Snowden-Dokumente: Was die NSA knacken kann - und was nicht

Von Jacob Appelbaum, Aaron Gibson, Christian Grothoff, Andy Müller-Maguhn, Laura Poitras, Michael Sontheimer und Christian Stöcker

AP/dpa

Die schlechte Nachricht: NSA und GCHQ knacken verschlüsselte Kommunikation im Internet - mit großem Einsatz und Erfolg. Das zeigen Dokumente Edward Snowdens. Die gute Nachricht: Es gibt Systeme, die den Spionen Probleme bereiten.

Montag, 29.12.2014 – 10:15 Uhr

Drucken | Senden | Merken

Nutzungsrechte | Feedback

Kommentieren | 80 Kommentare

Wenn Weihnachten naht, können sich die Mitarbeiter der Überwachungszentrale GCHQ im englischen Cheltenham vom harten Alltagsgeschäft des Ausspähens erholen. Statt Verschlüsselungen in aller Welt zu knacken, spielen sie ihr "Kryptos Kristmas Kwiz". Anspruchsvolle Zahlen- und Buchstabenrätsel sind zu lösen. Die stolzen Gewinner des Wettstreits erhalten eine besondere Teetasse, eine "Kryptos"-Tasse.

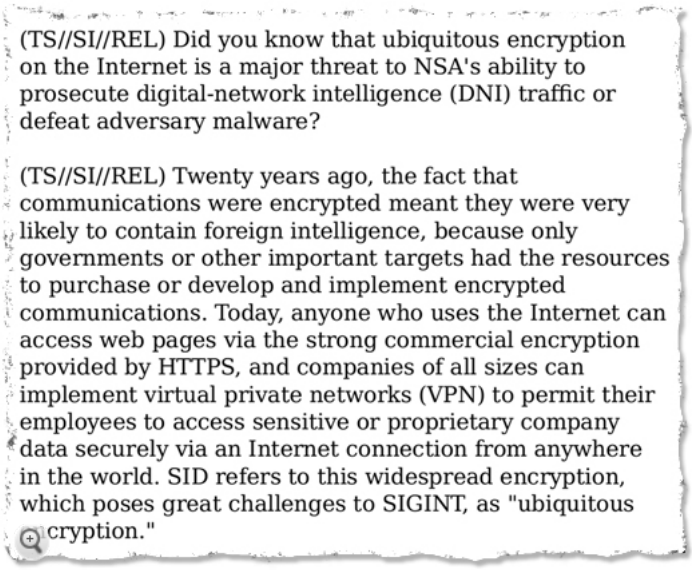
Verschlüsselung - die Nutzung mathematischer Methoden, um Kommunikation vor Ausspähung zu schützen - wird für elektronische Transaktionen aller Art genutzt, von Regierungen, Firmen und privaten Nutzern. Aber ein Blick in das Archiv des Whistleblowers Edward Snowden zeigt: Nicht alle Verschlüsselungstechniken halten, was sie versprechen.

Skype zum Beispiel, das von 300 Millionen Menschen genutzte Programm zum Videotelefonieren, wird als sicher gepriesen. In Wahrheit gibt es diese Sicherheit nicht. "Dauerhafte Skype-Sammlung begann im Februar 2011" - so steht es in einem NSA-Schulungspapier aus dem Snowden-Archiv. Knapp ein halbes Jahr später, im Herbst 2011, meldeten die Spione laut diesen Unterlagen Vollzug. Daten von Skype sind seitdem für die Überwacher zugänglich. Software-Gigant Microsoft, dem Skype gehört, erklärt dazu: "Wir versorgen Regierungen nicht mit direktem oder uneingeschränktem Zugang zu Kundendaten oder Codierungsschlüsseln." Das ist offensichtlich nur ein Teildementi: Eingeschränkte Übermittlung der Kommunikation der Skype-Nutzer ist damit nicht ausgeschlossen. Seit Februar 2011 ist Skype aufgrund der

Anordnung eines geheimen Gerichts als Datenquelle für die NSA verfügbar.

Die "dauerhafte Skype-Sammlung" ist ein weiterer Schritt der Behörde in dem Wettlauf, den sich Überwacher und Überwachte im Internetzeitalter liefern. Manche Codierungen sind allerdings auch so gut, dass sie Jahrzehnte überdauert haben und zu Standards geworden sind.

Für die NSA ist Kommunikation, wenn sie verschlüsselt abläuft, ein einziges Ärgernis. In einem internen Schulungsdokument, das der SPIEGEL einsehen konnte, fragt der Referent: "Wussten Sie, dass allgegenwärtige Verschlüsselung im Internet eine große Bedrohung für die Fähigkeit der NSA darstellt, Aufklärung in Datennetzen zu betreiben oder feindliche Schadsoftware zu bezwingen?"



(TS//SI//REL) Did you know that ubiquitous encryption on the Internet is a major threat to NSA's ability to prosecute digital-network intelligence (DNI) traffic or defeat adversary malware?

(TS//SI//REL) Twenty years ago, the fact that communications were encrypted meant they were very likely to contain foreign intelligence, because only governments or other important targets had the resources to purchase or develop and implement encrypted communications. Today, anyone who uses the Internet can access web pages via the strong commercial encryption provided by HTTPS, and companies of all sizes can implement virtual private networks (VPN) to permit their employees to access sensitive or proprietary company data securely via an Internet connection from anywhere in the world. SID refers to this widespread encryption, which poses great challenges to SIGINT, as "ubiquitous cryption."

Aus den Snowden-Dokumenten lässt sich ersehen, welche Verschlüsselungsverfahren wohl noch sicher sind und welche von der NSA geknackt wurden. Die Dokumente sind etwa zwei Jahre alt, aber Experten halten es für unwahrscheinlich, dass die Schnüffler mittlerweile wesentlich weiter gekommen sind. Snowden selbst erklärte nach seiner Flucht im Juni 2013 in Hongkong: "Richtig eingesetzte, starke Verschlüsselung gehört zu den wenigen Dingen, auf die man sich verlassen kann."

Eine durchaus erstaunliche Bilanz: Trotz aller Bemühungen gibt es Programme, die teilweise mehr als 20 Jahre alt sind - und dennoch wohl bis heute sicher.

Aufgrund der digitalen Revolution ist Kryptografie nicht mehr ein exklusives Werkzeug von Geheimagenten. Inzwischen nutzt nahezu jedermann verschlüsselte Internetverbindungen, sei es beim Onlinebanking, beim Internetshopping oder beim Telefonieren. Netzaktivisten organisieren Kryptopartys, auf denen sie Interessierten das Verschlüsseln beibringen, um sicher und privat zu kommunizieren.

Kanzlerin Angela Merkel und ihr Kabinett nutzen Kryptotelefone. Und die Bundesregierung fordert auch die Bürger auf, sich zu schützen. Der Präsident des Bundesamts für Sicherheit in der Informationstechnik, Michael Hange, erklärte: "Wir schlagen Kryptografie vor, also konsequente Verschlüsselung."

Das kann den Geheimdiensten nicht passen. Die Fünf-Augen-Allianz - die Geheimdienste Großbritanniens, Kanadas, Australiens, Neuseelands und der USA - verfolgt ein klares Ziel. Sie will Verschlüsselung im Netz an so vielen Stellen wie möglich aushebeln. Für ihren Feldzug gegen die Privatheit standen der NSA 2013 über zehn Milliarden Dollar zur Verfügung, der Etat des britischen GCHQ ist Staatsgeheimnis, dürfte aber bei über einer Milliarde Pfund im Jahr liegen.

Im vorigen Jahr berichtete der "Guardian" über eine Präsentation des NSA-Entschlüsselungsprogramms "Bullrun" von 2010. Darin heißt es: "Im vergangenen Jahrzehnt hat die NSA einen aggressiven, vielschichtigen Ansatz verfolgt, um die verbreiteten Verschlüsselungstechniken zu knacken." Und: "Gewaltige Mengen verschlüsselter Internetdaten, die bislang weggeworfen wurden, lassen sich nun auswerten."

REUTERS

Tor-Router zum Selberbauen: Internet-Tarnkappe für 65 Euro

Schutz gegen Internet-Spione: So verschlüsseln Sie Ihre E-Mails

Schutz gegen Internet-Spione: So chatten Sie verschlüsselt

E-Mails, Kurznachrichten, Dateien: Fünfmal Gratis-Sicherheit im Netz

Mehr auf SPIEGEL ONLINE

NSA-Attacken auf SSL, VPN, SSH, Tor etc.: Das sind die Snowden-Dokumente (29.12.2014)

Schutz gegen Internet-Spione: So chatten Sie verschlüsselt (26.07.2013)

NSA-Attacke auf Internetverbindungen: Verschlüsseln ist Notwehr (25.07.2013)

NSA-System XKeyscore: Die Infrastruktur der totalen Überwachung (31.07.2013)

Schutz gegen Internet-Spione: So verschlüsseln Sie Ihre E-Mails (04.07.2013)

Lesen Sie hier die Dokumente von Edward Snowden:

Allgemeine Angriffe gegen Verschlüsselung

Bedienungsanleitung für Analysten, um Skype Verbindungen zu entschlüsseln

Allgemeines Dokument des britischen GCHQ zum BULLRUN Programm

Präsentation des GCHQ zum BULLRUN Programm: Übersicht zu Entschlüsselungsverfahren

LONGHAUL Programm der NSA zum Knacken von Verschlüsselung

BLUESNORT - Ein Programm zur Entschlüsselung von Netzwerkverkehr, um Trojaner und andere Schadsoftware zu erkennen

Präsentation von der SIGDEV Conference 2012 über die unterschiedlichen Schwierigkeitsgrade, die Verschlüsselungstechniken für die NSA darstellen

NSA Programm SCARLETFEVER, mit dem verschlüsselte Verbindungen angegriffen werden (gehört zu TURMOIL)

Erläuterung von VOIP Verschlüsselungsverfahren und Cryptanalyseansätzen bzw. Entschlüsselungsmethoden

Noch ist es eine Minderheit der Internetnutzer, die sich um ihre Privatheit sorgt und ihre Daten schützt. Den anderen erscheint das Verschlüsseln, das sie fälschlicherweise für eine Geheimwissenschaft halten, schlicht zu kompliziert. Oder sie glauben, dass die Experten der Geheimdienste ihnen haushoch überlegen seien und jede Verschlüsselung knacken könnten.

Dem ist nicht so. Wie ein Dokument aus dem Snowden-Archiv belegt, scheiterte die NSA zumindest bis 2012 an der Entschlüsselung mehrerer Kommunikationsprotokolle. Welche das sind, lässt sich diesem Dokument, einer NSA-Präsentation für eine Konferenz im Jahr 2012, entnehmen. Die NSA-Kryptologen teilten ihre Ziele in fünf Gruppen ein, entsprechend dem Schwierigkeitsgrad des Angriffs und entsprechend seinem Ergebnis - von "trivial" bis "katastrophal".

Als "trivial" gilt demnach die Verfolgung des Weges, den ein Dokument im Netz nimmt. "Geringe" Probleme bereitet es angeblich, Facebook-Chats mitzuschneiden; immerhin "mäßiger" Aufwand ist zu betreiben, um Mails des Moskauer Anbieters Mail.ru zu entschlüsseln. Alle drei Schwierigkeitsstufen scheinen der NSA allerdings noch keinen großen Kummer zu bereiten.

Der beginnt wohl auf Stufe vier. "Größere" Probleme bereiten den NSA-Überwachern offenbar E-Mail-Dienstleister, die auf starke Verschlüsselung setzen, etwa Zoho oder das für anonymes Surfen im Internet entwickelte "Tor"-Netz*. Tor steht für "The onion router" und ist eine freie offene Software, mit der sich der Nutzer einen verschlungenen Weg durch mehr als 6000 Computer von Freiwilligen bahnt. Die Daten werden, wie bei einer Zwiebel, von einer Verschlüsselung nach der anderen umhüllt und wieder befreit. Für Überwacher ist so kaum zu rekonstruieren, woher der Aufruf einer bestimmten Website stammte.

Deanonymisierung

Erläuterung eines möglichen Verfahrens zur Deanonymisierung von TOR Datenverkehr

Analyse der Sicherheit von verborgenen Services im TOR Netzwerk

Übersicht über verfügbare Anonymisierungstechniken und wie sie funktionieren (2011)

Forschungsansätze zur Deanonymisierung von TOR Verbindungen

Übersicht über die Verfahren des TOR Netzwerks

Deanonymisierungsansätze gegen TOR

"Größere" Probleme hat die NSA auch mit Truecrypt, einem Programm zur Verschlüsselung von Dateien auf Computern, und mit dem sogenannten Off-the-record-Protokoll (OTR) zur Codierung von Chats. Beides sind Open-Source-Projekte, also Programme, deren Quellcode jeder Interessierte einsehen kann. Solche Software, darin sind sich die Experten einig, ist viel schwieriger von Geheimdiensten zu manipulieren als Systeme, die Konzerne wie Apple oder Microsoft entwickeln. Schließlich kann sich bei Open-Source-Projekten jeder den Programmcode ansehen, heimliche Hintertüren lassen sich kaum

einbauen. Bei der Überwachung eines Chats stellte die NSA frustriert fest: "Keine Entschlüsselung verfügbar für diese OTR-verschlüsselte Nachricht." Zumindest manchmal scheitert die NSA also an OTR.

"Katastrophal" - Stufe fünf - wird es für die NSA, wenn eine Zielperson beispielsweise eine Kombination aus Tor und einem weiteren Anonymisierungsdienst, wie dem quelloffenen Instant-Messaging-System Cspace, nutzt. "Fast vollständiger Verlust von Erkenntnissen über die Kommunikation und den Aufenthaltsort der Zielperson" sei die Folge einer solchen Kombination.

Kryptografische Analysen allgemein

Allgemeine Erläuterung, wie die NSA mit verschlüsseltem Datenverkehr umgeht

E-Mail Verschlüsselung funktioniert. Abgefangene, mit PGP verschlüsselte E-Mail kann die NSA nicht entschlüsseln

Klassifizierungsregelwerk für die Cryptoanalyse

Dokument des britischen GCHQ zur Einreichung von verschlüsseltem Datenverkehr an die Entschlüsselungsabteilung

Gemeinsames Arbeitspapier von NSA und GCHQ zum Vorgehen bei Entschlüsselungsprojekten (TLS/SSL, IPSEC)

Klassifizierungsrichtlinie für die Modernisierung der Nutzung von Verschlüsselung innerhalb der NSA

Newsletter des "National Information Assurance Research Laboratory (NIARL)": Stichwort TUNDRA führt zu einer AES Analysemethode

Was deine Mutter dir nie über die Entwicklung der Signalanalyse erzählt hat: Methoden zur Identifizierung von Netzwerken, Routern und VPN

Abgefangener Chat mit OTR, Entschlüsselung gescheitert

Zur sicheren Verschlüsselung von Gesprächen und Textchats auf Mobiltelefonen gibt es das Protokoll ZRTP, das der NSA anscheinend größere Probleme macht. Es wird etwa in den Open-Source-Programmen RedPhone und Signal verwendet. Ihr Entwickler Moxie Marlinspike sagt: "Es ist sehr befriedigend, dass für die NSA die mit unseren Apps verschlüsselte Kommunikation wie ein Blick durch Milchglas ist."

Entwickelt hat ZRTP unter anderen der Amerikaner Phil Zimmermann, der Mann, der den bis heute gebräuchlichsten Verschlüsselungsstandard für E-Mails und Dokumente geschaffen hat. Er ist bekannt unter der Abkürzung PGP, ausgeschrieben: Pretty Good Privacy - ziemlich gute Privatsphäre. Auch an diesem mehr als 20 Jahre alten Verschlüsselungsstandard beißen sich die NSA-Spione offenbar die Zähne aus. In einem weiteren Dokument, das der SPIEGEL einsehen konnte, heißt es über E-Mails, die sich die NSA vom E-Mail-Provider Yahoo verschafft hat: "Für diese PGP-verschlüsselte Nachricht ist keine Entschlüsselung verfügbar."

Phil Zimmerman schrieb PGP im Jahr 1991. Der Anti-Atomwaffen-Aktivist wollte sich unbehelligt mit Gleichgesinnten austauschen. Sein System erfreute sich schnell hoher Beliebtheit unter Dissidenten in aller Welt. Da es auch außerhalb der USA verwendet wurde, setzte die US-Regierung gegen Zimmermann Ermittlungen wegen des "Exports von Munition" in Gang. Zimmermann veröffentlichte daraufhin mit Freunden den Quellcode als Buch - dies war durch die in der Verfassung garantierte Meinungsfreiheit abgedeckt.

PGP gibt es heute in verschiedenen weiterentwickelten Varianten, die häufigste ist "GNU Privacy Guard" des deutschen Programmierers Werner Koch. Zu den Eigenheiten der Spionagewelt gehört es, dass auch britische und amerikanische Geheimdienstmitarbeiter eine PGP-artige Software zum Verschlüsseln nutzen.

Tatsächlich decken sich die Interessen von Hackern, die ihre Privatheit schützen wollen, und US-Behörden häufiger, als man erwarten könnte. Das Tor-Projekt - für das auch die Co-Autoren dieses Artikels, Jacob Appelbaum und Aaron Gibson, arbeiten - wurde ursprünglich mit Unterstützung der U.S. Navy entwickelt, um US-Geheimdiensten eine

sichere Kommunikation zu ermöglichen.

Die Snowden-Dokumente können einerseits also all jene beruhigen, die der NSA alles zugetraut haben: Es scheint noch geschützte Wege zu geben. Andererseits belegen die Dokumente, dass die Überwachung schon sehr weit geht.

Ein Beispiel: "Virtual Private Networks", VPN, wie es vor allem Mitarbeiter von Firmen und Institutionen mit mehreren Standorten nutzen. Der Schutz des Netzes ist hier tatsächlich nur virtuell, nicht echt. Denn die NSA betreibt ein großes VPN-Projekt, um solche Verbindungen massenhaft zu knacken und die darüber ausgetauschten Daten mitzulesen - etwa das Netz der griechischen Regierung.

Angriffe auf VPN

Beschreibung des TURMOIL / APEX Systems zum Angriff auf Virtuelle Private Netze (VPN)

Erläuterung des GALLANTWAVE Programms, mit dem innerhalb von LONGHAUL VPN Verbindungen entschlüsselt werden

NSA Einführung in den VPN Auswertungsprozess mit Hinweis auf die angegriffenen Protokolle (IPSEC, PPTP, SSL, SSH) und vielen Beispielen

Zusammenspiel aktiver und passiver Methoden im Kontext von Angriffen auf VPN

Erläuterung des Valiantsurf Programms im Kontext von Angriffen auf VPN

MALIBU Architektur um VPN Kommunikation ab– bzw. anzugreifen

POISONNUT Programm zum Angriff auf VPNs zur Entschlüsselung

Präsentation, die die Entwicklung von Angriffstechniken auf VPN behandelt

NSA Präsentation in der die Analyse, Kontextualisierung und Vorgehensweise zu Angriffen auf VPN erläutert wird

Beschreibung bestehender Projekte von VPN Entschlüsselungen

Erläuterung der TEe Komponenten um VPN Verbindungen anzugreifen

Erklärung des POISONNUT Produktes, um Angriffe auf VPN durchzuführen

Erläuterung des TURMOIL GALLANTWAVE Programms, um VPN Verbindungen anzugreifen

Verarbeitung von Daten aus angegriffenen VPN im TURMOIL Programm

Entschlüsselung von VPN Verbindungen im VALIANTSURF Programm

Technische Erläuterung, wie TURMOIL die IPsec Datenpakete von VPN Netzen abzweigt und angreift

Ausführliche Erläuterung des SPIN9 Programms zum Angriff auf bzw. zur Entschlüsselung von VPN

Schon für Ende 2009 ist in einem NSA-Dokument davon die Rede, dass tausend Anfragen zur Entschlüsselung von VPN-Verbindungen verarbeitet werden müssten - pro Stunde. Bis Ende 2011 sollte diese Zahl auf 100.000 pro Stunde gesteigert werden. "Mindestens 20 Prozent" dieser Anfragen sollte das System vollständig erfüllen, also den Datenverkehr "entschlüsseln und wieder einschleusen".

Mit anderen Worten: Bereits für Ende 2011 sahen die Pläne der NSA vor, 20.000 vermeintlich sichere VPN-Verbindungen pro Stunde parallel auszuspähen.

Als unsicher muss auch das Protokoll PPTP gelten, ein zentraler Bestandteil vieler VPN. In der NSA-Präsentation "Einführung in den VPN-Ausspähprozess" wird stolz vom Projekt "FOURSCORE" berichtet, das PPTP entschlüssle.

Dadurch sei der Zugang zu zahlreichen Netzwerken gelungen. Ausgespäht wurden etwa die russische Transaero Airlines, Royal Jordanian Airlines und die Moskauer Telekommunikationsfirma Mir Telematiki. Als Erfolg gepriesen wird auch die Überwachung der internen Kommunikation afghanischer, pakistanischer und türkischer Diplomaten.

Für die etwas besseren Verfahren wie IPSEC hat die NSA Angriffsmöglichkeiten entwickelt, mit denen nicht das Verfahren geknackt wird, sondern die Schlüssel entwendet werden.

Weniger Aufwand ist notwendig für einen Angriff auf all jene vermeintlich sicheren Verbindungen, die jeder Internetnutzer ständig verwendet: um Bankgeschäfte zu erledigen, online einzukaufen oder den Web-E-Mail-Account einzusehen.

Angriffe auf SSL/TLS

Experiment zur massenweisen SSL/TLS Entschlüsselung

Dokument des kanadischen CES zur Analyse von TLS Schlüsseln (Mai 2012)

Programm SCARLETFEVER zum Angriff auf SSL/TLS Verbindungen

Analyse von SSL/TLS Verbindungen durch den britischen GCHQ unter Nutzung der "Flying Pig" Datenbank

Sicher ist nichts davon. Die NSA kann mit einem Programm sogar das Protokoll SSH ("Secure Shell") knacken. Mit SSH-Verbindungen loggen sich Administratoren ein, um mit anderen Computern zu arbeiten und sie zu steuern. Die Schnüffler sammeln die so gewonnenen Daten zusammen mit anderen Informationen über geknackte Verschlüsselungen in einer Datenbank. Für andere Systeme gibt es ebenfalls Datenbanken.

Telefonsysteme in aller Welt beruhen auf entzifferter Verschlüsselung und sind so gestaltet, dass sie für das Abschöpfen anfällig sind. In den Snowden-Dokumenten lässt sich nachvollziehen, dass die NSA sich Zugang zu Daten verschafft hat, die von Strafverfolgern bei Ermittlungen beschafft wurden, zum Beispiel in Russland und im Irak. Die NSA erklärt zu diesen und allen anderen Vorwürfen, dass sie sich strikt an die US-Gesetze halte.

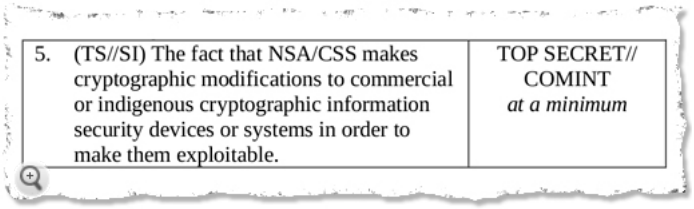
Die NSA reklamiert für sich und ihre Verbündeten, solche Verbindungen routinemäßig und millionenfach zu knacken. Für Ende 2012 sieht ein NSA-Dokument zehn Millionen geknackte https-Verbindungen pro Tag vor. Besonders interessieren sich die Überwacher für den Moment, in dem ein Nutzer sein Passwort eintippt: 20.000-mal im Monat sollte das System Ende 2012 jeweils "mindestens 100 Passwort-basierte Verschlüsselungsanwendungen entdecken". Erkenntnisse über Verschlüsselungen mit den verbreiteten Protokollen TLS und SSL sammelt der britische Geheimdienst in der Datenbank "Flying Pig", fliegendes Schwein.

Und wie kommt die NSA an all die geheimen Schlüssel?

Wie schaffen es die Nachrichtendienste, die Verschlüsselungsstandards und Systeme zu knacken? Die kurze Antwort lautet: Sie nutzen alle vorhandenen Mittel. Eine Methode ist es, bewusst die kryptografischen Standards dieser Systeme zu schwächen.

Snowden-Dokumente zeigen, dass NSA-Agenten zu den Treffen der Internet Engineering Task Force (IETF) anreisen, einer Organisation, die solche Standards entwickelt. Dort sammeln sie Informationen, aber sie versuchen wohl auch, die Diskussionen in ihrem Sinne zu beeinflussen. "Die Erweiterung der Sitzungs-Policy könnte unsere Fähigkeit verbessern, passiv zweiseitige Kommunikationen zu überwachen", heißt es etwa in einem kurzen Bericht über ein IETF-Treffen in San Diego.

Diese Bemühungen um geschwächte Verschlüsselungsstandards laufen schon längere Zeit. In einer Klassifizierungsanleitung aus dem Jahr 2005, in der die Einordnung in Geheimhaltungsstufen erklärt wird, heißt es: Es ist "Top secret", "dass die NSA/CSS an kommerziellen oder einheimischen kryptografischen Informationssicherheitssystemen oder -geräten kryptografische Veränderungen vornimmt, um sie angreifbar zu machen."



5.	(TS//SI) The fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information security devices or systems in order to make them exploitable.	TOP SECRET// COMINT *at a minimum*

Auf diese Weise aktiv geschwächte oder von Anfang an mangelhafte Verschlüsselungssysteme werden dann mit Hilfe von Supercomputern ausgebeutet. Longhaul etwa ist im NSA-Jargon "ein Dienst für die Orchestrierung von Ende-zu-Ende-Angriffen und die Gewinnung von Schlüsseln aus verschlüsseltem Netzwerk-Traffic".

Zu Deutsch: Longhaul ist der Ort, an dem die NSA Verschlüsselungen zu knacken versucht. Laut einem NSA-Dokument dient dazu Infrastruktur im Tordilla Supercomputer-Gebäude in Fort Meade in Maryland und im Oak Ridge Data Centers in Oak Ridge, Tennessee.

Longhaul kann entschlüsselte Daten weitergeben an Systeme wie Turmoil, einen Teil des geheimen Datennetzwerks, das die NSA rund um die Welt betreibt, um Daten abzusaugen. Das Ziel solcher Systeme ist es, fließenden Datenverkehr live zu entschlüsseln, natürlich ohne dass die Ausgespähten etwas davon merken.

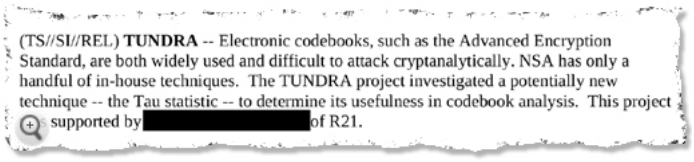
In anderen Fällen stehlen die Spione Schlüssel aus den Konfigurationsdateien, die sie in Internet-Routern finden. Ein "Discoroute" genanntes Depot enthält laut einem Dokument "Router-Konfigurationsdaten aus aktiver und passiver Sammlung". Aktiv bedeutet in diesem Zusammenhang, sich in einen Computer zu hacken oder ihn auf andere Weise zu infiltrieren, passiv meint das Sammeln von vorbeifließenden Daten aus dem Internet mithilfe geheimer NSA- oder GCHQ-Computer.

Um Verschlüsselungen knacken zu können, sammeln die Dienste riesige Mengen von Daten, zum Beispiel sogenannte SSL-Handshakes, also den ersten Kontakt, wenn Computer eine SSL-Verbindung aufbauen. Eine Kombination von Metadaten der Verbindungen und Metadaten der Verschlüsselungsprotokolle hilft dann dabei, auf die Schlüssel zu kommen. Das wiederum ermöglicht schließlich das Mitlesen.

Wenn alle Stricke reißen, greifen die NSA und ihre Verbündeten zu direkteren Methoden. Sie hacken die Computer oder Router ihrer Zielpersonen, um der geheimen Schlüssel habhaft zu werden. Oder sie halten neu bestellte Computer auf dem Weg zu Zielpersonen auf, schrauben sie auf und bauen Spionagewerkzeuge ein. Diesen Prozess nennen sie Interdiction.

Für die NSA ist der Kampf gegen die Verschlüsselung ein ständiger Interessenkonflikt. Die Behörde und ihre Verbündeten haben ihre eigenen geheimen Verschlüsselungsmethoden zur internen Verwendung. Aber die NSA hat auch die Aufgabe, für das National Institute of Standards and Technology, NIST, eine Art US-DIN, "technische Richtlinien für vertrauenswürdige Technologien" zu liefern, die für "kostengünstige Systeme zum Schutz sensibler Computerdaten" genutzt werden könnten. Mit anderen Worten: Die Beurteilung von Verschlüsselungssystemen ist Teil des Jobs der NSA. Ein Verschlüsselungsstandard, den NIST und NSA ausdrücklich empfehlen, ist etwa der Advanced Encryption Standard (AES). Er wird für eine Vielzahl von Aufgaben verwendet, vom Verschlüsseln der PIN-Nummern auf Bankkarten bis hin zur Absicherung von Festplatten.

Ein NSA-Dokument zeigt, dass die Agenten nach Wegen suchen, ebenjene Verschlüsselung zu knacken, wobei die Passage als "Top secret" eingestuft ist. "Elektronische Chiffren wie der Advanced Encryption Standard sind verbreitet und kryptografisch schwierig anzugreifen. Die NSA verfügt nur über eine Handvoll In-house-Techniken. Das TUNDRA-Projekt untersuchte eine potenziell neue Technik - die Tau-Statistik -, um ihren Nutzen bei der Chiffre-Analyse festzustellen."


(TS//SI//REL) **TUNDRA** -- Electronic codebooks, such as the Advanced Encryption Standard, are both widely used and difficult to attack cryptanalytically. NSA has only a handful of in-house techniques. The TUNDRA project investigated a potentially new technique -- the Tau statistic -- to determine its usefulness in codebook analysis. This project supported by [redacted] of R21.

Große Teile der Verschlüsselungssysteme, auf denen das Internet aufgebaut ist, haben die NSA und ihre Verbündeten gezielt geschwächt. Für alle anderen, die auf das Internet angewiesen sind, bedeutet das eine große Gefahr, seien es Individuen, die auf Privatsphäre Wert legen, oder Institutionen und Firmen, die Cloud Computing nutzen. Diese Schwächen können nicht nur von der NSA ausgenutzt werden, sondern von jedem, der sie kennt.

Diese Gefahr ist unter den Lauschern wohlbekannt. Laut einem NSA-

Dokument aus dem Jahr 2011 waren damals allein 832 Mitarbeiter des GCHQ über das Projekt BULLRUN unterrichtet worden. Dessen Ziel ist ebendieser Großangriff auf die Sicherheit des Internets.

**Anmerkung der Redaktion: Zwei der Autoren dieses Textes, Jacob Applebaum und Aaron Gibson, arbeiten auch am Tor-Projekt mit. Appelbaum ist auch in die Entwicklung von OTR involviert.*

Zur Startseite

Das könnte Sie auch interessieren

Neue Snowden-Dokumente

Die NSA rüstet zum Cyber-Feldzug

Die Geheimdienste betreiben nicht mehr nur Überwachung und Spionage. Dokumente aus dem Fundus von Edward Snowden, die dem SPIEGEL vorliegen, zeigen: Sie wollen die Herrschaft im Internet und bereiten digitale Kriege vor. mehr...

Rekordgewinn mit fragwürdigen Methoden

Apples schmutzige Milliarden

Apple verdiente 18 Milliarden Dollar in drei Monaten. Kein Konzern hat je so viel Gewinn gemacht. Profitabel ist der iPhone-Hersteller auch wegen fragwürdiger Geschäfte. Wir nennen vier besonders zweifelhafte Methoden. mehr...

Bettina Wulff bei Sarah Kuttner

Sülze mit der Ex

mehr...

Russlands Präsident

Glaubt Putin die eigene Propaganda?

Wladimir Putin hat ein taktisches Verhältnis zur Wahrheit: Vor der Krim-Annexion log er, um Zeit zu gewinnen. Doch Russlands Präsident verheddert sich im Netz der Lügen - und wirkt oft schlecht unterrichtet. mehr...

Video-Empfehlungen

Der Bürohit: Prism is fascism

TV-Interview mit Edward Snowden: "Ich war ein Hightech-Spion"

Bernd Luckes E-Mails: "Er schielt auf den rechten Rand"

Forum ▶

Diskutieren Sie über diesen Artikel
insgesamt 80 Beiträge

Alle Kommentare öffnen

Seite 1 von 16

1. Es gibt keine Sicherheit in der IT Branche
mweldag 29.12.2014
Jeder IT Security Spezialist wird dies bestätigen. Die Massnahmen dienen nur dazu um ein Eindringling das Leben so schwer zu machen so dass der Zeitaufwand -> Profit/Benefit zu gross wird um wieder abzulassen. Die NSA hat halt [...]

2. Überflüssig
winterfichte 29.12.2014
Auch andere Geheimdienste spionieren. Die Daten werden gescannt und nicht abgehört. Als Bürger fühle ich mich nicht bedroht, wohl aber von Terroristen. Mein Gespräch mit meinem Vater wird die kaum interessieren. Jedes [...]

3. Vielen Dank
Raphaeloo 29.12.2014
Vielen Dank für die Mühe und die Arbeit aller Autoren solcher Themen. Ich Schätze das sehr. Nicht unsere Geheimdienste sind die Beschützer unserer Demokratischen Werte, sondern diese Leute. Wie sollte unser Sytem noch [...]

4. Guter Artikel!
MHB 29.12.2014
Gut recherchiert, viele weitergehende Informationen. VIelen zu selten dieser Tage. Nun ja, für den Fall der Fälle hoffe ich, Bluffdale und Fort Meade sind bei den Russen und Chinesen jeweils mind. mit einem Sprengkopf bedacht [...]

5. Grob fahrlässig!
solarflair 29.12.2014
Die Vorstände und Geschäftsführer in Deutschland sollten alarmiert sein! Know-How Diebstahl selbst in firmeneigenen "abgeschlossenen" VPN Netzwerken scheint an der Tagesordnung zu sein. Die Industrie sollte sich [...]

Alle Kommentare öffnen

Seite 1 von 16

Ihr Kommentar zum Thema

Bitte melden Sie sich an, um zu kommentieren. Anmelden | Registrieren

Überschrift optional

Beitrag

Kommentar senden

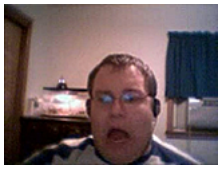
News verfolgen

Lassen Sie sich mit kostenlosen Diensten auf dem Laufenden halten: Hilfe

alles aus der Rubrik Netzwelt	Twitter |	RSS
alles aus der Rubrik Netzpolitik		RSS
alles zum Thema NSA-Überwachung		RSS

MEHR AUS DEM RESSORT NETZWELT

BEST OF WEB



Netz-Fundstücke: Was Sie im Internet unbedingt sehen müssen

SILBERSCHEIBEN

Das lohnt sich: Die besten CD- und DVD-Schnäppchen

BILDERWELTEN

Bessere Fotos: So holen Sie ganz einfach mehr aus Ihren Bildern raus

ANGEFASST

Gadget-Check: Handys und anderes Spielzeug in Matthias Kremps Praxistest

ANGESPIELT

Game-Tipps: Spiele für Computer und Konsole im SPIEGEL-ONLINE-Test

ÜBERSICHT NETZWELT ▶

▲ TOP