Redaktion: Helmut Reimer

Report

Elliptic Curve Cryptography „Made in Germany“

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 und darüber am 25.06.2014 in einer Pressemitteilung informiert. 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.

Neues Gütesiegel: Software Hosted in Germany

Der Bundesverband IT-Mittelstand e.V. (BITMi) bietet seit dem 31.07.2014 ein neues Gütesiegel an. „Software Hosted in Germany“ richtet sich an Software-Hersteller, die besonders sichere, per Internet nutzbare Software anbieten. Mit seiner Initiative möchte der BITMi den IT Standort Deutschland stärken und der vorherrschenden Verunsicherung im Bereich IT Sicherheit entgegentreten.

„Seit der NSA Affäre wird die Informations- und Kommunikationstechnik mit Misstrauen beäugt. Investitionen in Technologien wie Cloud Computing werden nur zögerlich getätigt, weil Unternehmen nicht wissen, wem sie Ihre Daten anvertrauen können“ erklärt Dr. Oliver Grün, Präsident des Bundesverbands IT-Mittelstand. „Unser Gütesiegel zeigt dem Nutzer, dass die Software und Daten in Deutschland gehosted werden und somit deutsches Recht – und vor allem das deutsche Datenschutzrecht – gilt. Indem wir die Software in unser Qualitätssiegel mit einbeziehen, ist nicht nur die Datenablage sicher, sondern auch die Verarbeitung der Daten. So wird Vertrauen in die IT-Sicherheit wieder hergestellt.“

Zur erfolgreichen Vergabe des Gütesiegels müssen vier Kriterien erfüllt sein:

- Die Software und die Daten werden in einem Rechenzentrum in Deutschland gehosted.
- Die Software und die Daten verlassen Deutschland nicht, außer der Auftraggeber verlangt dies.
- Für den Hostingvertrag gilt ausschließlich deutsches Recht, insbesondere das deutsche Datenschutzrecht, das BGB und das HGB.
- Die mit dem Siegel SOFTWARE HOSTED IN GERMANY ausgezeichneten Unternehmen hinterlegen den jeweils aktuellen Standard ihrer technischen und organisatorischen Maßnahmen in Bezug auf den Datenschutz (vgl. § 9 BDSG) beim BITMi e.V.

Weitere Informationen gibt es auf der Homepage *www.software-hosted-in-germany.org* und beim Bundesverband IT-Mittelstand.

NSA-Affäre: Unternehmen ändern Sicherheitsstrategien

68 % der Unternehmen haben im Zuge der NSA-Affäre rund um Edward Snowden und der steigenden Anzahl von Cyber-Angriffen im letzten Jahr ihre Sicherheitsstrategien geändert. So lautet das am 31.07.2014 veröffentlichte Ergebnis einer aktuellen CyberArk-Untersuchung.

CyberArk hat die Untersuchung „Global Advanced Threat Landscape“ bereits zum achten Mal durchgeführt. Dabei wurden 373 (IT-)Führungskräfte aus Unternehmen in Europa, Nordamerika und der Region Asien-Pazifik zu Themen rund um die Datensicherheit befragt.

Die Mehrheit der Befragten sieht die größte Sicherheitsgefahr in der missbräuchlichen Nutzung privilegierter Accounts – sowohl im Hinblick auf Insider- als auch Cyber-Angriffe. So vertreten auch 44%