Schlüssel für sichere Smartphone-Kommunikation

Schlüssel für sichere Smartphone-Kommunikation
Sichere Verschlüsselung ist auf sichere Schlüssel angewiesen. Anstatt diese mit speziellen Verfahren beispielsweise über das Internet zu erzeugen, schlagen Forscher am KIT vor, diese bei persönlichen Begegnungen automatisch zu erzeugen und von Smartphone zu Smartphone weitergeben zu lassen. Die Schlüssel werden bei jeder Begegnung neu modifiziert, sodass eine Nachricht nur von den beiden Gesprächsteilnehmern gelesen werden kann. "Verwendet man diese über persönliche Treffen ausgetauschten Schlüssel, so wird das Abhören enorm erschwert. Ein Angreifer muss eines der Geräte in der Kette korrumpiert haben, um den Schlüssel zu kennen. Kombiniert man das Verfahren mit heutigen Techniken, so wird der Aufwand für eine Massenüberwachung deutlich erhöht", erläutert Professor Jörn Müller-Quade, Leiter der Arbeitsgruppe für Kryptographie und Sicherheit am KIT.
Schlüsselaustausch in sozialen Netzen
Der Schlüsselaustausch folgt dabei dem sozialen Netz seiner Benutzer: Nur wer sich real begegnet, tauscht auch Schlüssel aus. So gelangen Schlüssel von Freunden zu Freunden der Freunde und so fort. Dadurch können auch zwei nur entfernte Bekannte dank gemeinsamer Freundschaften sicher verschlüsselt kommunizieren. Je mehr gemeinsame Freunde zwei Benutzer haben, desto höher werde die Wahrscheinlichkeit, dass selbst mit spezialisierten Viren oder Trojanern infizierte Smartphones in der Übermittlungskette den letztendlich für die Kommunikation verwendeten Schlüssel nicht berechnen können.
"Unsere Simulationen haben gezeigt, dass selbst bei vielen infizierten Smartphones immer noch ein Großteil der Kommunikationsvorgänge verlässlich vor dem Abhören geschützt ist", ergänzt Dirk Achenbach, ebenfalls Forscher in der Arbeitsgruppe.
Der Grund dafür liegt darin, dass das System bei jedem erneuten Aufeinandertreffen von zwei Personen einen neuen Schlüssel erzeugt. Gelangt auch nur einer dieser Schlüssel über einen Pfad ohne infiziertes Smartphone zum Empfänger, so ist die anschließende Kommunikation sicher. So kann im eigenen sozialen Netz ein stetiger Schlüsselaustausch mit langfristiger Sicherheit entstehen. Eine Gruppe von Studierenden hat im Rahmen der Lehrveranstaltung "Praxis der Software-Entwicklung" der Fakultät für Informatik bereits einen Prototyp entwickelt. Wann ein solches System jedoch auf dem Markt erhältlich sein wird, kann Professor Müller-Quade noch nicht abschätzen.
Tipps zur IT-Sicherheit: "Anti-Prism"-Party am 12.02.2014
Jeder, so Müller-Quade, solle sich aber Gedanken darüber machen, wie die eigenen Kommunikationskanäle vor Angriffen und Datenklau geschützt werden können. "Den hundertprozentigen Schutz gibt es derzeit nicht. Aber jeder kann mit wenigen Mitteln dazu beitragen, den Datendieben ihre Arbeit deutlich zu erschweren". Um diese oft einfachen und kostenfreien Möglichkeiten vorzustellen, veranstaltet die Arbeitsgruppe am 12. Februar 2014 gemeinsam mit der Karlsruher IT-Sicherheitsinitiative (KA-IT-SI) und dem Zentrum für Kunst und Medientechnologie (ZKM) in Karlsruhe eine Verschlüsselungsparty. In einer Abendveranstaltung werden hier verschiedene Möglichkeiten zum digitalen Selbstschutz vorgestellt und anschaulich erklärt.
Informationen zur Party: http://www.anti-prism-party.de/
Das Karlsruher Institut für Technologie (KIT) ist eine Körperschaft des öffentlichen Rechts nach den Gesetzen des Landes Baden-Württemberg. Es nimmt sowohl die Mission einer Universität als auch die Mission eines nationalen Forschungszentrums in der Helmholtz-Gemeinschaft wahr. Thematische Schwerpunkte der Forschung sind Energie, natürliche und gebaute Umwelt sowie Gesellschaft und Technik, von fundamentalen Fragen bis zur Anwendung. Mit rund 9000 Mitarbeiterinnen und Mitarbeitern, darunter knapp 6000 in Wissenschaft und Lehre, sowie 24 000 Studierenden ist das KIT eine der größten Forschungs- und Lehreinrichtungen Europas. Das KIT verfolgt seine Aufgaben im Wissensdreieck Forschung - Lehre - Innovation.
Diese Presseinformation ist im Internet abrufbar unter: www.kit.edu
Die Abbilung steht auf www.kit.edu zum Download bereit und kann angefordert werden unter: presse@kit.edu oder +49 721 608-47414. Die Verwendung des Bildes ist ausschließlich in dem oben genannten Zusammenhang gestattet.

Karlsruher Institut für Technologie
Kaiserstraße 12
76131 Karlsruhe
Deutschland
Telefon: +49 721 608-0
Telefax: +49 721 608-44290
Mail: info@kit.edu
URL: http://www.kit.edu/index.php

<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=556746" width="1" height="1">

Pressekontakt

Karlsruher Institut für Technologie

76131 Karlsruhe

kit.edu/index.php
info@kit.edu

Firmenkontakt

Karlsruher Institut für Technologie

76131 Karlsruhe

kit.edu/index.php
info@kit.edu

Das Karlsruher Institut für Technologie, kurz KIT, ist eine Technische Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft.