FH Wedel

Seminararbeit GnuPG

Informatik Seminar

Beke Ketelhut (wing103414)
09.07.2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CA	Certificate Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
GNU	GNU's not Unix
GnuPG	GNU Privacy Guard
GPL	GNU General Public License
MD5	Message-Digest Algorithm 5
PGP	Pretty good privacy
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Algorithm 1

1 Einleitung

Wer einen Brief verschickt, kann nicht entscheiden, auf welchem Weg dieser Brief zum Empfänger transportiert wird. Bei der elektronischen Kommunikation ist es ähnlich. Der Sender weiß nicht, über welche Server seine Nachricht übertragen wird. Der Unterschied zwischen diesen Kommunikationsmitteln ist die Vertraulichkeit. Während der Brief in einem Umschlag steckt und i.d.R. nur vom Empfänger gelesen wird, können unverschlüsselte E-Mails theoretisch von jedem mitgelesen werden. Mit ausreichendem Fachwissen können diese sogar manipuliert oder missbraucht werden. Unverschlüsselte E-Mails sind daher mit Postkarten zu vergleichen. Über E-Mails werden allerdings zum Teil auch private Informationen wie Bankdaten oder geheime Geschäftsberichte und nicht nur Urlaubsgrüße ausgetauscht. Um zu vermeiden, dass die Daten von anderen Personen, als von dem Empfänger gelesen werden, sollten diese E-Mails verschlüsselt werden.

Die Standard-Sicherheitseinstellungen bei dem E-Mail-Programm Outlook von Microsoft sehen keine Verschlüsselung vor. Es wird sogar davon abgeraten diese Konfigurationen zu ändern. In Artikel 10 Absatz 1 des Deutschen Grundgesetzes heißt es: „Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.“ Um diesem Recht nachzukommen und die Privatsphäre vor planmäßigem Eindringen von unterschiedlichen Organisationen zu schützen, ist die Nutzung von E-Mail-Verschlüsselung essentiell. Das Echelon-System ist ein Beispiel für das systematische Abhören elektronischer Medien, dass im Jahr 2001 für Schlagzeilen gesorgt hat. Es wurde von den USA, Kanada, Großbritannien, Australien und Neuseeland ursprünglich für das Belauschen des Ostblocks aufgebaut. Inzwischen wird es mit 120 Stationen betrieben, um durch Abhören von Satellitenverbindungen und Transatlantikkabeln Informationen über Einzelpersonen aber auch Regierungen zu gewinnen (Wikipedia, 2018). Es wird deutlich, dass sich eine Auseinandersetzung mit diesem Thema lohnt. Im Zuge dieser Seminararbeit wird daher die Verschlüsselungssoftware GnuPG sowie deren Anwendung vorgestellt.

1.1 Aufgabenstellung und Zielsetzung

Im Zuge dieser Seminararbeit soll der GNU Privacy Guard (GnuPG), ein Programm zur Verschlüsselung von Daten vorgestellt werden. Neben der schriftlichen Ausarbeitung fand am 25.06.2018 eine Präsentation in Form einer Kryptoparty statt. Hierbei handelt es sich um ein Treffen, bei dem sich gegenseitig Verschlüsselungstechniken beigebracht werden (Wikipedia, 2017). In diesem Fall wird das Verschlüsseln mit GnuPG erläutert und anschließend interaktiv angewendet.

1.2 Aufbau der Arbeit

Im ersten Teil werden die Entwicklung und Funktionsweise von GnuPG erläutert sowie auf kryptografische Grundlagen eingegangen, die für das weitere Verständnis relevant sind. In Kapitel 3 folgt ein kurzer Exkurs zur digitalen Signatur, bevor in Abschnitt 4 ausführlich die Durchführung der Kryptoparty beschrieben wird. Die Seminararbeit endet mit einem Abstecher zu einem jüngst in den Medien erschienenen Angriff auf Aspekte der GnuPG-Verschlüsselung und einem anschließenden Fazit.

2 Vorstellung von GnuPG

Der GNU Privacy Guard ist eine freie Software zum Verschlüsseln und Signieren von Daten. Der Namensteil „GNU“ hat seinen Ursprung in der GNU General Public License (GPL). Dies ist eine Lizenz, die Software als frei deklariert und im Rahmen des GNU-Projekts veröffentlicht wurde. Nach der GPL ist Software frei, wenn sie jeder nutzen, verbreiten und verändern sowie den Quellcode untersuchen kann (Free Software Foundation, 2007).

2.1 Entwicklung von GnuPG

Der GNU Privacy Guard wurde von Werner Koch entwickelt und unter der GPL veröffentlicht (Wikipedia, 2018). Die erste produktive Version von GnuPG wurde am 7. September 1999 herausgegeben. Zwei Jahre später wurde eine Umsetzung dieser Software für Windows Betriebssysteme im Rahmen der Aktion „Sicherheit im Internet“ durch das Bundesministerium für Wirtschaft und Technologie unterstützt. Die Software wird stetig weiterentwickelt und inzwischen vom Bundesamt für Sicherheit in der Informationstechnik unterstützt (Koch, et al., 2018).

GnuPG wurde als Alternative zu dem bereits bestehenden Verschlüsselungsprogramm PGP (Pretty Good Privacy) entwickelt, das seit 2002 nicht mehr als freie Version verfügbar ist (CHIP Digital GmbH, 2018). Sowohl GnuPG als auch PGP verwenden den gleichen Standard für Verschlüsselung, den OpenPGP Standard. Hierhinter verbirgt sich eine normative Spezifikation für Verschlüsselung im Internet, die z.B. die Verwendung von als sicher eingestufte Algorithmen empfiehlt und stetig mit dem technologischen Fortschritt weiterentwickelt wird.

2.2 Art der Verschlüsselung

GnuPG verwendet eine hybride Verschlüsselungstechnik, d.h. eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung, welche durch den OpenPGP Standard empfohlen wird (Callas, et al., 2007). Zunächst werden die Funktionsweisen und Eigenschaften dieser beiden Verfahren vorgestellt, sodass anschließend die hybride Verschlüsselung erklärt werden kann.

2.2.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird ein Schlüssel in Form eines Algorithmus zur Ver- und Entschlüsselung benötigt. Der Absender chiffriert seine Nachricht mit dem Schlüssel und der Empfänger kann die Nachricht anschließend mit dem gleichen Schlüssel dechiffrieren. Problematisch ist der Schlüsselaustausch, der geheim erfolgen muss, da mit Besitz des Schlüssels die Nachricht dechiffriert werden kann (Free Software Foundation , 2000). Die folgende Abbildung 1 soll die Verschlüsselungstechnik verdeutlichen.

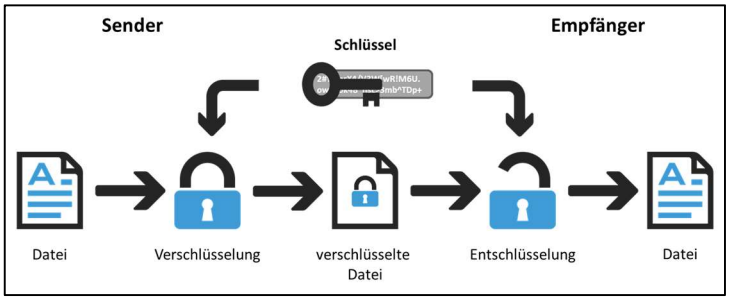

Abbildung 1: Symmetrische Verschlüsselung (Birkle, 2015)

2.2.2 Asymmetrische Verschlüsselung

Aufgrund des Schlüsselaustausch-Problems wurde ein weiteres Verschlüsselungsverfahren entwickelt, bei dem kein geheimer Schlüssel ausgetauscht werden muss. Es wird ein Schlüsselpaar verwendet, das aus einem privaten und einem öffentlichen Schlüssel besteht. Die beiden Schlüssel sind durch einen Algorithmus verbunden, lassen sich aber nicht auseinander herleiten (Koch, et al., 2018).

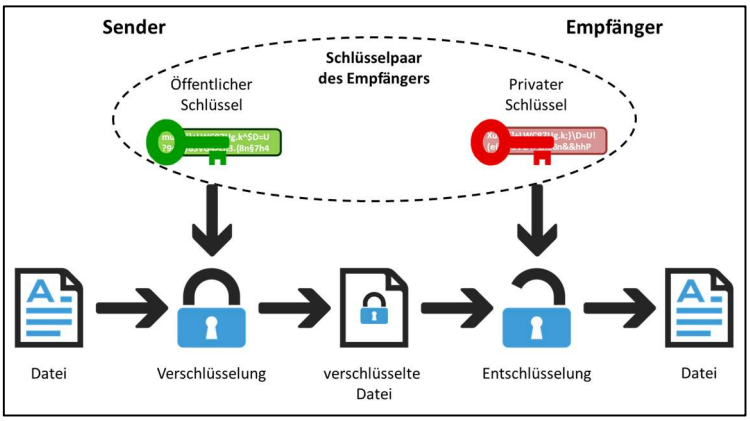

Abbildung 2: Asymmetrische Verschlüsselung (Birkle, 2015)

Wie Abbildung 2 zeigt, wird die Nachricht mit dem öffentlichen Schlüssel des Empfängers chiffriert und mit dem privaten Schlüssel des Empfängers dechiffriert. Entscheidend ist, dass die Nachricht nur mit dem privaten Schlüssel entschlüsselt werden kann. Der Empfänger kann eine Dechiffrierung vornehmen, weil er seinen zum Schlüsselpaar gehörenden privaten

Schlüssel besitzt. Der Absender kann eine Nachricht nur verschlüsseln, aber nicht wieder entschlüsseln. Vor Kommunikationsbeginn muss nur der öffentliche Schlüssel des Empfängers ausgetauscht werden. Dieser ist nicht geheim, da mit dem öffentlichen Schlüssel nur Nachrichten chiffriert werden können. Der Nachteil dieses Verfahrens ist allerdings die längere Rechenzeit aufgrund des komplexeren Algorithmen. (Free Software Foundation , 2000).

2.2.3 Hybride Verschlüsselung

Da die symmetrische Verschlüsselung das Schlüsselaustausch-Problem aufwirft und die asymmetrische Verschlüsselung viel Rechenzeit beansprucht, wird bei GnuPG ein kombiniertes Verfahren verwendet. Dieses ist in Abbildung 3 veranschaulicht. Die Nachricht wird mit einem Sitzungsschlüssel (Session Key) symmetrisch chiffriert. Dieser Session Key wird asymmetrisch mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Da nur der Sitzungsschlüssel asymmetrisch chiffriert wird, reduziert sich der Rechenaufwand gegenüber der reinen asymmetrischen Verschlüsselung. Der Empfänger entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel und dechiffriert mit dem Session Key die Nachricht (Bleich, 2018).

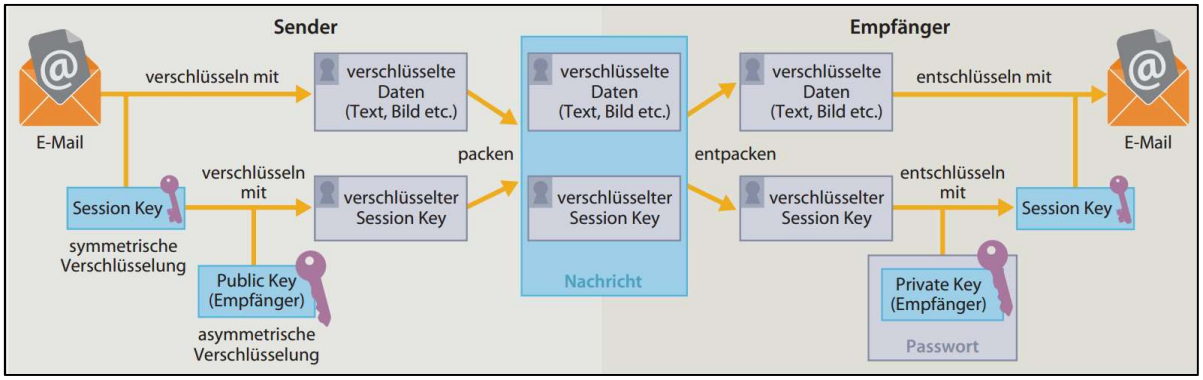

Abbildung 3: Hybride Verschlüsselung (Bleich, 2018)

2.3 Algorithmen und Beglaubigungskonzepte

Die GnuPG-Software bietet eine Vielzahl von Algorithmen, die zur Ver- und Entschlüsselung verwendet werden können, z.B. RSA, ECDSA und DAS. Seit Version 2.0.0 von GnuPG kann auf die Elliptische-Kurven-Kryptografie zurückgegriffen werden. Standardmäßig wird ein RSA-Algorithmus mit einem Schlüssel der Länge 2048 Bit verwendet.

Eine Beglaubigung von Schlüsseln wird angewendet, um sicherzustellen, dass sich hinter einem öffentlichen Schlüssel die Person befindet, mit der kommuniziert werden soll. Zwei verschiedene Beglaubigungskonzepte werden von GnuPG unterstützt. Das eine stützt sich auf den bereits erwähnten OpenPGP Standard und das andere Konzept nennt sich S/MIME (Secure/Multipurpose Internet Mail Extensions). Bei S/MIME handelt es sich um ein

hierarchisches Vertrauenskonzept, bei der Zertifikate von einer höheren Instanz, der sogenannten Certificate Authority (CA), beglaubigt werden (Koch, et al., 2018). Das OpenPGP-Konzept basiert auf dem Web of Trust. In diesem Netzwerk werden durch gegenseitig aufgebautes Vertrauen Beglaubigungen durchgeführt. Die beiden Verfahren sind nicht kompatibel, sondern bieten alternative Möglichkeiten zur Authentisierung der geheimen Kommunikation. GnuPG bietet die Nutzung beider Verfahren an (Koch, et al., 2018).

3 Exkurs: Digitale Signatur

Beim Thema Verschlüsselung wird oft die digitale Signatur ins Gespräch gebracht. Welche Verbindung es zwischen Verschlüsselung und Signatur gibt, soll im Folgenden kurz erläutert werden. Dafür wird auf die vier Eigenschaften von Nachrichten eingegangen, die durch kryptografische Verfahren gewährleistet werden sollen (Ertel, 2012):

- Geheimhaltung
- Integrität
- Authentifizierung
- Verbindlichkeit

Die ersten beiden Eigenschaften können durch Verschlüsselung sichergestellt werden. Eine verschlüsselte Nachricht kann während der Übermittlung weder gelesen noch verändert werden. Somit lassen sich die Forderungen nach Geheimhaltung und Integrität erfüllen. Zur Sicherstellung der anderen beiden Eigenschaften kann die Verschlüsselung nicht beitragen. Bei einer verschlüsselten Nachricht ist nicht bewiesen, von welchem Absender sie geschickt wurde. Hierfür kann sich der digitalen Signatur bedient werden.

Bei der digitalen Signatur handelt es sich um eine Datei, die mit dem privaten Schlüssel des Absenders verschlüsselt und einer E-Mail angefügt wird. Wenn der Empfänger die Datei mit dem öffentlichen Schlüssel des Absenders entschlüsseln kann, ist die Authentifizierung erfolgreich. Wenn das der Fall ist, kann der Absender nicht mehr von seiner Nachricht zurücktreten, sie ist verbindlich. Das zeigt, dass die digitale Signatur die anderen beiden Eigenschaften von Nachrichten gewährleisten kann.

Die Entscheidung, von welchen Eigenschaften der Nutzer Gebrauch machen möchte, liegt bei ihm. Durch Verschlüsselung und die digitale Signatur steht ihm jede Eigenschaft zur Verfügung.

4 Durchführung der Kryptoparty

Nachdem die Zuhörer erfahren haben, wie E-Mails standardmäßig verschickt werden und die GnuPG-Software kennengelernt haben, wird mit den Vorbereitungen zum Download des

Programmes begonnen. Die Erklärung der Funktionalitäten der Verschlüsselungssoftware wurde bewusst vor die Benutzung gesetzt, da die Anwender wissen sollten, was für eine Software sie herunterladen.

Die Kryptoparty lässt sich in vier Schritte unterteilen, die als Unterkapitel dienen sollen. Zuerst wird die Installation inklusive möglicher Integritätschecks erklärt, anschließend folgt die Erstellung des Schlüsselpaars. Es wird der Schlüsselaustausch und schließlich das Verschicken verschlüsselter Nachrichten an zwei Beispielen erläutert. Weiterhin gibt es verschiedene Installationspakete der GnuPG-Software, auf die im ersten Unterkapitel kurz eingegangen wird.

4.1 Pakete von GnuPG

GnuPG ist als Kommandozeilen-Programm ohne grafische Oberfläche und als Teil von Installationspaketen verfügbar. Die Pakete Gpg4win für Windows Betriebssysteme und GPG Suite für MacOS bestehen jeweils aus vier Komponenten.

Komponenten	**Windows**	**MacOS**
Verschlüsselungsprogramm	GnuPG	MacGPG
Zertifikatsmanager	Kleopatra	GPGMail
Erweiterung für Microsoft Outlook bzw. Apple Mail	GpgOL	GPG Keychain
Erweiterung zur Dateiverschlüsselung	GpgEX	GPG Services

Tabelle 1: Komponenten der Installationspakete von GnuPG

Im Folgenden wird das Installationspaket am Beispiel des Windows-Paketes beschrieben. Die eigentliche Funktion der Software, die Chiffrierung und Dechiffrierung, wird vom Verschlüsselungsprogramm GnuPG erfüllt. Kleopatra ist ein Zertifikatsmanager, mit dem Schlüssel generiert, importiert, exportiert und gesammelt werden können. Außerdem ermöglicht der Zertifikatsmanager eine einheitliche Benutzerführung für alle Krypto-Operationen (Intevation GmbH, 2018). Inhalt des Windows-Pakets ist außerdem eine Microsoft Outlook Erweiterung (GpgOL) sowie eine Erweiterung für den Windows Explorer (GpgEX), die es möglich macht, Dateien über das Kontextmenü zu verschlüsseln (Intevation GmbH, 2018). Auf diesem Wege können verschlüsselte Inhalte ohne spezielle Erweiterung für das E-Mail-Programm übermittelt werden, indem die verschlüsselte Datei als Anhang verschickt wird.

Neben den Installationspaketen gibt es auch einzelne Softwareausführungen, die eine Verschlüsselung über GnuPG anbieten. Hierzu zählt z.B. Enigmail für das E-Mail-Programm Thunderbird.

4.2 Installation und Integritätscheck

Nach Vorstellung der GnuPG-Varianten beginnt nun der erste Schritt der Kryptoparty. Die GnuPG-Software kann in ihren verschiedenen Ausführungen auf der Internetseite des GNU Privacy Guards (www.gnupg.org) unter dem Reiter Download gefunden werden. Nach Auswahl von Gpg4win bzw. GPG Suite wird der Anwender auf die jeweiligen Projektseiten weitergeleitet, wo die Software zum Download zur Verfügung steht. Empfehlenswert ist es, die Software auf den offiziellen Internetseiten herunterzuladen, da dort die Informationen für einen Integritätscheck bereitgestellt werden.

Vor der Ausführung des Installationsprogramms sollte die Integrität der geladenen Datei überprüft werden. Dadurch wird sichergestellt, dass es sich um die echte Datei handelt und sie nicht zwischen Up- und Download verändert wurde. Für die Integritätsprüfung gibt es verschiedene Möglichkeiten:

- Prüfung über das Code Signing Certificate
- Prüfung über Checksummen
- Prüfung über die OpenPGP-Signatur

Die Prüfung des Code Signing Certificate übernimmt der Windows Installer vor der Ausführung der Installation. Manuell kann dieses Zertifikat über die Datei-Eigenschaften eingesehen und mit den Angaben auf der Internetseite des Softwareanbieters verglichen werden. Eine weitere Möglichkeit ist die Prüfung der Integrität über Checksummen. Gpg4win unterstützt die Hash-Algorithmen SHA-1, SHA-256 and MD5 zum Kreieren und Verifizieren von Checksummen. Des Weiteren kann die Integrität über die OpenPGP-Signatur überprüft werden. Dafür muss das auf der Website angebotene OpenPGP-Zertifikat, also der öffentliche Schlüssel, importiert werden, sodass anschließend die Signatur mit der GpgEX-Erweiterung über den Explorer geprüft werden kann (Intevation GmbH, 2018).

Problematisch ist, dass zwei der drei Möglichkeiten erst mit Gpg4win oder einer gleichwertigen Software möglich sind. Beim ersten Download kann der Anwender für einen umfangreichen Integritätscheck nur auf einen Partner zurückgreifen, der die Integrität einer Software für ihn prüfen kann. Ist das GnuPG-Softwarepaket einmal installiert, kann sie für zukünftige Integritätschecks verwendet werden.

Nach erfolgreichem Integritätscheck kann mit dem Ausführen des Installationsprogramms begonnen werden. Bei negativem Ergebnis der Integritätsprüfung, sollte die Installation nicht durchgeführt werden, da sich nicht mehr das gewünschte Programm im Download befindet.

Der Anwender wählt eine Sprache für die Installation aus und entscheidet sich für die Komponenten, die er aus dem Installationspaket installieren möchte. Eine Alternative zu Kleopatra bietet das Programm GPA, dass eine Zertifikatsverwaltung über mehrere Plattformen anbietet (Intevation GmbH, 2018). Für diese Kryptoparty sollten die vier in Kapitel 4.1 beschriebenen Komponenten gewählt werden, damit sowohl die Verschlüsslung über Microsoft Outlook als auch die Datei-Verschlüsselung mit einem webbasierten E-Mail-Programm demonstriert werden kann. Nachdem sich für ein Zielverzeichnis entschieden wurde, kann die Installation gestartet werden. Nach erfolgreichem Abschluss der Installation erfolgt die Information über die Fertigstellung und es kann mit der Schlüsselerstellung innerhalb des Zertifikatsmanagers Kleopatra begonnen werden.

4.3 Erstellung des Schlüsselpaars

Um verschlüsselte E-Mails erhalten zu können, ist ein eigenes Schlüsselpaar bestehend aus öffentlichem und privatem Schlüssel notwendig, welches in diesem Schritt erstellt werden soll. Dafür wird der Zertifikatsmanager Kleopatra verwendet und über „Datei“ > „Neues Schlüsselpaar“ kann ein Schlüsselpaar erstellt werden. Gpg4win unterstützt sowohl den OpenPGP-Verschlüsselungsstandard, als auch S/MIME. Auf die Unterschiede wurde bereits in Kapitel 2.3 eingegangen. In diesem Fall soll ein OpenPGP-Schlüsselpaar erstellt werden, da die Schlüssel gegenseitig durch die Teilnehmer beglaubigt werden können.

Bei einem OpenPGP-Schlüsselpaar ist zur Identifizierung die Eingabe eines Namens und optional die E-Mail-Adresse notwendig. Dadurch ist anonyme Kommunikation nur beschränkt möglich. Falls Anonymität gefordert ist, sollte auf andere Kommunikationswege z.B. innerhalb des Tor-Browsers zurückgegriffen werden. Unter „Erweiterte Einstellungen“ lässt sich der Algorithmus für die Verschlüsselung ändern. Sowohl die Art des Algorithmus (RSA, DAS, ECDSA) als auch die Schlüssellänge (2048 bis 4096 Bit). Außerdem kann entschieden werden, wofür der öffentliche Schlüssel, bzw. das Zertifikat, verwendet werden soll: zum Verschlüsseln oder ebenfalls zum Signieren und Beglaubigen. Dadurch ist es möglich, verschiedene Zertifikate für verschiedene Anwendungen zu erstellen und zu benutzen, z.B. ein Schlüsselpaar zum Signieren und ein anderes Schlüsselpaar zum Ver- und Entschlüsseln. Des Weiteren kann ein Gültigkeitszeitraum für das Zertifikat vorgegeben werden.

Nachdem die Einstellungen durch den Anwender überprüft wurden, wird das Schlüsselpaar aus Zufallszahlen erzeugt. Zum Schutz des Schlüsselpaares ist eine Passphrase notwendig. Hier sollte ein möglichst leicht zu merkender und schwer zu erratender Satz gewählt werden. Die Sicherheit wird erhöht, indem neben Klein- und Großbuchstaben auch Zahlen und Sonderzeichen bei der Wahl der Passphrase verwendet werden. Falls die Passphrase nicht

schnell genug eingegeben wurde, wird der Vorgang abgebrochen und die Schlüsselgenerierung muss erneut gestartet werden.

Wenn das Schlüsselpaar erfolgreich erstellt wurde, wird der Fingerabdruck des Schlüssels angezeigt. Hierbei handelt es sich um einen 40-stelligen Code, der weltweit einmalig ist. Bereits die letzten acht Stellen des Fingerabdrucks kommen mit großer Wahrscheinlichkeit nicht erneut vor, weshalb sie auch Schlüssel-ID genannt werden (Koch, et al., 2018).

Nun gibt es verschiedene Möglichkeiten, weiter zu verfahren. Es kann eine Sicherheitskopie des Schlüsselpaares erstellt werden, der erstellte öffentliche Schlüssel per E-Mail versendet werden oder an einen Verzeichnisdienst übermittelt werden. Mit dem Schlüsselaustausch befasst sich das anschließende Kapitel.

4.4 Schlüsselaustausch

Bei der hybriden Verschlüsselung gibt es anders als bei der symmetrischen Verschlüsselung kein Schlüsselaustausch-Problem, da mit dem Schlüssel, der ausgetauscht wird, nur chiffriert, nicht aber dechiffriert werden kann.

Der öffentliche Schlüssel kann auf einem Schlüsselserver veröffentlicht werden oder nur dem Korrespondenzpartner mitgeteilt werden. Der Vorteil von einem einfachen Schlüsselaustausch per E-Mail ist, dass keine weitere Person erfährt, dass eine Kommunikation zwischen zwei Personen stattfindet. Bei der Veröffentlichung des öffentlichen Schlüssels auf einem Schlüsselserver auf Grundlage des Web of Trusts geht die Anonymität verloren. Zusätzlich sollte beachtet werden, dass beglaubigten Schlüsseln auf Schlüsselservern nicht blind vertraut werden sollte. Da eine Beglaubigung einfach durch einen Korrespondenzpartner möglich ist, können sich auf Schlüsselservern auch gefälschte Schlüssel befinden. Aus diesen Gründen soll der Schlüsselaustausch in diesem Fall per E-Mail stattfinden.

Der Absender benötigt zum Verschlüsseln der Nachricht den öffentlichen Schlüssel des Empfängers. Dieser kann aus Kleopatra exportiert werden, indem das Zertifikat markiert und auf „Exportieren“ geklickt wird. Es muss ein Speicherort gewählt werden und anschließend wird der öffentliche Schlüssel im asc-Format abgespeichert.

Der Schlüssel kann einer E-Mail angefügt werden und so dem Korrespondenzpartner übermittelt werden. Die Übermittlung muss nicht zwingend über einen sicheren Kanal erfolgen. Was ein möglicher Angreifer erfahren würde, wäre nur die Tatsache, dass die beiden Personen über geheimem Wege miteinander kommunizieren wollen.

Nach Erhalt eines öffentlichen Schlüssels kann dieser in den Zertifikatsmanager Kleopatra importiert werden. Dafür wird der empfangene Schlüssel abgespeichert und anschließend Kleopatra durch Klicken auf „Importieren“ hinzugefügt. Bei Gpg4win ist eine manuelle

Beglaubigung des Schlüssels erforderlich. Dafür wird der Fingerabdruck des Kommunikationspartners überprüft. Stimmt dieser beim Partner und beim Gläubiger überein, kann der Gläubiger mit seinem Schlüssel das Zertifikat des Partners beglaubigen. Das kann er, wie in diesem Fall, für sich selbst oder für einen Schlüsselserver machen.

Nach erfolgreichem Austausch und Import der beiden öffentlichen Schlüssel können sich die Korrespondenzpartner verschlüsselt E-Mails verschicken. Dies soll im nächsten Abschnitt erläutert werden.

4.5 Versand verschlüsselter E-Mails

Der E-Mail-Versand von verschlüsselten Nachrichten soll an zwei Beispielen aufgezeigt werden. Zum einen mithilfe Microsoft Outlook und zum anderen über einen beliebigen Web-Client. Der Unterschied besteht darin, dass über Outlook auch die Nachricht selbst verschlüsselt wird, während bei der Nutzung eines Web-Servers der Anhang einer E-Mail verschlüsselt wird.

4.5.1 Versand über Microsoft Outlook

Die Outlook-Erweiterung von GnuPG nennt sich GpgOL, wobei OL für Outlook steht. Erkennbar ist das aktivierte Add-In in der oberen rechten Ecke des Programms, indem dort GpgOL angezeigt werden sollte. Zum Schreiben einer verschlüsselten E-Mail wird die Nachricht auf üblichem Weg geschrieben und im oberen rechten Rand bei „Absichern“ kann gewählt werden, ob die Nachricht verschlüsselt und/oder signiert werden soll.

Der Empfänger kann die Nachricht entschlüsseln, indem er seinen privaten Schlüssel verwendet. Das passiert entweder automatisch bei Erhalt der Nachricht oder kann über die Einstellungen so gewählt werden, dass der Empfänger zum Entschlüsseln jedes Mal seine Passphrase eingeben muss. Die zweite Möglichkeit erhöht die Sicherheit, da so selbst eine Person, die Zugriff auf den Computer hat, ohne Passphrase die Nachricht nicht lesen kann.

Weitere Eigenschaften von Gpg4win können unter „GnuPG konfigurieren“ verändert werden. So lässt sich dort u.a. einstellen, ob Nachrichten per Voreinstellung verschlüsselt oder signiert werden sollen.

4.5.2 Versand über Web-Server

Die Komponente GpgEX aus dem Installationspaket Gpg4win ermöglicht die Verschlüsselung von Dateien. Wenn diese per E-Mail verschlüsselt verschickt werden sollen, müssen sie, wie bisher, mit dem öffentlichen Schlüssel des Empfängers chiffriert werden. Das funktioniert mit einem Rechtsklick auf die zu verschlüsselnde Datei unter „Mehr GpgEX Optionen“ > „Verschlüsseln“. Die Datei kann für einen selbst und für andere verschlüsselt werden, wobei bei der Verschlüsselung für andere Personen das Zertifikat dieser Personen

in Kleopatra importiert sein muss. Es sollte das Zertifikat des E-Mail-Empfängers zur Verschlüsselung gewählt werden. Nach erfolgreicher Verschlüsselung befindet sich der chiffrierte Inhalt in einer zweiten Datei im gpg-Format.

Diese verschlüsselte Datei kann nun einer E-Mail angefügt werden. Dafür kann jedes E-Mail-Programm verwendet werden, da nur der Anhang verschlüsselt ist. Auf diesem Weg können verschlüsselte Informationen in E-Mails über Webbrowser übermittelt werden.

Zur Entschlüsselung benutzt der Empfänger seinen privaten Schlüssel, indem er die Passphrase eingibt. Er erhält eine neue dechiffrierte Datei mit gleichem Namen.

5 Efail-Angriff

Zum Ende dieser Seminararbeit wird auf einen Angriff eingegangen, der im Mai 2018 in den Medien war und GnuPG betrifft. Bei dem sogenannten Efail-Angriff soll der Angreifer Zugriff auf den Klartext einer Nachricht bekommen haben, wenn er vorher im Besitz der verschlüsselten Nachricht war. Indem dem verschlüsselten Inhalt weiterer Text hinzugefügt wurde, wurde ein Code für ein http-Request eingefügt. Wenn das E-Mail-Programm des Empfängers diesen aktiven Inhalt ausführt, wird der entschlüsselte Klartext an den Angreifer zugeschickt (Schmidt, 2018).

Anfänglich hieß es in den Medien, dass es sich um eine Sicherheitslücke des OpenPGP-Standards handelt, allerdings wurde der Vorwurf von den Entwicklern von OpenPGP schnell zurückgewiesen. Grund für den Erfolg des Angriffs sei nicht eine Schwäche von OpenPGP, sondern die Konfiguration des E-Mail-Programms (Wiesend, 2018). Entscheidend ist, dass aktive Inhalte (wie HTML oder JavaScript) bei der E-Mail-Anzeige deaktiviert sind und das automatische Nachladen externer Inhalte (z.B. Bilder) unterdrückt wird. Sind diese Einstellungen getroffen, ist die Verwendung von GnuPG mit dem OpenPGP Standard gegen diese Art von Angriffen weitestgehend sicher. Es gibt bereits Versionen von Enigmail, der Thunderbird-Erweiterung von GnuPG, die Efail-Angriffe unmöglich machen sollen (Schmidt, 2018).

6 Fazit

Die Seminararbeit zeigt, dass es wichtig ist sich mit dem Thema Geheimhaltung und Verschlüsselung auseinander zu setzen. Es gibt gute freie Software, die eine Integration von Verschlüsselungsprogrammen in Standard-E-Mail-Programme bietet und auch von Nicht-Informatikern bedient werden kann.

Allerdings haben die Pakete Gpg4win und GPG Suite auch Nachteile. Dadurch, dass die Handhabung für den Anwender erleichtert werden soll, geschieht vieles automatisch. Der

Nutzer führt die Verschlüsselung mit der Outlook-Erweiterung nicht bewusst selbst durch, sondern gibt sie aus der Hand und kann daher weniger nachvollziehen, was passiert. Dadurch vertraut er die Verschlüsselung jemandem an, obwohl in diesem Gebiet inzwischen „Zero Trust“ eine große Rolle spielt.

Entscheidend ist, dass jeder selbst entscheiden kann, ob, wie und wann er Nachrichten verschlüsselt verschicken möchte. Durch den Artikel 10 im Grundgesetz hat jeder ein Recht auf die Unverletzlichkeit des Briefgeheimnisses, welches durch die Nutzung von Verschlüsselung wahrnehmbar ist.

Heutzutage ist undurchsichtig, welche Informationen von Privatpersonen und Organisationen abgefangen und gespeichert werden. Noch weniger ist absehbar, wozu diese Informationen jetzt oder in Zukunft verwendet werden. Daher sollte sich jeder über die Möglichkeit einer Überwachung bewusst sein, sodass der Anwender selbst entscheiden kann, wie er damit umgehen möchte. Die GnuPG Software bietet eine verschlüsselte Kommunikation über Betriebssysteme und Softwarelösungen hinweg, die einen Aspekt der verschlüsselten Kommunikation darstellen kann.

Quellenverzeichnis

Birkle, Jürgen. 2015. Verschlüsselung für Dateien - einfach erklärt. [Online] doubleSlash, 26. August 2015. [Zitat vom: 2. Juli 2018.] https://blog.doubleslash.de/verschluesselung-fuer-dateien-einfach-erklaert/.

Bleich, Holger. 2018. Einfach erklärt: E-Mail-Verschlüsselung mit PGP. [Online] Heise Medien, 28. März 2018. [Zitat vom: 12. Juni 2018.] https://www.heise.de/ct/artikel/Einfach-erklaert-E-Mail-Verschluesselung-mit-PGP-4006652.html.

Callas, J., et al. 2007. OpenPGP Message Format. *Request for Comments: 4880.* [Online] PGP Corporation & IKS GmbH, November 2007. [Zitat vom: 3. Juli 2018.] https://tools.ietf.org/html/rfc4880.

CHIP Digital GmbH. 2018. PGP (letzte Freeware-Version). [Online] 2018. [Zitat vom: 3. Juli 2018.] http://www.chip.de/downloads/PGP-letzte-Freeware-Version_66630758.html.

Ertel, Wolfgang. 2012. *Angewandte Kryptographie.* München : Carl Hanser Verlag, 2012.

Free Software Foundation . 2000. Das GNU-Handbuch zum Schutze der Privatsphäre. [Online] 2000. [Zitat vom: 12. Juni 2018.] https://gnupg.org/gph/de/manual/book1.html.

Free Software Foundation. 2007. GNU GENERAL PUBLIC LICENSE. *Version 3.* [Online] 29. Juni 2007. [Zitat vom: 2. Juli 2018.] https://www.gnu.org/licenses/gpl-3.0.html.

Intevation GmbH. 2018. Check integrity of Gpg4win packages. [Online] 2018. [Zitat vom: 3. Juli 2018.] https://www.gpg4win.org/package-integrity.html.

—. 2018. Über Gpg4win. *Die Gpg4win-Kompenenten.* [Online] 2018. [Zitat vom: 3. Juli 2018.] https://www.gpg4win.de/about-de.html.

Koch, Werner, et al. 2018. *Das Gpg4win-Kompendium, Version 4.0.1.* s.l. : Intevation GmbH, 2018.

Schmidt, Jürgen. 2018. PGP und S/MIME: So funktioniert Efail. *heise security.* [Online] 14. Mai 2018. [Zitat vom: 3. Juli 2018.] https://www.heise.de/security/artikel/PGP-und-S-MIME-So-funktioniert-Efail-4048873.html.

Wiesend, Stephan. 2018. Efail – EFF warnt vor PGP: Verschlüsselungstool sofort deaktivieren. *PC Welt.* [Online] 14. Mai 2018. [Zitat vom: 3. Juli 2018.] https://www.pcwelt.de/a/eff-warnt-vor-pgp-verschluesselungstool-sofort-deaktivieren,3439030.

Wikipedia. 2017. CryptoParty. [Online] 2017. [Zitat vom: 12. Juni 2018.] https://de.wikipedia.org/wiki/CryptoParty.

—. 2018. ECHELON. [Online] 5. Juni 2018. [Zitat vom: 2. Juli 2018.] https://en.wikipedia.org/wiki/ECHELON.

—. 2018. GNU Privacy Guard. [Online] 20. Juni 2018. [Zitat vom: 3. Juli 2018.] https://en.wikipedia.org/wiki/GNU_Privacy_Guard.

Versicherung über Eigenleistung

Hiermit erkläre ich, dass ich die vorliegende Seminararbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Die Stellen der Seminararbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Wedel, den 09.07.2018