KWETSBAARHEID VAN SMARTCARDS

Vaandrig J.C.H. Veldhuis BSc, NLDA-School Verbindingsdienst

In dit artikel schetst vdg Veldhuis de kwetsbaarheid van smartcards. Er zijn ontwikkelingen gaande om de informatie van smartcards te verkrijgen, zonder daadwerkelijk fysiek in contact te komen met die smartcards, en hij gaat nader in op side-channel attacks.

Het artikel is geschreven naar aanleiding van het symposium *Digital Security* van de Technische Universiteit Eindhoven.

Smartcards komen we tegenwoordig overal tegen. Als defensiemedewerker gebruiken we smartcards voornamelijk om toegang te krijgen tot militaire complexen.. De SIM-kaart in onze mobiele telefoon, de PIN-pas of creditcard, de OV-chipkaart, allemaal hebben ze gemeenschappelijk dat ze ons toegang kunnen verschaffen tot een bepaalde dienst. Er wordt middels een authenticatieproces nagegaan of de houder van de smartcard toegang mag krijgen tot de dienst. Dit wordt vervolgens veelal geregistreerd om hem vervolgens te kunnen factureren of zijn gebruik te kunnen vastleggen. U krijgt immers aan het eind van de maand uw telefoonrekening met daarop gespecificeerd hoe vaak en hoe lang u mobiel heeft gebeld.

AUTHENTICATIE

Smartcards worden dikwijls in combinatie met een PIN-code gebruikt, zodat alleen degene die de PIN-code weet, in combinatie met de smartcard, gebruik kan maken van bepaalde diensten. Authenticatie vindt dus plaats op basis van twee authenticatievormen:

- bezit; iets dat alleen een rechtmatige gebruiker van een dienst heeft (de smartcard zelf) en
- kennis; iets dat alleen de rechtmatige houder weet (PIN-code).

Een derde authenticatievorm, op basis van een meetbare persoonlijke eigenschap (biometrie), komt tegenwoordig ook steeds vaker voor, maar is nog volop in ontwikkeling. Denk hierbij bijvoorbeeld aan een irisscan, vingerafdruk of stemherkenning.

Om te voorkomen dat men smartcards en de informatie die er op staat dusdanig kan wijzigen of kopiëren zodat bovengenoemde processen ontregeld of omzeild kunnen worden, waardoor men bijvoorbeeld gratis kan bellen, reizen, of ongeoorloofd toegang kan krijgen tot een complex of systeem, wordt de cruciale informatie op de smartcards vaak versleuteld. Een veelvuldig gebruikt versleutelingalgoritme bij smartcards is RSA.

RSA is een asymmetrisch encryptiealgoritme, dat veel gebruikt wordt voor elektronische handel (beveiliging van transacties en dergelijke). Het formele algoritme werd in 1977 ontworpen door Ron **R**ivest, Adi **S**hamir en Len **A**dleman (vandaar de afkorting RSA).
Clifford Cocks, een Britse wiskundige, die voor het Government Communications Headquarters (GCHQ) werkte, heeft in 1973 een gelijkwaardig algoritme beschreven in een intern document, dat pas in 1997 boven water is gekomen, omdat het als topgeheim geclassificeerd was.
De veiligheid van RSA steunt op het probleem van de ontbinding in factoren (bij heel grote getallen): op dit moment is het bijna onmogelijk de twee oorspronkelijke priemgetallen p en q te achterhalen als alleen p*q bekend is en p en q groot genoeg zijn; het zou te veel tijd in beslag nemen.
Het RSA algoritme maakt gebruik van twee sleutels, de zogenoemde *public key* en de *private key*. De eerste wordt gebruikt voor het encryptie-proces (versleuteling), de tweede voor het decryptie-proces (ontsleuteling) en moet dan ook geheim blijven. Dit noemt men asymmetrische cryptografie, in tegenstelling tot symmetrische cryptografie waarbij slechts één sleutel wordt gebruikt. Nog niemand is in staat geweest om dit algoritme te kraken en het wordt door de industrie als veilig geacht. De mate van beveiliging kan worden uitgedrukt in de lengte van de sleutels, omdat dit bepaalt hoeveel tijd een aanvaller nodig zou hebben om alle mogelijkheden te proberen. Sleutels met een lengte van 1024 bits worden als sterk beschouwd, maar er worden reeds sleutels van 2048 bits of langer gebruikt. Nieuwe ontwikkelingen op dit gebied zouden RSA onbruikbaar kunnen maken.

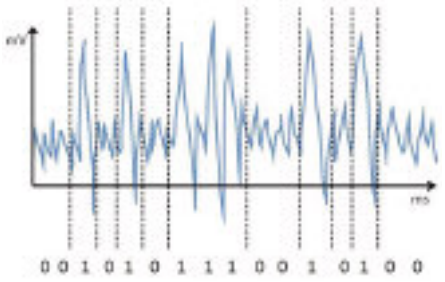
Bron: Wikipedia en vdg Veldhuis

SIDE-CHANNEL ATTACK

Omdat het praktisch onmogelijk is, mits er sterke sleutels gebruikt worden, om RSA te kraken door middel van *brute-force* aanvallen, waarbij een aanvaller alle mogelijke sleutels probeert tot hij de juiste vindt, zijn er andere manieren gezocht om de sleutels te achterhalen. Een aantal technieken om dit te bewerkstelligen zijn de zogenaamde *side-channel attacks*. Dit behelst een verzameling aanvallen op de implementaties van de cryptografische processen op smartcards gebaseerd op informatie die over de sleutels kan worden verkregen uit bepaalde fysische eigenschappen. Dit kan stroomverbruik zijn, maar ook elektromagnetische straling of thermodynamische of akoestische karakteristieken. De meest eenvoudige *side-channel attack* is *Simple Power Analysis* (SPA).

Elke smartcard bevat een chip met daarop een microprocessor die in staat is om simpele berekeningen uit te voeren. Tijdens deze berekeningen worden verschillende (tussentijdse) waarden opgeslagen in geheugencellen, waarbij de microprocessor stroom verbruikt. De ene berekening vereist echter meer stroom dan de andere. Met apparatuur, die vrij verkrijgbaar is op de markt, is het mogelijk om het stroomverbruik van een smartcard te meten. Een aanvaller kan, mits hij bekend is met de gebruikte implementatie van het RSA-algoritme, aan het stroomverbruik zien welke berekeningen achtereenvolgens uitgevoerd worden.

Een sleutel is in feite niet meer dan een reeks bits (enen en nullen). Wanneer er bewerkingen worden uitgevoerd met deze sleutel, is deze reeks enen en nullen te achterhalen doordat er lichte pieken te zien zijn in het stroomverbruikprofiel. Onderstaande grafiek geeft een schematisch voorbeeld van een dergelijk profiel, waarbij het stroomverbruik uitgezet is in de tijd. De 'geheime' sleutel is gemakkelijk af te lezen omdat de enen corresponderen met pieken in het stroomverbruik.



Stroomverbruikprofiel

Bovengenoemd voorbeeld is uiteraard sterk vereenvoudigd, maar geeft wel de essentie weer van SPA. Er zijn verschillende variaties hierop, waaronder *Differential Power Analysis (DPA)* waarbij statistische analyses worden gedaan aan de hand van verschillende invoeren waardoor aannames kunnen worden gedaan over de gebruikte sleutels, zelfs als er sprake is van veel ruis bij de metingen. Op deze wijze kan een aanvaller de mogelijkheden voor de geheime sleutel dusdanig indammen, dat hij in korte tijd de sleutel kan achterhalen met een *brute-force* aanval. Een andere techniek is *Differential Fault Analysis (DFA)* waarbij er met behulp van lasers, sterke elektrische of magnetische velden, hoge temperaturen of op andere wijzen veranderingen worden bewerkstelligd in de toestand van de microprocessor en de geheugencellen van een smartcard tijdens de uitvoer van een cryptografische berekening. Door de uitvoer te vergelijken met de normale uitvoer (waarbij er niks veranderd is), kan een aanvaller informatie krijgen over de geheime sleutel wat kan leiden tot ontrafeling hiervan.

BESCHERMINGSSTRATEGIE

Smartcardontwikkelaars bedenken allerlei manieren om dergelijke aanvallen tegen te gaan. De eerdergenoemde technieken kunnen bijvoorbeeld bemoeilijkt worden door willekeurige berekeningen toe te voegen (zogenoemde *dummy-computations*), waardoor het voor een aanvaller moeilijker te voorspellen en te timen is wanneer bepaalde cryptografische berekeningen worden uitgevoerd. Het nadeel hiervan is dat dit extra processorcapaciteit vergt, hetgeen een hoger stroomverbruik en een lagere effectieve rekensnelheid impliceert. Dit is in de huidige tijd van technologische vooruitgang waarbij steeds meer snelheid en efficiëntie gevraagd wordt niet wenselijk. Deze afweging tussen veiligheid en kostenbesparing kan grote consequenties hebben indien deze niet juist gemaakt wordt.

Hoe dan ook zal er een constante strijd blijven tussen smartcardontwikkelaars aan de ene kant en potentiële krakers aan de andere kant. De ene groep streeft er altijd naar om de andere een stap voor te zijn. Kenmerkend voor dit vakgebied: tijdelijk succes.

Noot van de redactie: Inmiddels is vdg Veldhuis bevorderd tot tweede-luitenant en werkzaam bij 101 CISbat als pelotonscommandant.

CARTOON

WIM RIETKERK