LESEN SIE HIER EINIGE HINTERGRÜNDE ZUM

WISSENSCHAFTSTHRILLER „ DIE NANOLITHOGRAFIE“

Datenverschlüsselung: Forscher knacken Quantenkryptografie

Quantenkryptografie gilt als sichere Methode, um Daten verschlüsselt zu übertragen. Doch schwedische Forscher berichten jetzt, sie hätten ein Schlupfloch beim sogenannten Quantenschlüsselaustausch gefunden. "Durch diese Sicherheitslücke ist es möglich, zu lauschen ohne entdeckt zu werden", sagt Jan-Ake Larsson von der Universität in Linköping. Sein Team berichtet zusammen mit Forschern der Uni Stockholm im Fachblatt "Science Advances" von entsprechenden Experimenten. Beim Quantenschlüsselaustausch mittels Verschränkung werden zwei Photonen zum selben Zeitpunkt in verschiedene Richtungen gesendet, schreibt die Universität Linköping in einer Mitteilung. Am anderen Ende der Leitung werden diese Lichtteilchen - vereinfacht gesagt - vermessen und verglichen. Würde jemand versuchen, die Datenübertragung zu belauschen, würde der Empfänger das mitbekommen, weil der Zustand der beiden Lichtteilchen dann nicht mehr gleich wäre. Diese Zustandsänderung durch Beobachtung ist ein Grundprinzip der Quantenmechanik. Haben Sender und Empfänger - in den Experimenten der Schweden stets Alice und Bob genannt - geklärt, dass die Übertagung sicher ist, nutzen sie die gesendeten Photonen, um einen Quantenschlüssel auszutauschen. Mit diesem kann dann einmalig eine auf anderem Weg, etwa per E-Mail, gesendete Nachricht codiert und decodiert werden.

Manipulation an der Quelle

Wie haben die Physiker dieses System geknackt? Sie haben sich in ihrem Experiment der Photonenquelle bemächtigt, des Geräts also, das die Lichtteilchen aussendet. Dieses haben sie durch eine traditionelle Lichtquelle ersetzt, sodass viel mehr Photonen als geplant durch die Leitungen strömten. Den Kontrollmechanismus, auf den sich Sender und Empfänger verlassen, konnten sie dadurch aushebeln. Der Lauscher, in den Experimenten Eve genannt, "muss nur auf die Photonenquelle zugreifen und nicht auf die Messgeräte oder Computer von Alice oder Bob", schreiben die Forscher in ihrem Fachartikel. Aber steht die Quelle nicht auch direkt bei Alice oder Bob? "Ja", antwortet Jonathan Jogenfors, einer der Studienautoren. "Aber trotzdem können beide der Quelle nicht einfach vertrauen. Schickt Alice den Quantenschlüssel, weiß Bob ja nicht, ob sie ihre Photonenquelle unter Kontrolle hat - und andersherum." Der Test, mit dem die Sicherheit des Systems überprüft wird, stelle das gesamte System auf die Probe, inklusive Glasfaserkabel, Spiegel und eben auch der Photonenquelle.

Die Forscher stellen mehrere mögliche Gegenmaßnahmen vor, von denen sie eine bevorzugen: sogenannte sich umarmende Interferometer. Durch die zusätzliche Sicherheitsmaßnahme fliegt Eves Schummelei mit der Lichtquelle auf. Der Nachteil des verbesserten Verfahrens: Es benötigt ein zweites Glasfaserkabel zwischen Alice und Bob. Und die Leitungen müssten perfekt synchronisiert

sein, sagt Jogenfors. Praktisch gesehen wird der Quantenschlüsselaustausch dadurch etwas teurer und aufwendiger.

Am Ende, sagt Jogenfors, gehe es darum, diese Form der Quantenverschlüsselung alltagstauglich zu machen. "Dazu muss das System stabil und sicher sein. Entdecken wir Sicherheitslücken, müssen wir Wege finden, sie zu schließen."

Was hat der Artikel mit meinem Buch zu tun? Achtung Spoiler! Nur so viel- Es treffen sich zwei Photonen…..

Spiegel online, 21.12.2015

Ausrüstung für die Überwachungsindustrie

Ein Katalog der US-Regierung gewährt Einblicke in die technischen Möglichkeiten, die heutzutage zum Abhören der Handy-Kommunikation verfügbar sind. Die Enthüllungsplattform "The Intercept" hat einen Katalog der US-Regierung mit Abhörgerätschaften veröffentlicht, der ihr von einer Geheimdienst-Quelle zugespielt worden sein soll. Die Geräte sind für den Einsatz bei Militär und Geheimdiensten konzipiert, sollen laut dem Bericht aber auch zunehmend von der Polizei eingesetzt werden. Viele der Abhörgeräte geben sich als Basisstation aus, was bei einigen von ihnen auch über mehrere Kilometer Entfernung funktionieren soll. Die einfachen Modelle erfassen dabei lediglich die Position des Handys, andere können auch Gespräche und SMS mitschneiden. Die leistungsfähigeren Abhörgeräte überwachen dabei Tausende Handys gleichzeitig. Der Katalog führt bei allen Abhörgeräten die Fähigkeiten und Grenzen auf. Häufig sind auch Hersteller und Preis genannt. "The Intercept" hat den Katalog der Abhörgerätschaften online gestellt und dabei die Rechtmäßigkeit ihres Einsatzes von Anwälten kommentieren lassen.

Hier der Link zum Katalog:

https://theintercept.com/surveillance-catalogue/

Heise online, KW51

Auch in meinem Buch wird fleißig von der Möglichkeit Gebrauch gemacht den Gegner abzuhören….

Neugierig auf mehr? Dann lesen Sie mein Buch- einfach auf das Bild klicken: