

ISSN 1861-0641

IT-Sicherheit & Datenschutz

Ausgabe 06/06
16.06. – 21.07.2006

Zeitschrift für rechts- und prüfungssicheres Datenmanagement

Praxis – Anwendungen – Lösungen

Deutschland deine Daten (VI): Blick über den Tellerrand	388
Knackstellen im Kopierschutz – Digital Rights Management im Ländervergleich	392

Sicherheits- und Datenschutz-Management

Aufgaben des betrieblichen Datenschutzbeauftragten: Datenschutzmanagement (V) – Stellungnahmen	398
---	-----

Grundlagen – Technik und Methoden

Kryptographie (I): Von der Geheimwissenschaft zur alltäglichen Nutzenanwendung	405
Mehr Sicherheit durch Windows Vista? (I)	411

EXTRA

Vorschriften – Gesetze – Urteile

Urteil des Europäischen Gerichtshofes zur Weitergabe von Fluggastdaten (Presseerklärung)	401–404
---	---------

 Online-Service
www.it-sd.com

Prof. Dr. Norbert Pohlmann, Malte Hesse

Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung

Einst den Militärs und der hohen Diplomatie vorbehalten, prägt Kryptographie in immer stärkerem Maß unser Alltagsleben. Das gilt nicht bloß fürs Online-Banking oder den Remote-Zugriff auf Firmennetze, die ohne die Nutzung von Techniken wie SSL und VPN praktisch nicht mehr vorstellbar sind: Selbst dort, wo wir sie zunächst nicht vermuten, sind heutzutage Verschlüsselungsmechanismen im Einsatz, zum Beispiel bei den elektronischen Wegfahrsperrn in unseren Autos oder wenn wir das Handy einschalten und uns beim Mobilfunknetz unseres Providers anmelden.

Aber auch in den aktuellen Debatten über die ausufernden Phishing-Attacken und das Digital Rights Management spielt Kryptographie eine tragende Rolle. *Kurz: Sie ist aus unserer Wissens- und Informationsgesellschaft nicht mehr wegzudenken*, und jeder, der sich darin zurechtfinden will, sollte zumindest einige ihrer Grundprinzipien kennen.

Kryptographie ist heute Bestandteil unseres Alltagslebens; ihre Prinzipien lassen sich am besten mit Hilfe der Verschlüsselung erläutern

Grundlagen der Kryptographie

Am einfachsten erläutern lassen sich diese am Beispiel der Verschlüsselung. Deren Ziel besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterwerfen, dass es einem Unbefugten unmöglich ist, die Original- aus den transformierten Daten zu rekonstruieren. Damit die verschlüsselten Daten für ihren legitimen Benutzer dennoch verwendbar bleiben, muss es diesem aber möglich sein, durch Anwendung einer inversen Transformation aus ihnen wieder die Originaldaten zu generieren. Die Originaldaten bezeichnet man als „Klartext“ (*clear text, plain text, message*), die transformierten Daten werden „Schlüsseltext“ (Chiffretext, Chiffrat, Kryptogramm, *cipher text*) genannt. Die Transformation heißt „Verschlüsselung“, ihre Inverse folglich „Entschlüsselung“.

Das generelle Ziel der Verschlüsselung kann folgendermaßen formuliert werden: Die Entschlüsselung darf nur dem legalen Empfänger/Besitzer der übermittelten/gespeicherten Informationen möglich sein, nicht jedoch anderen Personen – im Extremfall nicht einmal dem Absender selbst, der die Information verschlüsselt hat. Dieses Ziel lässt sich offensichtlich genau dann erreichen, wenn nur der legale Empfänger/Besitzer die zur Entschlüsselung benötigten Informationen – wie den Algorithmus und abhängig

Verschlüsselung dient zur Übertragung geheimer Informationen, die nur dem Empfänger zugänglich sein sollen

GRUNDLAGEN – TECHNIK UND METHODEN

vom Verfahren den Schlüssel – kennt und es ohne diese Kenntnis nicht möglich ist, die ursprüngliche Information aus dem Schlüsseltext zu bestimmen. Es wäre also auf den ersten Blick ausreichend, wenn Sender und Empfänger eine nur ihnen bekannte Transformation untereinander absprechen und die Kenntnisse darüber geheim halten (s. Abb. 1).



ABB. 1: Einfachste mögliche Vorgehensweise bei einer Verschlüsselung

Die Eigenentwicklung von Verschlüsselungsverfahren erfordert großen Aufwand und führt meist zu mangelhaften Resultaten

Dieser Ansatz ist jedoch aus drei Gründen nicht praktikabel:

- Definition und Realisierung eines Verschlüsselungsalgorithmus erfordern einen erheblichen Aufwand. Dieses Argument wiegt umso schwerer, als es von Zeit zu Zeit notwendig ist, die Verschlüsselung zu wechseln. In diesem Fall müsste ein neuer Algorithmus entwickelt werden.
- Zumindest theoretisch ist es jedem Unbefugten (im Folgenden: Angreifer) möglich, aus der Struktur der verschlüsselten Daten mittels geeigneter Verfahren, der sog. Kryptoanalyse, den Klartext oder die zur Verschlüsselung bzw. Entschlüsselung verwendete Transformation abzuleiten, also die Verschlüsselung zu „brechen“. Umgekehrt lässt sich der Gegenbeweis, dass ein - insbesondere willkürlich gewählter - Algorithmus gegen solche Attacken hinreichend gesichert ist, nur schwer führen. Der Einsatz solcher individuellen Verfahren bietet also zu wenig Schutz.
- Damit die gewünschte Vertraulichkeit gewahrt bleibt, muss für jeweils zwei Partner ein separater Verschlüsselungsalgorithmus zur Verfügung stehen. Der mit deren Entwicklung, Übermittlung, Aufbewahrung und Geheimhaltung verbundene Aufwand ist organisatorisch kaum zu bewältigen und wirtschaftlich nicht vertretbar.

In der Praxis werden daher nur Algorithmen eingesetzt, die nachweislich sicher sind

Als Lösung dieser Probleme bietet sich an, zur Verschlüsselung nur einige wenige Algorithmen einzusetzen, deren Sicherheit erwiesen ist. Um dennoch die Forderung nach einer Vielzahl von Verschlüsselungsverfahren zu erfüllen, kann man diese zusätzlich von einem Parameter abhängig machen, dem so genannten Schlüssel, der den Ablauf der Transformation so stark beeinflusst, dass ohne seine Kenntnis keine Entschlüsselung möglich ist (s. Abb. 2).



ABB. 2: Grundlegende Vorgehensweise bei einer sicheren Verschlüsselung

Bleibt dieser Schlüssel geheim, so kann der Verschlüsselungsalgorithmus selbst durchaus publik gemacht werden; dies sollte sogar der Regelfall sein, da sich dessen Sicherheit nur in einer öffentlichen Diskussion hinreichend beweisen lässt.

„No Security by Obscurity“

Diese Betrachtungsweise hat unter Mathematikern, die sich wissenschaftlich mit Verschlüsselung befassen, eine lange Tradition und geht zurück auf den niederländischen Linguisten und Kryptologen Auguste Kerckhoffs von Nieuwenhof, der 1883 in seiner Abhandlung *La Cryptographie militaire* einige Grundsätze für schlüsselbasierte Verfahren entwickelte, von denen einer noch heute als Kerckhoffs-Prinzip bekannt ist:

„Die Sicherheit eines Kryptosystems darf nur von der Geheimhaltung der Schlüssel, aber nicht von der Geheimhaltung der Verfahren abhängig sein.“

Dennoch sind noch immer wesentliche Einsatzfelder von Kryptographie durch den gegenteiligen Ansatz geprägt, der oft mit „Security by Obscurity“ (Sicherheit durch Geheimhaltung) bezeichnet wird, von dem sich die Entwickler entsprechender Verfahren eine stärkere Sicherheit erhoffen.

Ein Beispiel für geheime Verfahren stellen die Kryptoalgorithmen des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI) dar, die zum Schutz der geheimen Informationen der Bundesrepublik Deutschland genutzt werden; ein ebenfalls recht kritisches Beispiel sind die bei der zurzeit meistverbreiteten Mobilfunktechnik GSM eingesetzten Algorithmen A3, A8 und A5/1. Diese gelten schon seit ca. 7 Jahren nicht mehr als sicher und sind mit moderner Technik leicht zu brechen.^[1]

Ob diese Herangehensweise einer Überprüfung Stand hält, darf indes mit einigem Recht bezweifelt werden: Denn die Entwicklung neuer kryptographischer Verfahren ist äußerst schwierig, weswegen die wenigen auf diesem Gebiet tätigen Fachleute ihre Arbeit in der Regel einem fachkundigem Publikum vorstellen.

Dieses bewertet zunächst die theoretische Stärke des vorgestellten Verfahrens, also die Wahrscheinlichkeit, dass es durch eine der im nächsten Abschnitt beschriebenen Methoden der so genannten Kryptoanalyse gebrochen (kompromittiert) wird. Erst wenn ein Verfahren einige Jahre nicht gebrochen wurde, gilt es als sicher und darf sich dann praktisch bewähren.

^[1] Ein leicht lesbarer historischer Abriss zur Geschichte der Kryptographie findet sich in Walter Gora/Thomas Krampert (Hg.): *Handbuch IT-Sicherheit. Strategien, Grundlagen und Projekte*. München 2003. S. 113-122. Detaillierter und „mathematischer“ ist die Darstellung in Reinhard Wobst: *Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung*. 3. Auflage, München 2001. S. 29-64.

Ob ein Verfahren als sicher gelten kann, lässt sich nur in der öffentlichen Diskussion nachweisen

Die wichtigsten Begriffe in Kurzdefinition

Kryptographie ist die Wissenschaft von den Methoden der Ver- und Entschlüsselung.

Kryptoanalysis ist die Wissenschaft von den Methoden der unbefugten Entschlüsselung von Daten zum Zweck ihrer Rückführung in die ursprüngliche Information.

Beide zusammen bilden die **Kryptologie**, die sich damit definieren lässt als Wissenschaft der Geheimhaltung von Informationen durch Transformation von Daten.

Ein **Kryptosystem** dient zur Geheimhaltung von (übertragenen oder gespeicherten) Informationen gegenüber Dritten und besteht aus Verschlüsselungsverfahren (Algorithmus) und dem gewählten Schlüssel.

Die **Kryptoanalyse** dient der Überprüfung eines gegebenen Verschlüsselungssystems und zur Bewertung seiner Stärke.

Analyse und Einschätzung von Kryptosystemen

Um die Stärke von Algorithmen und Schlüsseln zu bewerten, hat die Fachwelt verschiedene Methoden entwickelt

Algorithmus und Schlüssel bilden zusammen ein so genanntes Verschlüsselungs- oder Kryptosystem. Für die Analyse derartiger Systeme gibt es verschiedene grundlegende Strategien, aus denen sich Anforderungen an die Qualität ableiten lassen.

Die **vollständige Suche** (Brute-Force-Methode) besteht im Wesentlichen im Ausprobieren aller möglichen Schlüsselkombinationen. Bei einem „Known-Plaintext-Angriff“ verschlüsselt man z. B. den bekannten Klartext in jeder möglichen Weise und vergleicht den entstehenden Schlüsseltext mit dem bekannten Original. Bei einer Schlüssellänge von 128 Bits gibt es 2^{128} ($3.4 \cdot 10^{38}$) verschiedene Kombinationen, die ausprobiert werden müssen. Unter der Voraussetzung, dass eine Operation $1 \cdot 10^{-9}$ s benötigt, dauert die vollständige Suche $5,3 \cdot 10^{19}$ Jahre, d. h. solche Verfahren sind praktisch sicher. Forderung: Der Schlüssel muss lang genug gewählt werden.

Bei der **Trial-and-Error-Methode** wird die vollständige Suche dadurch reduziert, dass man aus dem gesamten Schlüsselraum Teilräume herausgreift, in denen der gesuchte Schlüssel vermutet wird. Dies ist etwa der Fall, wenn es viele äquivalente Schlüssel mit übereinstimmenden Eigenschaften gibt (z.B. Vornamen, Spitznamen etc.).

Beispiel:

Es werden als Schlüssel nur darstellbare ASCII-Zeichen verwendet, also die Ziffern 0 bis 9 sowie alle Klein- und Großbuchstaben des lateinischen Alphabets – insgesamt 62 verschiedene ASCII-Zeichen, die in 5 Bit codiert werden können. Damit reduziert sich die Zahl der möglichen Kombinationen auf 2^{80} und damit die Entschlüsselungszeit. Forderung: Eine qualitative Schlüsselgenerierung ist sehr wichtig.

GRUNDLAGEN – TECHNIK UND METHODEN

Bei den **statistischen Methoden** versucht der Analytiker, statistische Strukturen wie z. B. Buchstaben- oder Worthäufigkeiten einer Sprache im Chifftrat wieder zu finden, um dadurch an den Klartext zu gelangen. Forderung: Ein Verschlüsselungsverfahren muss solche Angriffe nach Möglichkeit ausschließen.

Die **Strukturanalyse** des Kryptosystems (Short-Cut-Methode) ist immer nur auf ein spezielles Kryptosystem zugeschnitten. Sind alle Parameter außer dem Schlüssel bekannt, versucht der Analytiker mit ihrer Hilfe eine Funktion aufzustellen, mit der sich der Klartext berechnen lässt. Das kann z. B. dann schnell zum Erfolg führen, wenn er den Schlüsseltext, den verwendeten Algorithmus und die Struktur des Originaldokuments kennt. Forderung: Ein Verschlüsselungsverfahren muss mindestens fünf Jahre öffentlich diskutiert werden, bevor es als sicher gelten kann.

Anhand der hier vorgestellten Verfahren lassen sich Kryptosysteme in zwei Kategorien einteilen – solche, die absolute, und solche, die rechnerische oder praktische Sicherheit bieten. **Absolute Sicherheit** liegt vor, wenn es auch theoretisch unmöglich ist, das System zu brechen. Diese Anforderung erfüllen zurzeit nur Einmal-Schlüssel-Verfahren mit definierten Eigenschaften. Die **rechnerische oder praktische Sicherheit** ist dagegen bereits dann gegeben, wenn die Kompromittierung so viel Rechenzeit bzw. Speicherplatz erfordert, dass der damit verbundene Aufwand einem jeden Kryptoanalytiker sinnlos erscheinen muss. Dies ist z. B. bei allen Verfahren der Fall, die sich nur mit der Brute-Force-Methode brechen lassen. Ob ein Kryptosystem dieser Anforderung genügt, kann durch eine mathematische Analyse der Komplexität festgestellt werden.

Zu unterscheiden ist hierbei zwischen Verfahren, die absolute, und Verfahren, die praktische Sicherheit bieten, also beim derzeitigen Stand der Technik nicht zu brechen sind

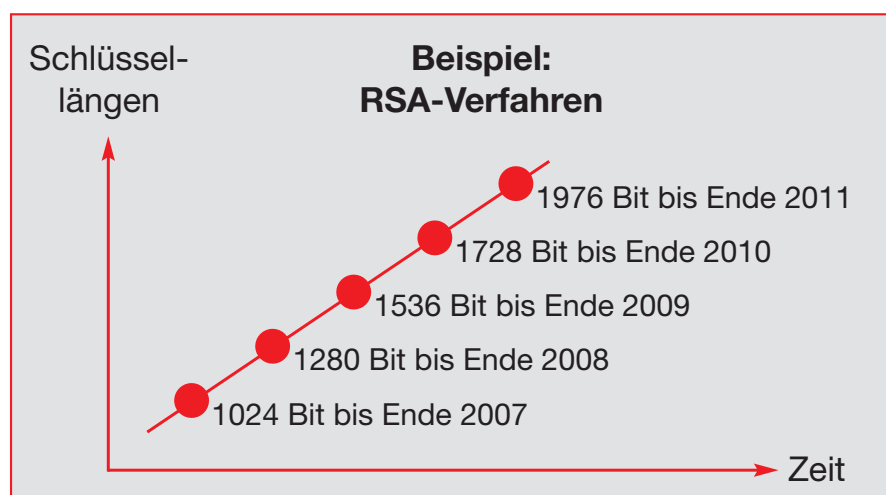


ABB. 3: Empfehlungen des BSI für Schlüssellängen am Beispiel des RSA-Verfahrens

Ein Wettlauf um die Sicherheit

Da Computer immer leistungsfähiger werden, sind vor allem die verwendeten Schlüssellängen regelmäßig anzupassen

Für die Sicherheit einer Verschlüsselung sind vier Faktoren ausschlaggebend: der verwendete Algorithmus, die Schlüsselgenerierung, die Schlüssellänge sowie die Aufbewahrung des Schlüssels. Bei symmetrischen Verschlüsselungsverfahren geht man heute davon aus, dass die praktische Sicherheit gegeben ist, wenn die Schlüssellänge 128 Bit beträgt.

Um einen solchen Schlüssel zu ermitteln, sind 2^{128} Versuche nötig. Damit stößt man auf ein praktisches Problem, denn mit den derzeitigen Ressourcen ist die Berechnung in einer angemessenen Zeit nicht möglich. Da aber die Rechenleistung von Computern ständig wächst, müssen auch die Schlüssellängen von Zeit zu Zeit angepasst werden: Gegenüber den vor zehn Jahren gebräuchlichen Verfahren wie DES hat sich diese inzwischen verdoppelt, im Jahr 2016 werden wir möglicherweise 256-Bit-Schlüssel wie z.B. AES benötigen.

Gesetzliche Anforderungen an Schlüssellängen

Welche Verfahren und Schlüssel als sicher gelten, bestimmt in Deutschland die Bundesnetzagentur; die Qualitätsprüfung obliegt dem BSI, das sich an internationale Standards hält

Neben den technischen Möglichkeiten bestimmt auch der Gesetzgeber, welche Verschlüsselungsverfahren als sicher gelten, wobei dieser i. d. R. recht allgemeine Anforderungen formuliert, die per Verordnung konkretisiert werden. In Deutschland sind diese im Signaturgesetz (SigG) sowie in Anlage 1 Abschnitt I Nr. 2 der Signaturverordnung (SigV) niedergelegt. Ob ein Verschlüsselungsverfahren und die zugehörigen Parameter als sicher gelten können, legt diesen zufolge die Bundesnetzagentur (BNetzA) fest. Für die technische Überprüfung ist das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) zuständig, das internationale Standards zugrunde legt und mit Experten aus Wirtschaft und Wissenschaft zusammenarbeitet. Die BNetzA hat die Ergebnisse das letzte Mal am 23. März 2006 im Bundesanzeiger Nr. 58, S. 1913-1915, veröffentlicht. Dort finden sich eine Liste geeigneter Verfahren mit ihren Schlüssellängen sowie Angaben zum Zeitraum des sicheren Einsatzes und Empfehlungen für den Einsatz längerer Schlüssel.

Weitere Informationen:

<http://www.bundesnetzagentur.de/>

<http://www.internet-sicherheit.de>

<http://www.bsi.de>

Zu den Autoren:

Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen.

E-Mail-Kontakt: norbert.pohlmann@informatik.fh-gelsenkirchen.de

Malte Hesse ist Mitarbeiter am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: hesse@internet-sicherheit.de