



PERSBERICHT

LEUVEN, 17 augustus 2011

Onderzoekers ontdekken eerste barst in Advanced Encryption Standard

Onderzoekers hebben een zwak punt in het AES-algoritme ontdekt. Ze hebben een intelligente nieuwe aanval bedacht waarmee de geheime sleutel vier maal sneller bepaald kan worden dan totnogtoe werd verwacht.

Deze aanval is het resultaat van de samenwerking van drie onderzoekers: Andrey Bogdanov (ESAT/COSIC, K.U.Leuven en gastonderzoeker bij Microsoft Research), Dmitry Khovratovich (Microsoft Research) en Christian Rechberger (ENS Parijs, gastonderzoeker bij Microsoft Research).

Met meer dan honderd miljoen gebruikers wereldwijd is de Advanced Encryption Standard of kortweg AES het belangrijkste algoritme voor de beveiliging van het internetbankieren, draadloze netwerken en bestanden op harde schijven. In 2000 werd het Rijndael-algoritme door het Amerikaanse NIST (National Institute for Standards and Technology) uitgekozen tot Advanced Encryption Standard, een nieuwe encryptiestandaard die de Data Encryption Standard opvolgde. Het Rijndael-algoritme werd ontwikkeld door de Belgische cryptografen Joan Daemen van ST Microelectronics en professor Vincent Rijmen van de K.U.Leuven. Vandaag wordt deze AES gebruikt in meer dan 1700 door NIST gecertificeerde producten en duizenden andere toepassingen. AES is door NIST, ISO en IEEE gestandaardiseerd en door het Amerikaanse National Security Agency (NSA) goedgekeurd voor de bescherming van "secret" en zelfs "top secret" informatie.

Gedurende 15 jaar hebben heel wat wetenschappers de veiligheid van de AES bestudeerd, zonder er ook maar één zwak punt in te vinden. In 2009 werd een probleem zwak punt gevonden wanneer het AES-algoritme gebruikt wordt voor het versleutelen van data met vier verschillende sleutels waartussen een door de aanvaller gekozen verband moet bestaan. Hoewel deze aanval interessant is vanuit wiskundig oogpunt, bestaat er geen toepassing waarin hij relevant zou zijn. De nieuwe aanval daarentegen werkt voor alle versies van de AES, zelfs als er maar één sleutel wordt gebruikt. Deze aanval toont aan dat het bepalen van een AES-sleutel vier maal sneller mogelijk is dan verwacht; met andere woorden: AES-128 gedraagt zich als AES-126. Zelfs met de nieuwe aanval blijft de complexiteit van het bepalen van de sleutel enorm: het aantal vereiste rekenoperaties is een 8 gevolgd door 37 nullen. Dit betekent dat er zelfs met behulp van een biljoen computers die een miljard sleutels per seconde zouden kunnen testen, nog steeds twee miljard jaar nodig zouden zijn om een AES-



128-sleutel te kraken. Ter vergelijking: Google beschikt naar schatting over ruwweg 1 miljoen computers, en een recente machine kan slechts 10 miljoen sleutels per seconde testen.

Omwille van zijn enorme complexiteit heeft deze aanval geen gevolgen voor de praktische veiligheid van de gegevens; toch is dit het eerste echte zwakke punt dat in het veelgebruikte AES-algoritme werd ontdekt.

Meer informatie: Andrey Bogdanov, tel. 0488 156780, e-mail:

andrey.bogdanov@esat.kuleuven.be en website: <http://homes.esat.kuleuven.be/~abogdano/>