KULTUR NEU ENTDECKEN

SWR KULTUR

Das Wissen

Datenverschlüsselung - Wie Kryptografie unser Leben bestimmt

Von Sven Ahnert

Sendung vom: Freitag, 3. Mai 2024, 08.30 Uhr
Redaktion: Ralf Kölbel
Regie: Günter Maurer
Produktion: SWR 2024

Im Alltag verschicken wir verschlüsselte Textnachrichten, kaufen online ein. Quantencomputer und KI stellen die Kryptografie vor neue Herausforderungen – ein Wettlauf mit der Zeit.

Das Wissen können Sie auch im **Webradio** unter www.swrkultur.de und auf Mobilgeräten in der **SWR Kultur App** hören – oder als **Podcast** nachhören:
https://www.swr.de/~podcast/swrkultur/programm/podcast-swr-das-wissen-102.xml

---

Bitte beachten Sie:
Das Manuskript ist ausschließlich zum persönlichen, privaten Gebrauch bestimmt. Jede weitere Vervielfältigung und Verbreitung bedarf der ausdrücklichen Genehmigung des Urhebers bzw. des SWR.

Die SWR Kultur App für Android und iOS

Hören Sie das Programm von SWR Kultur, wann und wo Sie wollen. Jederzeit live oder zeitversetzt, online oder offline. Alle Sendung stehen mindestens sieben Tage lang zum Nachhören bereit. Nutzen Sie die neuen Funktionen der SWR Kultur App: abonnieren, offline hören, stöbern, meistgehört, Themenbereiche, Empfehlungen, Entdeckungen …
Kostenlos herunterladen: https://www.swrkultur.de/app

MANUSKRIPT

Musikakzent / Rechenmaschine

OT 01, Markus Hinkelmann:
Wenn Sie einen Kryptografen fragen, oder einen aus der Sicherheit: There is no perfect security. Es gibt keine perfekte Sicherheit.

Sprecherin:
So wie Sicherheitsanalyst Markus Hinkelmann es formuliert, könnte dies als Leitmotiv für das gesamte Feld der Kryptografie dienen: Perfekte Sicherheit existiert nicht auf einem Gebiet, das uns alle tagtäglich betrifft: Wir verschlüsseln unsere Kommunikation, senden Textnachrichten, Fotos und kaufen online ein. Normalerweise schützen uns diese Techniken der Verschlüsselung davor, gehackt oder ausgespäht zu werden. Mit den bewährten kryptografischen Algorithmen, die es seit den 1970er-Jahren gibt, funktionierte das bislang relativ gut, doch neue Technologien stellen uns vor neue Herausforderungen: Mit dem Aufkommen von Künstlicher Intelligenz und Quantencomputern steht auch die Verschlüsselungstechnik vor einem Wandel, der die Sicherheit digitaler Kommunikation grundlegend verändern könnte. Ein Wettlauf um die beste Verschlüsselungstechnologie ist entbrannt, der die Zukunft digitaler Kommunikation nachhaltig prägen wird.

Sprecher (Ansage):
„Datenverschlüsselung - Wie Kryptografie unser Leben bestimmt“. Von Sven Ahnert.

Sprecherin:
Verschlüsselung ist Teil unseres Alltages. Immer, wenn wir mit dem Handy telefonieren, einen Online-Shop besuchen, E-mails senden oder Bankgeschäfte erledigen, ist computergesteuerte Verschlüsselung im Spiel. Nicht selten geht dabei etwas schief, wie das Beispiel der Studentin Lisa aus Heidelberg zeigt.

OT 02, Lisa:
Mein Vater hat tatsächlich schon mal sein E-Mail-Programm gehackt bekommen. Und dann wurden Spam-E-Mails von seiner privaten E-Mail-Adresse versendet und dann infolgedessen seine E-Mail eben gesperrt, weil er ja als Scammer erkannt wurde. Dabei war er das gar nicht. Und das war dann auch wirklich ein langwieriger Prozess, seine E-Mail wiederzubekommen.

Sprecherin:
Was im Umfeld verschlüsselter Kommunikation alles misslingen kann, zeigt auch ein brisantes Beispiel aus jüngster Zeit: Das vom russischen Geheimdienst abgehörte Gespräch hochrangiger Luftwaffenoffiziere über den Lenkkörper Taurus. Einer der Teilnehmer hat sich vermutlich über eine nicht sichere Datenleitung in die Konferenz eingewählt, und nicht, wie üblich, über das sichere Konferenzsystem Webex. So konnte das vermeintlich geheime Gespräch leicht gehackt werden und wurde so zum Politikum.

Atmo / Musik

Sprecherin:
Solche und ähnliche Sicherheitslücken, die ein Einfallstor für Hacker und Angreifer bieten, beschäftigen auch die IT-Industrie. Die Firma NXP produziert Mikrochips, die in Autos, Kommunikation und Versorgungssystemen zum Einsatz kommen. Jeder Mikrochip ist mit einer kryptografischen Verschlüsselung versehen. Einige Stockwerke über den Forschungs- und Designräumen in Hamburg befindet sich eines von mehreren Sicherheitsanalysten-Labors, in dem Hacking-Angriffe auf verschlüsselte Mikrochips simuliert werden. Alexander Schlösser ist Sicherheits-Analyst bei NXP und demonstriert einen simulierten Hacker-Angriff auf die verschlüsselte Sicherheitsarchitektur eines Mikrochips mit Blitz-Licht.

Atmo: Labor

Sprecherin:
Auf einem kleinen Tisch steht ein handelsüblicher Laptop an dem zwei Hacking-USB-Sticks mit zwei eingelegten Mikrochips angeschlossen sind. Mit einfachem Equipment, das jeder Elektronikfachmarkt anbietet, ist dieser Experimental-Aufbau selbst für geübte Laien-Hacker durchführbar.

OT 03, *A*lexander Schlösser:
Wir haben zwei Stück. Einmal, das ist das Originale und dann eins, das ich gerne zum Original machen möchte als böswilliger Hacker, indem ich den Geheimschlüssel, der das zum Original erklärt, vom ersten Device auf das zweite Device kopiere. Das heißt, ich muss das aus dem ersten Chip jeweils irgendwie rauskriegen. Das mache ich über einen Angriff auf die Kryptografie, auf die Verschlüsselungstechnologien, die das Ganze ermöglicht. Und zwar läuft auf diesem Device ein Algorithmus, der nennt sich RSA. Der benutzt einen intern gespeicherten Schlüssel, um eine sogenannte Signatur zu generieren, die dem Computer in meinem Fall erklärt: Das ist Original. Das ist gut, kann man benutzen, kann den vollen Strom bekommen vom Ladegerät oder was auch immer. Und dieser Schlüssel, der auf dem Device gespeichert ist, ist das Geheimnis, was der Hersteller bewahren will.

Geräusch / Atmo

Sprecherin:
Wir verlassen uns beim digitalen Verschlüsseln auf eine Technologie, die in ihren Ursprüngen bis in die Antike zurückreicht und möglicherweise sogar schon kriegsentscheidend war. Während der beiden Weltkriege im 20. Jahrhundert konkurrieren die Großmächte darum, die besten Verschlüsselungsmaschinen zu entwickeln und die Nachrichten des Feindes als Erste zu entschlüsseln. Diese Ära markiert einen Höhepunkt in der Geschichte der Kryptografie. Während des Zweiten Weltkriegs ragt vor allem „Enigma“ als eine der bekanntesten Chiffriermaschinen des 20. Jahrhunderts hervor, die sowohl für ihre Komplexität als auch für ihre Effektivität bekannt war.

Musik / Geräusch

Sprecher:
Die „Enigma“ ähnelt einer gewöhnlichen Schreibmaschine und besteht aus drei Walzen mit 26 elektrischen Kontakten, die Buchstaben des Alphabets entsprechen.

Sprecherin:
Alan Turing und sein Team von Krypto-Analytikern spielen eine wichtige Rolle bei der Entschlüsselung von Enigma, die in der legendären Geheimdienstanlage von Bletchley Park, 70 Km nordwestlich von London, stattfand. Eine Arbeit von kriegsentscheidender Bedeutung und sicher die Geburtsstunde der modernen Kryptografie. Kryptografie ist hier ein Teamwork von tausenden Menschen, die im Grunde nichts anderes taten als alle Krypto-Analytiker seit der Antike: Tüfteln, probieren, entschlüsseln.

Sprecherin:
Kryptografie ist mittlerweile eine Alltags-Technik, die sich seit der Antike bis zum Computerzeitalter in den Grundzügen wenig verändert hat. Albrecht Beutelspacher, Mathematiker und Experte für Geheimsprachen, umreißt zunächst das Gebiet der Kryptologie:

OT 04, Albrecht Beutelspacher:
Das klassische Thema ist die Verschlüsselung, also die Übermittlung von Nachrichten von A nach B, so dass kein Dritter aus der übermittelten Nachricht verstehen kann, um was es geht. Da geht es natürlich darum, Verfahren zu entwickeln, mit denen das möglich ist. Das ist die Kryptografie. Andererseits gibt es natürlich auch diejenigen, an die man zunächst nicht denkt, die man ausschließen möchte – nämlich die Angreifer. Die möchten das System knacken. Das ist die Kryptoanalyse. Und in der Regel sagt man, alles zusammen, das Gesamtgebiet ist dann die Kryptologie.

Musik / Geräusch

OT 05, Albrecht Beutelspacher:
Ganz früher war es mit Papier und Bleistift, wo man irgendwelche Geheimzeichen benutzte. Es hat alles nichts mit gedanklicher Durchdringung zu tun. Das leistet die Mathematik.

Sprecherin:
Kryptografie ist (spätestens seit den legendären Tagen der Enigma-Maschine) eine mathematische Wissenschaft, deren wegweisende Arbeiten der US-amerikanische Mathematiker Claude Shannon formuliert hat. Seine entscheidenden Beiträge, veröffentlicht Shannon Ende der 1940er-Jahre. In diesen Arbeiten beschreibt er auf systematische und klare Weise die Konzepte von Verschlüsselung, Systemen, Schlüsseln und der Sicherheit solcher Systeme. So weist er bereits Sätze nach, die erklären, unter welchen Bedingungen perfekte Sicherheit gegeben ist. Albrecht Beutelspacher gibt ein einfaches Beispiel klassischer Verschlüsselung.

OT 06, Albrecht Beutelspacher:
Stellen Sie sich vor, einen Abreißblock, auf dem Nullen und Einsen stehen, in völlig zufälliger Reihenfolge. Und ich nehme das erste Blatt, um meinen ersten Buchstaben zu verschlüsseln. Vielleicht mein erstes Bit. Nimm nun das zweite Blatt, um einen zweiten Buchstaben zu verschlüsseln, das dritte Blatt um einen dritten zu verschlüsseln und werfe die alle anschließend weg. So erhalte ich einen unknackbaren Code, und Shannon hat bewiesen: Das ist die einzige Möglichkeit, einen unknackbaren Code zu erhalten. Also das sind sehr aufwendige Verfahren. Der Schlüssel ist genauso lang wie der Klartext oder der Geheimtext. Praktisch fast nicht zu gebrauchen.

Sprecherin:
Die Ära der mechanischen Verschlüsselung endet spätestens mit dem Aufkommen der ersten Computer. In den 1970er-Jahren sind Computer aufgrund ihrer hohen Anschaffungskosten hauptsächlich Regierungen, Forschungseinrichtungen und großen Unternehmen vorbehalten. In dieser Zeit haben sich zwei grundlegende Verschlüsselungsverfahren etabliert, erläutert Albrecht Beutelspacher.

OT 07, Albrecht Beutelspacher:
Es sind die sogenannten symmetrischen Verfahren. Da gibt es zwei Leute. Einer verschlüsselt, der andere entschlüsselt. Der Verschlüssler hat einen Schlüssel, also eine geheime Information zum Verschlüsseln. Und der Empfänger benutzt genau die gleiche geheime Information zum Entschlüsseln. (…) Die ganz andere Klasse sind die asymmetrischen Verfahren oder auch Public Key- Verfahren genannt. Die wurden erst in der zweiten Hälfte der 70er-Jahre entdeckt. Da ist es so, dass man zum Verschlüsseln keine geheimen Informationen braucht. Ich kann jedem Menschen auf der Welt, ohne vorher mit ihm irgendwie kommuniziert zu haben, das Schlüsselmaterial von ihm empfangen zu haben, eine geheime Nachricht schicken. Nur der Empfänger braucht ein spezifisches Geheimnis, um entschlüsseln zu können. Das war eine Sensation, als das herauskam. Das war eine Revolution des Denkens.

Sprecherin:
Wie nun genau funktioniert dieser asymmetrische Schlüssel? Um das Konzept zu verdeutlichen, nehmen wir zwei fiktive Personen, Peter und Maria, als Beispiel:

Sprecher:
Peter möchte Maria eine verschlüsselte Nachricht senden. Maria generiert ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel, den sie jedem zugänglich macht, und einem privaten Schlüssel, der geheim bleibt. Peter verwendet dann Marias öffentlichen Schlüssel, um die Nachricht zu verschlüsseln. Sobald die Nachricht verschlüsselt ist, kann nur Maria sie mit ihrem privaten Schlüssel entschlüsseln. Auf diese Weise bleibt die Kommunikation sicher, da nur Maria Zugang zum privaten Schlüssel hat.

Sprecherin:
Dieses Beispiel verdeutlicht die grundlegende Funktionsweise des RSA-Algorithmus und die sichere Übertragung von Nachrichten in der Kryptografie.

Der öffentliche Schlüssel funktioniert wie ein Schloss, das jeder nutzen kann, um eine Nachricht zu verschließen und wird daher oft für sichere Kommunikation und digitale Signaturen verwendet, um die Authentizität von Daten zu gewährleisten – wie bei unserer alltäglichen Internetkommunikation.

Atmo: Computergeräusch

Sprecherin:
Schauen wir einfach auf die Browserleiste an unserem Computer, erkennen wir ein kleines Schlüsselsymbol. Es zeigt uns an, dass Server und Computer über eine asymmetrische Sicherheitstechnik sicher kommunizieren. Unsere Kommunikation ist somit verschlüsselt und mehr oder weniger sicher vor Hackern und Zugriffen.

Atmo: Computergeräusch

Sprecherin:
In der analogen Welt weisen wir uns mit offiziellen Ausweisdokumenten aus, um unsere Identität zu belegen. In der digitalen Welt können Zertifikate diese Funktion übernehmen. Marian Margraf, Professor für Informationssicherheit an der Freien Universität Berlin, erläutert ein weiteres alltägliches Beispiel digitaler Signatur.

OT 08, Marian Margraf:
Das Typische, was die meisten draußen kennen, ist Verschlüsselung. Also ich will Daten verschlüsseln, aber es gibt ja auch so etwas wie eine Unterschrift. Also ich bestätige beispielsweise einen Vertrag. Da schreibe ich heute meine Unterschrift drunter und das kann ich auch elektronisch machen, indem ich eine elektronische Signatur benutze. Also ich bin der Inhaber des Geheimschlüssels und stelle meinen öffentlichen Schlüssel zur Verfügung. Dann signiere ich das Dokument mit dem Geheimschlüssel. Und jeder, der den öffentlichen Schlüssel kennt, kann die Signatur überprüfen. Bei asymmetrischer Verschlüsselung ist es ja so: Ich gebe auch meinen Public Key raus. Jeder kann für mich Dokumente verschlüsseln und nur ich als Inhaber des Geheimschlüssels kann die Daten wieder Entschlüsseln.

Sprecherin:
Ein ähnliches Beispiel aus dem Alltag asymmetrischer Verschlüsselung ergibt sich bei der Eingabe unserer Geheimzahl am Bankautomaten. Albrecht Beutelspacher beschreibt dieses routinierte Verschlüsselungsverfahren:

OT 09, Albrecht Beutelspacher:
Nun denkt man zunächst mal, na ja, ganz einfach, auf der Karte steht auch meine Geheimzahl und der Automat liest das. Könnte man so machen, wäre aber blöd, weil dann könnte jeder diese Geheimzahl lesen. Also ist ein Verschlüsselungsalgorithmus zwischengeschaltet. Meine Geheimzahl wird verschlüsselt und mit der verschlüsselten Geheimzahl auf der Karte verglichen. Das heißt, bei Erstellung der Karte wird eine Geheimzahl sich ausgedacht und zufällig gewählt und die wird dann verschlüsselt und auf die Karte geschrieben. Und dann kann das immer wieder verglichen werden, so dass da nichts passieren kann.

Sprecherin:
Ein Meilenstein in der Computerkryptografie ist die Einführung des Verschlüsselungsverfahrens Data Encryption Standard, ein symmetrisches Verschlüsselungsverfahren, das zur sicheren Datenübertragung und -speicherung verwendet wird. Es basiert auf einem Algorithmus, der mithilfe von kompakten Datenpaketen Klartexte in Geheimtexte verwandelt. Zahlenfolgen, Nullen und Einsen, codieren die Buchstaben des Klartextes und werden beständig getauscht, verschoben oder wie bei einem Würfelspiel zufällig erstellt.

Musikakzent

Sprecherin:
Ob ein Schlüssel bei staatlichen Institutionen, dem persönlichen Datenverkehr oder Geschäftstransaktionen eingesetzt wird, spielt bei der Schlüsselberechnung, keine Rolle, erklärt Marian Margraf.

OT 10, Marian Margraf:
Bei Kryptografie machen wir selten so was, dass wir sagen: okay, wir nehmen jetzt mal einen moderaten Angreifer an und deswegen können wir ein schwächeres Verfahren nehmen, hier nehmen wir einen Angreifer mit einem hohen Angriffspotenzial und deswegen müssen wir den Algorithmus besser machen. Das wird in der Kryptografie eigentlich nicht gemacht. Also sobald die Verfahren irgendwie auch nur in die Nähe eines Angriffs kommt, wird es weggeschmissen.

Musik / Geräusch

Sprecherin:
Doch letztlich ist nicht nur ein genialer Schlüssel entscheidend für die Sicherung von Daten und Geheimnissen, sondern auch die technische Einbettung – und vor allem der Faktor Mensch. So sicher auch Verschlüsselungsverfahren wie die am Geldautomaten oder beim Browsen sind, bietet gerade der tagtägliche Mail-Verkehr im Internet oftmals ein attraktives Angriffsziel für Hacker. Lisas Erfahrungen mit ihren Internet-Accounts sind keine Seltenheit.

OT 11, Lisa:
Ich habe bei ganz vielen Accounts früher zumindest nahezu das gleiche Passwort gehabt, und das ist es nicht. Also ich habe dann auch mehrfach zum Beispiel bei Booking.com so Mails bekommen, dass sich jemand in meinen Account eingehackt hat. Dann musste ich meinen booking-Account zum Beispiel schon zurücksetzen. Und dann wurde mir ein bisschen bange, weil ich gedacht habe: Oh Mann, bei dem booking-Account habe ich ja das gleiche Passwort wie überall sonst auch. Und dann habe ich ein bisschen angefangen, das zu ändern.

Sprecherin:
Schwache Passwörter, nichtverschlüsselte Kommunikation, und das Vermischen von privater und beruflicher Kommunikation machen es oftmals sehr leicht für potentielle Angreifer in Sicherheitsstrukturen einzudringen.

Klaus Schmeh, Informatiker und Experte für Kryptografie, gibt zu Bedenken, dass erst ein funktionierendes technisches Umfeld eine gelingende Verschlüsselung garantiert. Ganz gleich, ob im privaten Bereich oder in sicherheitsrelevanten Einrichtungen.

OT 12, Klaus Schmeh:
Wenn wir jetzt so vom Hochsicherheitsbereich reden, da werden dann zwar die gleichen Verschlüsselungsverfahren eingesetzt wie im alltäglichen Bereich, aber da gibt es dann halt für allerlei zusätzliche Sicherheitsvorschriften, wo der Schlüssel gespeichert wird und in welcher Umgebung so ein Verfahren läuft. Am besten nur auf einem Computer ohne Netzwerkanschluss und mit allen möglichen Sicherheitsvorkehrungen und Schutz vor Viren, damit der Schlüssel nicht geklaut wird. Ob überhaupt Passwörter verwendet werden dürfen und wenn ja oder nein, was dann verwendet werden darf als Schlüssel, Spalten und so weiter. Im Drumherum gibt es wesentliche Unterschiede, aber nicht in dem Verfahren selber.

Musikakzent

Sprecherin:
In den nächsten Jahren werden erste Quantencomputer serienmäßig zum Einsatz kommen: Eine neue rechenstarke Technologie, die auch eine neue Form der Verschlüsselung einfordern wird. Quantencomputer sind zunächst einmal keine Wundermaschinen – und sie machen im Prinzip nichts anderes als einen Algorithmus zu berechnen, merkt Albrecht Beutelspacher an:

OT 13, Albrecht Beutelspacher:
Das Hauptproblem der heutigen Kryptografie ist, dass es nur sehr wenige Public Key-Algorithmen gibt. Es gab eine Zeit, in der es nur einen gab, dann einen zweiten. Heutzutage gibt es vielleicht eine Handvoll, wenn man großzügig ist, zwei Handvoll. Jeder neue Algorithmus verändert jedoch unser Verständnis ein wenig. Das besondere Problem besteht darin, dass alle real eingesetzten Algorithmen letztlich auf ähnlichen mathematischen Problemen basieren, wie etwa der Faktorisierung großer Zahlen. Und diese Probleme können alle leicht von Quantencomputern gelöst werden. Was genau Quantencomputer können, ist noch nicht vollständig bekannt. Aber eines ist sicher: Sie können Zahlen faktorisieren.

Sprecher:
Zahlen faktorisieren bedeutet, eine Zahl in kleinere Zahlen zu zerlegen, die, wenn sie multipliziert werden, die ursprüngliche Zahl ergeben. Zum Beispiel: Die Faktoren von 12 sind 1, 2, 3, 4, 6 und 12.

Musik / Geräusch

Sprecherin:
Was sind Quantencomputer und die daran anknüpfende Verschlüsselungstechnik? Quantenkryptografie ist ein Bereich der Kryptografie, der auf den Prinzipien der Quantenmechanik basiert. Die Quantenmechanik beschreibt das Verhalten von Teilchen auf atomarer und subatomarer Ebene. Diese Teilchen können sowohl

Wellen- als auch Teilcheneigenschaften besitzen. Quantenphänomene wie Verschränkung und Unsicherheit prägen dieses mathematische Modell der Natur. Das grundlegende Prinzip der Quantenkryptografie liegt darin, dass das Abhören oder Abfangen von Informationen durch die Gesetze der Quantenmechanik entdeckt werden kann. Klaus Schmeh, Informatiker und Experte für Kryptografie, beschreibt die Zusammenhänge von Kryptografie und zukünftigen Quantencomputern.

OT 14, Klaus Schmeh:
Quantenmechanik ist die Physik der kleinsten Teilchen. Also wenn es um Atome und Elektronen und Atomkerne und solche Dinge geht, dann spielt die Quantenmechanik eine Rolle. Und das interessante daran ist eben, dass es da Dinge gibt, Phänomene, die es im normalen Alltag einfach nicht gibt. Zum Beispiel, dass ein bestimmter Gegenstand an zwei Stellen gleichzeitig sein kann. Das gibt es ja normalerweise nicht, aber auf Quantenebene, auf der kleinsten Ebene, sind solche Phänomene eben trotzdem möglich.

Sprecherin:
Im Gegensatz zur herkömmlichen Kryptografie, die auf mathematischen Problemen wie der Aufteilung großer Zahlen beruht, nutzt die Quantenkryptografie die besonderen Eigenschaften von kleinsten Quantenobjekten, wie zum Beispiel Photonen. Klaus Schmeh:

OT 15, Klaus Schmeh:
Photonen sind ja auch sehr kleine oder minimal kleine Teile oder Wellen, je nachdem wie man es definiert. Und auf dieser sehr kleinen Ebene ist es so, wenn ich ein Photon – was man sich als Lichtblitz vorstellen kann – lese oder wenn ich den Lichtblitz beobachte, dann verändere ich ihn auch und das heißt, wenn ich den lese, dann kommt der nicht mehr unverändert beim Empfänger an und der merkt sofort: Moment, da hat jemand die Finger drin. Also etwas übertrieben gesprochen, ein Werkzeug, um mitzulesen. Und deshalb kann man mit Photonen sehr gut Geheimnisse übertragen, weil sobald jemand das Geheimnis erfährt, verändert er die Photonen und der Empfänger merkts, wenn man es natürlich entsprechend richtig macht.

Sprecher:
Wenn Licht polarisiert ist, bedeutet das, dass die Schwingungen des Lichts in eine bestimmte Richtung ausgerichtet sind, ähnlich wie bei einer Schwingung auf einer Schnur.

Sprecherin:
Im Gegensatz zu herkömmlichen Methoden, bei denen ein Angriff unbemerkt bleiben kann, führt das Abhören von Quantenbits zwangsläufig zu Fehlern im übertragenen Schlüssel. Sender und Empfänger können jedoch durch den Vergleich einiger weniger Bits feststellen, ob ihre Kommunikation sicher war. Der Schlüssel, den sie auf diese Weise erhalten, kann verwendet werden, um Nachrichten zu verschlüsseln, was bisher eine sichere Kommunikation ermöglicht hat.

Atmo: Labor

Sprecherin:
Nicht nur in der alltäglichen Kommunikation, sondern auch in selbstfahrenden Autos, Sicherheitstechnik und Versorgungstechnik spielt die Kryptografie eine zentrale Rolle. In der Hamburger Niederlassung des niederländischen Chipherstellers NXP werden Chips entwickelt, die beispielsweise zu Tausenden in einem Auto verbaut werden. Markus Hinkelmann ist Sicherheitsarchitekt und verantwortlich für Sicherheitskonzepte im Bereich der Halbleitertechnik. Denn auch Mikrochips sind verschlüsselte Systeme und im Zeitalter der Quantencomputer ein mögliches Ziel von Hackerangriffen.

OT 16, Markus Hinkelmann:
Wenn Sie einen Kryptografen fragen oder einen der Sicherheit: There is no perfect security. Es gibt keine perfekte Sicherheit. Aber was wir hier natürlich machen können, ist, das praktisch so weit sicher zu machen, dass man es gut benutzen kann und dass es auch geeignet ist für die Anwendungsfälle und dass man für den Fall, dass noch etwas passiert, auch noch Sicherheitsmaßnahmen einbaut. Sogenannte Fallbacks, dass es dann noch geschützt wird, wie zum Beispiel Safety Mechanism im Auto. Selbst wenn noch etwas schlimmes passiert ist, gibt es noch Sicherheitsmaßnahmen, dass das Auto nicht auf einmal „crasht“.

Atmo: Labor

Sprecherin:
Alexander Schlösser demonstriert einen simulierten Hacker-Angriff auf die verschlüsselte Sicherheitsarchitektur eines Mikrochips mit einem Blitz-Licht.

OT 17, *A*lexander Schlösser:
Jetzt nehme ich mal eine Blitzlampe, also einen ganz normalen Foto-Blitz und schieße auf diesen geöffneten Chip. Das heißt, ich lasse den hier einfach so blitzen. Sieht man auf dem Monitor, dass die Kommunikation irgendwann anfängt auszusetzen. Da ist der Chip komplett aus dem Tritt gekommen. Ist jetzt noch nichts Schlimmes passiert, aber er hat nicht korrekt gerechnet. Und wenn ich das in exakt dem richtigen Abstand mache, dann sieht man: Hier ist er nicht nur aus dem Tritt gekommen, so dass das abgestürzt ist, wie ein Computer abstürzen würde, sondern er hat sich verrechnet. Das heißt, ich habe einen für mich jetzt als Angreifer nutzbaren Fehler erzeugt, wo der kryptografische Algorithmus sich kritisch verrechnet hat.

Sprecherin:
Für den Angreifer sind nun Tür und Tor geöffnet, den Chip auszulesen, neu zu programmieren und zu vermarkten. Oder ihn zu manipulieren und größeren Schaden an sensibler Infrastruktur vorzunehmen. Auf Industrieseite wird mit Hochdruck an neuen Verfahren experimentiert, um diese Lücke zu schließen. So will man die Störanfälligkeit, die auch Rauschen genannt wird, nutzen und mit einer neuen Generation von Zufallsgeneratoren diesen Makel beseitigen helfen.

Musik / Geräusch

Sprecherin:
Wie viel politische Brisanz in der Kryptografie steckt, zeigt nicht nur das vom russischen Geheimdienst abgehörte Gespräch deutscher Luftwaffenoffiziere. In naher Zukunft könnten Quantencomputer in der Lage sein, über Jahre gesammelte, aber nicht dechiffrierte politisch relevante Geheimdaten zu entschlüsseln. Marian Margraf weist auf dieses Problem hin, das besonders die internationale Sicherheits-Politik bestimmen wird.

OT 18, Marian Margraf:
Es gibt aber auch sogenannte Langzeitgeheimnisse, die man heute verschickt. Stellen Sie sich vor, das Auswärtige Amt kommuniziert mit seinen Botschaften und da werden Dokumente hin und her geschickt, die vielleicht zwanzig Jahre vertraulich sein sollen. Was wir wissen ist, wir wissen es von den Amerikanern. Die Chinesen machen das vielleicht genauso. Die Amerikaner nehmen heute ganz viel Internet-Kommunikation auf und speichern diese in der Hoffnung, die irgendwann entschlüsseln zu können. Das ist dieses Thema: Store now, decrypt later – das ist dieses Schlagwort. Deswegen ist man, wenn man heute Langzeitgeheimnisse verschlüsselt, mit unseren Standardverfahren praktisch schon verloren.

Sprecherin:
Ein prominenter Langzeit-Datensammler ist die National Security Agency der Vereinigten Staaten. Der amerikanische Auslandsgeheimdienst sammelt umfangreiche Mengen an verschlüsselten Daten aus verschiedenen Quellen, darunter elektronische Kommunikation, Netzwerkverkehr und andere digitale Informationen. Mit Unterstützung von Künstlicher Intelligenz, wie Deep Learning, wird es möglich sein, selbstlernende Strukturen zu schaffen, die diese Unmengen von Daten nach gängigen Kodierungen abtasten – und den Entschlüsselungs-Vorgang zu beschleunigen. Insofern beinhalten diese schlummernden Daten, die mit Quantencomputern geknackt werden könnten, ein für die nahe Zukunft ungeahntes politisches Machtpotential.

Musik / Geräusch

Sprecherin:
Angekommen auf dem Boden der Tatsachen werden wir jedoch wieder von den Problemen der Alltags-Kryptografie eingeholt. Nicht der Algorithmus, sondern schlicht eines unserer unzähligen Passwörter bereitet Kopfzerbrechen. Lisa jedenfalls setzt auf die Hilfe eines Passwort-Managers.

OT 19, Lisa:
Also generell finde ich diese Passwort-Manager schon supersinnvoll – vor allem auch wenn man jetzt irgendwie ein iPhone hat oder so, dass man das mit Face-ID dann sperren kann und sich diese Passwörter immer automatisch einsetzen kann. Aber da zu hundert Prozent darauf vertrauen – weiß ich auch nicht, ob man das immer kann.

Sprecherin:
Hier kommt es darauf an, ein gutes Hauptpasswort zu finden, das mit Zufallselementen arbeitet, auf die ein durchschnittlicher Hacker gar nicht kommen wird. Zum Beispiel kann man aus einer Fernsehserie oder einem Kriminalroman

einen Satz zitieren, der verkürzt und mit Zahlen versehen, dann einen im Auge des Hackers sinnlosen Anstrich bekommt.

Musik / Geräusch: Rechner

Sprecherin:
Wohin geht die Reise zukünftiger Kryptografie? Angesichts der Herausforderung durch Quantencomputer konzentriert sich die Forschung nun verstärkt auf quantenresistente Kryptografie, um künftige Sicherheitsbedrohungen zu bewältigen. Dabei werden auch Lernsysteme aus dem Bereich der Künstlichen Intelligenz zum Einsatz kommen, die die Produktion von Algorithmen automatisieren werden. Das wird den Handel mit Krypto-Währungen genauso betreffen, wie die alltägliche Kommunikation über das Smartphone. Die Zukunft der Kryptografie wird aber auch von regulatorischen und politischen Entwicklungen beeinflusst sein. Fragen der staatlichen Überwachung, des Datenschutzes und der internationalen Sicherheit spielen hier dann eine wesentliche Rolle: Gibt es vielleicht ein Grundrecht auf Verschlüsselung? Endet das womöglich dort, wo das organisierte Verbrechen oder Kinderpornographie-Plattformen Verschlüsselung für Kapitalverbrechen nutzen? Doch am Ende bleibt die nüchterne Erkenntnis: „Knackbar“ ist irgendwann jede Verschlüsselung. Perfekte Datensicherheit ist und bleibt daher eine Illusion.

Musik / Geräusch

Abspann über neues Jingle „Das Wissen“ mit Musikbett

Sprecher:
„Datenverschlüsselung - Wie Kryptografie unser Leben bestimmt“. Von Sven Ahnert. Sprecherin: Ulrike Schulze. Redaktion: Ralf Kölbel, Regie: Günter Maurer.

* * * * *