica, informatietheorie, informatica en wiskunde met theoretische fysica. Het is derhalve niet ondenkbaar dat hier op deze plaats over enige tijd een theoretisch fysicus als cryptoloog zijn entree maakt.

De crypto-analyse zal ook kunnen profiteren van de ontwikkelingen in de quantumfysica: nu reeds wordt er wereldwijd ruim aandacht besteed aan Quantum Computing. Hoewel zeer veelbelovend - alle bestaande cryptografische systemen zouden simpel te breken zijn

door een zg. exhaustive search, met uitzondering van quantum cryptosystemen - is de praktische implementatie van deze technieken nog een groot probleem en het is vooralsnog niet duidelijk of het wel praktisch uitvoerbaar is.

Behalve door fundamentele doorbraken, zoals quantum computing of uitgekiende factorisatie algoritmen ziet de crypto-analist zijn mogelijkheden steeds meer toenemen vanwege de beschikbaarheid van snelle communicatienetwerken, krachtige computers en goedkope hardware. Een voorbeeld daarvan is de factorisatie van RSA130 ([5]), waarvoor 500 MIPS-jaar nodig was; stelt u zich eens voor: een jaar lang rekenen met een half miljard operaties per seconde om een getal van 130 cijfers te ontbinden in twee factoren. Nog recenter is de "zoektocht" naar een DES sleutel ([6]), uitgevoerd op een speciaal gebouwd apparaat, dat in staat is om 92 miljard sleutels per seconde te doorzoeken en slechts 250 duizend US dollar gekost heeft. Na 56 uur werd de sleutel gevonden...

De crypto-analist zelf blijft echter vooral de creatieve slimme puzzelaar, die bij zijn speurwerk naar zwakheden in een cryptosysteem soms een bijdrage kan leveren aan de theorie van cryptografische systemen. Want dat is tenslotte het probleem waar het om draait: het ontbreken van voldoende theorie; het begrijpen hoe de dingen echt in elkaar zitten. Nog steeds een enorme uitdaging, met name voor de wiskundige cryptoloog!

De gebruiker van cryptografisch beveiligde systemen was in het verleden slecht af. De kwaliteit en prestatie van de toepassing of service waren meestal lager na beveiliging; klassieke voorbeelden zijn de spraakverstaanbaarheid van de eerste generaties beveiligde telefoons en de beperkte doorvoersnelheden van antieke datavercijferapparatuur. Ook diende de gebruiker nogal wat extra handelingen te verrichten om het systeem in werking te stellen, waaronder niet in de laatste plaats het verkrijgen van de juiste sleutel. Op dit gebied is er een duidelijke trend merkbaar. Cryptografische beveiliging wordt steeds vaker zodanig toegepast dat het bijna onmerkbaar is voor de gebruiker, die alle applicaties kan blijven gebruiken zonder verlies van kwaliteit en performance en zonder dat er veel extra handelingen verricht moeten worden om beveiliging te verkrijgen.

Cryptografische functionaliteit wordt steeds meer ingebed in de applicatie of service en steeds minder een "add-on" of "add-in-between" welke achteraf is aangebracht.
Dit alles draagt in positieve zin bij tot het niveau van beveiliging van informatie en maakt in toenemende

mate cryptografie tot de gewoonste zaak van de wereld. Een vergelijk met de auto dringt zich op. Nog maar enkele jaren geleden waren zaken als ABS en air bags luxe artikelen, waar men behoorlijk voor in de geldbuidel moest tasten. Nu zijn het soms al standaard accessoires en waarschijnlijk over een paar jaar zit het in iedere auto en wordt er niet meer over gesproken.

Beveiliging op de Information Super Highway

Hoe is het vandaag de dag eigenlijk gesteld met de beveiliging van elektronische informatie? Allereerst kunnen we constateren dat, hoewel de initiatieven om te komen tot papierloze kantoren nog niet echt geslaagd genoemd kunnen worden, opslag, transport en verwerking van informatie steeds meer elektronisch plaatsvinden. Elektronische informatie welke in toenemende mate ook waarde vertegenwoordigt, bijvoorbeeld bedrijfsgegevens, klantenbestanden, concurrentie-informatie, product- en productieprocesgegevens. Elektronische informatie welke anderszins waardevol is zoals gegevens over criminelen en criminele transacties voor justitie en politie. Elektronische informatie welke in digitale vorm bestaat van en voor totaal verschillende toepassingsgebieden zoals spraak, fax, video en computergegevens. Opslag, transport en verwerking vinden vaak op meerdere locaties plaats en hiervoor zijn de informatieverwerkende systemen via netwerken verbonden. Netwerken die geheel of gedeeltelijk onder het beheer en controle van een andere dan de eigenaar van de informatie vallen. Voeg daarbij de betrekkelijke ongrijpbaarheid van elektronische informatie en de gemakkelijke toegankelijkheid ervan voor de gebruikers van de systemen en het beeld is compleet. Het is alsof men een belangrijk document in een open envelop met de eerste de beste bezorger meegeeft, terwijl het document niet is voorzien van een handtekening of fysieke kenmerken en de bezorger niet tekent en laat tekenen voor ontvangst. Hoewel deze karikatuur voor eenieder herkenbaar is, wordt het elektronisch equivalent zonder problemen geaccepteerd. Als reden wordt vaak opgevoerd dat de informatiesystemen en de gebruikte technieken zo ingewikkeld zijn, dat het in de praktijk wel heel moeilijk is om de eerdergenoemde dreigingen ten uitvoer te brengen, met andere woorden het risico is klein of tenminste acceptabel. Het is deze betrekkelijke unawareness, dit gebrek aan bewustzijn van de dreigingen en risico's bij het omgaan met elektronische informatie, die men vindt in alle gelederen van gebruikers, aanschaffers, adviseurs en beslissers, welke debet is aan de geringe mate van beveiliging van elektronische informatie en informatiesystemen.

Het is typisch menselijk om gevaren enigszins gering in te schatten en pas als het kalf verdronken is de put te dempen. We kijken reikhalzend uit naar nieuwe IT-applicaties en pas als er een aantal ongelukken mee gebeurd zijn wordt er over beveiliging gepraat, heel natuurlijk...

Een goed voorbeeld van deze handelwijze vinden we op de Elektronische Snelweg bij uitstek: het Internet. Inmiddels zijn er over de hele wereld miljoenen gebruikers van het Internet en de groei verloopt exponentieel. Internetgebruikers wisselen zeer snel en goedkoop boodschappen uit via E-mail, vragen informatie op over de meest uiteenlopende onderwerpen en producten en kunnen zelfs via bewegende beelden en geluid met elkaar communiceren. De vertrouwelijkheid, integriteit en authenticiteit van de uitgewisselde gegevens zijn meestal niet gegarandeerd, maar het gaat meestal goed,... of niet soms?

Men surft op het world wide web, op zoek naar interessante plekjes (sites) met informatie, welke steeds vaker zijn voorzien van geluid en animaties. Steeds meer bedrijven gaan hun waar aanbieden op het web en men spreekt nu vrij algemeen over elektronic commerce. De gebruiker wordt uitgenodigd om informatie op te vragen of meteen maar het product of dienst te bestellen door naam, adres en voor-al creditkaartgegevens in te vullen en on-line op te sturen. En het werkt meestal nog ook... Gelukkig waarschuwen sommige snuffelprogramma's (ofwel *browsers*, software om op het net te surfen) dat de informatie die het net opgestuurd wordt, niet beveiligd is; de vertrouwelijkheid van de gegevens is in het geding. En wanneer het om betalingsgegevens gaat, is dit niet zonder risico. Maar ook het simpelweg binnenhalen (downloaden) van gegevens is niet zonder gevaar. Er is een gerede kans op het binnenhalen van computervirussen of trojaanse paarden in gratis software of zelfs in documenten in de vorm van zg. macrovirussen. De virusscanner mag gerust continu aanstaan als men zich op de elektronische snelweg begeeft.

Maar zelfs alleen maar het kijken naar de homepages is niet geheel zonder gevaar. Zonder dat de gebruiker het zich echt realiseert, komen er kleine stukjes software mee naar binnen zoals de Java applets of ActiveX commando's, waarmee in principe de gehele computer bestuurd kan worden. De meeste browsers ondersteunen deze Java applets en commando's en derhalve kan het gebeuren dat men al surfend op het net zonder het te weten een programmaatje binnenhaalt dat de hele PC in de war schopt of kostbare bestanden vernietigt. Maar er kan op deze manier natuurlijk ook alleen maar

even op de harde schijf van de gebruiker gekeken worden en zonder dat de gebruiker het merkt kunnen allerlei gegevens teruggestuurd worden naar bepaalde geïnteresseerde websites. In kleine bestandjes, zg. cookies, kan de browser interessante gegevens opslaan; misschien ook wel serienummers van geïnstalleerde software, namen, telefoonnummers, etc. Het is dus goed mogelijk dat als een gebruiker de website van een softwareleverancier aandoet, automatisch even gekeken wordt of deze gebruiker een product van de leverancier geïnstalleerd heeft en indien dit het geval is worden vervolgens de installatiegegevens naar de leverancier opgestuurd. Ik zeg niet dat dit vaak gebeurt, maar het kan wel.

De elektronische snelweg kent nog meer gevaren. Zo is het onlangs mogelijk gebleken [7] om ongemerkt en op afstand de microfoon of camera welke op een PC zijn aangesloten, te activeren en zodoende de surfende gebruiker af te luisteren en af te kijken via zijn eigen PC. De gebruiker merkt het meestal niet; er wordt niets vooraf meegedeeld noch om toestemming gevraagd. Men kan zich daarom afvragen of dit soort praktijken niet aan banden moet worden gelegd. Helaas loopt de wetgeving ver achter bij de IT-praktijk en bovendien gaat het hier om communicatie welke vrijwel altijd de nationale grenzen overschrijdt.

De geschetste situatie van het Internet nader beschouwend, dringt zich een beeld op van de elektronische snelweg dat meer weg heeft van een zandpad vol hobbels en kuilen waarvan sommige zeer verraderlijk zijn en met struikrovers overal op de loer. Snel voortbewegen over zo'n pad is al lastig, handel drijven en waardevolle transporten verzorgen zeer risicovol.

De beveiliging van de elektronische snelweg is nog voornamelijk een braakliggend terrein, maar gelukkig worden er in toenemende mate initiatieven ontplooid om tot ontginning te komen. Elektronic Commerce zal pas echt een vlucht nemen, als er ook veilige elektronische betaalsystemen zullen zijn, waarbij de anonimiteit van de gebruikers tot op zekere hoogte gewaarborgd is. Een beveiligde infrastructuur waar berichten niet zomaar onderschept kunnen worden en faciliteiten voor de gebruiker om zijn boodschappen te kunnen beveiligen zijn noodzakelijk. Een van de belangrijkste aspecten hierbij lijkt de zg. Public Key Infrastructure te zijn: een infrastructuur gericht op het veilig en efficiënt kunnen verstrekken van sleutels aan gebruikers voor de uitwisseling van berichten waarbij de vertrouwelijkheid, integriteit en authenticiteit gewaarborgd zijn.
Een dergelijke infrastructuur is een typisch voorbeeld van een sleutelbeheer- ofwel key managementsysteem, waarover ik nu iets meer wil zeggen.

Key Management

Zoals ik in de inleiding van mijn betoog reeds heb gezegd, hebben cryptografische systemen tot gevolg dat er een hoeveelheid geheime informatie bestaat, waarmee het cryptografische algoritme de klare tekst in crypto tekst omzet en vice versa. Deze informatie wordt kortweg sleutel genoemd. Dit geldt in het bijzonder voor de eerdergenoemde symmetrische systemen. Asymmetrische systemen daarentegen hebben als eigenschap dat er naast een geheime sleutel ook een publieke sleutel bestaat waarvan de authenticiteit gewaarborgd dient te worden. Het veilig en efficiënt omgaan met deze sleutels met als doel de juiste sleutel op de juiste plaats en tijd te krijgen omvat een aantal activiteiten welke zeer veelomvattend kunnen zijn. Het gaat hierbij ondermeer om het opwekken, certificeren, distribueren, bewaren, gebruiken, transformeren, herroepen en vernietigen van meestal geheime, maar ook publieke sleutelinformatie voor de meest uiteenlopende applicaties.

Het moge duidelijk zijn dat de beveiliging van sleutelmateriaal essentieel is voor de beveiliging die cryptografische systemen kunnen verschaffen en men kan zich afvragen wat men ermee wint om informatie te vercijferen teneinde die te beveiligen, aangezien men nog steeds een informatiebeveiligingsprobleem overhoudt in de vorm van een geheim te houden sleutel. Een antwoord hierop is dat men de hoeveelheid informatie welke vervolgens nog beveiligd moet worden drastisch verkleint; een typisch verschijnsel ook in veel key management systemen waarin zg. sleutelhiërarchieën voorkomen, oftewel een sleutel die sleutels beveiligt, die sleutels beveiligen, die sleutels beveiligen, etc. Een situatie die mij reeds zo'n 17 jaar geleden door Fred Hafkamp, voormalig directeur van het Nationaal Bureau voor Verbindingsbeveiliging, uitgelegd werd als het probleem van de Droste-verpleegster.

Ik noemde ook efficiency als belangrijke eigenschap van key managementsystemen. Het gaat hierbij onder meer om het gemak waarmee de gebruiker van een beveiligde applicatie de juiste sleutel kan verkrijgen (als hij of zij zich daar überhaupt al om moet bekommeren) en de last die het sleutelbeheer veroorzaakt voor de beherende instantie. Het is mij na veel jaren ervaring met de praktijk duidelijk geworden dat sleutelbeheersystemen een essentiële rol spelen in de beveiliging van informatie door middel van cryptografie. Key managementsystemen dienen te zijn afgestemd op de toepassing waarvoor, de organisatie waarin en het beleid waaronder ze gebruikt worden. Ik vind het dan ook van weinig inzicht in de praktijk van de

cryptografische informatiebeveiliging getuigen als men het sleutelbeheerprobleem bagatelliseert door te beweren dat het toch eenvoudig opgelost kan worden met behulp van public key-systemen. Het is inmiddels wel algemeen geaccepteerd dat public key-systemen een belangrijke rol zullen gaan vervullen teneinde te komen tot een algemene, zelfs internationale infrastructuur voor het verdelen van sleutels aan gebruikers van beveiligingsapplicaties, de al eerder genoemde public key infrastructure.

Een sleutelrol lijkt hier te zijn weggelegd voor de zg. vertrouwde derde partij ofwel trusted third party, kortweg TTP genoemd. In een van de modellen van TTP's is dit een instantie waarbij men na zich gelegitimeerd te hebben een public key sleutelpaar kan verkrijgen, veilig opgeslagen in een fysiek beschermd hebbeding ofwel 'token', bijvoorbeeld een smart card met pincode. De TTP belooft dan om de publieke sleutel eenmalig uit te geven en ook om de geheime sleutel daadwerkelijk geheim te houden. Dit laatste lijkt vanzelfsprekend, maar is het niet. Er kunnen zich situaties voordoen waarbij bepaalde partijen zeer geïnteresseerd zijn in de informatie die uitgewisseld wordt of opgeslagen is. Zo zal justitie bij vermeende criminele praktijken mogen afluisteren of inzage in gegevens mogen hebben en ingeval de informatie cryptografisch beveiligd is, is dit vrijwel onmogelijk. Het ligt derhalve voor de hand dat de TTP ingeval van een gerechtelijk bevel de geheime sleutel beschikbaar stelt aan de autoriteiten.

Het geschetste voorbeeld noemt men wel Key Escrow: het in bewaring geven van de geheime sleutel, waarbij onder zekere voorwaarden toegang aan bepaalde partijen verschaft wordt. Dit principe stuit op nogal wat verzet onder potentiële TTP-gebruikers. Veel overheden houden echter vast aan het principe dat er zich omstandigheden kunnen voordoen waarbij de beveiligde informatie voor hen in klare vorm beschikbaar moet kunnen zijn. Hoewel er al veel gediscussieerd is over dit dilemma en verschillende alternatieve TTP-principes zijn gepresenteerd, zoals Split Key Recovery, ben ik van mening dat er nog sprake is van een impasse. Beleidsmakers dienen zich te realiseren dat systemen aanvaardbaar moeten zijn voor de gebruikers ervan; zoniet dan zullen deze systemen niet op grote schaal gebruikt worden; een TTP is hierop geen uitzondering. Het lijkt mij zinvol om serieus onderzoek te verrichten naar alternatieve TTP-modellen, waarbij zoveel mogelijk de belangen van alle betrokken partijen in ogenschouw genomen worden. In het bijzonder zouden standaardisatie-activiteiten meer aandacht hieraan dienen te besteden in

plaats van ad hoc oplossingen te kiezen, waarvan de acceptatie bij het grote publiek betwijfeld mag worden.

Uit het voorgaande moge duidelijk zijn dat Key Management een praktisch relevant gebied van onderzoek is. Er zijn verschillende sleutelbeheerprobleemgebieden aan te wijzen waar de discreet wiskundige een bijdrage kan leveren. Naast de genoemde TTP-problematiek wil ik hier nog noemen protocollen en sleutelopslag. Protocollen spelen zich o.a. af tussen twee of meer partijen ingeval er een gemeenschappelijke sleutel afgestemd moet worden; men kan het uitleggen als een cryptografisch vraag-en-antwoordspel. Er zijn diverse publicaties (o.a. [8]) die een goed beeld van dit soort protocollen geven. Met name het toepassingsgericht ontwerpen van key managementprotocollen, waarbij randvoorwaarden als executietijd en rekenvermogen een rol spelen, is relevant in de praktijk. Dat de protocollen ook nog veilig dienen te zijn staat buiten kijf. Het platgetreden pad van de X.509 standaard is niet voordehandliggend voor menige applicatie, maar ja...., het is tenslotte een standaard.

Sleutelopslag heeft te maken met het interne sleutelbeheer van de applicatie. Afhankelijk van de hardware en software-omgeving van een applicatie kunnen specifieke eisen gesteld worden aan sleutelopslag teneinde te voldoen aan criteria van veiligheid en efficiency. Ook in dit geval is het gebruik van eerdergenoemde sleutelhiërarchieën niet ongebruikelijk. Zo is het veel eenvoudiger om de sleutelvercijfersleutel te wissen dan alle afzonderlijke sleutels die hiermee beschermd zijn.

Overigens zijn er toepassingen waarbij de beschikbare geheugencapaciteit, als gevolg van de toegepaste technologie, beperkingen oplegt aan de hoeveelheid sleutelbits die opgeslagen kan worden. Een voorbeeld hiervan is de smart card, welke u tegen kunt komen in de vorm van elektronische portemonnee zoals Chipper en Chip-Knip. Vanwege mechanische eisen mag de elektronische schakeling, de chip, slechts een gering deel van de oppervlakte van de kaart innemen en kan als gevolg daarvan slechts een beperkte hoeveelheid sleutelbits opslaan. Deze opslagbeperking wordt in de praktijk vaak vertaald in het gebruik van een beperkt aantal verschillende sleutels, waardoor het welhaast onontkoombaar is dat een sleutel op veel meer dan twee plaatsen in het systeem aanwezig is. Ik ken toepassingen waarbij slechts één geheime sleutel gebruikt wordt, die op duizenden locaties aanwezig is.

Men zegt wel dat een dergelijk systeem een lage compartimentatie-

graad heeft, of ook wel dat de bescherming tegen geheime samenzwering gering is, al naar gelang welk dreigingscenario men voor ogen heeft. De dreiging kan namelijk bestaan uit het feit dat compromittatie van sleutelbits van een gebruiker consequenties heeft voor de beveiliging van een groot aantal andere gebruikers. Ook kan de dreiging bestaan uit het feit dat een beperkt aantal gebruikers samenwerken waardoor alle overige gebruikers niet meer beveiligd zijn.

Er bestaan echter sleutelopslagreductiemethoden waarbij sprake is van een afweging tussen beschikbare opslagcapaciteit enerzijds en compartimentatiegraad anderzijds. Een voorbeeld hiervan zijn de methoden die gebaseerd zijn op Key Distribution Patterns (KDP's), block designs met een bijzondere structuur. Voor constructieve methoden van KDP's en methoden voor sleutelopslagreductie in het algemeen is er nog ruimte voor wiskundig onderzoek.

Streamciphers

Dames en Heren,

In mijn inleiding heb ik reeds gewezen op het belang van symmetrische cryptografische systemen, in het bijzonder streamciphers, voor praktische toepassingen waarbij randvoorwaarden als implementatiecomplexiteit, prestatie en beveiligingsniveau gelden. Dit belang wordt onderstreept door de steeds sneller wordende computersystemen en communicatienetwerken.

De Information Super Highway wordt in toenemende mate gedragen door glasvezelnetwerken waarover informatie volgens de Synchronous Digital Hierarchy standaard met snelheden van 155 miljoen bits per seconde tot zelfs 10 miljard bits per seconde wordt uitgewisseld. Deze snelheden van informatieoverdracht worden in moderne informatieverwerkende systemen, personal- en andere computers eveneens gehaald. Het toepassen van cryptografische beveiliging mag de performance van deze systemen en netwerken niet noemenswaardig nadelig beïnvloeden, met andere woorden: alle applicaties moeten nog steeds en ongeveer even snel blijven werken teneinde de acceptatie door de gebruiker te kunnen garanderen.

Een interessante klasse van streamciphers wordt gevormd door schuifregisterconstructies.
Een schuifregister is in feite een eenvoudig geheugenelement, dat zeer efficiënt in hardware geïmplementeerd kan worden. Schuifregisters worden gebruikt om het elektronisch equivalent van een pseudo-toevalsgenerator te construeren; zoiets als een elektronische roulette. Zo'n roulette geef je

een draai, waarna er een ogenschijnlijk willekeurige rij getallen geproduceerd wordt. Vroeger noemde men dit ook wel een elektronisch wiel naar analogie van de mechanische vercijfersystemen.

Voor zover mij bekend is, zijn de streamciphersystemen op basis van schuifregisterconstructies steeds als meest haalbare en efficiënte oplossing uit de bus gekomen gedurende de afgelopen 20 jaar. Ik ben van mening dat dit nog steeds en met name voor de genoemde hoge snelheden geldt. Opvallend genoeg wordt er nauwelijks nog aandacht besteed in de literatuur aan het ontwerp en analyse van streamciphersystemen. Dit terwijl er toch nog volop interessante fundamentele problemen naar voren komen bij het beschouwen van 'eenvoudige' schuifregisterconstructies. Voor dat je het weet heb je te maken met het discrete-logaritmeprobleem, denk je na over de existentie van klassen van irreducibele polynomen of de generalisatie naar andere lichamen dan GF(2) en struikel je over optimale implementaties in hardware of software.

Vooral bij het toepassen van niet-lineaire constructies heb je een probleem: veel theorie is er sinds de publicatie van Golomb's boek in 1967 [9] niet bijgekomen. Andere gebieden zoals de cryptografische complexiteit van rijen opgewekt door streamciphers en de grootte van klassen van periodieke binaire rijen liggen nog steeds braak voor gedegen onderzoek. En wat te denken van een efficiencymaat, zoiets als de sterkte-snelheid per gate-equivalent-MHz of per MIPS van een vercijfersysteem?

Onderzoek en onderwijs

Uit het voorgaande moge duidelijk geworden zijn dat er alleen al op het gebied van key management en symmetrische systemen volop onderwerpen voor onderzoek aangewezen kunnen worden, die ook in belangrijke mate praktisch relevant zijn. Ik zie deze praktisch relevante onderzoeksactiviteiten als een belangrijke drager voor alle onderzoek op het vakgebied, ook het meer theoretische en niet direct toepasbare. Het is essentieel dat de wetenschapper wetenschap bedrijft en daarbij theorieën ontwikkelt, niet al te zeer gehinderd door praktische beperkingen. Het is eveneens essentieel, dat dezelfde wetenschapper zich gepast commercieel opstelt en zijn onderzoeksresultaten kan 'verkopen' en al doende ook zorgt voor vervolgonderzoek. Het is mijns inziens hierbij niet noodzakelijk om aan elke hype mee te doen (omdat we als onderzoeksinstituut anders niet zouden meetellen), maar beter ons te concentreren op een paar kerngebieden.

Samenwerking met het bedrijfsleven en industrie, welke ook op andere gebieden van de wiskunde al jarenlang plaatsvindt, blijkt hierbij een win-win situatie op te leveren. Ik ben echter geen voorstander van een al te grote invloed van bedrijfsleven en industrie op de inhoud van onderwijs en onderzoek aan universiteiten, zoals sommige geledingen uit de politiek die voorstaan. Dit heeft iets kunstmatigs, dat van bovenaf opgelegd is. Een gezonde marktwerking verdient ook in dit geval de voorkeur!

Het blijkt overigens dat de pas afgestudeerde TUE-ingenieur met de juiste opleiding een goede marktwaarde heeft. Dat geldt met name ook op het gebied van de informatiebeveiliging, waar menig wiskundig ingenieur en -ontwerper zijn of haar weg naar industrie, overheid en bedrijfsleven gevonden heeft. Het afleveren van adequaat opgeleide aspirant cryptologen impliceert een gedegen opleiding op dit inmiddels veelomvattende vakgebied. Een opleiding waarin de diverse facetten van de wiskunde, informatietheorie, informatica, elektrotechniek, maar ook van management en gebruik evenwichtig vertegenwoordigd zijn.

Dankwoord

Dames en Heren, aan het eind gekomen van mijn rede, wil ik graag enige woorden van dank uitspreken.

Geachte leden van het College van Bestuur, Mijnheer de Rector Magnificus: ik wil u graag bedanken voor mijn benoeming en het daarmee in mij gestelde vertrouwen. Ik zal mijn inzet en energie richten op onderzoek en onderwijs in overeenstemming met de regels, ambities en cultuur van deze universiteit.

Zeer erkentelijk ben ik iedereen die heeft bijgedragen aan mijn wetenschappelijke vorming en mij de liefde voor het cryptovak heeft bijgebracht.

- Piet Schalkwijk: In het eerste college Informatietheorie dat ik zo'n 20 jaar geleden bij je volgde was ik meteen gefascineerd door de onderwerpen die je behandelde en besloot in dit vakgebied verder te gaan.
- Jack van Lint: Tijdens het volgen van jouw college over foutencorrigerende codes heb ik ernstig getwijfeld of ik er wel goed aan had gedaan om elektrotechniek als studierichting te kiezen. De combinatie van informatietheorie en discrete wiskunde is achteraf echter zeer nuttig en zinvol gebleken.
- Dick Boekee: Bij jou heb ik een stukje Delftse cultuur geproefd.

De juiste mix van praktisch en theoretisch relevante onderwerpen in onderzoek en onderwijs bleek succesvol te zijn.

- Henk van Tilborg: Jij introduceerde mij zo'n 16 jaar geleden aan de toenmalige Crypto Werkgroep van het Mathematisch Centrum in Amsterdam. De vele voordrachten van jou die ik in de loop van de jaren heb bijgewoond, zijn stuk voor stuk een voorbeeld hoe men complexe materie eenvoudig kan uitleggen.
- Jim Massey: Ik ben van mening dat de cursus Cryptologie die jij vanaf 1981 tot en met vorig jaar hebt gegeven een van de beste ter wereld was; met genoegen denk ik hieraan terug en ook aan de inspirerende discussies die we hebben gehad.
- Ton van den Ende: Jij nam mij als werknemer van Philips Usfa B.V. aan, waardoor ik in aanraking kwam met de vele praktische implementatieaspecten van cryptografische systemen zoals key management en synchronisatieproblematiek.
- Hans van Lottum†: Een postume dank voor het bijbrengen van gevoel voor de waarde en kracht van klassieke systemen.

Geachte collegae van de sectie Discrete Wiskunde van de faculteit Wiskunde en Informatica: Het nadeel van een deeltijdbetrekking is dat je elkaar nogal eens misloopt, niet onmiddellijk kunt reageren op vragen en mededelingen en nogal eens een verjaardagstractatie moet missen. Dat is even wennen, voor jullie en voor mij. Ik dank jullie voor de manier waarop ik, ondanks mijn beperkte aanwezigheid, in de groep ben opgenomen en zie uit naar een vruchtbare samenwerking.

Geachte collegae van Philips Crypto B.V.: Het afgelopen jaar schitterde ik nog vaker door afwezigheid dan voorheen. Jullie hebben dat echter goed weten op te vangen en de 'status aparte' die voor mij in veel routinematige zaken gehanteerd wordt, ervaar ik als positief. In het bijzonder wil ik Henk Algra bedanken: Henk, zonder jouw bijdrage en motivatie zou ik hier vandaag niet gestaan hebben.

Geachte toehoorders: Werken doet een mens maar een gedeelte van zijn beschikbare tijd; sommigen een tamelijk beperkt gedeelte, anderen een zeer aanzienlijk gedeelte. Bovendien wordt de resterende tijd soms nog gevuld met activiteiten die in het verlengde liggen van de professionele werkzaamheden. Voor het invullen van de rol van echtgenoot en vader is de tijd die effectief overblijft, soms wel eens aan de krappe kant. Daarom is mijn laatste dankwoord speciaal gericht aan Maria, Richard en Irene: jullie steun en vooral begrip is van doorslaggevend belang geweest voor het bereiken van deze mijlpaal.

Ik heb gezegd.

Referenties

1. Shannon, C.E., "Communication Theory of Secrecy Systems", Bell System Technical Journal, 1949
2. Diffie, W. and Hellman, M.E., "New directions in cryptography", IEEE Trans. Informat. Theory, vol. IT-22, 1976
3. Rivest, R.L., Shamir, A. and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", CACM, vol. 21, 1978
4. Deavours, C.A., Kahn, D., Kruh, L., Mellen, G. and Winkel, B., *Cryptology Yesterday, Today and Tomorrow*, Norwood, MA, Artech House,1987
5. http://www.rsa.com/rsalabs/html/status.html
6. http://www.eff.org/descracker/, http://www.cryptography.com/des/index.html
7. Dagblad "De Telegraaf", "Afluisteren via het Web", 26 mei 1998, pag. T23
8. Diffie, W., Van Oorschot, P.C. and Wiener, M.J., "Authentication and Authenticated Key Exchanges", Designs, Codes and Crytptography, vol. 2, no. 2, 1992
9. Golomb, S.W., *Shift Register Sequences*, San Francisco, CA, Holden-Day, 1967

Cees J.A. Jansen werd geboren op 19 november 1953 te Roosendaal. Na de middelbare school koos hij voor een studie aan de Hogere Technische School Breda. In 1975 behaalde hij het HTS-diploma en ging vervolgens elektrotechniek studeren aan de Technische Universiteit Eindhoven. Hij studeerde in 1980 af als elektrotechnisch ingenieur op het vakgebied van de informatie- en communicatietheorie, waarna hij in dienst trad bij Philips Usfa B.V. om zich met ontwerp en implementatie van cryptografische systemen bezig te houden. In 1989 promoveerde hij aan de Technische Universiteit Delft op een proefschrift getiteld "Investigations on Nonlinear Streamcipher Systems. Construction and Evaluation Methods". Momenteel is hij werkzaam bij Philips Crypto B.V. als senior consultant, waar hij adviseert inzake cryptografie en sleutelbeheer en inhoudelijk verantwoordelijk is voor het research programma. Hij is Senior Member van de IEEE Information Theory Society, lid van de International Association for Cryptologic Research en bestuurslid van de Werkgemeenschap voor Informatie- en Communicatietheorie. Sinds 2 oktober 1997 is hij als deeltijdhoogleraar Cryptologie werkzaam aan de Technische Universiteit Eindhoven.

Vormgeving en druk:
Universiteitsdrukkerij TUE
Technische Universiteit Eindhoven

Informatie:
Front Office Auditorium
Telefoon (040-247)2250/4676

ISBN 90 386 12 11 7