Universitätsleitung

Abteilung Kommunikation und Marketing

Pressemitteilung

Auskunft erteilt	Anja Schuster 0851 509-1430
Telefax	0851 509-1433
E-Mail	kommunikation @uni-passau.de
Datum	2. August 2019

Neuer Weltrekord im Codeknacken stellt Online-Sicherheitssysteme in Frage

Unter Beteiligung der Universität Passau hat ein internationales Team von Mathematikern ein neues Verfahren zum Knacken kryptographischer Codes entwickelt und einen neuen Weltrekord aufgestellt. Die Forscher gehen davon aus, dass eine bestimmte Variante von Verschlüsselungssystemen, die aktuell bei der Absicherung von Online-Transaktionen im Einsatz sind, damit nicht mehr sicher nutzbar ist.

Die Kryptographie, die Kunst des geheimen Schreibens, ist etwa so alt wie die Verbreitung der Schrift selbst, ihre Geschichte so spannend wie aufschlussreich. Die Erkenntnisse der Kryptographie finden in unserem Alltag Anwendung in Form von Verschlüsselungs- und Signatursystemen. Derartige Systeme verwenden Zahlen mit hunderten Stellen um zum Beispiel Bankdaten bei Onlinezahlungen oder vertrauliche Informationen im E-Mailverkehr zu schützen. Die Sicherheit der verbreiteten Public-Key-Verschlüsselungsverfahren beruht im Wesentlichen auf zwei algorithmischen Problemen, dem diskreten Logarithmusproblem und dem Faktorisierungsproblem. Dies sind hochgradig schwierige mathematische Probleme, welche bisher selbst bei Verwendung aktueller Supercomputer Billionen von Jahren zur Lösung benötigten.

Fünf Forschende von der Universität Passau, der École Polytechnique Fédérale de Lausanne (EPFL), dem niederländischen Centrum Wiskunde & Informatica (CWI) und der englischen University of Surrey haben nun ein solches Problem geknackt: Sie berechneten diskrete Logarithmen in einem mathematischen Rechenbereich, einem sogenannten binären Körper, mit genau 30750 Bits, was Dezimalzahlen mit 9257 Stellen entspricht. Diese Größe schlägt den vorherigen Rekord in einem Körper mit 9234 Bits bzw. 2780 Dezimalstellen, welcher 2014 von Robert Granger (Surrey), Thorsten Kleinjung (EPFL) und Jens Zumbrägel (Passau) aufgestellt wurde. Dieses Trio hatte bereits 2014 auch einen 128-Bit-sicheren Industriestandard geknackt, der ebenfalls auf dem diskreten Logarithmusproblem basiert.

Seither haben Granger, Kleinjung und Zumbrägel einen noch schnelleren Algorithmus entwickelt. Einige Kryptographieexperten waren bisher weiter von der Sicherheit entsprechender Verschlüsselungsmethoden ausgegangen und empfahlen diese teils sogar explizit zur Verwendung für Zahlen ab ca. 16000 Bits Größe.

Zusammen mit Arjen K. Lenstra (EPFL) und Benjamin Wesolowski (CWI) hat das Forschertrio das diskrete Logarithmusproblem nun in 30750 Bits gelöst – und so demonstriert, dass solche Empfehlungen nicht haltbar sind. Der neue Rekord benötigte drei Jahre auf verschiedenen Computerclustern. Dies entspricht ca. 2900 Jahre auf einem Single-Core-PC, wie er bis 2005 Standard war. Auch wenn drei Jahre immer noch nach einer langen Zeit klingen: Die mathematischen Fortschritte der letzten Jahre und die immense Steigerung der Rechenleistung machen deutlich, dass diese Variante von Verschlüsselungssystemen bereits heute keine absolute Sicherheit mehr bietet.

Nach der Einschätzung von Dr. Robert Granger, Lecturer in Secure Systems an der University of Surrey, sei der Weltrekord eine fantastische Leistung, welche zeige, dass dieser bislang wesentliche Teil der kryptographischen Welt nun der Vergangenheit angehören sollte. Andererseits gebe es auch konstruktive Anwendungen solch schneller Algorithmen, sogar in der Kryptographie selbst, weswegen Granger von einer Win-Win-Situation spricht. Prof. Dr. Jens Zumbrägel, Inhaber der Professur für Mathematik mit Schwerpunkt Kryptographie, ergänzt: “Solch großformatige Berechnungen helfen uns zu verstehen, wo Gefahren lauern und können zu Einsichten führen, welche in anderen Szenarien angewandt werden. Deswegen sind diese Experimente immens wichtig für die Beurteilung der Sicherheit der heutigen Kryptographie.” Zumbrägel stellt jedoch auch klar, dass andere Kryptosysteme, welche etwa auf Faktorisierung oder diskreten Logarithmen in Primkörpern oder elliptischen Kurven beruhen, nach derzeitigem Stand weiterhin sicher seien.

Rückfragen zu dieser Pressemitteilung richten Sie bitte an das Referat für Medienarbeit, Tel. 0851-509 1439.