Praktische Anwendung kryptographischer Prüfsummen

Mit einer Einführung in Signierung und Verschlüsselung

Peter Jockisch, Freiburg i. Br.
peterjockisch.de

1. Mai 2024

Computerdateien können auf viele Weisen unbemerkt manipuliert werden. Kryptographische Prüfsummen, Hashwerte, dienen dem Schutze Ihrer Daten: Durch Bildung eines elektronischen Fingerabdrucks einer Datei wird ein stets gleichbleibender Zahlenwert erstellt. Weicht dieser zu einem späteren Zeitpunkt ab, liegt Beschädigung oder Manipulation vor. Mit einem einzigen Mausklick läßt sich so jederzeit die Unversehrtheit einer Datei prüfen.

Inhaltsverzeichnis

1 Begriffe und Einsatzgebiete

1.1 Einleitung

Kryptographische Prüfsummen bilden die Grundlage für kryptographische Signierung und Verschlüsselung, für Netzseiten- und E-Mail-Zertifikate, für die qualifizierte elektronische Signatur, sowie für das technische Verständnis der revisionssicheren E-Mail-Archivierung, zu der alle Vollkaufleute gesetzlich verpflichtet sind.

Diese Einführung stellt zwei freie grafische Programme für die Prüfsummenbildung vor, CyoHash und Jacksum, für die Bedienung per Dateimanager.

Konsolenbasierte Programme werden ebenfalls beschrieben, sie sind betriebssystemplattformübergreifend erhältlich und sowohl unter MS-Windows als auch unter den meisten Unix/BSD- und GNU/Linux-Systemen bereits vorinstalliert. D.h., daß keinerlei Programme installiert werden müssen, die vorhandenen Betriebssystem-Bordmittel reichen vollkommen aus, um Prüfsummen zu bilden.

1.2 Funktionsweise

1.2.1 Elektronische Fingerabdrücke

Menschen sind komplexe Lebewesen. Für ihre schnelle und unkomplizierte Identifizierung werden oftmals Fingerabdrücke erstellt. Nach demselben Prinzip können Computerdateien identifiziert werden: durch Erzeugung eines „elektronischen Fingerabdrucks“, der so genannten kryptographischen Prüfsumme, einer stets gleichbleibenden Zahl. Mittels standardisierter Verfahren kann so eine schnelle Integritäts- und Echtheitskontrolle von Dateien jedweder Art vorgenommen werden. Menschliche Fingerabdrücke werden mit Stempelkissen erstellt, elektronische mit einem Prüfsummenprogramm.

1.2.2 Qualitätskriterien

Wir betrachten *kryptographische* Prüfsummen. Sie basieren auf Streuwert- bzw. Hashfunktionen, die zu einer beliebigen Datei Streu- bzw. Hashwerte als Ergebnis liefern. Dieser Wert wird auch Hashcode bzw. Hash genannt.

Eine Datei, sowie identische Kopien von ihr, weist stets dieselbe Hashwert-Prüfsumme auf. Ändert sich jedoch auch nur ein einziges Bit oder Zeichen durch Beschädigung oder Manipulation, sollte ein gänzlich anderer Hashcode entstehen.

Ein Hashfunktions-Prüfsummenverfahren sollte also zu unterschiedlichen Computerdateien immer unterschiedliche Werte liefern. Die berechnete Prüfsumme ist, abhängig vom verwendeten Verfahren, immer gleichlang. Deshalb kann natürlich nur eine begrenzte Anzahl von Zahlen dargestellt werden: Es

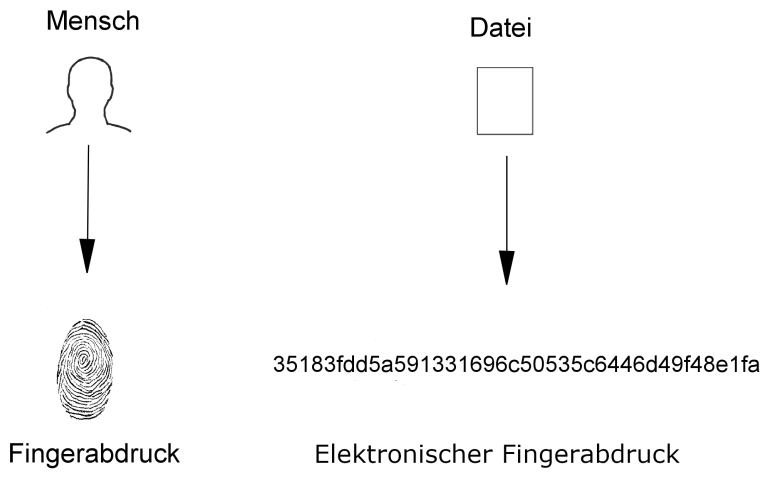

Abbildung 1: Echtheitsnachweis bei Mensch und Computerdatei

gibt praktisch unendlich viele Computerdateien, so daß mit einer Zahl fester Länge unmöglich jeder dieser Dateien ein unterschiedlicher Wert zugewiesen werden kann.

Unter Sicherheitsaspekten stellen sich verschiedene Angriffsszenarien dar, unter anderem die Fälschung von Dokumenten. Ein Angreifer möchte von einer gegebenen Originaldatei, beispielsweise einer geschäftlichen Bestellung, eine gefälschte Version mit einer manipulierten, erhöhten Bestellmenge erstellen, welche dieselbe Hashwert-Prüfsumme aufweist. Nachdem er die Änderungen im Dokument vorgenommen hat, versucht er anschließend durch Ausprobieren, vielleicht mittels Einfügung unsichtbarer Steuerzeichen, eine Dateiversion zu erhalten, deren kryptographische Prüfsumme identisch zur derjenigen der Originaldatei ist. Bei solch einem Angriff kommen natürlich unterstützende Computerprogramme zum Einsatz.

Gelingt es nun tatsächlich einem Angreifer, in zeitlich vertretbarem Aufwand eine zweite Datei zu erzeugen, die die erwünschten Manipulationen enthält und die dieselbe kryptographische Prüfsumme der Originaldatei aufweist, so ist das betreffende Hashfunktions-Verfahren „gebrochen“. Nach Bekanntwerden solch einer Schwäche sollte es keine Verwendung mehr finden. Durch stetige Forschungsarbeit werden Schwächen schon längere Zeit im voraus erkannt.

Gäbe es einen unendlich berechnungsstarken Computer, so könnte, theoretisch, möglicherweise jedes Verfahren durch schlichtes Ausprobieren sämtlicher Möglichkeiten gebrochen werden (Brute Force Angriff). Für die Praxis wird solch eine Vorgehensweise in der Mehrzahl aller Fälle als nicht praktikabel erachtet, da die erforderlichen Berechnungen fast nie in vertretbarer Zeit durchführbar sind.

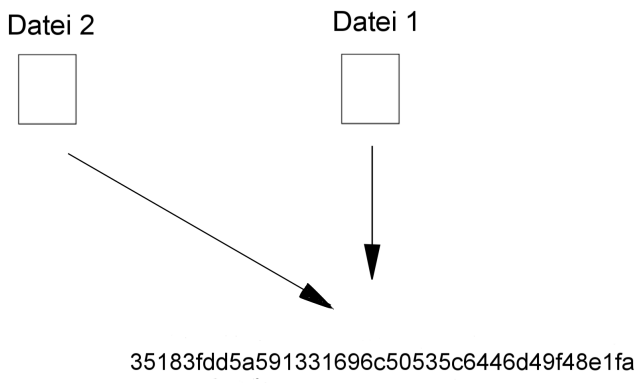

Abbildung 2: Prüfsummenkollision

Die meisten Hashfunktionen wiesen bisher nur eine begrenzte Lebensdauer auf und wurden irgendwann aus Sicherheitsgründen von Nachfolgeverfahren abgelöst.

Berechnungsstärkere Computergenerationen tragen zur Verkürzung der Lebensdauer bei. Neben den rechenkraftbasierten Angriffen existieren jedoch auch anders orientierte und es kann niemals ausgeschlossen werden, daß mithilfe mathematischer Kreativität bereits heute praktikable Angriffe möglich sind.

Im Hintergrund arbeitet und forscht ein riesiges Heer von Mathematikern, insbesondere für Nachrichtendienste. Nicht alle wissenschaftlichen Erkenntnisse werden veröffentlicht.

1.2.3 Vorherrschende Standards im Westen und in Rußland

Die westliche IT-Infrastruktur basierte bis 2016 überwiegend auf dem SHA-1-Algorithmus (Secure Hash Algorithm 1). Dieser gilt seit 2017 als endgültig gebrochen, die erforderliche Rechenzeit, um ihn zu korrumpieren, ist drastisch gesunken. Experten empfehlen mittlerweile die SHA-2-Varianten SHA256, SHA384, oder SHA512. Der empfohlene Nachfolgealgorithmus zu SHA-2, SHA-3[1], steht bereits seit 2012 offiziell fest.

In Rußland und vielen weiteren GUS-Staaten war GOST R 34.11-94 beziehungsweise GOST 34.311-95 der bisherige Hash-Standard in Behörden sowie

[1] „Hash-Verfahren SHA-3 als offizieller Standard verabschiedet“, 06. August 2015, heise Security.

in verschiedenen Wirtschaftsbereichen.[2] Wie bei SHA-1 wurden auch bei ihm strukturelle Schwächen gefunden.

1.3 Existieren für die Öffentlichkeit gesperrte Technologien?

1.3.1 Veraltete Rechnersysteme

Alle berechnungskraftbezogenen Aussagen dieser Einführung beziehen sich auf öffentlich verfügbare bzw. auf für die Allgemeinheit freigegebene Computersysteme und Forschungsarbeiten. Die Nutzung der jeweils aktuellsten, fortgeschrittensten Computertechnologie bleibt gegenwärtig vermutlich noch den Nachrichtendiensten vorbehalten, um diesen stets einen Berechnungskraftvorsprung zu gewährleisten, für eine effektive Aushebelung etablierter Verschlüsselungstechnologie.

Die auf breiter Ebene freigegebenen Verschlüsselungsverfahren mögen für untere Verwaltungsebenen nicht ohne weiteres zu brechen sein. Ganz oben in der Hierarchie, das heißt auf Nachrichtendienstebene, dürfte jedoch ein uneingeschränkter Zugriff auf modernste Computertechnologie vorhanden sein. Zudem werden vermutlich sämtliche über das Weltnetz transferierte Daten archiviert, für eine automatisch erfolgende Auswertung. Unter diesem Aspekt relativiert sich die Widerstandsfähigkeit von über das Internet versandten Dateien, die mit öffentlich standardisierter Technologie verschlüsselt wurden.

Schon seit langer Zeit existieren Überlegungen, daß bestimmte, zu offiziellen Standards erhobene Kryptographiealgorithmen inhärente mathematische Schwächen aufweisen könnten, die nur den Experten der Nachrichtendienste bekannt sind. Eine möglicherweise vorhandene Einflußnahme der Geheimdienste auf die Gestaltung von Sicherheitsprodukten (Software- und eventuell Hardware-Hintertürenproblematik, offene Fragen zu Standards usw.) ist Thema zahlreicher Artikel zur Computersicherheit, beispielsweise in „Did NSA Put a Secret Backdoor in New Encryption Standard?“ und in „Der Verschlüsselungsstandard AES: Das Danaer-Geschenk der US-Regierung für die Welt?“. Mehrere renommierte Firmen haben bereits direkt oder indirekt bestätigt, bei ihrer Produktentwicklung mit Nachrichtendiensten zusammenzuarbeiten. Offiziell begründet wurde dies unter anderem mit der Absicht, die technische Sicherheit von Firmenprodukten optimieren zu wollen. Wie groß der ausgeübte Druck zur „Zusammenarbeit“ war, sei dahingestellt.

Korrumpierte Elektronik, bekannte oder unbekannte „fortschrittliche“ Hardwarearchitekturen mit ab Werk eingebauten „Fernwartungsfunktionen“, möglicherweise sogar mit einem im Prozessor eingebautem Funksystem, stellen, die andere Seite des Problems dar.

[2] 02. Februar 2014, Informationen zu den von RHash unterstützten Verfahren, „Hash Functions“, Kurzauszug: „GOST is a hash function defined in Russian national standard GOST R 34.11-94. It has two widely used versions with testparameters and CryptoPro ones. It's relatively slow, but it is used for digital signature in Russian State banks and enterprises. Hash is a hexadecimal string of length 64.“

1.4 Anwendungsbeispiele: Geschäftswelt, Internet, Archivierung

Der gesetzlich anerkannte personengebundene Echtheitsnachweis ist fast immer an die Nutzung von proprietärer Soft- und Hardware gekoppelt, Abschnitt 1.5.5 enthält weiterführende Informationsquellen zu den umfassenden Voraussetzungen der so genannten qualifizierten elektronischen Signatur, die WP-Artikel „Elektronische Signatur“ sowie „Digitale Signatur“ nehmen Bezug auf die rechtlichen bzw. auf die mathematisch-technischen Aspekte (Begriffsabgrenzung).

Die Erstellung kryptographischer Prüfsummen gibt nicht nur Anhaltspunkte zur Echtheit und Unversehrtheit von Dateien. Sie ermöglicht auch Empfangsbestätigungen sowie eine schriftliche Bestätigung über den letzten Bearbeitungsstand einer Datei, wie folgende Beispiele demonstrieren.

1.4.1 Wahrung der Dateiintegrität

Sie erstellen eine Geschäftsbilanz und gehen anschließend in den Urlaub. Zur Qualitätskontrolle notieren Sie sich vor der Abreise die kryptographische Prüfsumme der fertiggestellten Bilanzdatei. Nach dem Urlaub bilden Sie erneut die Prüfsumme und verifizieren so, ob die Datei unversehrt ist oder ob sie beschädigt oder manipuliert wurde.[3]

Unautorisierte Zugriffe, z. B. auf eine Buchhaltungsdatei, können auf diese Weise entdeckt werden. Benachrichtigen Sie in solchen Fällen die Systemadministratoren und bestehen Sie auf einer Wiederherstellung der ursprünglichen Dateiversion, die natürlich nur dann erfolgreich ist, wenn die Datei wieder die notierte Prüfsumme aufweist.

Die Dateidatumsangabe und Versionsverwaltungssysteme sind kein Ersatz für kryptographische Prüfsummen, da sich beide direkt oder indirekt manipulieren lassen. Spezialisierte Programme, wie beispielsweise die Freeware Datei-Datums-Änderer, können sowohl das Erstellungs- als auch das Änderungsdatum von Dateien ändern, sogar verzeichnisweit.

Die Konsistenzprüfung über Prüfsummen funktioniert schneller, effektiver und sicherer und ist jederzeit möglich, dank vorinstallierter Betriebssystemprogramme, die normalerweise unter Standard-Benutzerkonten ausführbar sind (Beschreibung in Abschnitt 2.3).

1.4.2 Anhaltspunkt für den Bearbeitungsstand einer Datei

Beim Verlassen einer Firma möchten Sie sich den letzten Bearbeitungsstand einer Computerdatei schriftlich bestätigen lassen, Beispieltext: *„Bestätigung. Hiermit wird bestätigt, daß die zuletzt von [Vorname Name] gepflegte Datei*

[3] Beispiel entnommen aus „Die erstaunliche Macht der Hash-Funktionen“, Simson Garfinkel, 09.08.2004, heise.de. Original: „Fingerprinting Your Files“, MIT Technology Review.

[Dateiname] in ihrem letzten Bearbeitungsstand am [Datum] die SHA-256-Prüfsumme [konkrete Prüfsumme] aufwies. [Firmenstempel, Datum, Name und Unterschrift vom Vorgesetzten]".

Bestehen Sie auf einer rechtsverbindlichen Namensunterschrift (keine Paraphe).[4] Auf diese Weise bleibt das Firmengeheimnis gewahrt und Sie können sich trotzdem bis zu einem gewissen Grad absichern. Sollte es jemals Rückfragen geben, haben Sie einen schriftlichen Anhaltspunkt über Ihren letzten Bearbeitungsstand.

Möglicherweise empfehlen sich zwei oder drei verschiedene kryptographische Prüfsummenverfahren. Das könnte langfristig etwas sicherer sein, eines der Verfahren hält vielleicht länger durch in der Zukunft.

1.4.3 Wappnung gegen Wirtschaftskriminalität, Schutz vor Mobbing

Im Rahmen der allgemeinen Qualitätskontrolle und immer dann, wenn Korruption, Lügen, Intrigen, Mobbing, Sabotage und Wirtschaftskriminalität wahrscheinlich werden, empfiehlt sich zum eigenen Schutz der Gebrauch kryptographischer Prüfsummen, auch vor Präsentationsterminen (Dateiüberprüfung). Signierungssoftware scheidet oftmals aus, da sie naturgemäß mit Verschlüsselungsfunktionen gekoppelt ist und deshalb nicht auf jedem Arbeitsplatzrechner geduldet wird. Firmengeheimnisse könnten verschlüsselt nach außen gelangen bzw. Schadsoftware unentdeckt nach innen. Ein freies Prüfsummenprogramm – nicht zu verwechseln mit Freeware[5] – kann jedoch verantwortlich auf Firmenrechnern installiert werden, wenn dies der Systemadministrator für passend erachtet.

1.4.4 Dateibezugnahme in Verträgen und Eingangsbestätigungen

Bei schriftlichen Verträgen und Eingangsbestätigungen erleichtern elektronische Fingerabdrücke die Bezugnahme auf Computerdateien. Dateien jedweder Art können eindeutig über ihren Hashwert identifiziert werden z. B. Textdokumente, Videofilme, Gesprächsmitschnitte und Interviews (allgemein Tondateien), Programme, CAD- Dateien. Auch erbrachte Dienstleistungen, die abschließend in Form eines Datenträgers, z. B. einer abzuliefernden CD-ROM oder DVD vorliegen, lassen sich auf diese Weise schriftlich bestätigen.

Auch von Archivdateien[6] können elektronische Fingerabdrücke erstellt werden. Empfangsbestätigungen bilden ein breites Einsatzgebiet.

[4] Weiterführende Informationen: WP-Artikel „Paraphe", „Paraphieren eines Vertrags: Was ist das und was ist die rechtliche Bedeutung?", Google-Suche „Paraphe vs Unterschrift", „Unterschreiben Sie noch, oder paraphieren Sie schon?", „Paraphe oder Unterschrift?".

[5] Der Begriff „Freeware" ist nicht eindeutig definiert. Er kann sich auf „Freie Software" (Quelltext/„Programmcode" ist verfügbar, darf modifiziert und verbreitet werden) beziehen oder auch nicht. Tendentiell vorherrschend bezeichnet er kostenlos verteilte Software, deren Programmtext jedoch unveröffentlicht bleibt.

[6] „Packprogramme" dienen der Erstellung von Archivdateien bzw. Dateiarchiven, kurz „Archiv" genannt. Sie bieten insbesondere die Möglichkeit, mehrere Einzeldateien sowie verschachtelte, das heißt

Im Rahmen von Bildlizenzierungen kann über Prüfsummen Bezug auf Fotos genommen werden.

1.4.5 Telefonisch übermittelter Anhaltspunkt für die Echtheit versandter Dokumente

Dem Empfänger einer Datei oder eines per Briefpost versandten Datenträgers kann zur Kontrolle telefonisch die Hashfunktions-Prüfsumme mitgeteilt werden. Das Fälschen einer Stimme ist zwar seit der Einführung der Software „Adobe Voco“[7] wesentlich einfacher geworden, es bleibt aber immer noch aufwendig. Die personengebundene Signierung wäre jedoch komfortabler und sicherer.

1.4.6 Hashwerte-Veröffentlichung als ersatzweiser Echtheitsnachweis

Manche Staaten erlauben nur eingeschränkt Verschlüsselung und Signierung (personengebundener elektronischer Echtheitsnachweis). Bis zu einem gewissen Grad können kryptographische Prüfsummen als ersatzweiser Notbehelf dienen:

1. Erstellen Sie zunächst separat die Nachricht bzw. das Dokument als Computerdatei (Text- oder PDF-Datei, Bild, Video, u. a.). Fügen Sie die Datei einer E-Mail an und versenden Sie die Nachricht.
2. Veröffentlichen Sie auf einer Netzseite tagebuchähnlich die Hashcodes der versandten Dokumente. Mehrere seriöse kostenlose (werbefinanzierte) Webhoster bieten sich dafür an. Auch ohne (X)HTML-Kenntnisse lassen sich Internetseiten erstellen, z. B. mit freien HTML-Editoren.

Alternativ empfehlen sich kostenlose Blogsysteme, die keinerlei technische Gestaltungskenntnisse voraussetzen, u.a. Blogger.com und WordPress.com, Kommentarfunktionen lassen sich deaktiviert halten.

Achten Sie bei Ihrer Auswahl auf eine SSL-/TLS-gesicherte Netzseitenauslieferung, Ihr Benutzerpaßwort sollte ebenfalls immer verschlüsselt über das Internet transportiert werden.

Erstellen Sie schließlich schematische Einträge, beispielsweise in der Form Prüfsummenverfahren – Dateiprüfsumme. Mehr Information bedarf es nicht. Bei umfangreichen täglichen Einträgen könnten Sie optional noch eine Dateinamensabkürzung hinzufügen. Aus dem E-Mailanhang „Anfrage.pdf“ würde dann „A...e.pdf“ oder einfach nur „A...e“werden.

Unterordner enthaltende Dateiordner zu einer einzigen Datei zusammenzufassen. Dadurch können beispielsweise ganze Weltnetzseiten und umfangreiche persönliche Zusammenstellungen von Dokumenten komfortabel als einzelne Datei einem E-Brief beigefügt werden, oder auf einen Datenträger gespeichert werden. WP-Artikel „Packprogramm“, Packprogrammempfehlung „7zip“, freie Datenkompressionsprogramme.

[7] Hinsichtlich der Authentizität gesprochener Sprache sei nahegelegt, im WP-Artikel „Adobe Voco“ die Abschnitte „Funktionsweise““ und „Kritik“ zu lesen.

1.4.7 Dokumente mit Hashwerten veröffentlichen

Für die Veröffentlichung von Dokumenten im Weltnetz oder im Intranet (Firmennetzwerke u.a.) empfiehlt sich die Angabe von Hashwerten, eventuell auf einer Unterseite, im so genannten Herunterlade- bzw. „Download“-Bereich. Die Nutzung eines gesetzlich anerkannten SSL-/TLS-Zertifikates[8] zur verschlüsselten Übertragung der Netzseiten mit den veröffentlichten Prüfsummen verstärkt die Sicherheit. Durch Abgleichen der Hashwerte können sich Nutzer relativ sicher sein, daß von seriösen Quellen heruntergeladene Dokumente frei von Schadcode (Viren usw.), Manipulationen und Transferschäden sind. Von äußeren Instanzen ausgestellte Zertifikate sind jedoch möglicherweise[9] mit Restrisikenverbunden.

1.4.8 Archivierung von Dateien

Bei der Datei-Archivierung auf CD-ROMs und DVDs empfiehlt sich die Notierung des Datenträger-Hashcodes. Zur Überprüfung gleichen Sie in regelmäßigen Abständen den Istwert mit dem ursprünglich notierten Hashwert ab. Auf diese Weise können frühzeitige Schäden erkannt werden. Das regelmäßige Umkopieren auf neue archivierungsspezialisierte Datenträger, in relativ kurzen Zeitabständen, ist momentan leider noch unumgänglich.

1.4.9 Erhöhte Sicherheit bei der Paßwortspeicherung

In der Informatik und in der Elektrotechnik existieren zahlreiche weitere Anwendungsmöglichkeiten, beispielsweise eine Variante der sicherheitserhöhten Speicherung von Benutzerkontodaten: Paßwörter lassen läßt sich auch ausschließlich in Form ihrer zugehörigen Hashwerte speichern. Gibt der Nutzer sein Klartextpaßwort erneut ein, wird der Hashwert erneut gebildet und mit dem gespeicherten abgeglichen. Im Falle eines Dateneinbruchs oder Datendiebstahls gehen so vorerst keine Klartextpaßwörter verloren.

Gute zeitgemäße Streuwertfunktionen wirken wie Einwegfunktionen. Sie weisen einer Datei einen individuellen Hashwert zu. Der umgekehrte Weg, die Berechnung der Originaldatei aus dem Hashwert, ist jedoch nicht in praktikabler Zeit möglich – gemäß gegenwärtigem öffentlich bekanntem Wissensstand, beim dem die öffentlich verfügbaren Verfahren und Technologien als Maßstab zugrundegelegt werden.

[8] Zertifikate sind Ausweise für das Internet (Netzwerke allgemein), meistens E-Mail- oder Netzseitenzertifikate, sie ermöglichen die verschlüsselte Datenübertragung (https://), wodurch ein Mitlesen für unter dem Gesetz stehende Menschen und Organisationen relativ unmöglich ist (WP-Artikel: „Digitales Zertifikat“)

[9] „EFF zweifelt an Abhörsicherheit von SSL“, heise.de, 25.03.2010.

1.4.10 Gesetzlich anerkannte, revisionssichere E-Mail-Archivierung

In manchen Wirtschaftszweigen werden E-Mails, die zu Geschäftsabschlüssen/-Aufträgen führen, rechtlich als Handelsbriefe betrachtet. Für ihre Archivierung reichen ein einfaches Abspeichern oder Ausdrucken nicht mehr aus, stattdessen muß revisionssicher archiviert werden, auf eine technische Weise, die ein nachträgliches, nicht feststellbares unbemerktes Manipulieren der E-Mail-Daten ausschließt.

Die technische Umsetzung erfolgt vermutlich bei den meisten Programmen mit Hilfe von kryptographischen Prüfsummen. Dabei werden von allen ein- und ausgehenden E-Mails elektronische Fingerabdrücke erstellt und in verschlüsselter Form gespeichert. Möchte z. B. ein Wirtschaftsprüfer Einblick in eine bestimmte E-Mail erhalten, so wird die gespeicherte E-Mail-Datei in das entsprechende E-Mail-Archivierungsprogramm geladen, z. B. von einer CD- ROM. Beim Einlesen wird erneut die kryptographische Prüfsumme der E-Mail- Datei gebildet und mit der ursprünglich archivierten zugehörigen Prüfsumme auf Übereinstimmung verglichen.

Nur ganz bestimmte Software- und/oder Hardwarelösungen von bestimmten Herstellern werden im Rahmen der gesetzlichen Anforderungen rechtlich anerkannt.

Im Weltnetz sind zahlreiche hochwertige Einführungsartikel zu diesem Thema erhältlich, verfaßt von spezialisierten Rechtsanwälten und IT-Experten. Eine kleine Auswahl:

- „FAQ der IT-Recht Kanzlei: zu den Themen E-Mail-Archivierung und IT-Richtlinie“
- „Mangelhafte Archivierung elektronischer Post hat Konsequenzen[,] Gesetzliche Vorgaben für die eMail-Archivierung“
- „Rechtssichere E-Mail-Archivierung – Teil 1 Einführung und Rechtsvorschriften“
- WP-Artikel „E-Mail-Archivierung“
- „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“
- Beispiel für eine kommerzielle softwarebasierte Lösung, mit einem „Leitfaden zur rechtssicheren E-Mail-Archivierung“, jeweils für Deutschland, Österreich und die Schweiz erhältlich, „Mailstore Server“: „Vorteile der E-Mail-Archivierung“

1.5 Kryptographische Signatur, Netzseiten- und E-Mail-Zertifikate

1.5.1 Kryptographische Signatur und E-Mail-Zertifikate

In der Vergangenheit versahen Menschen bzw. Ämter ihre Dokumente mit einem zusätzlichen Echtheitsnachweis, indem sie mit Siegellack bzw. Siegel-

wachs und Siegelstempeln komplexe Muster, Siegel, auf die Dokumente auftrugen. Heute übernehmen kryptographische Schlüssel bzw. Zertifikate die Funktion des Siegelstempels: Für ein Dokument, z. B. eine E-Mail-Datei, wird mit Hilfe eines Zertifikates (eines Ausweises) ein begleitender, personengebundener Echtheitsnachweis berechnet, die so genannte kryptographische Signatur. Nach Eingang der Nachricht stellt das E-Mail-Programm des Empfängers (u. a. mit Hilfe dieser Signatur) vollautomatisch fest, ob das Dokument wirklich vom angegebenen Versender (Zertifikatsinhaber/Ausweisinhaber) erstellt wurde.

E-Mail- und Netzseitenzertifikate haben also eine Ausweisfunktion, mit der Korrespondenzpartner und Internetseiten ihre Identität nachweisen können.

Klassische Ausweise werden von staatlichen Behörden ausgestellt. E-Mail- und Netzseitenzertifikate werden von so genannten Zertifizierungsstellen ausgestellt (Certification Authorities, CAs). Und hier liegen die zwei entscheidenden Unterschiede: Klassische Ausweise sind untereinander alle gleichwertig und amtlich anerkannt, es gibt nur einen einzigen Aussteller, der zugleich als Beglaubigungsinstitution fungiert: den Staat.

E-Mail und Netzseitenzertifikate hingegen existieren in unterschiedlichen Güteklassen, mit unterschiedlicher Aussagekraft. Nur Zertifikate höchster Güteklasse (Class-3-E-Mail-Zertifikate bzw. EV-Netzseitenzertifikate), ausgestellt von staatlich anerkannten Zertifizierungsstellen, werden rechtlich anerkannt.

Der Verschlüsselungsstandard OpenPGP funktioniert sowohl mit als auch ohne Zertifizierungsinstanzen, d.h., daß Sie auch ohne CAs selbsterstellte Schlüsselzertifikate für Signierung und Verschlüsselung verwenden können:

1.5.2 Signierung und Verschlüsselung von Dateien und E-Mails mit OpenPGP

Der Verschlüsselungs-Standard OpenPGP ermöglicht die signierte E-Mail-Kommunikation sowohl mit als auch ohne Zertifizierungsstellen (CAs). Für die signierte (und für die verschlüsselte) Kommunikation fertigen Sie sich einen (geheimen) Schlüssel (Zertifikat) an, dessen zugehörigen öffentlichen Zertifikatsteil Sie Ihren Kommunikationspartnern per E-Mail zusenden, oder im Internet publizieren oder den Sie vor Ort auf einem Datenträger überreichen. Ihr privater, geheimer Schlüssel läßt sich auch auf Papier archivieren.[10]

Beim Signieren von Dokumenten oder E-Mails geben Sie dann Ihre Paßphrase ein, woraufhin eine (Begleit)Signatur zu Ihrer E-Mail bzw. zu Ihrer Datei erstellt wird; die Paßphrase kann optional zwischengespeichert werden. Das E-Mail-Programm Ihres Korrespondenzpartners verifiziert anschließend vollautomatisch im Hintergrund (mit Hilfe Ihres öffentlichen Zertifikatsteils),

[10] Lesen Sie hierzu: „Paperkey – an OpenPGP key archiver“, „Backup your PGP key with pencil and paper“, „Paperkey“ und „How to backup gpg keys on paper“.

ob die beigefügte Signatur mit Ihrem geheimen Schlüssel(zertifikat) erstellt wurde.

Möchten Sie ein Dokument verschlüsselt versenden, so benötigen Sie dazu das öffentliche OpenPGP-Zertifikatsteil des Datei- bzw. E-Mail-Empfängers, auch, um dessen beigefügte E-Mail-Signaturen auf Echtheit zu überprüfen.

Installation: Ein Verschlüsselungsprogramm und die Befehlszeile würden an sich völlig ausreichen, die meisten Nutzer bevorzugen jedoch grafische Schnittstellen. So benötigen Sie zwei oder drei Programme:

1. Verschlüsselungssoftware
GnuPG, Gnu Privacy Guard (WP-Artikel) ist ein freies, plattformübergreifend erhältliches, zu 100 % kostenlos Verschlüsselungsprogramm für Unix/BSD, GNU/Linux, MS-Windows und MacOS. Die MS-Windows-Version heißt Gpg4win (*keine* Spende erforderlich für Download). Die GPG4win-Suite enthält bereits die grafische Schnittstelle, den Krypto-Manager Kleopatra sowie die Programmerweiterung GpgEX für den Microsoft Dateimanager Windows Explorer, für die Dateiverschlüsselung- und Signierung per Rechtsmausklick.

2. Grafische Schnittstelle
Desweiteren brauchen Sie eine der zahlreichen freien grafischen Schnittstellen (Frontends), beispielsweise das bereits erwähnte Kleopatra für MS-Windows und Unix/BSD bzw. GNU/Linux, um per grafischem Menü Schlüssel(zertifikate) zu erstellen und um Dateien zu signieren bzw zu verschlüsseln.

3. E-Mail-Programm bzw. -Erweiterung
Für den Vollautomatikbetrieb mit E-Mail-Programmen nutzen Sie die standardmäßig eingebaute Funktion oder Sie verwenden eine der zahlreichen freien und kostenlosen (Erweiterungs)Schnittstellen, beispielsweise das bereits in der GPG4win-Suite enthaltene GpgOL für MS-Outlook.

1.5.3 Schlüsselerzeugung, E-Mail-Verwendung, Dateien signieren und verschlüsseln

Erzeugen Sie nun Ihren geheimen Schlüssel, zum Ausprobieren können Sie beliebig viele Testschlüssel erzeugen.

Schlüssel generieren
Denken Sie sich eine Paßphrase aus und erstellen Sie anschließend Ihren Schlüssel mit Kleopatra: „Datei“ → „Neues Schlüsselpaar“ → „Persönliches OpenPGP-Schlüsselpaar erstellen“. Fertigen Sie im Anschluß eine Sicherheitskopie an, auf USB-Stick und/oder CD-ROM/DVD. Nutzen Sie hierzu die Export-Funktion von Kleopatra (zuvor den Schüssel per Mausklick auswählen): „Datei“ → „Sicherungskopie geheimer Schlüssel erstellen“. Für den Export des geheimen Schlüssels werden Sie dazu aufgefordert, Ihre geheime Paßphrase einzugeben. Sie können den Schlüssel in einem Dateibetrachter

oder in einem Texteditor öffnen bzw. hineinziehen, zu Beginn bzw. am Ende der Datei steht jeweils „-----BEGIN PGP PRIVATE KEY BLOCK-----“ bzw. „-----END PGP PRIVATE KEY BLOCK-----“. Zwischengespeicherte Schlüsselkopien könnten ausgelesen werden.

Öffentlichen Schlüssel exportieren

Ihren öffentlichen Schlüsselteil exportieren Sie über „Datei“ → „Exportieren“. Prüfen Sie unmittelbar, daß es sich um den öffentlichen (public) Schlüsselteil handelt, speichern Sie diesen beispielsweise auf dem Desktop und ziehen Sie die Datei anschließend in einen Texteditor oder in einen Browser, zum Beispiel in Mozilla Firefox. Am Ende bzw. am Beginn steht „-----BEGIN PGP PUBLIC KEY BLOCK-----“ bzw. „-----END PGP PUBLIC KEY BLOCK-----“.

E-Mail-Nutzung

Manche E-Mail-Programme unterstützen standardmäßig Signierung und Verschlüsselung mit OpenPGP, bei anderen muß zuvor eine Erweiterung installiert werden. Suchen Sie nach einer entsprechenden Anleitung.

Nach der Aktivierung können Sie Ihre E-Mails standardmäßig signieren. Um die Signaturen eingehender E-Mails überprüfen zu können (oder um für Dritte zu verschlüsseln), müssen Sie den öffentlichen Schlüsselteil Ihres jeweiligen Korrespondenzpartners einmalig in Ihr Programm geladen haben. Manche Programme verfügen über eine eigene OpenPGP-Implementierung. Bei GnuPG-Nutzung wählen Sie im Kleopatra-Menü „Datei“ → „Importieren“, um den öffentlichen Schlüsselteil zu importieren.

Jeder Schlüssel weist einen Fingerabdruck auf, den man auch mündlich am Telefon übermitteln kann. Für seine Anzeige wähle man unter Kleopatra den Schlüssel aus, öffne per Rechtsklick das Menü und wähle „Details“. Schlüssel können auch von Dritten beglaubigt werden. Lesen Sie: „The Kleopatra Handbook“.

Machen Sie sich vertraut mit den Funktionen, schreiben Sie zuallererst eine an sich selbst adressierte, signierte Test-E-Mail. Lesen Sie weiterführende Anleitungen u.a. den Heise-Artikel „Einfach erklärt: E-Mail-Verschlüsselung mit PGP“ und den WP-Artikel „OpenPGP“.

Dateien signieren und verschlüsseln

Sie können zu Ihren Dateien Signaturen erstellen, oder diese mit Ihrem eigenen Schlüssel (oder mit öffentlichen Schlüsseln Dritter) verschlüsseln. Probieren Sie es mit einem beliebigen Dokument aus, beispielsweise mit einer Textdatei. Unter MS-Windows: Gehen Sie auf das Dokument und drücken Sie die rechte Maustaste, es öffnet sich das Ausklappmenü, wählen Sie dort die GpgEX-Optionen (Symbol mit geöffnetem Schloß) und wählen Sie die „Signieren”-Funktion, woraufhin nach Eingabe Ihrer Paßphrase die Signatur erstellt wird. Gehen Sie im Anschluß auf diese erstellte Begleitsignatur-Datei und wählen erneut die entsprechende GpgEX-Option, wodurch Sie eine

Überprüfung automatisiert vornehmen können. Probieren Sie die zahlreichen Funktionen des GpgEX-Optionen-Menüs aus.
Verschlüsselung mit Paßwort: Sie können eine Datei auch nur mit einem Paßwort verschlüsseln, so daß anschließend nur diejenigen die Datei öffnen können, die um das Paßwort wissen.

Dateien lassen sich auch einfach in das geöffnete Kleopatra-Fenster hineinziehen, woraufhin ein Aktionsmenü erscheint, oder Sie wählen im Kleopatra-Datei-Menü eine entsprechende Aktion aus, wodurch sich der Dateimanager öffnet.

Wenn Sie eine Datei für einen bestimmten Empfänger verschlüsseln möchten, so müssen Sie dessen öffentlichen Schlüssel auswählen. Erstellen Sie sich einen Testordner und probieren Sie alle Funktionen aus.

Weiterführende Informationsquellen: Das Raven Wiki, eine ausgezeichnete praktisch-orientierte Netzseite zum Thema angewandte Kryptographie und Privatsphäre (Übersichtsseite), bietet eine äußerst ausführliche „GnuPG Anleitung“.

1.5.4 Netzseitenzertifikate-Branche in der Kritik

Der Abruf von Internetseiten kann in verschlüsselter Form erfolgen (https), so daß *unter dem Gesetz stehende* Dritte die Inhalte der aufgerufenen Netzseiten sowie eine eventuell erfolgte Korrespondenz (Paßwortübergabe, Datenübergabe usw.) nicht mitlesen können. Über dem Gesetz stehende Institutionen (Nachrichtendienste auf höchster Ebene) können vermutlich alles mitlesen, dies notfalls mittels reiner Rechenkraft verwirklicht, mit für die Öffentlichkeit gesperrter Computertechnologie. Sieht man von der Möglichkeit direkter oder indirekter Hintertüren in Computersystemen sowie von möglichen inhärenten mathematischen Schwächen der Algorithmen ab, läuft gegenwärtig letztlich alles auf eine Primfaktorzerlegung hinaus, was wiederum ein reines Rechenkraftproblem darstellt. Lesen Sie im Artikel „Elliptische Kurven Verschlüsselung“ den leichtverständlichen Abschnitt „Was kommt danach? Kurz: Wir brauchen mehr Post Quantum Crypto.”, um sich mit dem Begriff „Post-Quantum-Kryptographie” vertraut zu machen; Auszug: „[...] Um es noch einmal zu betonen: Quanten-Computer bedeuten das Ende aller derzeit etablierten Public-Key-Verfahren unter anderem für digitale Signaturen und Schlüsselaustausch. Damit bricht ein beträchtlicher Teil des Fundaments aktueller Krypto-Systeme komplett weg. Adäquater Ersatz ist bislang nicht in Sicht.[...]”; lesen Sie auch den WP-Artikel „Post-Quanten-Kryptographie”, um einen Überblick kritischer Faktoren und Aspekte zu bekommen.

Die verschlüsselte Übertragung von Internetseiten erfolgt mit Hilfe von (Netzseiten)Zertifikaten. Die internationale Netzseiten-Zertifikateaussteller-Branche in ihrer Gesamtheit sieht sich seit Jahren schwerer Kritik ausgesetzt. Zum einen, weil es immer wieder vorkommt, daß einzelne CAs (Certification Authorities) an Unberechtigte Zertifikate vergeben, aufgrund mangelhafter

Überprüfungsverfahren bei der Antragsstellung. Zum anderen aufgrund von erfolgten Hackereinbrüchen durch die es Dritten zeitweise unbemerkt gelang, sich formal anerkannte Zertifikate auszustellen, für verschiedene populäre Internetseiten bzw. für Firmen. Die Kritik läßt sich dahingehend zusammenfassen, daß die gegenwärtige technische Grundlage des Zertifikatesystems zu verletzlich ist für solche Fehler und Angriffe und daß mit ihr nicht effektiv und schnell genug Gegenmaßnahmen ergriffen werden können. Suchbegriffe wie *SSL-GAU*, *SSL-Desaster*, oder englisch *SSL debacle* führen auf Diskussionsbeiträge und auf weiterführende Artikel im Weltnetz. Umfangreiche Informationsquellen: CA/Browser Forum, „The EFF SSL Observatory“.

1.5.5 Die qualifizierte elektronische Signatur in der BRD

Signaturgesetzrelevante Begriffsbestimmungen in der BRD

Das sogenannte„Bundesamt für Sicherheit in der Informationstechnik“ führt die Übersichtsseite „Grundlagen der elektronischen Signatur“. Dort findet man ein gegenwärtig nur in Englisch herunterladbares PDF-Dokument, „Basics of Digital Signature Techniques and Trust Services“, das Bezug nimmt auf das Begriffsbestimmungen enthaltende „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“

Netzseite der Bundesnetzagentur

Die Bundesnetzagentur führt eine „Übersicht aller elektronischen Vertrauensdienste“.

1.5.6 Zentrale Informationsquellen zur angewandten Kryptographie

Kryptographie auf internationaler Geschäftsebene

Bert-Jaap Koops’ „Cryptography Law Survey“ gibt Auskunft über die grundsätzliche Gesetzeslage zur Kryptographie in den einzelnen Staaten bzw. Verwaltungskonstrukten der Welt. Jeder Eintrag ist mit einer umfassenden weiterführenden Quellensammlung versehen (Stand 2014): cryptolaw.org

Einführung in grundlegende Begriffe

Die auf Computer- und IT-Sicherheit spezialisierte Netzeite heise Security bietet einen fünfteiligen Übersichts- bzw. Einführungsartikel zu grundlegenden Begriffen der angewandten Kryptographie:

1. „Kryptographie in der IT – Empfehlungen zu Verschlüsselung und Verfahren“ • 2. „Hashes und MACs“ • 3. „Symmetrische Verschlüsselung“ • 4. „Asymmetrische Verschlüsselung“ • 5. „Elliptische Kurven Verschlüsselung“.

Zur Geschichte der Kryptographie

Wikipedia bietet ausführliche Informationen zur öffentlich bekannten Geschichte der Kryptographie, unter anderem: „Geschichte der Kryptographie“, „History of cryptography“, „Histoire de la cryptologie“.

Verschiedene Quellen
„Einfache, Fortgeschrittene oder Qualifizierte Elektronische Signatur: Definitionen und Unterschiede“

1.6 Weitere Anwendungsmöglichkeiten

Prüfsummen werden auch in der Elektrotechnik schon seit vielen Jahrzehnten eingesetzt, unter anderem zur Gewährleistung einer fehlerfreien Datenübertragung.

1.7 Mißbrauchsmöglichkeiten

1.7.1 Vollautomatische Identifizierung konsumierter Inhalte

Kryptographische Prüfsummen lassen sich auch für fragwürdige Zwecke einsetzen. Der Medienabspieler eines Softwareherstellers soll in der Vergangenheit ungefragt Hashcodes der abgespielten Dateien versandt haben[11].

Theoretisch ließe sich über einen vollautomatischen Abgleich mit Datenbanktabellen feststellen, ob genutzte Inhalte lizenziert wurden und welche politischen Filme und Tondateien sich ein Nutzer bevorzugt anschaut. Individuelle Rechner könnten durch eine Merkmalkombination identifiziert werden, und Prüfsummen natürlich auch auf Betriebssystemebene versandt werden. Dasselbe wäre auch bei proprietären PDF-Programmen möglich.

Alternativ sind freie PDF-Betrachter und freie Medienabspieler, beispielsweise der sehr empfehlenswerte VLC-Mediaplayer erhältlich. Eine umfassende, größtmögliche Sicherheit setzt jedoch immer auch eine freie Betriebssystembasis voraus.

In der IT-Forensik und in unzähligen weiteren informationstechnischen Bereichen ist die Bildung bzw. Abfrage kryptographischer Prüfsummen allgegenwärtig. Eine durchaus konstruktive Anwendung, insbesondere auch unter dem Aspekt der Beweissicherung bei Computerdelikten, wie z. B. nach Netzwerkeinbrüchen.

In Diktaturen bzw. in besetzten, fremdbestimmten Ländern besteht die Gefahr, daß vor Ort oder aus der Ferne Festplattendurchsuchungen vorgenommen werden. Durch Hintertüren von Software- und Hardware-Herstellern können routinemäßig kryptographische Prüfsummen aller vorhandenen Festplattendateien erstellt werden und anschließend vollautomatisch mit den Prüfsummen „indizierter“ und zensierter Inhalte, wie z. B. politischer Aufklärungsfilme, abgeglichen werden. Auf diese Weise kann schnell und effektiv überprüft werden, ob Bürger dazu tendieren, eine eigene Meinung zu pflegen, und ob sie politische Inhalte konsumieren, die im Widerspruch zu offiziell verkündeten Dogmen stehen. Freidenker lassen sich so leicht ausfindig machen.

[11] „Windows Media Player: Ich weiß, was du letzten Sommer geschaut hast“, heise.de, 21.02.2002 und „Serious privacy problems in Windows Media Player for Windows XP“, 20. Februar 2002.

Bei einem automatisierten regelmäßigem Versand sämtlicher Prüfsummen der vom Nutzer neuerstellten sowie geänderten Dateien könnte auch im nachhinein festgestellt werden, in welchem Netzwerk bzw. auf welchem Rechner ein Dokument erstmalig erstellt wurde. Die Datenmenge ist winzig und, wenn sie zusätzlich verschlüsselt wird, praktisch unentzifferbar. Das Ändern des Dateinamens ändert nicht die Prüfsumme. Auch andere Merkmale, wie z. B. Hardware- und Softwarekonfigurationen (einschließlich nichtlizenzierter Programme), lassen sich analysieren und vollautomatisch „melden“.

Rechtsanwalt Udo Vetter erwähnt in einem an der Universität Bielefeld gehaltenen Vortrag vom 23.06.2010 eine von der Polizei verwendete Software für die Festplattendurchsuchung, bei der auch schon ein Fehlalarm ausgelöst worden sein soll.[12]

Es kann nicht ausgeschlossen werden, daß Rechner von Regimekritikern aus der Ferne gezielt lahmgelegt werden. Beispielsweise reicht bereits die Ferninstallation eines einzigen permanent ab Rechnerstart arbeitenden Prozesses, der die gesamte Rechenkraft verbraucht, ein Prozeß, der sich möglicherweise über ps -e noch erkennen, jedoch nicht mehr terminieren läßt (siehe auch pstree). Die Installation von funktionalen Programmfehlern stellt eine weitere Möglichkeit dar, um die Rechner von Andersdenkenden teilweise oder vollständig lahmzulegen.

Sabotagemaßnahmen könnten auch automatisiert erfolgen, wenn Statistikauswertungen im Hintergrund ergeben, daß ein hohes Maß an politischen Aufklärungsfilmen konsumiert wird und die „Gefahr“ der Verteilung oder des Publizierens kritisch-hinterfragender Artikel besteht.

1.7.2 Softwareaktivierung und Rechneridentifikation über elektronische Fingerabdrücke

Die Free Software Foundation (FSF führt in einem Artikel zur Privatsphäre Computermerkmale auf, über die sich ein Rechner eindeutig identifizieren und wiedererkennen läßt. Solche Kenndaten werden höchstwahrscheinlich in einem Hash zusammengefaßt und in einer Datenbank archiviert. Bei manchen proprietären Produkten ist die Softwareaktivierung (Produktaktivierung) an die ermittelte Hardwarekonfiguration gekoppelt. Der Versuch, die gekaufte Software gleichzeitig auf einem zweiten Rechner zu installieren scheitert dann oftmals.

[12] „Netzwoche Bielefeld - Udo Vetter - Das überwachte Netz“, Einstiegspunkt in der 18. Minute, Direktverweis. Der gesamte Vortrag ist äußerst aufschlußreich hinsichtlich der „Qualität“ der BRD-“rechtsstaatlichen“ Ermittlungen im Internet- und im IT-Bereich. Netzpräsenz von Udo Vetter: lawblog.de. Das Portal Wikimannia.org pflegt im Personen-Portal einen Kurzportraitartikel zu Udo Vetter, mit Netzverweisen.

1.8 Signierung und Verschlüsselung von Dateien

1.8.1 Realexistierender Schutz mit öffentlich zugelassenen Verschlüsselungsverfahren

Es kann nicht ausgeschlossen werden, daß offiziell empfohlene, zu Standards erhobene Kryptographie-Algorithmen inhärente mathematische Schwächen aufweisen, um Nachrichtendiensten die Entschlüsselung zu erleichtern. Vermutlich wird wirklich fortgeschrittene Computertechnologie der Öffentlichkeit vorenthalten bzw. allgemein gesperrt gehalten, um Geheimdiensten einen Berechnungskraftvorsprung zu garantieren. Unter diesem Aspekt und angesichts der höchstwahrscheinlich vorhandenen Einflußnahme auf die Firmenproduktgestaltung (Software- und Hardware-Hintertürenproblematik) ist die Effektivität der realexistierenden Verschlüsselungspraxis fragwürdig, auch dann, wenn durchgängig offene, freie IT-Infrastruktur zum Einsatz kommt.

Konsequent angewandte Signierung und Verschlüsselung wehren jedoch zumindest einen Teil des infragekommenden Personenkreises möglicher Geschäftsangreifer ab und verhindern einen direkten Datenzugriff bei Diebstahl und Verlust von Datenträgern.

Die Komplexitätsreduzierung auf Programm- und Betriebssystemebene ist ein weiterer zentraler Faktor. Darüberhinaus können alte und sehr alte Rechner, auf denen noch veraltete proprietäre Betriebssysteme und Programme installiert sind, mit laufend aktualisierten spezialisierten leichtgewichtigen freien Betriebssystem-Distributionen modernisiert und sicherheitsoptimiert werden.[13]

2 Freie Prüfsummenprogramme

Aus der großen Menge freier grafischer Prüfsummenprogramme heben sich CyoHash und Jacksum hervor. Jacksum, veröffentlicht unter einer OSI-zertifizierten Freie-Software-Lizenz, der GPL, gelistet im FSF-Verzeichnis und basierend auf Java, läuft auf vielen Betriebssystemplattformen (Programmeigenschaften). Es eignet sich damit auch für heterogene IT-Infrastrukturen von Firmennetzwerken. Zahlreiche international gängige Prüfsummenverfahren werden berücksichtigt, die Dateimanagerintegration gewährleistet eine komfortable Bedienung.

Jacksum-Dateimanagerversionen sind erhältlich für GNOME, KDE, ROX und Thunar (Unix/BSD, GNU/Linux) sowie für den Windows-Explorer von MS-Windows und den Finder von Apple Macintosh. Vom Programmautor Johann Löfflmann wird eine Netzseite mit ausführlichen Informationen gepflegt, Jacksum.net. Vorschläge zur Programmerweiterung können eingereicht werden, der Austausch unter den Nutzern wird ebenfalls gefördert.

[13] „Einführung in Freie Software und Betriebssysteme“, Artikelabschnitt „Moderne Betriebssysteme für alte Computer“

CyoHash, eine Erweiterung für den MS-Windows Dateimanager Explorer, bietet nur einen Bruchteil der Algorithmen, unterstützt jedoch ebenfalls die zeitgemäßen SHA2-Algorithmen und funktioniert auch ohne Java.

Einige gängige unter den vielen plattformübergreifenden Textmodus-Programmen für BSD/Unix und GNU/Linux sind beispielsweise sha224sum, sha256sum, sha384sum, sha512sum, shasum, sha3sum. sha1sum wird nicht mehr empfohlen, der WP-Artikel „sha1sum“ listet Alternativen auf.

Eine vergleichende Übersicht zu zahlreichen freien und proprietären Prüfsummenprogrammen fand man im WP-Artikel „Comparison of file verification software“ (Stand: 2020, archivierte Version). Grundlegende Begriffe und zentrale Verweise zu freier Software werden im Artikel „Einführung in Freie Software und Betriebssysteme“ erörtert.

2.1 Cyohash

Cyohash ist eine freie Dateimanagererweiterung für den MS-Windows-Explorer, herunterladbar über die offizielle Projektseite oder über ein renommiertes Programmeverzeichnis.

2.1.1 Prüfsummenbildung

Zeigen Sie mit dem Mauspfeil auf die entsprechende Datei und klicken auf die rechte Maustaste. Im erscheinenden Menü drücken Sie auf „Cyohash“ und wählen einen Prüfsummen-Algorithmus, z.B. SHA-256.

Es erscheint ein Fenster, das den Dateinamen mitsamt dem Verzeichnispfad sowie dem Prüfsummenverfahren und der kryptographischen Prüfsumme anzeigt, bzw. es erscheint eine Tabelle, in der diese Daten aufgeführt sind. Für jede gebildete Prüfsumme erscheint ein eigener Eintrag.

Sie können nun die ermittelte Prüfsumme mit einem Sollwert abzugleichen. Hierzu klicken Sie doppelt auf den jeweiligen Tabelleneintrag, um das zugehörige Fenster zu öffnen.

Ein Anwendungsbeispiel: Im Weltnetz angebotene Programmdateien werden fast immer zusammen mit ihren Prüfsummen veröffentlicht. Nach dem Herunterladen solch einer ausführbaren Datei, vorzugsweise von der offiziellen Programmprojektseite,kopieren Sie die dort veröffentlichte zugehörige kryptographische Prüfsumme, fügen diese anschließend in die unten im Programmfenster erscheinende Eingabezeile („Validate:“) ein und drücken auf „OK“. Stimmen die Werte überein, färbt sich die Eingabezeile grün, andernfalls rot.

2.1.2 Prüfsummen zu mehreren Dateien bilden

Zeigen Sie entweder auf einen Tabelleneintrag oder auf eine leere Tabellenzeile und betätigen Sie die rechte Maustaste, um sich weitere Funktionen anzeigen zu lassen.

Sie können die Prüfsummen zu mehreren Dateien gleichzeitig bilden. Wählen Sie die Funktion „Hash File(s)...“. Es öffnet sich ein Fenster, in dem Sie das gewünschte Prüfsummenverfahren wählen. Anschließend drücken Sie auf „Browse...”, woraufhin sich ein Windows-Verzeichnisfenster öffnet. Wählen Sie im entsprechenden Verzeichnis die Dateien aus, halten Sie die STRG-Taste gedrückt und drücken die Maustaste, um die einzelnen Dateien zu markieren. Zum Schluß klicken Sie auf „Öffnen“. Das Windows-Verzeichnis-Fenster verschwindet daraufhin, im Vordergrund erscheint das CyoHash-Fenster, in dem Sie mit „OK“ Ihre Datei-Auswahl bestätigen. Im Tabellenfenster werden anschließend sämtliche Prüfsummen angezeigt.

2.2 Jacksum

2.2.1 Installation von Java und Jacksum

Installation von Java

In Unix- und unixartigenBetriebssystem-Distributionen ist Java meistens schon enthalten, in der freien Variante OpenJDK. Als MS-Windows-Benutzer rufen Sie eine Suchmaschinenseite auf, zum Beispiel Google, und tippen „Java“ oder „JRE“ ein, das ist die Kurzbezeichnung für „Java Runtime Environment“ (Java-Laufzeitumgebung). Dieser Schritt entfällt, wenn bereits eine Java-Laufzeitumgebung vorhanden ist.

Beispiel für eine Java-Installation unter MS-Windows:

1. Rufen Sie eine Suchmaschine auf, beispielsweise google.de und geben „Java“ ein
2. An erster Stelle erscheinen die Einträge des offiziellen Java-Herstellers Oracle (Java.com), für verschiedene Betriebssystemplattformen. Gehen Sie auf eine dieser Netzseiten und folgen Sie den dortigen Anweisungen bzw. alternativ:
3. Ttippen Sie als Suchbegriff „Java Runtime Environment“ ein, um zur offiziellen Herunterladeseite zu gelangen

Sollte vom Java-Hersteller eine Vorauswahl für die (Mit)Installation einer Yahoo-Toolbar angeboten werden, so deaktivieren Sie das Häkchen durch draufklicken, so daß das Ankreuzfeld leer bleibt Google-Suche für diese Thematik: Java Installation Yahoo Toolbar. Solche Toolbars können jederzeit auch nachträglich entfernt werden. Google-Artikelsuche: Toolbars deinstallieren.

Installation und Anwendung von Jacksum unter MS-Windows

Eine ausführliche Anleitung finden Sie in der Installationsrubrik der offiziellen Programmseite sowie in den dem Jacksum-Download beigefügten liesmich- bzw. readme.txt-Dateien.

Wählen Sie auf der offiziellen Netzpräsenz, jacksum.net, die Rubrik „Download“. Dort laden Sie sich, im Abschnitt „Integration in den Dateibrowser

(optional)", die „[...]-windows-explorer-integration-[...]"-Datei (Dateiname variiert mit der Programmversionsnummer [Version (Software)]) herunter, eine ZIP-Datei. Öffnen Sie diese, direkt per Doppelklick oder über Rechtsmausklick und öffnen Sie den entkomprimierten Ordner, lesen Sie die Datei liesmich.txt bzw. starten Sie die Installation durch Doppelklicken auf die ausführbare Datei „Jacksum Windows Explorer Integration.exe". Ein Fenster erscheint mit der Aufforderung, alle Dateien zu extrahieren

Gehen Sie nun in den vollständig extrahierten Ordner, dort sehen Sie die exe-Installationsdatei, symbolisiert durch einen grünen Kreis

Durch Doppelklicken starten Sie die Programminstallation. Von da an können Sie über Rechtsklick → „Senden an" → [Verfahren, z.B.: „Jacksum - 3) Alle Algorithmen"] kryptographische Prüfsummen bilden. Die Prüfsumme(n) erscheinen in einem separaten Textfenster.

2.2.2 GNOME Nautilus

Öffnen Sie den Dateimanager. Klicken Sie zum Wählen der Datei auf die rechte Maustaste → „Aktion" → „Jacksum" → [gewünschte Funktion wählen].

Die Anwendungsmöglichkeiten von Jacksum sind zahlreich. Über die Kommandozeilenversion entfaltet sich das ganze Potential dieser vorzüglichen Software, einschließlich der Interaktion mit anderen Programmen. Die Bereitstellung einer offenen Programmschnittstelle (API) fördert die breite Akzeptanz.

2.3 Konsolenbasierte Prüfsummenbildung

Im Textmodus (Konsolenanwendung) lassen sich kryptographische Prüfsummen unter jedem Betriebssystem bilden, praktisch alle Hersteller von proprietären (proprietäre Software) und von freien Betriebssystemen bieten standardmäßig entsprechende Programme an.

Seit der Einführung von Microsoft's Windows PowerShell können MS-Windows-Nutzer neben den klassischen MS-DOS-Befehlen standardmäßig auch grundlegende Dateioperationsbefehle der BSD/Unix-Welt nutzen (Gegenüberstellung). Die GNU Core Utilities ermöglichen es darüberhinaus, auch weitere Unix-Standardprogramme unter MS-Windows zu nutzen (List of Unix commands).

2.3.1 Bordeigene Algorithmen unter MS-Windows, Unix/BSD- und GNU/Linux-Systemen

SHA-Algorithmen sind standardmäßig auf zahlreichen Unix- und unixartigen Betriebssystemen sowie unter MS-Windows-Systemen vorinstalliert.

Kryptographische Prüfsummen bilden unter MS-Windows: Die PowerShell unterstützt zahlreiche grundlegende Befehle der Unix-Shell; für eine Über-

sicht überfliegen Sie den zugehörigen Vergleichsabschnitt im englischen WP-Artikel zur PowerShell.

Darüberhinaus werden auch aktuelle SHA-Algorithmen unterstützt, über den Befehl "Get-FileHash". Offizielle Informationen finden Sie im gleichnamigen Artikel von Microsoft; standardmäßig voreingestellt ist SHA-256.

1. *Programm starten*: Gehen Sie in das Suchfeld der Windows-Taskleiste und geben ein: PowerShell. Es öffnet sich die Befehlszeilenumgebung. Für die Schriftgrößenanpassung klicken Sie mit der rechten Maustaste auf den oberen Fensterrahmen und wählen den Menüpunkt „Eigenschaften“ aus. Im Reiter „Schriftart“ legen Sie nun unter „Schriftgrad“ die Schriftgröße fest, drücken Sie anschließend auf „OK“.

2. *In das entsprechende Verzeichnis wechseln*: Wechseln Sie nun in das Dateiverzeichnis in dem sich die Datei befindet, zu der die Prüfsumme gebildet werden soll. Die Sprachdarstellung ist nur teilweise in English gehalten. Im verwendeten Beispiel-Prompt (Abbildung 3) „`PS C:\Users\nutzer-01>`“, steht „Users“ für den Windows-Benutzer-Ordner, „nutzer-01“ ist in diesem Beispiel der Name des Kontos des angemeldeten Nutzers. Geben Sie ls ein, um sich eine Ordnerübersicht anzeigen zu lassen: „`PS C:\Users\nutzer-01> ls`“. Es folgt eine Verzeichnisauflistung, in der auch die zentralen Ordner „Desktop“, „Documents“ (Dokumente) sowie „Downloads“ enthalten sind; Sie können die Inhalte per Mausrad oder per Schieberegler nach oben und unten schieben. Hier im Beispiel wird nun in den Desktop-Ordner gewechselt, dessen Dateien standardmäßig auch auf dem Desktop-Bildschirm angezeigt werden; hierzu verwenden Sie den cd-Befehl (change directory): „`PS C:\Users\nutzer-01 > cd Desktop`“, jetzt befinden Sie sich im Desktop-Ordner: „`PS C:\Users \nutzer-01\Desktop>`“; durch erneute Eingabe von ls kann man sich dessen Inhalt anzeigen lassen.

3. Prüfsumme einer Datei bilden. In diesem Beispiel befindet sich auf dem Desktop die Bilddatei foto-01.jpeg, zu der eine Prüfsumme erstellt werden soll. Wie die Unix-Shell verfügt auch die PowerShell über eine Autovervollständigungsfunktion (WP-Artikel Befehlszeilenergänzung).

Es reicht, wenn Sie in Kleinschreibung „`get-f`“ in die Befehlszeile schreiben („`PS C:\Users\nutzer-01\Desktop> get-f`“) und anschließend für die Autovervollständigung auf die Tab-Taste drücken, woraufhin der Befehl in voller Länge und in korrekter Groß- und Kleinschreibung erscheint:
„`PS C:\Users\nutzer-01\Desktop> Get-FileHash`“. Anschließend fügen Sie noch den Dateinamen hinzu (auch dafür kann die Autovervollständigung benutzt werden): „`PS C:\Users\nutzer-01\Desktop> Get-FileHash foto-01 .jpeg`“ und erhalten die SHA-256-Prüfsumme (siehe Bildschirmfoto).

Unter unixartigen Systemen: Öffnen Sie eine Befehlszeilenumgebung (Shell), schreiben Sie „sha“ und drücken Sie dann die Tabulatortaste für die Be-

```
PS C:\Users\nutzer-01\Desktop> Get-FileHash foto-01.jpeg

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          382F8051EC6E42F019771BB36118E064DB49B9AA2963C0F37E6FF61C4BB93C5C       C:\Users\nutzer-01\De...


PS C:\Users\nutzer-01\Desktop>
```

Abbildung 3: Prüfsummenbildung mit der PowerShell

fehlszeilenergänzung, um sich alle vorhandenen SHA-Verfahren anzeigen zu lassen:

```
> sha
> sha1sum sha224sum sha256sum sha384sum sha512sum shasum
> sha
```

Gehen Sie in das entsprechende Verzeichnis, wählen Sie ein Verfahren, fügen Sie den Namen der gewünschten Datei an und drücken Sie die Eingabetaste. Im folgenden Beispiel wird die SHA256-Prüfsumme der Datei test.html gebildet:

```
> sha256sum test.html
> e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991
b7852b855 test.html
```

Der SHA256-Prüfsummenwert und der Name der zugehörigen Datei werden angezeigt. Implementierung und Befehlsbezeichnungen können variieren. Praktisch alle Unix- bzw. unixartigen Systeme und Distributionen verfügen über entsprechende Vorinstallationen. Es gibt dutzendfach freie Programme zur Bildung kryptographischer Prüfsummen, sowohl grafische wie auch textbasierte, u.a. bei sourceforge.net (WP-Artikel).

2.3.2 Textmodusprogramme für die professionelle Computernutzung

Die Nutzung der Befehlszeilenumgebung ermöglicht ein hocheffektives Arbeiten am Computer. Manche Anwendungen werden ausschließlich für den heutzutage meist emulierten Textmodus geschrieben, andere bieten zusätzlich zur grafischen auch eine textbasierte Programmschnittstelle. Textbasierte Programme ermöglichen die effektivste Nutzung von Computern.

Linux-Distributionen enthalten neben den grafischen Desktopumgebungen und Anwendungsprogrammen standardmäßig auch Textmodus-Software. Programme mit zeichenorientierter Benutzerschnittstelle, im Englischen auch „Text-based user interface“ genannt, sind äußerst leistungsfähig und gehören zu den bevorzugten Werkzeugen vieler Anwender, Administratoren, IT-Profis und Wissenschaftler. Netzseiten und empfohlene Artikel zu Textmodus-Programmen: „freie Textmode-Software“ • Webseiten zum Thema Textmode

• WP-Artikel: „Console application“ • „Text-based (computing)“ • „Shell (computing)“ • „Kommandozeile“ • Hervorragende Einführung: Floss Manual „Introduction to the Command Line“ • WP-Artikel: „GNU Screen“ • „Terminal (Computer)“.

3 Impressum

Peter Jockisch
Habsburgerstraße 11
D-79104 Freiburg
E-Post: info@peterjockisch.de
OpenPGP: https://peterjockisch.de/schluessel/key-pub.asc

Dokumentpermanentlink:
DIN A4: peterjockisch.de/Pruefsummen.pdf

Die PDF-Datei enthält sämtliche Verweise der ursprünglichen HTML-Version, verweissensitiver Text ist farbig eingerahmt, sichtbar beim Lesen im Browser oder mit einem separaten PDF-Betrachter; beim Drüberfahren mit dem Mauszeiger wird die Adresse angezeigt, beim Draufklicken öffnet sich die Netzseite im Webbrowser. Der Druck erfolgt ohne Farbrahmen. [14]

Freie Software für die professionelle Dokumentenerstellung, Einführungsartikel:peterjockisch.de/Schriftsatzprogramme/Schriftsatzprogramme.html

[14] Am PC können Sie mit der Tastenkombination ALT + TAB zwischen den Anwendungsfenstern umschalten, lesen Sie hierzu den Wikipedia-Artikel: „Tastenkombinatio“.