„Skalierbare Kryptographie“ – Verschlüsselung einfach nutzen

Prof. Bernhard Esslinger, Dr. Sibylle Hick und Lars Wittmaack

Haben Sie jemals darüber nachgedacht, Ihre Gehaltsabrechnung auf eine Postkarte zu schreiben und nach Hause zu senden? Warum erlauben Sie nur bestimmten Personen Zugriff auf Ihre private Briefkorrespondenz? Es geht doch niemanden etwas an, werden die Meisten antworten; es sind private Informationen.

Warum nur verhalten wir uns dann in der elektronischen Welt anders? Die E-Mail beispielsweise hat sich entwickelt, um Nachrichten elektronisch zu übertragen. Dabei wurde das Abbild eines realen Briefes herangezogen (so werden technisch z.B. Envelope und Body unterschieden wie Umschlag und Inhalt). Ein maßgeblicher Unterschied existiert jedoch – der technische Umschlag ist nicht blickdicht.

Eine E-Mail ist also nichts anderes als eine elektronische Postkarte, die Sie über das Internet versenden. Sie müssen sich aktiv entscheiden, mittels Verschlüsselung einen „blickdichten Umschlag“ zu verwenden, wenn Sie unbefugtes Mitlesen privater oder geschäftlicher Informationen verhindern wollen.

Warum wird E-Mail-Verschlüsselung dann noch nicht umfassend eingesetzt?

Erinnern Sie sich noch, wie Kinder sich die Augen zuhalten und sagen „Du siehst mich nicht“? Aus den Augen, aus dem Sinn; nicht mehr existent. Der E-Mail wird offensichtlich unbewusst unterstellt, sie könne nicht mitgelesen werden. Awareness-Programme können helfen, diesem Missverständnis entgegenzuwirken (vgl. [1] Internetseite des BSI für Bürger, [2] Deutschland sicher im Netz). Die nächsten Hürden folgen direkt – einfache Einrichtung, benutzerfreundlicher Umgang, vollständige Interoperabilität und kontinuierlicher Betrieb mit entsprechender Verbreitung.

Der folgende Beitrag greift diese Aspekte auf und beschreibt Voraussetzungen für eine erfolgreiche Skalierung kryptographischer Lösungen anhand des Beispiels E-Mail-Verschlüsselung.

Für den Awareness-Teil wird u.a. die frei verfügbare E-Learning Software CrypTool (https://www.cryptool.org) genutzt, die es dem interessierten Leser auf spielerische Weise erlaubt, sich in dieses dann gar nicht mehr ganz so komplexe Themengebiet einzulesen.

Autoren:
Prof. Bernhard Esslinger, Dr. Sibylle Hick, Lars Wittmaack aus dem Bereich CISO (Chief Information Security Office) der Deutschen Bank. Prof. Esslinger lehrt zudem angewandte IT-Sicherheit und Kryptologie an der Universität Siegen.

Kryptographisches Grundwissen spielerisch entdecken

Gratulation – Sie haben sich entschieden, dem Thema mehr Beachtung zu schenken. Aber was nun? Wo anfangen?

Beginnen Sie mit grundlegendem Wissen. Es ist nicht mehr notwendig, Krypto-Experte zu sein, um E-Mail-Verschlüsselung einzusetzen. Dennoch, um etwas richtig zu verwenden, ist das Verständnis der Zusammenhänge von Funktion, Rahmenbedingungen und Wirkung wichtig. Bei vielen Dingen erarbeiten wir uns dieses Verständnis intuitiv und durch Ausprobieren, selbst wenn wir dann doch beispielsweise mal einen Blick in die Anleitung des neuen High-Tech-Fernsehers werfen.

Kryptographische Methoden werden bereits seit rund 3.000 Jahren eingesetzt, um Vertraulichkeit sicherzustellen. Deshalb sind wir der Meinung, dass der moderne Smartphone-Besitzer ebenso in der Lage ist, ein grundlegendes kryptographisches Verständnis zu entwickeln.

Eine gute Unterstützung für den Aufbau eines kryptographischen Grundverständnisses bietet das Open-Source-Programm CrypTool. Es ist so konzipiert, dass es dem menschlichen Drang, etwas auszuprobieren, entgegenkommt und trotzdem wichtige Grundsätze bis hin zu Detailwissen vermitteln kann. So können selbst mathematische Verfahren durch Visualisierungen, kleine Zahlenbeispiele

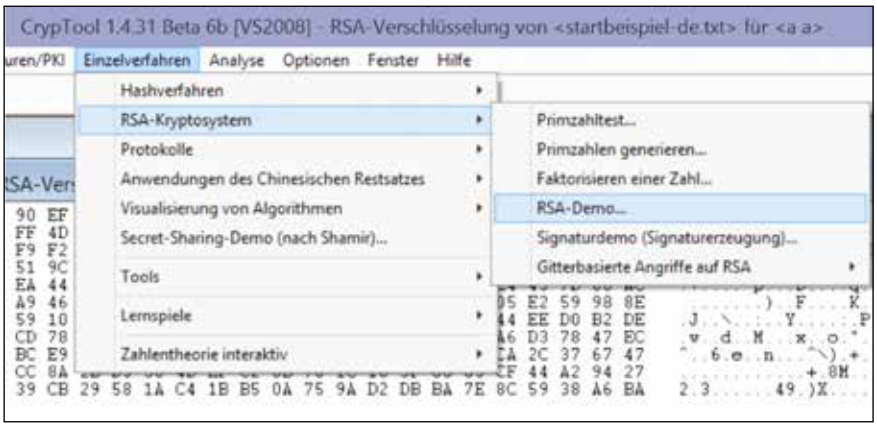

Abbildung 1: Auswahl von Visualisierungen im CrypTool 1

Abbildung 2: RSA-Verschlüsselung mit Zahlenbeispiel

und zusätzliche Erklärungen nachvollzogen werden [vgl. Abb. 1]. Als Grundlage für die Skalierung kryptographischer Lösungen, die ist bei Anwendern wahrscheinlich aktuell wichtiger als Awareness – bietet CrypTool auch die Möglichkeit, einen Einstieg in das Thema Verschlüsselung zu finden; seien es Zertifikate, asymmetrische Verschlüsselung oder SSL (Secure Socket Layer-Verschlüsselung für Internetseiten bzw. zwischen Servern).

Ein bekanntes Verschlüsselungsverfahren ist RSA. Eine Demonstration dazu mit Zahlenbeispielen findet sich in CrypTool 1 unter dem Menü „Einzelverfahren/RSA-Kryptosystem/RSA-Demo…" [vgl. Abb. 2].

Eine E-Mail Verschlüsselung mit S/MIME wird ebenfalls in CrypTool für Anwender visualisiert [3]. Bei S/MIME handelt es sich neben PGP [4] um *das* Standard-Verfahren, das weltweit zur Verschlüsselung und zum Signieren von E-Mails eingesetzt wird. Die Visualisierung zu S/MIME lässt sich in CrypTool 1 über das Menü „Einzelverfahren/Protokolle/Sichere E-Mail mit S/MIME …" aufrufen. Sie erklärt Schritt für Schritt wie E-Mail-Verschlüsselung funktioniert [vgl. Abb. 3, 4]. Ferner enthält CrypTool eine ausführliche Online-Hilfe zu allen Themen.

Auch CrypTool 2 und JCrypTool bieten gute Möglichkeiten, Verschlüsselung besser zu verstehen, und diese selber einmal auszuprobieren. Das AES-Verfahren gehört zu den aktuellen symmetrischen kryptographischen Verfahren. Ein interessierter Nutzer kann sich anhand von CrypTool 2 weitere Details des Protokolls anzeigen und erklären lassen, indem er sich das Verfahren aus den bereitgestellten Templates im Startcenter heraussucht [vgl. Abb. 5].

Bei CrypTool-Online findet der Nutzer eine schnelle Übersicht zu Verschlüsselungsverfahren und AES-Nutzung vom Smartphone aus.

Interoperable Implementierungen

Entgegen der weit verbreiteten Meinung, dass Verschlüsselung schwierig anzuwenden sei, gibt es mittlerweile eine Vielzahl von Lösungen, die gut auf die Anforderungen des Anwenders angepasst sind. Z.B. kommt ein iPhone bereits mit einer integrierten S/MIME-Lösung, in die der Besitzer „nur" noch sein eigenes Zertifikat einspielen muss. Dies kann durch wenige Klicks erreicht werden.

Zuvor jedoch muss man ein solches (Verschlüsselungs-)Zertifikat besitzen. Man kann ein solches kostenlos beantra-

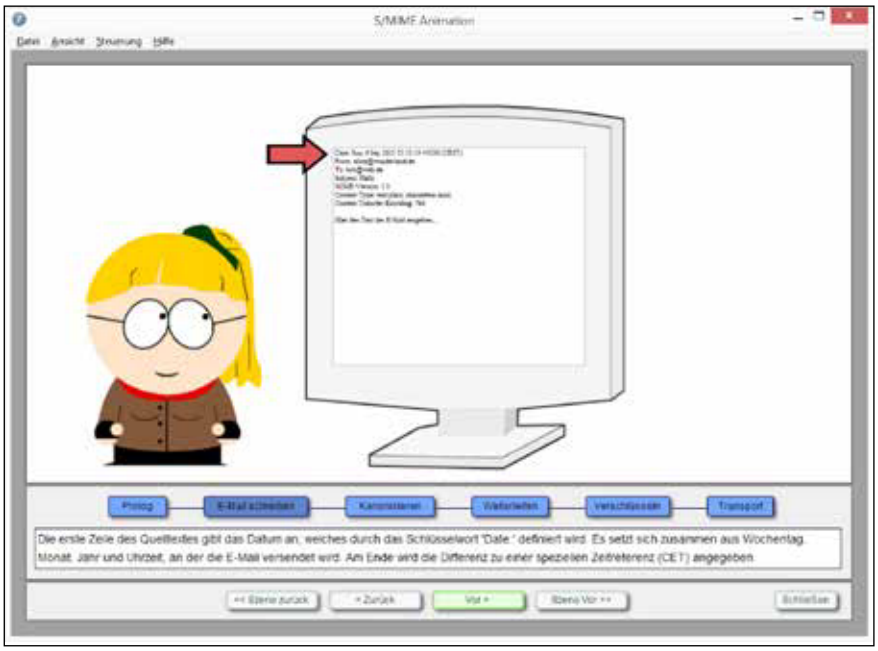

Abbildung 3: Animation zur E-Mail-Verschlüsselung mit S/MIME

Abbildung 4: Animation mit S/MIME-Zertifikat

gen. Eine gute und erprobte Anleitung zur Nutzung von S/MIME finden Sie unter [5]. Diese Anleitung beschreibt die Installation und den Gebrauch sowohl für Nutzer mit PCs (mit Thunderbird oder Outlook) als auch mit Smartphones (unter iOS und Android). Darin wird nicht nur beschrieben, wie man die Software zur Verschlüsselung einrichtet, sondern auch, wie man ein Zertifikat beantragt und in das jeweilige System einspielt [vgl. Abb. 6].

Für Leute, die sich mit dem Thema auseinander setzen wollen, existieren also annehmbare Möglichkeiten. Für Jedermann reichen diese aber bei weitem nicht aus – die Forderung aus der Digitalen Agenda ist also nicht erfüllt: „Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden" [6].

Für Organisationen stellen sich bei der Nutzung einer E-Mail-Verschlüsselung weitere Fragen. Je integrierter die Verschlüsselung in den jeweiligen E-Mail-Client ist, desto besser. Nichtsdestotrotz bedarf es Supportpersonal, Richtlinien für die korrekte Nutzung und weiterer technischer Maßnahmen und Prozesse, um Organisations-eigene und fremde Zertifikate zu zu verwalten [vgl. Abb. 7]. Dies führt zu zusätzlichen Betriebskosten für den Aufbau und den kontinuierlichen Betrieb einer E-Mail-Verschlüsselungslösung.

Ansprechpartner und Experten für Fragen zu individuellen Fällen sind insbesondere dann wichtig, wenn die Verschlüsselungslösung für bestimmte Use cases nicht out-of-the-box funktioniert. Z.B. wenn ein Unternehmen mit einem anderen Unternehmen kommunizieren möchte und das Verschlüsselungsverfahren, die verwendeten Zertifikate oder die Implementierungen nicht automatisch miteinander kompatibel sind. Dies liegt häufig daran, dass die zugrundeliegenden Standards von den Produkten unterschiedlich umgesetzt wurden. Einen allgemein gültigen Interoperabilitätstest gibt es (noch) nicht, obwohl zahlreiche Organisationen, wie „TeleTrusT e.V. (https://www.teletrust.de) mit der European Bridge-CA, oder AWV („http://www.extra-standard.de" www.extra-standard.de)," an kryptographischen Vereinheitlichungen arbeiten. Länderübergreifend sind dann noch weitere Hürden zu überwinden.

Anwender unterschiedlicher Organisationen eine verschlüsselte E-Mail austauschen zu lassen, klingt also einfacher als es organisatorisch dann wirklich ist.

Anwendbare, interoperable E-Mail-Verschlüsselung

Obwohl es E-Mail-Verschlüsselung schon seit rund 15 Jahren gibt, ist ihr Einsatz noch immer nicht wirklich benutzerfreundlich. Einfachheit und intuitive Bedienung sind noch immer nicht vollständig umgesetzt. Die Rückmeldungen an den Anwender, z.B. im Fehlerfall, bieten noch viel Verbesserungspotential [vgl. Abb. 8]. Eine One-Click-Installation wäre wünschenswert, um eine hohe Verbreitung und bessere Awareness der Anwender zu schaffen [7].

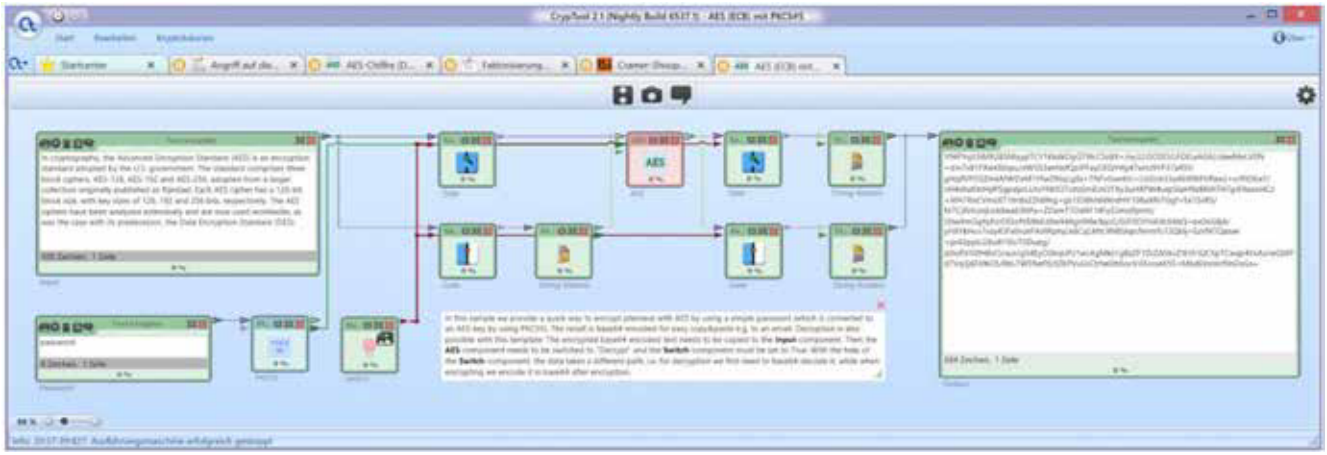

Abbildung 5: Workflow zur Benutzung des sicheren AES-Verschlüsselungsverfahrens

Ein weiterer, häufig bemängelter Umstand ist die fehlende Interoperabilität, z.B. zwischen den dabei verwendeten Protokollen S/MIME und PGP.

Eine Analyse mehrerer Universitäten unter Leitung der Uni Bochum ergab Ende 2014, dass man diese Anforderungen vollständig umsetzen könnte – in weniger als drei Jahren und für weniger als zehn Millionen Euro. Aber es sieht so aus, als ob öffentliche Gelder dafür im Gegensatz zu den Beteuerungen in der Digitalen Agenda [6] nicht zur Verfügung stehen. Trotz der Erkenntnisse durch Snowden werden deutlich größere Summen für den Ausbau von Abhörmaßnahmen und Cyber-Angriffsfähigkeiten bereitgestellt als dafür, dass

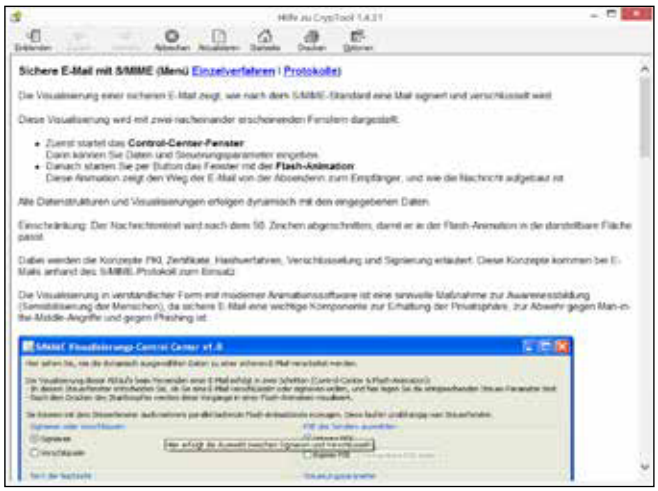

Abbildung 6: CrypTool-Hilfe als Beispiel einer Anwenderunterstützung

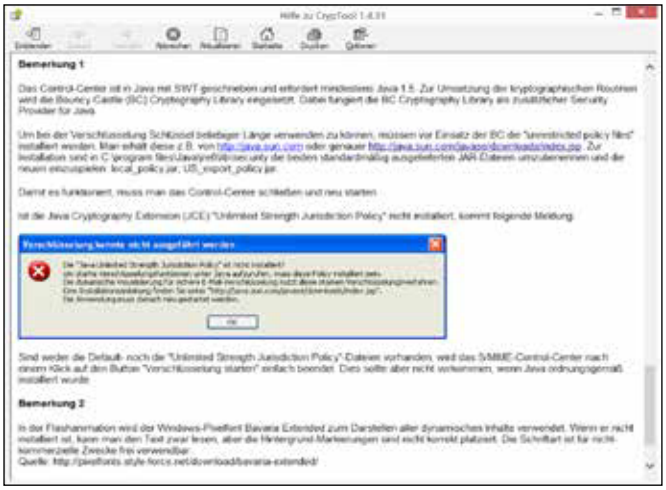

Abbildung 7: Beispiel aus CrypTool bzgl. gängiger Interoperabilitätseinschränkungen

sich die Bevölkerung selbst wirkungsvoll schützen kann (wie wenig die Ressourcen damit richtig allokiert werden, zeigte eine amerikanische Studie der New-America-Foundation vom Januar 2014: Danach wurden 92,5 Prozent aller untersuchten 225 Terroranschläge ausschließlich mittels normaler Polizeiarbeit und nicht durch geheimdienstliche Überwachung aufgedeckt [10]).

Doch es gibt auch Fortschritte: Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat einen Entwurf einer Technischen Richtlinie für E-Mail-Diensteanbieter veröffentlicht [8].

Die E-Mail-Provider innerhalb des 1&1-Bereiches bieten ihren Kunden inzwischen PGP an [9]. Außerdem arbeiten im Open-Source-Bereich das Schweizer Projekt Pretty-Easy-Privacy und Enigmail erfolgreich zusammen, um die Verschlüsselung voran zu bringen (Thunderbird plus Plugins für Outlook, Apps für Android und iOS) und auch verstärkt Firmenkunden anzubinden [11].

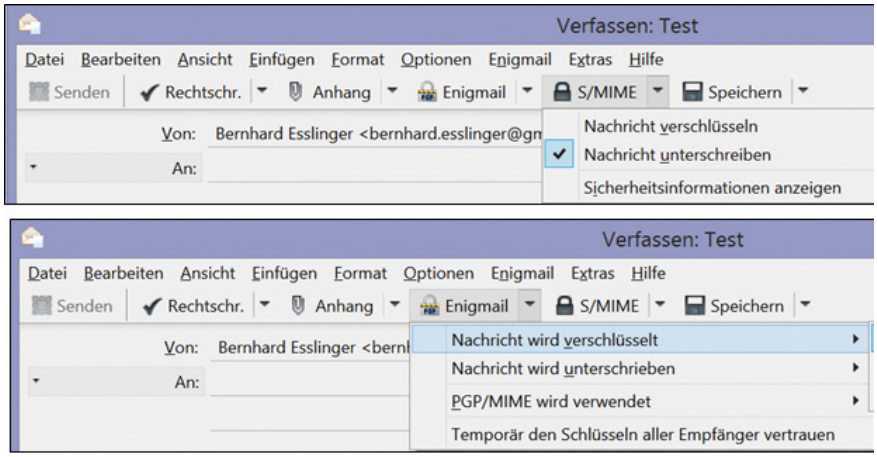

Abbildung 8: SMIME-Einstellung überschreibt die PGP-Einstellung

Für einen dauerhaft erfolgreichen und leicht bedienbaren Einsatz müssten die vorhandenen Programme aber noch deutlich verbessert werden. Da die meisten davon Open-Source sind, wäre das ein Leichtes, wenn das nötige Budget dazu von der öffentlichen Hand zur Verfügung gestellt werden würde.

Oft wird empfohlen, dass die Anwender sich nach der Installation von E-Mail-Verschlüsselung informiert halten sollen, welche Weiterentwicklungen und Sicherheitsprobleme es gibt. Massentauglich dagegen ist Software erst dann, wenn sie das dem Benutzer abnimmt, indem sie sich permanent selbst updated und die Entwickler dahinter das nötige Budget bekommen, für die Sicherheitsupdates zu sorgen.

Fazit

Kryptographie ist eine wichtige Maßnahme zum Schutz von Informationen. Sie wird aber vernachlässigt. Zu großen Teilen lässt sich die hohe Hemmschwelle auf vermutete hohe Komplexität, mangelnde technische Interoperabilität, geringe Integration in bestehende Anwendungen und viel zu geringe Benutzerfreundlichkeit zurückführen. Zahlreiche Interessierte arbeiten daran, dass anwendergerechte Lösungen bereitgestellt werden. Eine Beteiligung durch Hersteller, Firmen, Regierungen und letztendlich durch die Anwender gehört dazu. Den echten Brief kleben Sie ja auch zu, bevor Sie ihn zur Post bringen. ■

Quellen und weitere Informationen:

[1] BSI für Bürger. Verschlüsselt kommunizieren. https://www.bsi-fuer-buerger.de
[2] Deutschland sicher im Netz. Für Verbraucher. E-Mails und soziale Netzwerke. https://www.sicher-im-netz.de/
[3] S/MIME. Secure / Multipurpose Internet Mail Extensions. RfC 5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2. https://tools.ietf.org/html/rfc5751
[4] PGP. Pretty Good Privacy. OpenPGP: RfC 5581: OpenPGP Message Format. https://tools.ietf.org/html/rfc4880
[5] Anti-Prism-Party. Anleitung „Sichere email am PC und mit dem Smartphone“ https://www.anti-prism-party.de
[6] Die Bundesregierung: Schutzziele der Digitalen Agenda 2014-2017. http://www.digitale-agenda.de
[7] Datenschutz und Datensicherheit (DuD), Mai 2014, Seite 305-313, „Sichere E-Mail mit S/MIME – Eine Anleitung aus Anwenderperspektive“; und die Forderungen der Gesellschaft für Informatik unter http://www.gi.de
[8] BSI. Sicherer E-Mail-Transport, https://www.bsi.bund.de
[9] Heise: GMX und Web.de integrieren PGP in ihre Mail-Dienste, http://www.heise.de
[10] New America Foundation, Jan 2014: IS NSA Surveillance., https://static.ewamerica.org (Beitrag in Deutsch dazu: http://t3n.de/news/nsa-massenueberwachung-erfolg-terrorismus-522181)
[11] PEP. Pretty-Easy-Privacy Enigmail und Pep Project wollen Verschluesselung voranbringen, http://www.heise.de und http://pep-project.org