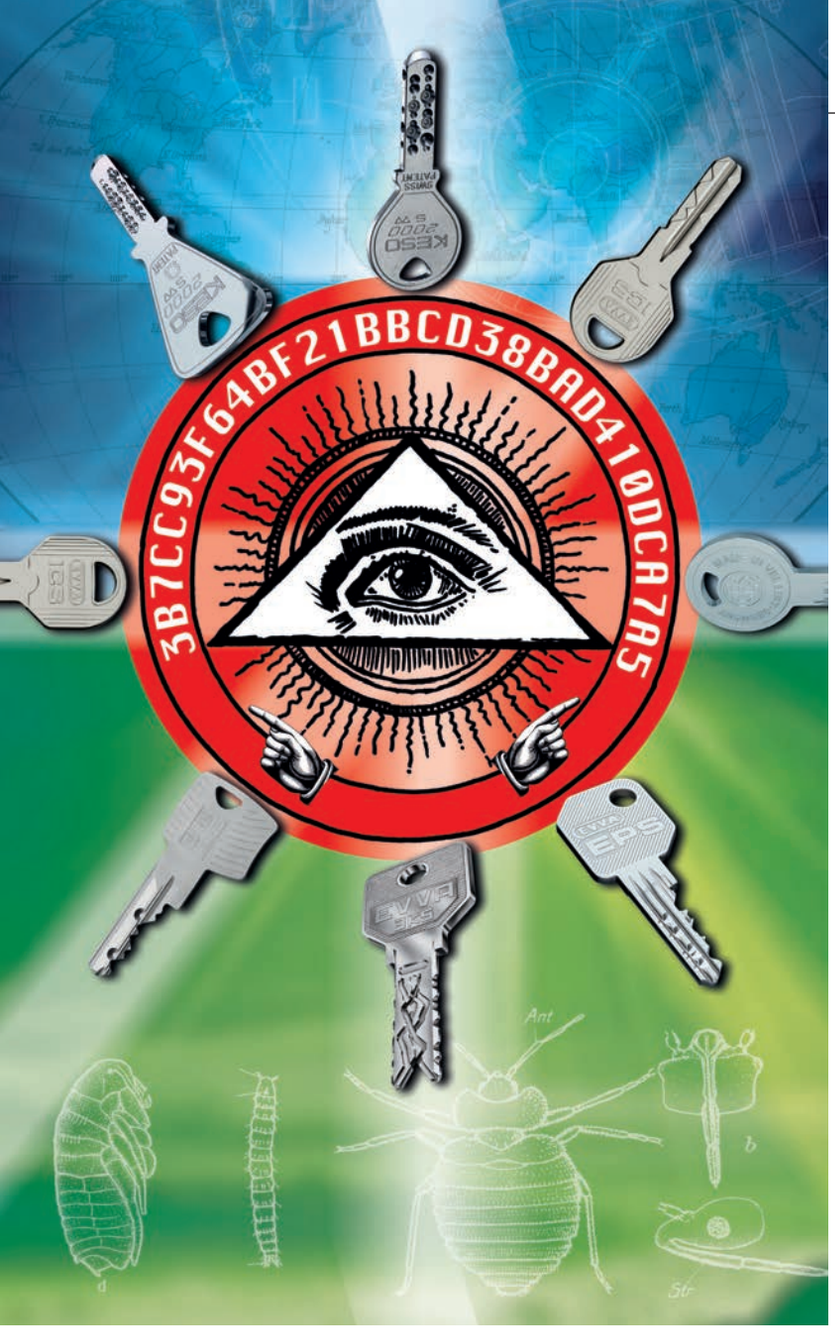

Krypto + NSA = ?

Kryptografische Folgerungen aus der NSA-Affäre

Die „scheibchenweise" Veröffentlichung der Informationen aus dem Datenschatz von Edward Snowden hat für viel Verwirrung gesorgt – zudem war die Berichterstattung längst nicht immer fachlich fundiert und exakt. Unsere Autoren fassen die Erkenntnisse zusammen und bewerten ihre Konsequenzen für die heutige und zukünftige Kryptografie.

Von Bernhard Esslinger, Siegen, Martin Franz und Michael Schneider, Frankfurt/Main

Mittlerweile haben unübersichtlich viele Sendungen und Artikel über die Erkenntnisse berichtet, die im Zuge der NSA-Affäre seit 2013 an das Licht der Öffentlichkeit geraten sind. Da diese Thematik sehr komplex und damit für den Nicht-Experten nicht immer verständlich ist, wird sie in den Massenmedien häufig stark vereinfacht dargestellt oder – noch schlimmer – überdramatisiert.

Und selbst für IT-Sicherheitsexperten ist es schwierig, einen klaren Überblick darüber zu behalten, was noch als sicher gelten kann und was als überholt gelten muss. Auch die sich ständig ändernde Bedrohungslage – wer weiß schon, welche Erkenntnisse in der nächsten Woche veröffentlicht werden? – machen es für die CISOs dieser Welt derzeit nicht einfach, den Vorständen ihrer Unternehmen die richtigen Antworten zu liefern.

Doch auch positive Effekte sind zu beobachten: Begriffe wie „Perfect Forward Secrecy" werden mittlerweile nicht mehr nur auf Kryptografie-Konferenzen verwendet, sondern auf breiter Front berücksichtigt (vgl. [1]). Schließlich sind es auch nicht zwangsweise nur Geheimdienste, die eine Bedrohung darstellen: Auch und gerade gegen Wirtschaftsspionage und gegen kriminelle, Mafia-ähnliche Organisationen können und müssen sich Unternehmen schützen. Wichtig ist es, wie immer, auf allen Ebenen gleichermaßen sinnvolle Schutzmaßnahmen zu ergreifen – es bringt nichts, wenn einige Sicherheitsmaßnahmen der neuesten Mode entsprechen, etliche IT-Systeme selbst aber unsicher bleiben. Doch zurück zu NSA & Co.:

Angriff auf breiter Front

Im Zuge der Veröffentlichungen wurde bekannt, dass Geheimdienste wie folgt vorgehen (vgl. Abb. 1): Zunächst verschaffen sie sich Kontrolle über die Netzwerke und damit Zugriffsmöglichkeiten auf alle Systeme und übertragenen Daten. Anschließend greifen sie auf drei verschiedenen Ebenen an: Mathematik, Implementierung und Datenhaltung.

Die erste (unterste) Angriffsebene führt über die verwendete Kryptografie, die Mathematik: Kann ein Angreifer diese Basis brechen, so hat er anschließend leichtes Spiel, denn ein solches Vorgehen ist fast nicht nachzuweisen oder aufzuhalten – der Angreifer entschlüsselt dabei

© SecuMedia Verlags-GmbH · 55205 Ingelheim ·

mitgelesene Daten durch rein passives Lauschen und Offline-Entschlüsseln.

Die zweite Angriffsebene ist bereits komplexer: Über fehlerhafte Implementierungen in der Software erlangt ein Angreifer Zugriff auf sensitive Daten und Systeme. Schwachstellen (Backdoors) werden auch bewusst in Software eingebaut, um dem Angreifer im Nachhinein Zugriff auf das System oder die dadurch verarbeiteten Daten zu geben – hier greift der Angreifer aktiv ein.

Der letzte Angriffsweg führt über die Anwendungsebene: Software-Anwender beziehungsweise Cloud-Service-Nutzer werden dabei in der Regel offen gezwungen, bestimmte Operationen auszuführen oder Daten direkt preiszugeben.

Mathematik

Einen Angriff auf ein etabliertes Kryptosystem zu finden und einzusetzen, ist sicher die Königsklasse für einen Geheimdienst. Im Zuge der 2013er Veröffentlichungen wurde zwar bekannt, dass die NSA und andere Geheimdienste massiv die breit eingesetzte Kryptografie angreifen (und nach eigenen Angaben maßgeblich gebrochen haben). Jedoch wurde demzufolge kein etabliertes Kryptosystem mit unbekannten mathematischen Angriffen gebrochen. Allerdings wurden Standardisierungen – wie die des bis dato hoch angesehenen US-amerikanischen National Institute of Standards and Technology (NIST) – beeinflusst.

Was bekannt ist

_____ Es gilt als gesichert, dass der NIST-Standard **Dual_EC_DRBG** für einen Zufallszahlengenerator auf Basis elliptischer Kurven eine Backdoor enthält und keine wirklich zufälligen Zahlen erzeugt – ohne „guten" Zufall ist darauf aufbauende Kryptografie jedoch unbrauchbar.

_____ Das (ohnehin veraltete) symmetrische Kryptosystem **DES** gilt als gebrochen.

_____ Im Zuge der Veröffentlichungen wurde viel diskutiert, ob der **RC4**-Algorithmus weiterhin als sicher eingestuft werden kann. Angesichts der vielen Publikationen, die Angriffe darauf beschreiben, gilt er in der akademischen Welt bereits als gebrochen und sollte nicht mehr verwendet werden.

Was angenommen werden muss

_____ **SHA-1** gilt zwar weiterhin als sicher – da allerdings erste Angriffe auf diesen Algorithmus bekannt geworden sind, kann man vermuten, dass bereits weitere Angriffe gefunden wurden oder bald veröffentlicht werden.

_____ Auch wenn noch kein erfolgreicher Angriff auf **RSA-1024** bekannt ist, sollte man bereits jetzt auf längere Schlüssel umsteigen. Das BSI empfiehlt Schlüssel mit einer Länge von mindestens 2000 Bit [2].

_____ Auch wenn der Algorithmus auf breiter wissenschaftlicher Basis evaluiert und als sicher bewertet wurde, gab es zu **SHA-3** im Zuge der NSA-Veröffentlichungen erneut viele Diskussionen, weil das NIST für die künftige Standardisierung andere als die von Wissenschaftlern getesteten Parameter betrachtet. Diese werden von Experten als weniger sicher angesehen – man vermutet eine Beeinflussung durch Geheimdienste. Wie sich die Standardisierung von SHA-3 entwickelt, bleibt abzuwarten.

_____ Es gibt Zweifel, ob alle **standardisierten elliptischen Kurven** als sicher eingeschätzt werden können. Allerdings wurde, bis auf den bereits erwähnten Zufallszahlengenerator Dual_EC_DRBG, noch kein auf elliptischen Kurven basiertes System als unsicher enttarnt.

Was weiterhin als sicher gilt

_____ **RSA** mit Schlüssellängen über 2000 Bit gelten bis über das Jahr 2019 hinaus als sicher [2].

_____ Moderne symmetrische Verfahren wie **AES** und **SHA-2** gelten als sicher; auch für das etwas ältere **Triple-DES**-Verfahren wird angenommen, dass es bekannten Angriffen noch für viele Jahre standhalten wird.

_____ Kryptografie, die auf **„gut" gewählten elliptischen Kurven** basiert, gilt als sicher.

Implementierung

Wie sich in den letzten Monaten herausgestellt hat, liegt die Achillesferse der IT-Sicherheit in der Implementierung von Kryptografie: Hier wird am häufigsten

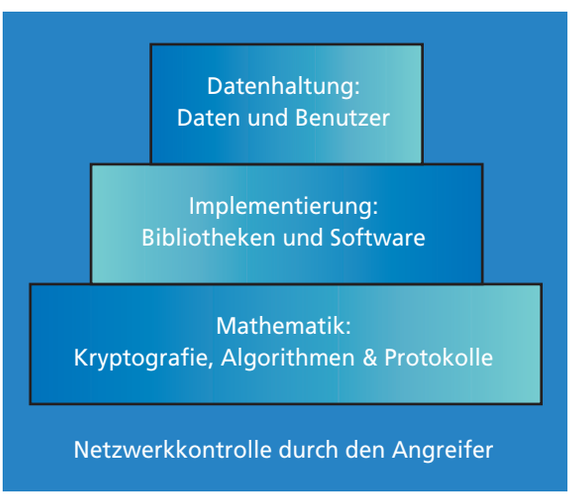

Abbildung 1: Betrachtung der Angriffs-Ebenen Mathematik, Implementierung und Datenhaltung

angegriffen. Und solche Attacken bieten dem Angreifer ein gutes Preis-/Leistungsverhältnis: Man erhält direkt Zugriff auf unverschlüsselte Daten und die Chance, entdeckt zu werden, ist relativ gering.

Was bekannt ist oder angenommen werden muss

Viele **namhafte Soft- und Hardware-Hersteller** arbeiten offenbar mit Geheimdiensten zusammen und bauen auf deren Anweisung hin entweder direkt Schwachstellen ein oder implementieren Funktionen, welche die Datenlieferung an die Geheimdienste vereinfachen. Beispiele sind etwa Router mit nicht-abschaltbaren Wartungs-Passwörtern, in Client-Software fest einkodierte Authentifizierungsdaten oder Protokolle, die das schwächste Verfahren zum Default haben.

Auch und gerade bei **Cloud-Services** ist anzunehmen, dass Schwachstellen in der Implementierung Daten im Umfeld der Services bewusst kompromittieren.

Was weiterhin als sicher gilt

Implementierungen mit viel Eigenkontrolle dürften weithin sicher sein. Ist ein Kunde beispielsweise in der Lage, die eingesetzten Bibliotheken selbst zu wählen, kann er diese zeitig austauschen, sobald Unsicherheiten bekannt werden. Idealerweise arbeiten die eingebundenen Bibliotheken aus Sicht der Herstellersoftware wie eine

Chronologie der Veröffentlichungen

6. Juni 2013: Veröffentlichungen in den Zeitungen „The Guardian" und „Washington Post" berichten erstmals über das PRISM-Programm der NSA. PRISM gibt Zugriff auf die Daten aller wichtigen Anbieter im Internet (inkl. Microsoft, Google, Apple etc.). Auch die enge Zusammenarbeit und der weitreichende Datenaustausch zwischen NSA und dem britischen „Government Communications Headquarters" (GCHQ) werden bekannt.

8. Juni: Mit „Boundless Informant" wird ein Data-Mining-Tool bekannt, das mit Big-Data-Methoden riesige Datenmengen auswerten, gezielt nach Zusammenhängen suchen und Auskunft über einzelne Personen geben kann.

21. Juni: The Guardian berichtet über das Tempora-Programm des GCHQ – der Artikel beschreibt, wie der britische Geheimdienst internationale Datenleitungen anzapft und darüber fließende Daten auswertet.

8. Juli: Die brasilianische Zeitung „O Globo" berichtet zum ersten Mal über XKeyScore. Diese Software stellt in Echtzeit verschiedenste (Meta-)Daten zu einer beliebigen Person dar – wie vom Spiegel berichtet, wird die Software auch vom BND verwendet.

5. September: New York Times und The Guardian veröffentlichen Artikel mit den kryptografisch bisher größten Auswirkungen. Die Projekte „Bullrun" und „Sigint" sollen mit einer ganzen Fülle von Methoden gezielt weltweit eingesetzte Verschlüsselung angreifen – dazu gehören die Schwächung von Krypto-Standards, Einführung unsicherer Standards sowie Manipulationen an kryptografischen Implementierungen und Software. In diesen Veröffentlichungen wird offenbar, dass bewusst eine Schwächung der Sicherheit von gängigen Systemen herbeigeführt wird, um den Geheimdiensten Zugangsmöglichkeiten zu eröffnen. Ein Artikel berichtet davon, wie eine vermutete Schwäche in einem standardisierten Zufallszahlengenerator direkt auf den Einfluss der NSA zurückzuführen ist.

7. September: Ein Artikel im Spiegel offenbart, dass Daten von fast allen Smartphones ausgespäht werden können, allem voran von Blackberry, Android und iPhones.

10. September: Die New York Times berichtet, dass der von der amerikanischen Normierungsbörde NIST im Jahr 2006 standardisierte Zufallszahlengenerator „Dual_EC_DRBG" vermutlich eine Hintertür für die NSA enthält. Einige Tage später informiert RSA Security seine Kunden über ein mögliches Problem mit dem Zufallszahlengenerator und rät, diesen nicht mehr zu benutzen. Im Dezember stellt sich heraus, dass RSA Security von der NSA einen Betrag von 10 Mio. US$ dafür erhielt, den Dual_EC_DRBG-Algorithmus zum Standard in ihrem Produkt BSAFE zu machen.

10. Dezember: Die Verdachtsmomente, dass im großen Stil auch Wirtschaftsspionage betrieben wurde, lagen schon länger auf der Hand. In einem Beitrag legt die ZDF-Sendung Frontal21 Dokumente vor, die belegen sollen, dass durch Spionage in der Tat gezielt Daten an US-Unternehmen weitergegeben und zum wirtschaftlichen Vorteil verwendet wurden.

30. Dezember: Auf dem „Chaos Communication Congress" (CCC) in Hamburg berichten Jacob Appelbaum und andere über die NSA-Abteilung ANT, die einen umfassenden Werkzeugkasten an Soft- und Hardware anbietet, um gezielte Angriffe durchzuführen, zu denen auch die Nutzung eines Alternativ-Netzes (Quantumtheory) und die Verseuchung von Hardware zum Beispiel auf dem Bestellweg gehören (vgl. www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html).

2. Januar 2014: Die Washington Post beschreibt in einem Artikel das „Penetrating Hard Targets Project", das sich darin versucht, einen Quantencomputer zu bauen, der auch sichere Kryptosysteme mit großen Schlüssellängen brechen kann.

© SecuMedia Verlags-GmbH · 55205 Ingelheim ·

Black-Box, sodass der Kunde selbst entscheiden kann, welche Verschlüsselungsverfahren verwendet werden.

Datenhaltung

Wie sich gezeigt hat, greifen Datenspione besonders gerne unmittelbar auf gespeicherte Daten zu. Hierzu arbeiten sie direkt mit großen Software- und Cloud-Service-Anbietern zusammen: Private Daten und geheimes Schlüsselmaterial werden nach Ausübung von Druck auf das Unternehmen (ein bekanntes Beispiel ist der E-Mail-Anbieter LavaBit) direkt an den Geheimdient ausgehändigt. Dieser Angriffsweg hat indess nichts mit Kryptografie und ihrer Implementierung zu tun, weswegen an dieser Stelle nicht weiter darauf eingegangen werden soll.

„I trust the Math"

Wie beschrieben sind die Krypto-Verfahren selbst nicht die Ursache heutiger Probleme: Die Sicherheit der meisten kryptografischen Systeme beruht auf der Unlösbarkeit mathematischer Fragestellungen. Vor allem die Public-Key-Verfahren gelten als sicher, solange bestimmte – seit vielen Jahren bekannte – mathematische Fragestellungen nicht (leichter) gelöst werden können. Algorithmen zum Lösen dieser Fragestellungen werden seit vielen Jahren entwickelt und verbessert; daher weiß man relativ sicher, wie schwer es ist, diese Fragestellungen zu lösen, und hat eine gute Sicherheitsabschätzung für die zugehörigen Verfahren.

RSA – ElGamal

Alle modernen kryptografischen Verfahren lassen sich über die Schlüssellänge parametrisieren – für das RSA-Verfahren beispielsweise gelten Schlüssel der Länge 512 Bit längst als gebrochen, da das dem Algorithmus zugrunde liegende Faktorisierungs-Problem für 512-Bit-Zahlen auf heutigen Computersystemen leicht zu lösen ist. RSA-Schlüssel der Länge 2048 Bit gelten dagegen als nach wie vor sicher, da sich das Faktorisierungs-Problem für so große Zahlen nicht in akzeptabler Zeit lösen lässt.

Die rasante Entwicklung der Rechenleistung und algorithmische Entwicklungen sorgen aber dafür, dass man auch zukünftig die Wahl der Parameter sorgsam treffen muss. Die internationale Forschung im Gebiet der Kryptoanalyse zeigt in ihren Publikationen, wie aufwändig das Lösen schwerer Probleme ist. Zwar ist es denkbar, dass Geheimdienste und auch kriminelle Organisationen mit höheren Budgets ausgestattet sind als die Forschungsinstitute – trotzdem ist eine umfassende Attacke auf viele Nutzer in solchen Fällen äußerst unwahrscheinlich. Mit ausreichend großen Schlüsseln gelten Public-Key-Verfahren wie RSA oder ElGamal daher heute noch als sehr sicher, sofern die Schlüssel „richtig" erzeugt werden (siehe [3]).

Praktisch gebrochene Kryptografie

Es gibt einige Fälle, in denen schwache Krypto-Algorithmen noch lange nach Bekanntwerden ihrer Schwächen eingesetzt wurden und teils noch immer werden.

Beispielsweise gilt der Verschlüsselungs-Algorithmus A5/1, der bei der GSM-Telefonie im Mobilfunk verwendet wird, seit 2003 als gebrochen. Allerdings wurde diese Chiffre auch bereits 1987 entwickelt und seitdem hatte sich die Kryptoanalyse selbstverständlich stark verändert (u. a. aufgrund der Entwicklung der Rechner). A5/1 sollte in Anwendungen nicht mehr eingesetzt werden. Ähnliches gilt für die WEP-Verschlüsselung in kabellosen Netzwerken (WLANs). Und auch der von vielen Webservern im Internet immer noch gern verwendete RC4-Algorithmus ist nicht mehr sicher genug und lässt sich vermutlich in Echtzeit brechen.

Kryptografie auf Basis elliptischer Kurven

Es gibt zahlreiche Kryptoverfahren, deren Sicherheit auf mathematischen Problemen über elliptischen Kurven beruht (Elliptic Curve Cryptography – ECC). Diese Probleme sind ebenfalls sehr gut untersucht und somit ist auch die Sicherheit dieser Verfahren sehr gut verstanden. Elliptische Kurven sind zwar durch die Veröffentlichung der NSA-Backdoor im Zufallszahlen-Generator Dual_EC_DRBG in Verruf geraten. Die Schwäche ergibt sich hierbei aber keineswegs aus der Verwendung elliptischer Kurven selbst, sondern nur daraus, dass das NIST einen festen Punkt *Q* der Kurve als Parameter im Standard festgelegt hat (statt jedes Mal ein neues *Q* zu wählen) und dass der Output der Zufallsquelle (Seed) fast in voller Länge und unverändert im Output des Zufallszahlengenerators (PRNG) auftaucht. Elliptische Kurven selbst gelten nach wie vor als sichere Basis kryptografischer Verfahren.

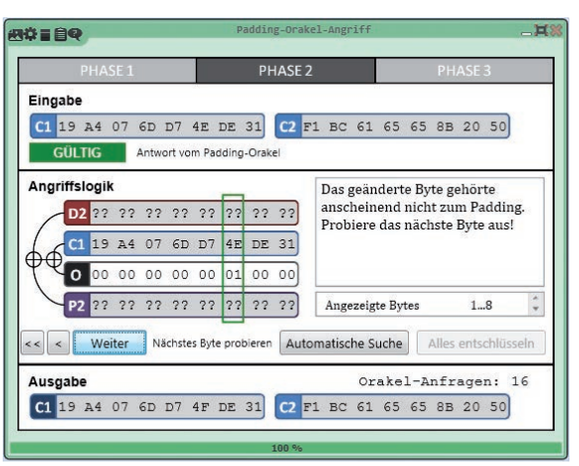

Abbildung 2: Padding-Oracle-Angriff gegen SSL (Visualisierung in CrypTool 2 [7])

Sicherheit symmetrischer Kryptografie

In der symmetrischen Kryptografie werden meist keine mathematischen Probleme als Grundlage gewählt, die Sicherheit der Verfahren bestimmt sich vielmehr aus der Absenz bekannter Angriffe: Solange die akademische Welt keine Angriffe gegen ein symmetrisches Verfahren kennt, gilt dieses als sicher.

Manche Verfahren der Kryptografie können auch aus Bausteinen instanziiert werden, die sich beim Auftauchen von Schwachstellen einfach ersetzen lassen: Einen Message-Authentication-Code (MAC) kann man zum Beispiel aus jeder kryptografischen Hashfunktion konstruieren – sollte eine verwendete Hashfunktion irgendwann als schwach gelten, kann sie leicht ausgetauscht werden.

Im Bereich der symmetrischen Kryptografie gibt es nach wie vor Algorithmen, die als sehr stark und ungebrochen gelten. Dazu gehören unter anderem die SHA-2-Hashfunktionen (SHA-256, SHA-384, SHA-512), die SHA-3-Hashfunktion sowie diverse Block- und Stromchiffren (AES, Triple-DES, Camellia).

Implementierungsprobleme

Während die mathematische Sicherheit der Kryptografie also nach wie vor als sehr hoch anzusehen ist, sieht es bei ihrer Implementierung deutlich problematischer aus. Die Annahmen, die Entwickler von Kryptoverfahren treffen, sind meist idealisiert. Beispielsweise setzen sie das Vorhandensein einer perfekten Zufallsquelle voraus.

Da solche Annahmen in der Praxis nicht komplett erfüllbar sind, müssen sie bei der Implementierung wenigstens so gut wie möglich abgedeckt werden. Hier zeigten sich 2012 Schwachstellen in den Zufallszahlen-Generatoren vieler Hersteller (vgl. [3,4,5]).

Seitenkanalangriffe

Ein weiteres Problem, das sich erst zur Laufzeit zeigt, sind Seitenkanalangriffe: Dabei wird nicht das kryptografische Verfahren selbst attackiert – stattdessen versucht ein Angreifer, geheimes Material wie Schlüssel aus physikalischen „Konsequenzen" der Datenverarbeitung abzuleiten. Solche Seitenkanäle können unter anderem die Laufzeit, Lärmentwicklung oder der Energieverbrauch bei Ausführung eines Algorithmus sein. Sind die Informationen, die über den Seitenkanal abgefangen werden, abhängig vom geheimen Schlüssel, so lässt sich ein Teil davon oder sogar der gesamte Schlüssel rekonstruieren.

Seitenkanalangriffe sind aber nicht immer physikalischer Natur: Man kann auch Protokollschwächen durch „ungebräuchliches" Verhalten ausnutzen, wie etwa beim Padding-Oracle-Angriff gegen SSL (siehe [6]) – Abbildung 2 zeigt eine Visualisierung dieses Angriffs in CrypTool 2 [7].

Umgang mit praktisch gebrochenen Verfahren

Es gibt einige bekannte Fälle, in denen kryptografische Verfahren in der Praxis tatsächlich gebrochen wurden. Wenn eine Schwäche in einem Verfahren bekannt wird, sollte das Verfahren in produktiven Systemen natürlich möglichst rasch ausgetauscht werden. Gelingt ein auf der offengelegten Schwäche beruhender Angriff, so liegt das eigentliche Problem des gelungenen Angriffs daher weniger in der Schwäche des Verfahrens als in der vernachlässigten Wartung des Systems.

Als Beispiel kann hier die Hashfunktion MD5 dienen: Durch die Berechnung einer Kollision (Konstruktion zweier ungleicher Nachrichten mit demselben MD5-Hashwert) gelang es 2008, ein CA-Zertifikat zu fälschen und damit vertrauenswürdige, verschlüsselte Verbindungen im Internet aufzubauen (siehe [8]). Allerdings waren bereits seit 1996 erste Ansätze bekannt, dass es möglich sein könnte, solche Kollisionen zu berechnen – und seitdem war auch davor gewarnt worden, MD5 weiterhin einzusetzen.

Die komplexen Architekturen in bestimmten Branchen (etwa bei Telekommunikation oder Banken) bedingen, dass es oft über 15 Jahre dauert, bis sich neue Standards wirklich manifestieren. Dies ist ein weiterer Grund, in Standards sehr hohe Sicherheitsanforderungen anzusetzen und nur Verfahren zu verwenden, an denen keinerlei Zweifel bestehen. Standards sollten dabei möglichst so konzipiert sein, dass man sowohl auf Software- als auch auf Hardware-Ebene Teilkomponenten leicht austauschen kann.

Backdoors

Absichtliche Backdoors von Herstellern sowie Programmierfehler sind ebenfalls eine große Bedrohung: Zwar sollte von so etwas nur ein kleiner Kreis wissen – es ist aber nie auszuschließen, dass nicht doch etwas bekannt wird, wie der Fall Snowden gerade zeigt. Der Einbau von Backdoors bietet demnach eine

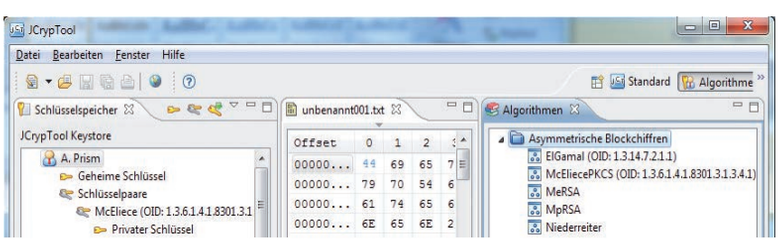

Abbildung 3: Post-Quantum-Kryptoverfahren lassen sich auch heute schon ausprobieren (im Bild per JCrypTool [7])

© SecuMedia Verlags-GmbH · 55205 Ingelheim · <kes> 2014#1

potenzielle Schwachstelle für Angreifer aller Art. Die Ursache der Schwachstelle ist aber auch hier nicht die Mathematik, sondern die Implementierung beziehungsweise Integration in Hardware.

Wie weiter?

Sicherheitstipps für Nutzer (Endanwender und Firmen)

Sicherheitsbewusste Nutzer von Software und Systemen sollten sich darüber im Klaren sein, welche ihrer Daten grundsätzlich frei zugänglich sind – unverschlüsselte E-Mails oder Daten in Cloud-Speichern sollten generell als ungeschützt gelten. Alle Daten, die der Nutzer selbst als vertraulich einschätzt, muss er verschlüsseln. Dabei ist er auf die Nutzung fremder Software angewiesen: Zur E-Mail-Verschlüsselung kann S/MIME oder PGP dienen – beides setzt jedoch voraus, dass auch der Empfänger die gleiche Verschlüsselungs-Technik unterstützt. Hier wird es notwendig sein, in der Gesellschaft für ausreichendes Interesse an Datensicherheit zu sorgen und die Sicherheitskomponenten der vorhandenen Software deutlich benutzerfreundlicher zu machen.

Für die verschlüsselte Speicherung von Daten empfiehlt es sich, Open-Source-Produkte zu verwenden (z. B. TrueCrypt) – allerdings kann man sich auch bei diesen nie 100%-ig sicher sein, dass sie fehlerfrei und ohne Backdoors implementiert sind. Zu den meisten Open-Source-Projekten kann jeder Programmierer beitragen; es wäre also auch hier denkbar, dass Geheimdienste oder kriminelle Organisationen Hintertüren oder absichtliche Programmierfehler einschleusen. Da normalerweise niemand den gesamten Code eines Open-Source-Projekts komplett überprüft, könnte das unbemerkt passieren. Trotzdem ist die Wahrscheinlichkeit sehr hoch, dass solche Machenschaften von anderen Programmierern des Projektes entdeckt werden, weil jede Änderung für jeden einsehbar geloggt wird.

Relativ sicher ist auch, dass solche absichtlich eingebauten Fehler in Open-Source-Produkten schneller behoben werden als in kommerziellen Produkten. Zumindest hat man bei Open-Source-Software eine Chance, Fehler und Backdoors in der Breite zu finden, während man bei Closed-Source-Produkten chancenlos ist und dem Hersteller vertrauen muss. Aus diesen Gründen sollte man Software aus der Open-Source-Welt eher vertrauen als nicht-einsehbarer Software von (evtl. fragwürdigen oder erpressbaren) Herstellern. Optimal ist es, wenn dem Anwender selbst das Kompilieren aus dem Quellcode möglich ist – denn selbst bei Open-Source-Produkten kann man sonst nicht sicher sein, dass der ausführbare Code tatsächlich aus dem Quelltext entstand, der einem Review unterzogen wurde.

Sicherheitstipps für Entwickler

Generell ist es empfehlenswert, kryptografische Funktionen selbst einzubauen (inkl. der Schnittstellen zur Anwendung) – das ermöglicht im Falle eines Falles den einfachen Austausch eines kryptografischen Verfahrens oder einer Bibliothek. Wenn der Einsatz von Open-Source-Produkten nicht möglich ist und man auf die Nutzung von Fremd-Software angewiesen ist, kann man sich detailliert vom Hersteller darlegen lassen, welche kryptografischen Verfahren er in seinem Produkt verwendet (inkl. Dokumentation und Testfällen). Ebenso wichtig sind Details über die verwendeten Bibliotheken (OpenSSL, Bouncy Castle etc.), Quellen der Zufallsverfahren, Schlüssellängen und Implementierungen. Das ermöglicht eine tiefgehende Kontrolle während des Einsatzes; sollten zukünftig Probleme mit gewissen Bestandteilen der Software bekannt werden, ermöglichen die gesammelten Informationen zudem eine schnellere Reaktion.

Ein standardisiertes Vorgehen bei der Software-Entwicklung, wie etwa Microsofts „Trustworthy Computing Secure Development Lifecycle“ (SDL) kann das Vertrauen in das entwickelte System ebenfalls erhöhen. Größere Firmen haben heutzutage zur Minimierung ihrer Lizenzkosten und aufgrund von Ereignissen wie dem Jahr-2000-Problem (Y2K) ein Repository all ihrer IT-Anwendungen. Darin sollte man zusätzlich für jede

Sichere Konfiguration von SSL/TLS

Zur Absicherung der Kommunikation über das Internet ist SSL/TLS das am häufigsten verwendete Protokoll – zu seiner sicheren Verwendung ist folgende Konfiguration zu empfehlen:

- _____ Verwendung in Version TLS 1.2
- _____ Nutzung von „Perfect Forward Secrecy“ durch den Einsatz von Diffie-Hellman beim Schlüsselaustausch (DHE oder ECDHE)
- _____ Einsatz von RSA mit Schlüssellängen von 2048 Bit (oder mehr)
- _____ Nutzung von AES im Galois-Counter-Mode (GCM) mit einer Schlüssellänge von 128 Bit (oder mehr)
- _____ Ausschluss unsicherer Algorithmen wie DES und RC4 aus der Liste der vom Server akzeptierten Algorithmen
- _____ Bevorzugung von SHA256 und SHA512 als Hashfunktion – im Moment kann man auf SHA1 noch nicht ganz verzichten, um alte Browser nicht „auszusperren“, wohl aber SHA1 mit geringerer Priorität aufführen

Anwendung die verwendeten kryptografischen Verfahren samt ihrer Parameter und Details nachhalten.

Vielfalt der kryptografischen Annahmen

Es ist ebenfalls empfehlenswert, sich nicht auf nur eine einzige Sicherheitsannahme zu verlassen: Zwar ist es unwahrscheinlich, dass ein mathematisches Problem, wie etwa das Faktorisierungsproblem, plötzlich leicht gelöst werden kann. Quantencomputer könnten aber mithilfe von Shors Algorithmus praktisch alle heute eingesetzten Verfahren der Public-Key-Kryptografie brechen – nur existieren bislang keine Quantencomputer ausreichender Größe für praxisrelevante Angriffe. Auch die NSA ist den Snowden-Dokumenten zufolge hier nicht weiter als die bekannte Industrie und Forschung.

Trotzdem ist nicht auszuschließen, dass sich diese Situation in den nächsten Jahren grundlegend ändert und dann alle bisherigen Public-Key-Verfahren (u. a. RSA) ausgetauscht werden müssen. Alternative Verfahren werden bereits entwickelt und stehen zur Verfügung (z. B. McEliece, s.a. [7]), sind allerdings in der Praxis so gut wie gar nicht im Einsatz – diesen Zweig der Forschung bezeichnet man als Post-Quantum-Kryptografie (PQC – nicht zu verwechseln mit der Quantenkryptografie).

Sollte ein Wechsel notwendig werden, wäre es hilfreich, wenn man Alternativen bereits erprobt und parat hat. Denn leider gibt es bisher keine verbreiteten Recovery-Szenarien für die Umstellung von einem Kryptoverfahren auf ein anderes (z. B. von RSA zu ECC zu McEliece). Immerhin wurden solche neuartigen Szenarien aber schon im Zuge des BMI-Projekts „Kritische Infrastrukturen“ (KRITIS) diskutiert.

Hilfe bei der Auswahl von Verfahren und Parametern

Es gibt zahlreiche Institutionen, die bei der Auswahl kryptografischer Algorithmen und ihrer Parameter unterstützen. Das BSI [2], die ENISA [9] oder das European Payments Council (EPC, [10]) geben beispielsweise Empfehlungen über kryptografische Verfahren und Schlüssellängen heraus. Es ist davon auszugehen, dass weder Geheimdienste noch kriminelle Angreifer die empfohlenen Krypto-Verfahren mit richtig gewählten Parametern und ohne Implementierungsschwächen in sinnvoller Zeit brechen können. Das amerikanische National Institute of Standards and Technology (NIST) veröffentlicht ebenfalls solche Empfehlungen; allerdings litt das Vertrauen in diese Behörde sehr stark unter den Veröffentlichungen der NSA-Spähaffäre.

Da der Austausch eines kryptografischen Verfahrens oder auch nur seiner Parameter erfahrungsgemäß recht lange dauert, müssen alternative Verfahren rechtzeitig eingeplant, eingesetzt oder zumindest vorbereitet werden.

Schlüssel-Management

Besonderes Augenmerk ist auch auf die Generierung, Verwaltung und Speicherung kryptografischer Schlüssel zu legen – diese sind geschützt zu speichern und dürfen auch während ihrer Verwendung nicht kopiert werden können. Dazu empfiehlt sich für kritische Anwendungen die Verwendung von spezieller Hardware (Hardware Security Module, HSM), die Operationen mit geheimen Schlüsseln durchführt, ohne dass diese das Modul verlassen. Der interne Speicher eines HSM ist dabei auch gegen physische Zugriffe gesichert – dass Kryptografie sich allerdings auch benutzen lässt, um Hardware schon zusammen mit der Firmware derart zu manipulieren, dass sich das von außen nicht nachweisen lässt, wurde beispielsweise in [11] beschrieben.

Daten-Minimalisierung

Eine gute Empfehlung aus dem Bereich des Datenschutzes ist die der Minimalisierung: Daten, die erst gar nicht gespeichert oder transportiert werden, können auch von niemandem abgehört oder entschlüsselt werden. Man sollte sich bei allen Daten fragen, ob sie tatsächlich nötig sind: Das betrifft hauptsächlich Metadaten wie beispielsweise Logfiles oder Standortdaten. Nicht nur in sozialen Netzwerken, auch in Unternehmen kann man durch Daten-Minimalisierung dafür sorgen, dass wichtige Informationen nicht abhanden kommen. Hierbei ist, wie in allen Bereichen dieser Diskussion über IT-Sicherheit, auch die Awareness der Mitarbeiter gefragt.

Europäische und deutsche Standards und Verfahren

Eine weitere mögliche Schlussfolgerung ist es, sich langfristig von vermeintlich kompromittierten Produkten zu trennen und auf europäische oder deutsche Entwicklungen zu setzen. Zwar kann man dort ebenfalls nicht sicher sein, dass die entwickelnden Unternehmen keine Backdoors einbauen oder womöglich aufgekauft werden – aber gerade deutsche Unternehmen unterliegen immerhin der deutschen Rechtsprechung.

Langfristig sollte es auch das Ziel sein, europäische Standards zu entwickeln, die im Gegensatz zum NIST nicht dem Einfluss amerikanischer oder nationaler Geheimdienste unterliegen. Die Forschung der Kryptografie ist in Europa ebenso stark wie in den USA (siehe ECRYPT, PRESENT, SHA3). Fand die Forschung zum SHA-3-Wettbewerb, dessen Ziel eine neue kryptografische Hash-Funktion war, zu großen Teilen in Europa statt,

© SecuMedia Verlags-GmbH · 55205 Ingelheim · <kes> 2014#1

erfolgte seine Standardisierung aber dennoch durch das US-amerikanische NIST.

Die Grundlage zur Entwicklung europäischer Standards ist vorhanden, es fehlt lediglich ein Standardisierungsablauf in Europa. Kryptografie-Experten der „International Association for Cryptologic Research" (IACR) haben bereits auf diesen Missstand aufmerksam gemacht. Es ist also zu hoffen, dass zukünftig kryptografische Standards aus Europa nutzbar sein und auch in den Beschaffungsanforderungen festgeschrieben werden.

Fazit

Wenn man die Auswirkungen der Veröffentlichungen des letzten Jahres auf die Kryptografie betrachtet, fällt das Urteil besser aus, als es zuerst scheint: Es gibt zahlreiche kryptografische Verfahren und Protokolle, die ausreichende Sicherheit bieten können. Problematisch sind allerdings ihre Implementierungen – hier muss mit größerer Sorgfalt vorgegangen werden, um den aktuellen Bedrohungen durch fremde Geheimdienste (und auch Kriminelle) zu begegnen. Die Snowden-Affäre hilft immerhin dabei, die IT-Sicherheit in den Blickpunkt der Öffentlichkeit zu stellen. Dieser Fokus kann im positiven Sinne dazu beitragen, dass mehr IT-Nutzer auf die Sicherheit ihrer Daten und Systeme achten.

Dieser Artikel hat sich mit den Auswirkungen der „Snowden-Veröffentlichungen" auf die Kryptografie beschäftigt. Mindestens ebenso wichtig ist jedoch eine Diskussion über gesellschaftliche Auswirkungen der Affäre: Welches Maß an (erhoffter) Sicherheit berechtigt zu welchem Umfang an Überwachung, und inwiefern sind Überwachungsmaßnahmen effizient und zielführend im Vergleich zu alternativen Maßnahmen der Prävention und Strafverfolgung? Die Debatte, ob die Ausgaben der Überwachung nicht besser und effektiver in andere Maßnahmen fließen sollten, die gesellschaftlichen Wohlstand schaffen, hat beispielsweise noch gar nicht stattgefunden. ■

Prof. Bernhard Esslinger lehrt IT-Security und Kryptografie an der Uni Siegen und leitet das Open-Source-Projekt CrypTool (www.cryptool.org). Dr. Martin Franz und Dr. Michael Schneider sind freie Autoren, forschen zu Fragen der Kryptografie und arbeiten als IT-Sicherheitsexperten bei einer internationalen Bank.

Literatur

[1] Jürgen Schmidt, Zukunftssicher verschlüsseln mit Perfect Forward Secrecy, heise Security, Juli 2013, www.heise.de/security/artikel/Zukunftssicher-Verschluesseln-mit-Perfect-Forward-Secrecy-1923800.html

[2] BSI, Kryptografische Verfahren: Empfehlungen und Schlüssellängen, Technische Richtlinie TR-02102, www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.htm

[3] Bernhard Esslinger, Jörg Schneider, Volker Simon, RSA-Sicherheit in der Praxis, <kes> 2012#2, S. 22

[4] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter, Public Keys, in: Advances in Cryptology – CRYPTO 2012, Springer 2012, S. 626, ISBN 978-3-642-32008-8

[5] Nadia Heninger, Zakir Durumeric, Eric Wustrow, J. Alex Halderman, Mining your Ps and Qs: Detection of widespread weak keys in network devices, Usenix Security 2012, www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/heninger

[6] Serge Vaudenay, Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS, etc., in: Advances in Cryptology – Eurocrypt 2002, Springer 2002, S. 534, ISBN 978-3-540-43553-2

[7] Universität Siegen, Portal zum Open-Source-Projekt CrypTool, www.cryptool.org

[8] Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, MD5 considered harmful today, Dezember 2008, www.win.tue.nl/hashclash/rogue-ca/

[9] European Union Agency for Network and Information Security (ENISA), Algorithms, Key Sizes and Parameters Report, Version 1.0, Oktober 2013, www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

[10] European Payments Council (EPC), Guidelines on Algorithms Usage and Key Management, EPC342-08, Version 3.0, Oktober 2013, www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=192

[11] Bernhard Esslinger, Die dunkle Seite der Kryptografie – Kleptografie bei Black-Box-Implementierungen, <kes> 2010#4, S. 6

Sind Sie verantwortlich für die IT-Sicherheit?

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit
Zutrittskontrolle
Virenabwehr
Verschlüsselung
Risikomanagement
Abhör- und Manipulationsschutz
Sicherheitsplanung
Elektronische Signatur und PKI

<kes> ist seit 20 Jahren *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche, viele interessante Links, Stichwort-Lexikon IT-Security-Begriffe, Verzeichnis relevanter Veranstaltungen und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

PROBEHEFT-ANFORDERUNG

☐ **ja,** bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info

Datum | Zeichen | Unterschrift

Lieferung bitte an

Telefon Durchwahl

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim