**Elliptic Curve Cryptography „Made in Germany“**

***[Essen, 25. Juni 2014]* Elliptische Kurven sind mathematische Strukturen, die immer häufiger für Verschlüsselungsverfahren eingesetzt werden. secunet hat nun gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgreich die Aufnahme neuer elliptischer Kurven in internationale Standards betrieben. Die von der deutschen Arbeitsgruppe ECC Brainpool erzeugten „Brainpool-Kurven“ können somit in den Verschlüsselungsprotokollen TLS (Transport Layer Security) und IPsec (Internet Protocol Security) verwendet werden.**

Neben RSA sind auf elliptischen Kurven basierende Verfahren (Elliptic Curve Cryptography - ECC) die wichtigste Klasse asymmetrischer Krypto-Verfahren. ECC bietet gegenüber RSA unter anderem den Vorteil, dass bei vergleichbarem Sicherheitsniveau wesentlich kürzere Schlüssel zum Einsatz kommen. Dies wirkt sich, neben anderen Faktoren, auch in der Performance der Verschlüsselung, zum Beispiel auf mobilen und rechenschwachen Geräten, aus.

Die Sicherheit von ECC-Verfahren hängt allerdings von den verwendeten Parametern (z.B. den Koeffizienten der Kurve) ab. Da die Prüfung, ob eine Kurve wirklich sicher ist und sich für den Einsatz in der Kryptographie eignet, ungemein aufwendig ist, werden üblicherweise standardisierte Parameter verwendet, für die diese Prüfungen bereits durchgeführt wurden. Zudem vereinfacht die Nutzung einheitlicher Parameter die Interoperabilität zwischen verschiedenen Produkten.

Bislang konnten in Netzwerkprotokollen ausschließlich die vom amerikanischen Standardinstitut NIST festgelegten Kurven verwendet werden. Deren Erzeugung ist allerdings nicht vollständig nachvollziehbar, was im Zusammenhang mit Enthüllungen zu mutmaßlichen Hintertüren in amerikanischen Krypto-Standards aktuell zu erheblicher Kritik geführt hat. Im Unterschied dazu, leiten sich die 2005 von der deutschen Arbeitsgruppe „ECC Brainpool“ generierten Brainpool-Kurven direkt von der Kreiszahl Pi  und der Eulerschen Zahl  ab. Die Ableitung aus den zwei bekanntesten Naturkonstanten sorgt für eine maximale Nachvollziehbarkeit und Transparenz und somit auch für ein hohes Maß an Vertrauen durch die Anwender.

Zum Einsatz kommen die Brainpool-Kurven bereits in deutschen Personaldokumenten (neuer Personalausweis und Reisepass) sowie in den SINA Verschlüsselungsgeräten von secunet. In Zukunft werden sie auch vermehrt zur Absicherung von öffentlichen Infrastrukturen wie zum Beispiel im Smart Meter in intelligenten Stromnetzen oder im Gesundheitswesen verwendet werden.

Um die Brainpool-Kurven auch in TLS und IPSec verwenden zu können, mussten nun die entsprechenden Standards der Internet Engineering Task Force (IETF) erweitert werden. secunet hat diese Standardisierung für das BSI erfolgreich initiiert und begleitet. Damit können nun in diesen Protokollen erstmals elliptische Kurven verwendet werden, deren Auswahl vollständig nachvollziehbar ist und die somit über jeden Verdacht einer Hintertür erhaben sind.

Anzahl der Zeichen: 3.005

**Pressekontakt**

Christine Skropke

Pressesprecherin

Patrick Franitza

Pressereferent

secunet Security Networks AG

Kronprinzenstr. 30

45128 Essen/Germany

Tel.: +49 201 5454-1234

Fax: +49 201 5454-1235

E-Mail: presse@secunet.com

<http://www.secunet.com>

**Über secunet**

secunet ist einer der führenden deutschen Anbieter für anspruchsvolle IT-Sicherheit. Mehr als 300 Experten konzentrieren sich auf Themen wie Kryptographie, E-Government, Business Security und Automotive Security und entwickeln dafür innovative Produkte sowie hochsichere und vertrauenswürdige Lösungen. Zu den mehr als 500 nationalen und internationalen Kunden gehören viele DAX-Unternehmen sowie zahlreiche Behörden und Organisationen. secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

secunet wurde 1997 gegründet und erzielte 2012 einen Umsatz von 67,2 Millionen Euro. Die secunet Security Networks AG ist im Prime Standard der Deutschen Börse gelistet.

*Weitere Informationen finden Sie unter* [*www.secunet.com*](http://www.secunet.com)*.*