RSA-Schlüssel seit 2012 angreifbar

Sicherheitsforscher haben einen möglichen Angriff auf das RSA-Kryptosystem vorgestellt. Er erlaubt es, aus dem öffentlichen Teil des Schlüssels den privaten Teil des Schlüssels zu errechnen. Dadurch wird die Sicherheit von Verschlüsselungsschlüsseln untergraben, die unter anderem für die Signierung von Software und von Trusted Platform Modules (TPM) verwendet werden.

Wie Ars Technica berichtet, könnten sich Hacker nun als Inhaber eines geknackten Schlüssels ausgeben oder auch vertrauliche Daten entschlüsseln. Darüber hinaus wäre es möglich, Schadcode in digital signierte Software einzuschleusen oder den Schutz eines TPM zu umgehen, der beispielsweise im Fall des Verlusts eines PCs unerlaubte Datenzugriffe verhindern soll.

Die eigentliche Anfälligkeit steckt demnach in der RSA-Bibliothek Version 1.02.013, die der deutsche Chip-Hersteller Infineon entwickelt hat. Fehlerhaft ist ein Algorithmus, der RSA-Primzahlen generiert. Die Bibliothek wird benutzt, um Schlüssel mit Smartcards oder TPM-Modulen zu erzeugen. Sie ist in Hardware enthalten, die Infineon an zahlreiche Hersteller verkauft, die die Smartcard-Chips und TPMs wiederum in ihre Produkte einbauen. Betroffen sind lediglich RSA-Verschlüsselungsschlüssel, wenn diese mit einer Smartcard oder einem anderen Embedded Device mithilfe der fraglichen Bibliothek generiert wurden.

Da der Bug seit 2012 besteht, sind alle weltweit seitdem mit dieser Bibliothek erstellten Schlüssel als “schwach” einzustufen. Davon betroffen sind auch Regierungen und deren Zulieferer, da die Bibliothek auch von zwei international anerkannten Sicherheitsstandards benutzt wird.

Allerdings ist der Aufwand, einen privaten RSA-Schlüssel zu errechnen, weiterhin sehr hoch. Während dies bei korrekten Schlüsseln mit einer Länge von 2048 Bit als derzeit unmöglich angesehen wird, würde ein normaler Desktop-PC für die Errechnung eines schwachen Schlüssels immerhin noch rund 100 Jahre benötigen. Wird die Rechenlast beispielsweise in die Cloud ausgelagert, reduziert sich dieser Zeitraum deutlich. Tausend Instanzen von Amazon Web Services würden etwa 17 Tage benötigen und Kosten von rund 40.000 Dollar erzeugen, um einen 2048-Bit-RSA-Schlüssel zu knacken. Bei einer Schlüssellänge von 1024-Bit kämen Angreifer mit 45 Minuten und 76 Dollar deutlich schneller und günstiger zum Ziel.

Unter anderem wurden solche unsicheren 2048-Bit-RSA-Schlüssel für den estnischen Personalausweis generiert. Nach Angaben der estnischen Regierung sind nun rund 750.000 Ausweise angreifbar, was die Regierung veranlasste, die Datenbank der öffentlichen Schlüssel zu

schließen, um einen Missbrauch zu verhindern.

Auch Microsoft, Google und Infineon weisen inzwischen darauf hin, dass Produkte, die bestimmte TPM-Chips enthalten, möglicherweise nicht mehr die beworbenen zusätzlichen Sicherheitsfunktionen bieten. Unter anderem ist Microsofts Festplattenverschlüsselung BitLocker angreifbar, falls TPM-Version 1.2 zum Einsatz kommt. Beim TPM 2.0 lassen sich die für BitLocker erzeugten Schlüssel jedoch nicht errechnen. Aber auch PGP-Schlüssel für die Verschlüsselung von E-Mails oder Schlüssel für die Signierung auf GitHub angebotener Software sind betroffen.

Entdeckt wurde die Schwachstelle von Forschern der tschechischen Masaryk University, der Enigma Bridge im britischen Cambridge und der Ca' Foscari University in Italien. Technische Details ihres Angriffs werden sie Anfang November auf der ACM Conference on Computer and Communication Security präsentieren. Dort soll auch die KRACK genannte WPA2-Lücke demonstriert werden.

[mit Material von Stefan Beiersmann, ZDNet.de]