Dirk Fox

Mindestlängen von Passwörtern und kryptographischen Schlüsseln

Mindestlängen von Passwörtern und Schlüsseln sind regelmäßig an den technischen Fortschritt anzupassen. Der Beitrag gibt – vor dem Hintergrund aktueller Entwicklungen – Empfehlungen für eine geeignete Festlegung.

1 Hintergrund

Die Längen von Passwörtern und kryptographischen Schlüsseln – sowohl für symmetrische als auch für asymmetrische Verfahren – müssen mit der Entwicklung der Rechenleistung einerseits und der weiteren Verbesserung von Angriffsalgorithmen andererseits Schritt halten. Sie sind daher von Zeit zu Zeit an die aktuellen Entwicklungen in Forschung und Technik anzupassen.

In der Praxis erfolgt dies jedoch häufig nicht oder zumindest nicht im erforderlichen Umfang. Die Ursachen dafür sind vielfältig: So stößt die Forderung größerer Passwortmindestlängen unvermeidlich auf Widerstand und lässt sich nur selten ohne Unterstützung der Unternehmensleitung durchsetzen. Und der Wechsel auf längere Schlüssel ist zumindest bei asymmetrischen Verfahren zumeist mit weiterem Aufwand verbunden (Sperrung, Policy-Änderung, Ausstellung und Verteilung neuer Schlüssel und Zertifikate). Gelegentlich wird auch der Beobachtung aktueller Entwicklungen neben dem operativen Betrieb nicht die nötige Aufmerksamkeit geschenkt.

Umso wichtiger sind substantiierte Informationen über den Stand der Entwicklung. Der vorliegende Beitrag unternimmt den Versuch einer aktuellen Bestandsaufnahme.

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.
E-Mail: dirk.fox@secorvo.de

Tabelle 1 | Dauer einer „Brute Force"-Suche nach Windows-Passworten mit „Rainbow Crack"

Passwortlänge	Nur Buchstaben (52 Zeichen)	Buchstaben, Ziffern und Sonderzeichen (84 Zeichen)
4	nicht messbar	0,3 ms
5	3,7 ms	41 ms
6	0,2 s	3,4 s
7	10 s	4,8 Min.
8	8,75 Min.	6,7 Std.
9	7,6 Std.	23,2 Tage
10	16,4 Tage	5,4 J.
11	2,4 J.	454 J.
12	122 J.	38.147 J.

2 Passwortlängen

Die Bestimmung geeigneter Mindestlängen für Passwörter fußt unvermeidlich auf bestimmten Rahmenbedingungen und Annahmen – z. B. über das Angreifermodell (kann ein Angreifer nur über das Login-Fenster Passworte ausprobieren oder auch Offline-Attacken auf die Passwort-Hashtabelle durchführen? [FoSc_09]) oder über die bei der Passwortwahl tatsächlich genutzten Zeichen (nur alphabetische Zeichen? Unterscheidung von Groß- und Kleinbuchstaben? Ziffern? Sonderzeichen?).

Auch hängt eine sinnvolle Wahl der Passwortmindestlänge von einigen grundsätzlichen Festlegungen ab: Sollen die gewählten Passwörter regelmäßig oder nur Anlass bezogen gewechselt werden, z. B. bei Verdacht auf unberechtigte Kenntnisnahme oder nach jeder Änderung der Passwort-Policy? Können Trivialpasswörter bereits bei der Wahl systemseitig abgewiesen werden, oder erfolgt eine regelmäßige Überprüfung der Qualität der verwendeten Passwörter?

Vor diesem Hintergrund sind dann die Fortschritte bei der Entwicklung von Analyse-Algorithmen zu bewerten, die das Durchprobieren aller möglichen Passwörter mit „roher Gewalt" („Brute Force") optimieren.

Tatsächlich hat es hier in den vergangenen Jahren erhebliche Entwicklungssprünge gegeben: Zunächst die Entwicklung von „Rainbow Tables", die durch die Vorausberechnung von Teilergebnissen erhebliche Rechenzeit einsparen [Oechs_03], sowie in jüngster Zeit die Nutzung hochgezüchteter Grafik-Prozessoren auf handelsüblichen Grafikkarten als Rechenhilfe [ArDe_09].

Die Resultate sind ernüchternd: Auf einem heutigen Standard-PC mit schneller Grafikkarte erreicht die im Open-Source-Projekt „Rainbow Crack" entwickelte Software[1] die Bestimmung von über 100

1 Aktuelle Version 1.4 vom 17.08.2009; siehe http://project-rainbowcrack.com/

Milliarden (!) NTLM-Hashwerten von Windows-Passworten – pro Sekunde. Wie lange es dauert, bis so mit einem einzelnen PC alle möglichen Passworte ausprobiert (und damit gefunden) sind, zeigt Tabelle 1. Ein einzelnes Passwort ist im statistischen Mittel in der Hälfte der Zeit gefunden.

Den Werten der Tabelle liegt dabei die Annahme zu Grunde, dass die Nutzer auch tatsächlich den gesamten Passwort-Zeichenraum (52 Groß- und Kleinbuchstaben, 10 Ziffern und 22 Sonderzeichen = 84 Zeichen) nutzen – und keine Begriffe aus Wörterbüchern, Datumsangaben oder andere Trivialpasswörter verwenden. Ein Angreifer kann die Suche weiter beschleunigen, indem er mehrere PCs parallel arbeiten lässt.[2]

Die Konsequenz ist eindeutig: Wenn nicht durch geeignete technische Maßnahmen sicher ausgeschlossen werden kann, dass jemals eine Windows-Passwort-Hash-Tabelle – die SAM-Datei – in die Hände eines Unberechtigten fällt, dann müssen Passwörter mindestens 10 Zeichen lang sein – selbst bei monatlichen Passwortwechseln und komplexen Passwörtern. Werden nur Buchstaben oder Buchstaben mit (mindestens) einem Sonderzeichen oder einer Ziffer verwendet, wie in zahlreichen Passwort-Policies gefordert, ist eine Mindestlänge von 11 Zeichen erforderlich. Gute Passwörter dieser Länge erfordern jedoch ausgefeilte Merkregeln.

3 Schlüssellängen

Die Auseinandersetzung über die Mindestlängen von kryptographischen Schlüsseln wurde in den 90er Jahren von der Diskussion um verschiedene Formen der Kryptoregulierung bestimmt. Die Varianten reichten von Exportrestriktionen über Nutzungsverbote und Hinterlegungspflichten bis zur Beeinflussung von Standards. Erst mit der Aufgabe des Versuchs, die Nutzung von Kryptographie durch staatliche Regulierung zu kontrollieren, wurde eine vorurteilsfreie fachöffentliche Diskussion über sinnvolle Mindestlängen kryptographischer Schlüssel möglich.

3.1 Symmetrische Chiffren

Im Januar 1996 publizierte die *Business Software Alliance* (BSA) einen Report, an dem führende Kryptologen der USA mitgewirkt hatten, darunter Whitfield Diffie, Ronald Rivest und Bruce Schneier [BDRS_96]. In diesem mit „*Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*" überschriebenen Text forderten die Autoren überzeugend eine Schlüssel-Mindestlänge von 75 bit, um Schutz vor Brute-Force-Analysen auch eines Geheimdienstes zu bieten. Damit eine Verschlüsselung auch in den folgenden 20 Jahre nicht gebrochen werden könne, empfahlen die Autoren unter Berücksichtigung von „Moore's Law" einen Sicherheitsaufschlag von 14 bit.[3]

Auch Matt Blaze, damals Forscher bei AT&T, forderte in dem Ende 1996 veröffentlichten Standpunktpapier „*Cryptography Policy and the Information Economy*" (in deutscher Übersetzung publiziert in der DuD [Blaz_97]) eine symmetrische Chiffre mit mindestens 90 bit Schlüssellänge als Ersatz für den in die Jahre gekommenen „Data Encryption Standard" (DES) mit einer Schlüssellänge von 56 bit.

Drei Jahre später übertraf das US-amerikanische NIST in einem öffentlichen Selektionsverfahren, das mit der Wahl des Rijndael-Algorithmus als Nachfolger des DES abschloss, alle Erwartungen [LuWe_00]. 2001 wurde vom NIST der „Advanced Encryption Standard" (AES) verabschiedet, der wahlweise mit Schlüsseln der Länge 128, 192 oder 256 bit genutzt werden kann [NIST_01]. Sofern nicht eines Tages eine entscheidende Schwäche im AES-Algorithmus selbst gefunden wird, bietet nach der Prognose von 1996 selbst die kleinste AES-Schlüssellänge (128 bit) bis zum Jahr 2075 wirksamen Schutz vor einem Brute-Force-Angriff.

Mit der Einführung des AES wird eine Anpassung der Schlüssellängen symmetrischer Chiffren für viele Jahre nicht mehr erforderlich sein.

3.2 Asymmetrische Kryptosysteme

Für die Bestimmung geeigneter Mindestschlüssellängen für asymmetrische kryptographische Verfahren – z. B. zur Erzeugung digitaler Signaturen und Zertifikate – war eine Arbeit von Arjen Lenstra und Eric Verheul aus dem Jahr 1999 wegweisend [LeVe_00]. Darin entwickelten die Autoren ein Berechnungsmodell, das das Sicherheitsniveau der Schlüssellängen asymmetrischer Verfahren vor den besten bekannten mathematischen Angriffen in Beziehung setzt zu dem von symmetrischen Chiffren.

Aus diesem Modell leiteten Lenstra und Verheul Empfehlungen für die Schlüssellängen verbreiteter asymmetrischer Verfahren für die Jahre bis 2040 ab, für die ein dem Brechen von DES im Jahr 1982 äquivalenter Rechenaufwand erforderlich wäre. Für das Jahr 2009 empfahlen sie auf dieser Grundlage eine Mindestlänge von 1.323 bit für einen RSA-Modulus und 145 bis 157 bit für den endlichen Primkörper elliptischer Kurven.

Noch immer beziehen sich zahlreiche Prognosen auf diesen Ansatz, nicht zuletzt die jährlichen Empfehlungen der Bundesnetzagentur (BNetzA) für geeignete kryptographische Algorithmen gemäß Signaturgesetz [BNA_08] nach einer Vorlage des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Der BSI-Empfehlung liegt daher als Referenzniveau die Sicherheit des DES im Jahr 1982 zu Grunde. Daher akzeptiert die BNetzA eine Moduluslänge von 1.024 bit schon seit Ende 2007 nicht mehr; die Mindestlänge von 1.280 bit lief Ende 2008 aus. Seitdem fordert sie eine RSA-Moduluslänge von mindestens 1.536 bit, ab Anfang 2010 sogar von 1.728 bit.

Wie weit das dieser Empfehlung zu Grunde liegende Sicherheitsniveau jenseits der realistisch zu erwartenden Faktorisierungsmöglichkeiten liegt, zeigt die Tatsache, dass es bis heute nicht einmal gelungen ist, mit verteilter Berechnung auf zigtausenden Forschungscomputern auch nur einen einzigen 768 bit langen RSA-Modulus zu faktorisieren. Selbst unter Berücksichtigung des „Sicherheitspuffers" des Signaturgesetzes von sieben Jahren übersteigt die Empfehlung von BSI und BNetzA die bekannten Möglichkeiten deutlich. Selbst wenn es noch 2009 gelänge, einen 768 bit großen RSA-Modulus zu faktorisieren, wäre nach der Lenstra-Verheul-Tabelle erst in 13 Jahren, also im Jahr 2022, mit

2 Eine wirksame Gegenmaßnahme wäre „Password Stretching" (auch „Strengthening" genannt), wodurch das Passwort vor der Prüfung aufwändig umgerechnet wird. Ein solches Verfahren wird von Windows jedoch nicht unterstützt.

3 Mit „Moore's Law" wird die unbewiesene, aber mit der tatsächlichen Entwicklung überraschend übereinstimmende These von Gordon Moore aus dem Jahr 1975 bezeichnet, dass sich die Zahl der Transistoren auf einem Computerchip etwa alle zwei Jahre verdoppelt. Unter Berücksichtigung des gleichzeitigen Preisverfalls wird eine Verdoppelung der Leistungsfähigkeit von Computersystemen alle 1,5 Jahre abgeleitet.

einer erfolgreichen 1.024 bit-Faktorisierung zu rechnen, da dafür etwa die tausendfache Rechenleistung erforderlich ist [BKKLM_09b]. Damit bietet RSA mit einem 1.024 bit-Modulus also noch mindestens bis Ende 2012 ein ausreichendes Schutzniveau vor öffentlichen Angriffen.

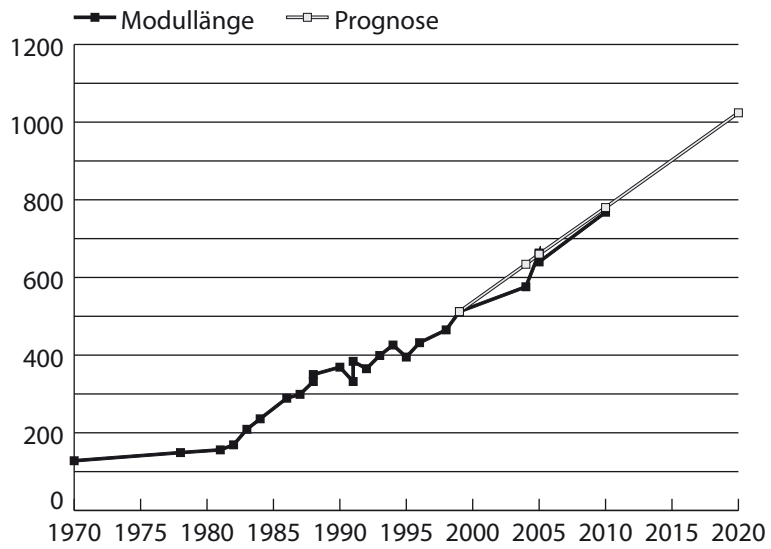
Unter Berücksichtigung der überraschend linearen Entwicklung der Faktorisierungserfolge in den vorausgegangenen 30 Jahren und der Tatsache, dass der DES nicht 1982, sondern erst 1997 Opfer einer „Brute Force"-Analyse wurde, kam der Zahlentheoretiker und Kryptologe Robert Silverman im Jahr 2000 zu anderen Ergebnissen als Lenstra und Verheul [Silv_00]: Nach seiner damaligen Einschätzung wären RSA-Moduli von 1.024 bit mindestens bis zum Jahr 2020 sicher vor einem Faktorisierungsangriff.

Ein ähnliches Modell liegt der Prognose zukünftiger Faktorisierungserfolge von Bourseau, Fox und Thiel aus dem Jahr 2001 zu Grunde [BoFT_02] – und deckt sich fast exakt mit den tatsächlichen Faktorisierungserfolgen der darauffolgenden Jahre (siehe Grafik 1). Die Faktorisierung eines 768 bit-Modulus ist danach frühestens im Jahr 2010 zu erwarten.

Diese Prognose wird gestützt von einem aktuellen Positionspapier zur Sicherheit von 1.024 bit RSA-Moduli und Elliptischen Kurven über 160 bit-Primkörpern, an dem u. a. Lenstra und sein Mathematiker-Kollege Peter Montgomery mitwirkten [BKKLM_09b]. Sie fußt auf der langjährigen Erfahrung der Autoren aus der Mitwirkung an der Weiterentwicklung theoretischer und praktischer Algorithmen zur Faktorisierung und der Bestimmung diskreter Logarithmen. Jüngst gelang es der Forschungsgruppe um Arjen Lenstra an der EPFL in Lausanne, innerhalb von knapp sechs Monaten einen diskreten Logarithmus auf einer elliptischen Kurve über einem 112-bit großen Primkörper zu bestimmen – mit über 200 vernetzten PlayStation 3-Systemen [BKKLM_09a]. Derzeit sind sie an einem Projekt zur Faktorisierung eines 768 bit-Modulus beteiligt – deren Ergebnis 2010 (sic!) erwartet wird.

Lenstra und Montgomery erwarten die erste 1.024 bit-RSA-Faktorisierung frühestens im Jahr 2020, und sicher nicht vor 2015. Daher sehen sie derzeit keinen Grund zu der Annahme, dass die Nutzung von 1.024 bit langen RSA-Schlüsseln bis zum Jahr 2015 ein Risiko birgt. Und elliptische Kurven über 160 bit großen Primkörpern seien noch mindestens für weitere 10 Jahre sicher – die erste Lösung eines diskreten Logarithmus über einem 160 bit-Primkörper prognostizieren sie für das Jahr 2030.

Abbildung 1 | Prognose der Entwicklung von Faktorisierungserfolgen [BoFT_02]



Demnach ist das RSA-Verfahren mit 1.024 bit-Schlüsseln deutlich sicherer, als von Lenstra und Verheul vor 10 Jahren angenommen. Lenstra und Montgomery gehen heute von einem Sicherheitsniveau[4] von 76 bit (statt 72 bit) aus. Dennoch: Auch wenn ein 1.024 bit-RSA-Modulus in den kommenden zehn Jahren nicht faktorisiert werden kann, liegt er unter dem derzeit empfohlenen Sicherheitsniveau von mindestens 80 bit. Ein Wechsel auf eine Mindest-Moduluslänge von 1.280 bit bis spätestens 2013 erscheint daher konsequent.

Längere Schlüssel brauchen nur dann gewählt werden, wenn dem Risiko eines plötzlichen mathematischen „Durchbruchs" bei der Faktorisierung oder dem Angriff eines Nachrichtendienstes oder der organisierten Kriminalität mit gigantischer Rechenleistung durch ein entsprechendes Sicherheitspolster vorgebeugt werden soll.

Das diskrete Logarithmusproblem auf elliptischen Kurven über Primkörpern hat sich als (im Verhältnis) „leichter" lösbar erwiesen, als von Lenstra und Verheul 1999 prognostiziert. Statt eines Sicherheitsniveaus von 90 bit gehen Lenstra und Montgomery heute von einem Niveau von 86 bis 87 bit aus. Dennoch liegt das Sicherheitsniveau einer elliptischen Kurve über einem 160 bit-Primkörper damit deutlich über dem derzeit empfohlenen Sicherheitsniveau von 80 bit. Als Mindestlänge sollten 160 bit mindestens bis zum Jahr 2020 ausreichen.

In einem im Juli 2009 veröffentlichten White Paper diskutiert das NIST einen Wechsel auf ein Sicherheitsniveau von 112 bit, dem Niveau des Triple-DES [NIST_09]. Für RSA-Schlüssel entspricht das einer Modulus-Mindestlänge von 2.048 bit[5], die das NIST bis zum Jahr 2030 empfiehlt [NIST_07].

Tatsächlich liegt ein „Brute Force"-Angriff auf 112 bit lange Schlüssel weit jenseits heute bekannter Möglichkeiten. Die längste erfolgreiche „Brute Force"-Suche nach einem symmetrischen Schlüssel ist die RC5-64-Challenge, die am 14.07.2002 nach knapp fünfjähriger verteilter Berechnung von distributed.net gelöst wurde. Die RC5-72-Challenge der Firma RSA, die den 256-fachen Rechenaufwand der RC5-64-Challenge erfordert, ist bis heute ungelöst.

Die „Brute Force"-Suche nach einem 112 bit langen Schlüssel würde den 1,1 Milliarden fachen Aufwand erfordern. Nach der Prognose von Lenstra und Verheul wäre eine erfolgreiche Lösung frühestens 50 Jahre nach der RC5-72-Challenge mit vergleichbarem Aufwand möglich. Ein Sicherheitsniveau von 112 bit, das inzwischen auch den Empfehlungen von BNetzA und BSI zu Grunde liegt, enthält daher einen riesigen Sicherheitspuffer.

4 Unter ‚Sicherheitsniveau' wird der Rechenaufwand verstanden, der für einen Brute-Force-Angriff auf einen symmetrischen Schlüssel einer bestimmten Bitlänge erforderlich ist.

5 Eine Moduluslänge von 2.048 bit empfiehlt das BSI für RSA seit dem Jahr 2000.

Literatur

[ArDe_09] Arbeiter, Stefan; Deeg, Matthias: Bunte Rechenknechte. c't 6/2009, S. 204-206.

[BDRS_96] M. Blaze, Matt; Diffie, Whitfield; Rivest, Ron; Schneier, Bruce; Shimomura, Tsutomu; Thompson, Eric; Wiener, Michael: Minimum Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security. Business Software Alliance (BSA), Januar 1996. http://people .csail.mit.edu/rivest/bsa-final-report.ps (08.09.2009)

[BKKLM_09a] Bos; Joppe W.; Kaihara, Marcelo E.; Kleinjung, Thorsten; Lenstra, Arjen K.; Montgomery, Peter L.: PlayStation 3 computing breaks 260 barrier – 112-bit prime ECDLP solved. http://lacal.epfl.ch/page81774.html (07.09.2009)

[BKKLM_09b] Bos; Joppe W.; Kaihara, Marcelo E.; Kleinjung, Thorsten; Lenstra, Arjen K.; Montgomery, Peter L.: On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography, Cryptology ePrint Archive, Report 2009/389 http://eprint.iacr.org/2009/389.pdf (06.09.2009)

[Blaz_97] Blaze, Matt: Kryptopolitik und Informations-Wirtschaft. DuD 4/1997, S. 209-213.

[BNA_08] Bundesnetzagentur (BNetzA): Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen). 17.11.2008 http://www.bundesnetzagentur.de/media/archive/14953.pdf (08.09.2009)

[BoFT_02] Bourseau, Frank; Fox, Dirk; Thiel, Christoph: Vorzüge und Grenzen des RSA-Verfahrens, DuD 2/2002, S. 84-89 http://www.secorvo .de/publikationen/rsa-grenzen-fox-2002.pdf (06.09.2009)

[FoSc_09] Fox, Dirk: Passwörter – fünf Mythen und fünf Versäumnisse. DuD 7/2009, S. 425-429. http://www.secorvo.de/publikationen/passwortsicherheit-fox-schaefer-2009.pdf (06.09.2009)

[Lens_04] Lenstra, Arjen K.: Key Lengths. Contribution to The Handbook of Information Security, 30.06.2004. http://www.keylength.com/biblio/Handbook_of_Information_Security_-_Keylength.pdf (09.09.2009)

[LeVe_00] Lenstra, Arjen K.; Verheul, Eric: Selecting Cryptographic Key Sizes. DuD 3/2000, S. 166.

[LuWe_00] Lucks, Stefan; Weis, Rüdiger: Der DES-Nachfolger Rijndael. DuD 12/2000, S. 711-713.

[NIST_01] National Institute of Standards and Technology (NIST): Advanced Encryption Standard (AES). FIPS-PUB 197, 26.11.2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (08.09.2009)

[NIST_07] National Institute of Standards and Technology (NIST): Recommendation for Key Management – Part 1: General. Special Publication SP 800-57, März 2007. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf (13.09.2009)

[NIST_09] National Institute of Standards and Technology (NIST): The Transitioning of Cryptographic Algorithms and Key Sizes. White Paper, 02.07.2009. http://csrc.nist.gov/groups/ST/key_mgmt/documents/Transitioning_CryptoAlgos_070209.pdf (13.09.2009)

[Oechs_03] Oechslin, Philippe: Making a Faster Cryptanalytic Time-Memory Trade-Off; Proceedings of Crypto '03, LNCS 2729, Springer 2003, S. 617-630.http://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf (12.09.2009)

[Silv_00] Silverman, Robert D.: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths. RSA Bulletin No. 13, 4/2000. ftp://ftp.rsasecurity.com/pub/pdfs/bulletn13.pdf (08.09.2009)