

Inhoudsopgave

1. Maar het duurt wel twee miljard jaar

2. 'Belgische' beveiligingsstandaard AES iets minder oersterk

Maar het duurt wel twee miljard jaar

Het Nieuwsblad



, , Aan Gent gebonden, Antwerpen, Brugge-Oostkust, Brugge-Oostkust, Brussel-Noordrand, Dender, Kempen, Kortrijk-Waregem-Menen, Leuven-Hageland, Limburg, Mechelen-Lier, Meetjesland - Leiestreek, Oostende-Westhoek, Oostende-Westhoek, Pajottenland, Roeselare-Tielt-Izegem, Vlaamse Ardennen - Gentse Rand, Waasland

18-08-2011, p. 11

De 'onkraakbare' code die de Vlaamse wetenschappers Vincent Rijmen en Joan Daemen elf jaar geleden in elkaar knutselden voor internetbeveiliging, blijkt nu toch enigszins kraakbaar. Maar het duurt wel... twee miljard jaar.

Bijna elke keer als u voor een beveiligde website een wachtwoord moet opgeven, bijvoorbeeld bij internetbankieren, is achter de schermen een stukje wiskundig vernuft van Vlaamse origine aan het werk, de Advanced Encryption Standard (AES), een soort 'geheime code' die de gegevens onleesbaar maakt voor onbevoegden.

In die AES is nu een barstje ontdekt. Dat hebben onderzoekers van de KU Leuven, Microsoft en de Ecole Normale Supérieure in Parijs verteld op een conferentie in de VS. Maar reden tot ongerustheid is er niet, zegt Andrey Bogdanov van de KU Leuven, een van de ontdekkers van de zwakke plek. Als je duizend miljard computers tegelijk aan het werk zou kunnen zetten, die elk een miljard sleutels per seconde zouden kunnen uitproberen (duizend keer meer dan een normale hedendaagse computer), dan werd tot nu toe gedacht dat het acht miljard jaar zou duren om een typische AES-sleutel te kraken. Dankzij de slimme vondst van Bogdanov blijkt nu dat dezelfde computers het in twee miljard jaar zouden kunnen. Nog altijd een hele poos en geen reden om te stoppen met internetbankieren. 'Het is een academische aanval', vindt Vincent Rijmen, een van de twee ontwerpers van AES. 'In de praktijk is er niemand die bezorgd moet zijn.' Rijmen en zijn collega-cryptograaf Joan Daemen verwierven elf jaar geleden kortstondige BV-status met hun beveiligingssysteem. De Amerikaanse overheid maakte toen de winnaar bekend van een internationale competitie om de nieuwe standaard te leveren voor databeveiliging, en die winnaar

was 'Rijndael', de inzending van de twee jonge Vlamingen. Rijndael werd officieel de AES, en wordt sindsdien wereldwijd gebruikt voor het beveiligen van data. Rijk zijn de twee daar niet van geworden, want ze mochten alleen meedoen aan de competitie als alles gratis ter beschikking werd gesteld. Maar het heeft hen wel een carrière in de cryptografie opgeleverd. (STS

)

pdb

© 2011 Corelio

'Belgische' beveiligingsstandaard AES iets minder oersterk



Antwerpen, Limburg, Oost-Vlaanderen, Vlaams-Brabant/Brussel, West-Vlaanderen

18-08-2011, p. 3

Elf jaar geleden verwierven twee Vlamingen internationale roem toen ze de nieuwe Amerikaanse beveiligingsstandaard ontwierpen. Nu is een barstje in hun systeem ontdekt.

Van onze redacteur

Bijna elke keer als u voor een beveiligde website een wachtwoord moet opgeven, bijvoorbeeld bij internetbankieren, is achter de schermen een stukje wiskundig vernuft van Vlaamse origine aan het werk, de Advanced Encryption Standard (AES), een soort 'geheime code' die de gegevens onleesbaar maakt voor onbevoegden. In die AES is nu een barstje ontdekt. Dat hebben onderzoekers van de KU Leuven, Microsoft en de Ecole Normale Supérieure in Parijs verteld op een conferentie in Santa Barbara in de VS.

Maar reden tot ongerustheid is dat niet, zegt Andrey Bogdanov van de KU Leuven, een van de ontdekkers van de zwakke plek in de AES. Als je duizend miljard computers tegelijk aan het werk zou kunnen zetten, die elk een miljard sleutels per seconde zouden kunnen uitproberen (duizend keer meer dan een normale hedendaagse computer), dan werd tot nu toe gedacht dat het acht miljard jaar zou duren om een typische AES-sleutel te kraken. Dankzij de slimme vondst van Bogdanov blijkt nu dat dezelfde computers het in twee miljard jaar zouden kunnen. Vier keer sneller dan gedacht dus, maar het blijft een hele poos. Geen reden dus om uw elektronische portemonnee voortaan gesloten te houden. Zelfs als de computertechnologie nog een paar decennia in het huidige tempo blijft vooruithollen, komt de veiligheid van AES praktisch gesproken niet in gevaar.

De ontwerpers van het AES, de Vlamingen Vincent Rijmen en zijn collega-cryptograaf Joan Daemen, verwierven elf jaar geleden BV-status met hun beveiligingssysteem. Ze wonnen toen een internationale competitie van de Amerikaanse overheid om een nieuwe standaard te leveren voor databeveiliging op computers en het internet. Rijndael, noemden ze hun systeem, met een verwijzing naar hun beider namen. Het Amerikaanse National Institute of Standards and Technology verkoos Rijndael boven de inzendingen van grote bedrijven als IBM en Deutsche Telekom, en van gevestigde namen in de cryptografie (de wetenschap van het versleutelen en ontcijferen van informatie). Rijndael werd officieel de AES, en wordt sindsdien wereldwijd gebruikt voor het beveiligen van data, van het draadloze netwerk bij u thuis tot top secret documenten van de Amerikaanse regering.

Rijk zijn de twee uitvindingsgenoten daar niet van geworden - een voorwaarde om te mogen meedoen aan de competitie was dat alles gratis ter beschikking moest worden gesteld. Maar het heeft ze wel een carrière in de cryptografie opgeleverd. Daemen werkt nu als beveiligingsexpert bij de computerchipfabrikant STMicroelectronics en Rijmen doceert cryptografie aan de KU Leuven - bij dezelfde onderzoeksgroep waar ook Bogdanov werkt, zodat hij de 'aanval' op Rijndael van nabij heeft kunnen volgen.

Al sinds Rijndael als kandidaat-AES werd ingestuurd, hebben onderzoekers geprobeerd er zwakke plekken in te vinden. Dat is nu voor de eerste keer gelukt.

Zou de vondst van een eerste barstje in het pantser van AES wetenschappers er niet toe aanzetten om met vernieuwde energie op zoek te gaan naar zwakke plekken? Rijmen: 'Ja, dat denk ik wel. Er gaan zeker meer mensen op deze wagen springen.' Dat is interessant vanuit wetenschappelijk standpunt, omdat het duidelijk kan helpen maken hoe veilig Rijndael nu precies is, maar Rijmen verwacht niet dat er snel een zwakke plek gevonden zal worden die meer dan een theoretisch gevaar oplevert.

'Het is een "academische, aanval", zegt hij. 'In de praktijk is er niemand die bezorgd moet zijn'. Al houdt hij er wel rekening mee dat nu enkele mensen die de klok hebben horen luiden, hard gaan roepen op blogs en discussieforums. 'Ik zou het me natuurlijk wel een beetje aantrekken als het gebroken zou worden, maar een echt praktische aanval waardoor mensen geld verliezen, daarvoor gaan ze toch nog veel straffere dingen moeten vinden'.

Steven Stroeykens

© 2011 Corelio