Novomodo, een nieuwe manier om certificaten te valideren

Door Thijs Veugen en Marjo Geers

<over de auteurs> Thijs Veugen en Marjo Geers zijn werkzaam als respectievelijk senior consultant en consultant bij TNO Telecom in het Business Innovation Team Network & Information Security.

De Novomodo PKI-oplossing weet door elegant gebruik van hashberekeningen de hoeveelheid data en het aantal RSA-berekeningen te beperken dat nodig is voor het valideren van een certificaat. Dit is nuttig bij gebruik van PKI in gelimiteerde omgevingen waar bandbreedte, rekencapaciteit en geheugen beperkt zijn. Ook biedt Novomodo voordelen op het gebied van efficiëntie en kosten, wat met name bij omvangrijke PKI's van belang is. Daarnaast biedt het mogelijkheden voor nieuwe toepassingen.

Inleiding

Elektronisch zakendoen en elektronisch communiceren krijgen een steeds belangrijkere rol in onze samenleving. De betrouwbaarheid van de communicatie (authenticiteit, vertrouwelijkheid en beschikbaarheid) moet daarbij vaak gegarandeerd zijn. Hiervoor kan een Public Key Infrastructure (PKI) een goede oplossing zijn. Het standaard PKI-concept [1] is inmiddels welbekend en in verschillende boeken en artikelen uitvoerig beschreven.

Het bepalen of certificaten al dan niet herroepen zijn, is bij grootschalig gebruik in de hedendaagse praktijk lastig te beheren en kostbaar. Voor de Certificate Revocation List (CRL) geldt dat deze onhandelbaar lang kan worden, en het Online Certificate Status Protocol (OCSP) zorgt voor een zware belasting van de centrale validatieserver in de zin van bandbreedte en rekenkracht.
Voor beide methoden geldt bovendien dat in het geval dat het certificaat gecompromitteerd raakt, waarmee respectievelijk de CRL- of het OCSP-antwoord wordt getekend, alle certificaten onbruikbaar worden. Er is immers niet meer vast te stellen of certificaten herroepen zijn.

Daarnaast zien we momenteel de ontwikkeling dat gebruikers er steeds meer van uitgaan dat ze elektronisch kunnen communiceren waar en wanneer ze maar willen. Draadloze communicatie en draagbare (mobiele) apparatuur zijn daarbij heel belangrijk. Hoewel in het algemeen de beschikbare bandbreedte, geheugen en rekencapaciteit in deze draadloze mobiele omgevingen zal toenemen, zullen er ook in de toekomst omgevingen zijn met beperkte beschikbaarheid daarvan. Denk hierbij aan ambient intelligence en ubiquitous computing, waarbij allerlei kleine apparaten de gebruiker van dienst zullen zijn. Een standaard PKI-oplossing is door het beroep dat deze doet op apparatuur en bandbreedte daardoor niet altijd geschikt. Voor gelimiteerde omgevingen is PKI over WAP [2] ontwikkeld, maar WAP is nooit echt doorgebroken en is bovendien minder veilig dan de standaard PKI-oplossing. Het gebruik van WAP voor draadloze PKI is reeds beschreven in [3].

Het Novomodo-systeem [4] dat in dit artikel wordt beschreven, kan zowel voor gelimiteerde omgevingen als voor omvangrijke PKI's een oplossing bieden om efficiënt certificaten te valideren.

Novomodo

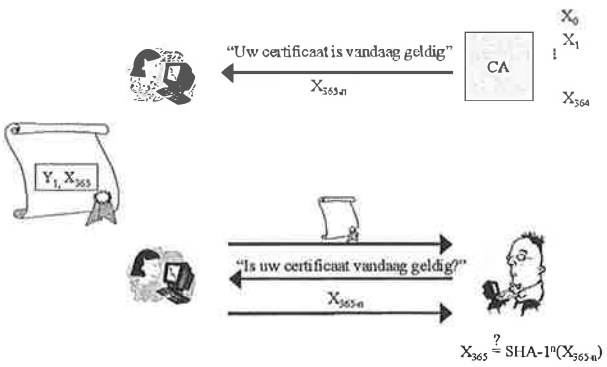
Novomodo [4] maakt gebruik van certificaten die naast de normale gegevens twee hashwaarden bevatten. Deze

<Referenties>
Dit artikel is gebaseerd op de volgende documenten waaraan in de tekst gerefereerd wordt:
[1] Dr.ir. P.J.M. Veugen e.a., Technische beveiligingsstudie Encryptie, PI standaarden en studies in informatiebeveiliging deel 1, Lemma, Utrecht, 2002.
[2] WPKI; WAP-217-WPKI; Version 24 April 2001.
[3] Thijs Veugen, Wireless PKI, Informatiebeveiliging, 8 december 2002.
[4] Silvio Micali, Novomodo, Scalable Certificate valdiation And Simplified PKI Management; 1st Annual PKI Research Workshop - Proceedings.

hashwaarden kunnen bijvoorbeeld berekend worden met SHA-1 en zijn dan ieder 20 bytes lang. Deze hashwaarden zijn het revocation target (Is het certificaat herroepen?) en het validity target (Is het certificaat vandaag geldig?).

Voor het revocation target wordt een random gekozen (20-byte) waarde Y0 genomen die als input dient voor de hash-functie SHA-1. De uitkomst van deze hashberekening wordt als het revocation target Y1 in het certificaat gezet. Y0 wordt door de CA geheim gehouden en opgeslagen. Het is ondoenlijk om een inverse hashberekening te doen en zo Y0 uit Y1 te bepalen. Er mag dus worden aangenomen dat uitsluitend de CA over Y0 beschikt. Indien het certificaat herroepen (gerevoceerd) moet worden, wordt Y0 door de CA gepubliceerd. Aangezien het uitvoeren van een hashberekening een eenvoudige en snelle handeling is, kan iedereen vervolgens controleren dat Y0 inderdaad het origineel van Y1 is. Aangezien Y0 uitsluitend bij de CA bekend was en de CA blijkbaar besloten heeft Y0 te publiceren, kan de conclusie getrokken worden dat het certificaat inderdaad herroepen is.
Een voordeel van deze manier van controleren of certificaten herroepen zijn is, dat het berekenen van een hash veel sneller is dan het controleren van een digitale handtekening. Volgens [4] is het berekenen van een hash als SHA-1 wel 10.000 keer sneller. Een ander voordeel is, dat de door de CA gepubliceerde waarde Y0 niet beveiligd hoeft te worden met de handtekening van de CA, omdat gemakkelijk nagerekend kan worden of deze correct is.

De andere hashwaarde in het certificaat, het validity target, gaat uit van hetzelfde principe. Er wordt een random gekozen (20-byte) waarde X0 genomen. Over deze waarde wordt een hashberekening uitgevoerd en over het resultaat ervan wordt weer een hashberekening gedaan. Dit wordt een aantal malen herhaald. Als het certificaat 365 dagen geldig blijft en de CA iedere dag wil laten weten dat het certificaat nog steeds geldig is, wordt 365 keer een hashberekening uitgevoerd over X0. Het resultaat van deze berekening (X365) wordt in het certificaat gezet. X0 en alle tussenliggende waarden (X1, X2, ..., X364) worden door de CA geheimgehouden en opgeslagen . De manier waarop de geldigheidscontrole van een certificaat plaatsvindt is geïllustreerd in Figuur 1. Op de eerste dag dat het certificaat geldig is, publiceert de CA X364. Het uitvoeren van een hashberekening over X364 levert X365 op. Aangezien X364 alleen bij de CA bekend was en de CA besloten heeft deze waarde te publiceren, kan de conclusie getrokken worden dat het certificaat geldig is. De volgende dag publiceert de CA X363. Het uitvoeren van twee hashberekeningen, levert weer de in het certificaat gepubliceerde waarde X365 op. Op deze manier kan gecontroleerd worden dat het certificaat ook op de tweede dag na uitgifte geldig is. Iedere dag wordt door de CA een nieuwe X-waarde gepubliceerd, die aangeeft dat het certificaat op die dag geldig is.



Figuur 1: De geldigheid van een certificaat op dagen binnen Novomodo

Een gebruiker kan elke dag het nieuwe validity proof (geldigheidsbewijs) voor zijn certificaat ontvangen. De gebruiker kan dit dan doorgeven aan iemand die de geldigheid wil controleren en dit kan vervolgens geheel offline gebeuren. Degene die het certificaat wil controleren, moet wel beschikken over de publieke sleutel van de CA om zoals gebruikelijk de handtekening over het certificaat na te rekenen. De hashwaarden zijn alleen bedoeld om te controleren of het certificaat de betreffende dag geldig is.

Voor meer details verwijzen we naar het artikel van Silvio Micali, de bedenker van Novomodo [4]. Novomodo wordt momenteel toegepast in het product Real Time Credential Validation van Corestreet [5].

Vergelijking

Door gebruik te maken van een revocation en een validity target die relatief klein zijn levert Novomodo een kleine besparing in bandbreedte en rekenkracht voor de eindgebruiker ten op zichte van de traditionele PKI. Dit is in [6, 7]

[5] Real Time Credential Validation, Secure, Efficient Permissions Management; White Paper, beschikbaar op http://www.corestreet.com/whitepapers/rtc-introduction.pdf.

[6] Marjo Geers en Thijs Veugen, PKI in draadloze omgevingen op mobiele apparatuur, Informatiebeveiliging nummer 7, november 2003.

[7] Marjo Geers, PKI-oplossingen voor omgevingen met beperkte bandbreedte en rekencapaciteit, NLUUG najaarsconferentie, Ede, 6 november 2003.

uitvoerig beschreven.
Er is een verschil met de traditionele PKI voor de manier waarop certificaten beveiligd zijn. In de traditionele PKI hangt de beveiliging met name op het al dan niet kunnen kraken van de digitale handtekening van de CA. Bij Novomodo is er een extra risico omdat wellicht de inverse van de hashfunctie berekend kan worden waardoor er geen zekerheid meer is over de status en geldigheid van certificaten. Volgens de cryptografische literatuur [8] is de beveiliging van een 2054 bits lange RSA sleutel vergelijkbaar met een 88 bits symmetrische sleutel, en is een symmetrisch algoritme qua snelheid vergelijkbaar met een hashfunctie als SHA-1. Aangezien SHA-1 een inputlengte van 20 byte oftewel 160 bits hanteert is de verwachting dat de beveiliging van Novomodo niet onder hoeft te doen voor de traditionele PKI met een RSA-sleutellengte van 2048 bits. Indien nodig kunnen er in de toekomst voor de validity target en de revocation target grotere waarden gekozen worden.

Voor het bepalen van de status van certificaten en het beheer daarvan zien we de volgende voordelen:

- Er hoeft geen (lange) CRL onderhouden te worden;
- In vergelijking met OCSP is de belasting van de centrale validatieserver gereduceerd;
- Wanneer het systeem wordt gecompromitteerd, is het niet mogelijk om reeds herroepen certificaten weer geldig te verklaren want de revocation target is bekend en alle validity targets zijn vernietigd;
- Indien gebruik gemaakt wordt van gedistribueerde servers voor het opvragen van de status van certificaten, hoeft er bij deze gedistribueerde servers geen beveiligde opslagplaats te vinden. Alleen de eigenlijke server, waar de revocation en validity proofs bewaard worden, moet goed beveiligd zijn. Dit kan een besparing in de kosten opleveren.

Daarnaast maakt Novomodo een aantal nieuwe toepassingen mogelijk. Doordat de geldigheid van een certificaat per tijdseenheid geregeld wordt middels validity targets, is het mogelijk om eenvoudig certificaten tijdelijk 'aan' of 'uit' te zetten. Denk bijvoorbeeld aan een certificaat om een jaar lang muziek te mogen downloaden waarbij de gebruiker per dag kan beslissen of hij ervan gebruik maakt. Een andere mogelijkheid is om attributen aan het certificaat toe te voegen op dezelfde manier als de validity target is toegevoegd. Hiermee zou je bijvoorbeeld roaming door telecom operators kunnen implementeren: het attribuut geeft in dat geval aan of je van een bepaalde operator gebruik mag maken.

De keerzijde van de medaille is dat het gebruik van revocation targets en validity targets niet interoperabel is met de standaard PKI-methoden.

Conclusie

Novomodo is een elegante manier om het valideren van certificaten te verbeteren ten opzichte van de traditionele methoden. De reductie in beheer is zeker voor grootschalige toepassingen van belang. Daarnaast biedt de besparing in bandbreedte en rekenkracht mogelijkheden voor gebruik in een wireless omgeving, en zijn er interessante andere toepassingen mogelijk.
Het nadeel is dat Novomodo niet interoperabel is met de gangbare methoden. Hoewel er reeds producten op basis van het Novomodo concept verkocht worden, lijkt deze achterstand moeilijk in te lopen.

http::

Het artikel van Silvio Micali:
http://www.cs.dartmouth.edu/~pki02/Micali/paper.pdf
Een productbeschrijving van CoreStreet gebaseerd op Novomodo:
http://www.corestreet.com/datasheets/rtcva2.6-datasheet.pdf
Het PKI-lab van TNO Telecom:
http://www.telecom.tno.nl/pkilab/

[8] Arjen Lenstra en Eric Verheul, Selecting cryptographic key sizes, Journal of Cryptology, november 1999.