Evaluation der Nutzbarkeit von PGP und S/MIME in Thunderbird

Marco Ghiglieri[1], Birgit Henhapl[1], Nina Gerber[2]

Technische Universität Darmstadt[1]
Karlsruher Institut für Technologie[2]

marco.ghiglieri@secuso.org, birgit.henhapl@secuso.org,
nina.gerber@kit.edu

Zusammenfassung
Die Nutzung von E-Mails zur Kommunikation steigt weiterhin täglich. Obwohl Nutzer glauben, dass ihre E-Mails mitgelesen werden und dies auch „schlimm“ finden, werden trotzdem keine Sicherheitsmechanismen genutzt. Einer der genannten Gründe ist der hohe Aufwand bei der Installation von Sicherheitsmechanismen in E-Mail-Programmen.

In diesem Artikel zeigen wir, ob die Benutzbarkeit von PGP und S/MIME in Mozilla Thunderbird gegeben ist, wenn sie durch einen versierten Anwender bereits vorinstalliert wurden. Wir führen einen Cognitive Walkthrough mit Experten und einem Laien durch. Auf Grundlage der Ergebnisse beschreiben wir Verbesserungsvorschläge und kommen zu dem Ergebnis, dass es weiterhin Verbesserungsbedarf gibt.

1 Einleitung

Die Anzahl an Nutzern von E-Mails wächst stetig (The Radicati Group, 2018): Obwohl über 60% der befragten Nutzer glauben, dass ihre E-Mails mitgelesen werden, und 72% dies sogar als schlimm bezeichnen, werden verfügbare E-Mail-Sicherheitsmechanismen wie Verschlüsselung nicht breitflächig eingesetzt. Viele beklagen einen hohen Installationsaufwand (Convios Consulting, 2017). Aktuelle Meldungen, dass die Implementierung in den meistgenutzten E-Mail-Programmen von PGP und S/MIME nicht sicher seien, wirken zusätzlich kontraproduktiv (TeleTrusT – Bundesverband IT-Sicherheit e.V, 2018).

Um die Nutzeranzahl trotz der Skeptiker zu steigern, muss die Absicherung von E-Mails gegen Mitlesen (Vertraulichkeit durch Verschlüsselung) und Manipulation (Integrität durch digitale Signaturen) für Laien vereinfacht und ermöglicht werden. Innerhalb eines größeren Projekts im Center for Research in Security and Privacy soll ein Rahmenwerk entwickelt werden, das (1) Usability- und Sicherheitsziele möglichst widerspruchsfrei vereinbart und (2) im Idealfall nicht einmal verlangt, dass der Empfänger bereits über ein gültiges Schlüsselpaar verfügt. Die Idee dazu wurde bereits in (Zimmermann, Henhapl, Gerber, & Enzmann, 2017) beschrieben.

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2018 in
R. Dachselt, G. Weber (Hrsg.):
Mensch und Computer 2018 – Workshopband, 02.–05. September 2018, Dresden.
 https://doi.org/10.18420/muc2018-ws08-0542

In diesem Artikel präsentieren wir die Ergebnisse unserer Untersuchung von Mozilla Thunderbird (Version 52.7.0 (32-Bit)), nachdem die Installation der Sicherheitsmechanismen PGP und S/MIME durch versierte Nutzer durchgeführt wurde. Wir entschieden uns für Thunderbird aufgrund seiner kostenfreien Verfügbarkeit. Er integriert, wie auch andere am Markt erhältliche E-Mail-Programme, S/MIME. Mit der Thunderbird-Erweiterung Enigmail (Version 2.0.5 (20180521-1522) mit gnupg 2.2.4) wird PGP unterstützt. Zur Untersuchung der Nutzbarkeit wurden für S/MIME mit Thunderbird und für PGP mit Enigmail/Thunderbird zwei unabhängige Cognitive Walkthroughs von IT-, bzw. IT-Security-Experten (siehe Kapitel 3) durchgeführt. Zusätzlich wurde einem Laien in einer Pilotstudie mit Think Aloud-Methode Aufgaben gestellt (siehe Kapitel 4). Aus den Ergebnissen der CWs und der Pilotstudie werden Verbesserungsvorschläge abgeleitet (siehe Kapitel 5).

2 Verwandte Arbeiten

Verschiedene Studien schlagen Verbesserungen vor (Whitten & Tygar, 1999), (Moecke & Volkamer, 2013), (Renaud, Volkamer, & Renkema-Padmos, 2014), (Naiakshina, et al., 2016), (Zimmermann & Henhapl, 2017), wie z.B. das Verstecken möglichst vieler Informationen oder die Registrierung mit Personenidentifikation und mindestens Zwei-Faktor-Authentifikation. Zu den aufgezeigten Problemen gehören unvollständige Gefahrenmodelle, falsche Nutzeranreize für Sicherheitsmechanismen beim E-Mail-Versand sowie mangelnde Kenntnisse zur Funktionsweise. Diese Arbeiten führen zu der Erkenntnis, dass die Benutzerführung bzw. die eingesetzten Mechanismen auf Zielgruppen angepasst sein sollten, so dass diese sie in kurzer Zeit erlernen können (Benenson, 2015), (Ferreira & Anacleto, 2017). In (Ruoti, 2016) wird beschrieben, dass ein Tutorial für Nutzer bei der Installation der Sicherheitsmechanismen wichtig ist. Nach (Ruoti, 2016) und (Lerner, Zeng, & Roesner, 2017) vertrauen Experten den Systemen weniger, die wenig technische Informationen bieten.

In (Schochlow, 2016) wurde mit einem Cognitive Walkthrough das Mailvelope Plugin für Online-Email-Dienste analysiert: Da die Sichtbarkeit der Symbole mangelhaft war, bestand die Gefahr, dass E-Mails ohne Verschlüsselung abgesendet werden. Ähnliche Probleme konnten wir auch in Thunderbird feststellen.

Die Volksverschlüsselung des Fraunhofer SIT ist ein Ansatz, um E-Mailverschlüsselung für Laien tauglich zu machen. Unsere Erkenntnisse könnten dort eingesetzt werden, da dort hauptsächlich die Probleme der Schlüsselverwaltung gelöst werden.

3 Cognitive Walkthrough

Ziel eines Cognitive Walkthroughs (CW) ist es, die Erlernbarkeit einer Anwendung aus der Perspektive eines Laiennutzers zu beurteilen (Wharton, 1994) (Schochlow, 2016). Durchgeführt wird die Methode in der Regel von Experten, die Annahmen über Fähigkeiten und Wissen von Laiennutzern treffen und typische Aufgaben auswählen. Diese werden im Anschluss von den Experten aus Sicht der Laien durchlaufen und anhand vorher festgelegter Kriterien bewertet, ob Laiennutzer zur Lösung der Aufgabe fähig wären.

Unser Ziel ist es zu analysieren, ob es Laiennutzern möglich ist, E-Mail-Verschlüsselung und -Signaturen einzusetzen, wenn vorher alle notwendigen Programme installiert wurden. Wir nehmen an, dass der betrachtete Laiennutzer nur minimales Wissen bzgl. Kryptographie hat und ihm Begriffe wie beispielsweise Zertifikat und digitale Signatur nicht geläufig sind. Der CW wurde von zwei Experten für PGP und S/MIME jeweils getrennt durchgeführt. Dabei waren die Ergebnisse des jeweils anderen Experten nicht sichtbar.

3.1 Kriterien und Setup

Die im Folgenden genannten Kriterien dienen dazu die in Unterkapitel 3.3 beschriebenen Aufgaben und deren Lösbarkeit aus Sicht der Laiennutzer zu bewerten. Als Bewertungskriterien wurden vier Kriterien in Anlehnung an (Wharton, 1994) mit Fokus auf Usability und Menüführung sowie zwei zusätzliche Kriterien, K5 und K6, definiert:

- K1: Wird der Nutzer probieren, seine E-Mails zu schützen?
- K2: Erkennt der Nutzer, dass die Möglichkeiten vorhanden sind?
- K3: Verbindet der Nutzer die korrekte Handlung mit dem erzielten Effekt?
- K4: Erhält der Nutzer Feedback über den Fortschritt/den Erfolg seiner Handlung?
- K5: Kann der Nutzer die gegebenen Informationen verstehen?
- K6: Kann der Nutzer versehentlich unsichere Handlungen durchführen?

Der Nutzer verwendet bereits Thunderbird. Die Installation der Programme, die Schlüsselerzeugung (PGP, S/MIME), die Zertifikatsbeantragung (S/MIME) und die Konfiguration bzw. Einbindung der Schlüssel bzw. Zertifikate wurden im Voraus durchgeführt. Dies sind die typischen Aufgaben eines Administrators im Unternehmen und bilden somit eine realistische Annahme. Nach der Inbetriebnahme erhalten Nutzer keine weitere Hilfestellung und nur wenig Anleitung.

3.2 Ergebnisse

Im Folgenden wird jeweils zuerst die Aufgabe definiert und im Anschluss daran die Ergebnisse für PGP und S/MIME dargestellt, um die Verfahren bzgl. der unterschiedlichen Kriterien zu bewerten. In der nachfolgenden Tabelle zeigen wir die von Thunderbird verwendeten Icons.

Icon Schloss (rotes Kreuz)		Icon gelbes Schloss	
Icon Stift (rotes Kreuz)		Icon Menü S/MIME	
Icon Brief mit rotem Siegel		Icon Brief mit Fragezeichen	
Icon Brief mit Kreuz			

A1) E-Mail an Person verschlüsseln, deren Schlüssel/Zertifikat nicht vorhanden ist

Der Nutzer startet mit dem Verfassen einer E-Mail und gibt die Adresse des Empfängers ein. Diese erscheint, ohne eine Erklärung zu bieten, rot. Thunderbird färbt eine Adresse rot, wenn sie nicht in den gesammelten Adressen enthalten ist.

PGP: In der Menüleiste gibt es das Icon Schloss für Verschlüsselung und das Icon Stift für das Signieren, jeweils mit einem roten Kreuz versehen. Über den Menüpunkt „Enigmail“ kann

man ebenfalls „Nachricht signieren“ und „Nachricht verschlüsseln“ aktivieren. Im vorliegenden Fall wird das rote Kreuz auf dem Verschlüsselungsicon durch einen grünen Haken ersetzt. Erst wenn die Nachricht abgeschickt werden soll, öffnet sich ein Fenster, u. a. mit dem Text „Empfänger nicht gültig, nicht vertrauenswürdig oder nicht gefunden“. Darunter werden alle bekannten Adressen gelistet, deren Schlüssel bereits bekannt sind, in diesem Fall aber nur der des Absenders. Es gibt keinen Hinweis, dass durch Betätigen der Schaltfläche „Fehlende Schlüssel herunterladen“ diese, sofern vorhanden, geladen werden, oder was der Nutzer tun soll. Wenn der Nutzer Schlüssel heruntergeladen und einen ausgewählt hat, werden Schlüsselstärke und Fingerabdruck des Schlüssels in Hexadezimaldarstellung angezeigt. Die anschließende Frage, ob auch der Betreff verschlüsselt werden soll, wird Laien ebenfalls verwirren.

S/MIME: In der Menüleiste gibt es den Punkt „S/MIME“. Es öffnet sich ein Fenster, wenn man „verschlüsseln“ für eine Person, deren Zertifikat noch nicht importiert ist, auswählt: Darin wird der Nutzer darauf hingewiesen, dass der Betreff der E-Mail nie verschlüsselt wird und dass die Verschlüsselung nicht möglich ist. Die einzige Erklärung dafür ist aber „Schlüsselstatus nicht gefunden“.

Fazit: Die Motivation eines Nutzers muss bei beiden Varianten recht hoch sein, um das Problem von nicht gefunden Zertifikaten oder Schlüsseln zu überwinden (K1). Die Möglichkeit des Verschlüsselns ist nur dann erkennbar, wenn das Schloss mit Verschlüsseln assoziiert wird oder der Begriff „S/MIME“ in diesem Zusammenhang bekannt ist (K2). Für Laien ist das Unterfangen nicht zufriedenstellend (K3), da die verfügbaren Informationen vollkommen unzulänglich sind (K5). Und bei beiden Varianten können Laien versehentlich unverschlüsselte E-Mails versenden (K6). Immerhin wird der Erfolg dem Nutzer mitgeteilt (K4).

Dieselben Beobachtungen gelten auch für das Versenden einer verschlüsselten E-Mail an mehrere Personen, von denen man nicht alle Zertifikate besitzt.

A2) E-Mail an Person verschlüsseln, deren Schlüssel/Zertifikat vorhanden ist

Der Nutzer startet mit dem Verfassen einer E-Mail und gibt die Adresse des Empfängers ein. Die Adresse bleibt in schwarzer Schrift.

PGP: Die beiden in A1) beschriebenen Icons zur Verschlüsselung und Signierung sind mit dem roten Kreuz versehen, das beim Auswählen auf einen grünen Haken wechselt.

S/MIME: Findet man hinter dem Menü „S/MIME“ die Möglichkeit der Verschlüsselung, gibt es auch hier keine weiteren Probleme.

Fazit: Nachdem A1) gelöst wurde, sollte der Nutzer alle notwendigen Schritte erlernt haben: Die Verschlüsselungsfunktion ist an der gleichen Stelle wie bei A1), somit bestehen hier keine weiteren Probleme (K2). Die Verschlüsselung ist einfach und schnell zu aktivieren (K1 und K3). Jedoch kann der Nutzer, von den schwachen Änderungen der Icons abgesehen, nicht erkennen, ob die Nachricht verschlüsselt wurde (K4 & K5). Es kann leicht passieren eine E-Mail versehentlich unverschlüsselt zu senden (K6).

A3) Verschlüsselt empfangene E-Mail entschlüsseln/lesen

Wenn die E-Mail mit dem korrekten Schlüssel verschlüsselt wurde, ist dies am Symbol des gelben Schlosses erkennbar.

PGP: Zusätzlich gibt es eine graue Statusleiste am oberen Rand mit der Schrift „Enigmail Entschlüsselte Nachricht“. Beide Merkmale sind relativ unauffällig.

S/MIME: Klickt man auf das Symbol gelbes Schloss, wird man darüber informiert, dass (bzw. ob) die E-Mail verschlüsselt (und signiert) ist mit einer kurzen, umgangssprachlichen Erläuterung, was Verschlüsselung (Nachricht kann nicht von Dritten gelesen werden) bedeute.

Fazit: Die Entschlüsselung ist mit beiden Varianten unproblematisch, automatisch und erfordert keinen erhöhten Aufwand (K1, K2 & K3). Sofern sich der Nutzer weitere Informationen über den Verschlüsselungsstatus der empfangenen Nachricht anzeigen lassen möchte, ist dies mit einem Klick möglich. Dies ist jedoch leicht zu übersehen. Für S/MIME wird erklärt, welchen Effekt diese Verschlüsselung hat, für PGP nicht (K4 & K5). Kriterium K6 ist bei der Aufgabe nicht relevant.

A4) Eine E-Mail digital signiert versenden

PGP: Wie beim Verschlüsseln von Nachrichten wird die digitale Signatur durch Anklicken des Stifticons aktiviert, wonach das rote Kreuz durch einen grünen Haken ersetzt wird. Erkennt der Nutzer den Stift als Zeichen für das digitale Signieren, entstehen hier keine Probleme.

S/MIME: Die Signatur wird hier mit dem Punkt „Nachricht unterschreiben“ im S/MIME-Menü aktiviert. Danach ist dieser mit einem Haken versehen. Zusätzlich erkennt man diese Aktivierung an dem kleinen Icon eines rot versiegelten Umschlags in der rechten unteren Ecke. Klickt man dieses an, informiert das bereits bekannte Fenster den Nutzer, dass die E-Mail signiert (und/oder verschlüsselt) wird.

Fazit: Nachdem der Nutzer die Möglichkeit der Signierung gefunden hat, ist diese einfach und schnell zu aktivieren (K1). Das Erkennen ist eine einmalige kleine Herausforderung, die sich danach nicht wiederholt (K2 & K3). Die Informationen über den Signierungsstatus der empfangenen Nachricht wird nur nach etwas Suchen gefunden (K4 & K5). Ein versehentliches Versenden einer unsignierten E-Mail ist leicht möglich (K6).

A5) Absender einer empfangenen, signierten E-Mail auf Authentizität prüfen

PGP: Korrekte Signaturen werden mit dem Text „Korrekte Signatur von [Absender]“ in einer blauen Statuszeile am Kopf der E-Mail angezeigt. Für den Nutzer ist es nicht nachvollziehbar, wieso ein rot versiegelter oder ein grau versiegelter Umschlag mit einem blauen Fragezeichen erscheint[1]. Auf Klick zeigen beide Schlüsselkennung, Fingerabdruck in Hexadezimaldarstellung sowie die Namen der verwendeten Algorithmen an. Eine Erklärung für die unterschiedlichen Icons gibt es nicht. Entspricht die im Zertifikat eingetragene E-Mailadresse nicht der des Absenders, erscheint ebenfalls das Fragezeichenicon. Das Problem wird nicht erläutert.

S/MIME: Eine Nachricht mit gültiger S/MIME-Signatur wird durch den rot versiegelten Umschlag angezeigt. Bei Anklicken wird man informiert, wer der Absender ist und dass die Nachricht seit dem Versand nicht verändert wurde. Entspricht die im Zertifikat eingetragene E-Mailadresse nicht der des Absenders, wird das Fragezeichenicon angezeigt. Hier wird die Problematik erläutert: Die digitale Signatur sei gültig, man könne aber nicht sicher sein, ob

[1] Enigmail erklärt dieses Verhalten auf https://www.enigmail.net/index.php/en/user-manual/signature-and-encryption

Absender und Unterzeichner dieselbe Person sind. Es wird empfohlen, sich im Unterschriftszertifikat anzusehen, wer die Nachricht unterschrieben hat.

Fazit: Ist die Signatur korrekt erstellt, gibt es keine Probleme (K1). Wenn der Nutzer Interesse daran hat, die Signaturen zu prüfen, wird er diese finden können (K2). Alle anderen Kriterien sind aber nicht erfüllt: Etwaige Fehler oder Fälschungen werden nicht deutlich genug angezeigt und die Informationen sind (bei PGP) ungenügend für das Verständnis (K3 – K5). Dem Nutzer können ohne sein Wissen falsch unterschriebene E-Mails untergeschoben werden (K6).

A6) Integrität einer empfangenen E-Mail verifizieren

PGP: Eine Nachricht mit gültiger PGP-Signatur wird, wie bei A5) beschrieben, durch den versiegelten Umschlag angezeigt. Wurde die E-Mail nachträglich verändert, macht ein gelber Balken mit der Beschreibung „Ungeprüfte Signatur“ im Kopf der E-Mail darauf aufmerksam.

S/MIME: Eine Nachricht mit gültiger S/MIME-Signatur wird auch durch den versiegelten Umschlag signalisiert. Die nachträgliche Veränderung der E-Mail wird nur durch den Umschlag mit rotem Kreuz markiert. Im Erklärungstext wird hingewiesen, dass die Nachricht nach dem Signieren verändert wurde und man der Korrektheit der Inhalte nicht trauen solle.

Fazit: Hier unterscheiden sich die Varianten PGP und S/MIME erheblich, indem Probleme mit der PGP Signatur deutlich angezeigt, aber nicht (verständlich) erläutert werden. Für PGP ist K1 und K2 daher erfüllt, K3 - K6 hingegen nicht. Bei S/MIME dagegen kann man die Probleme leicht übersehen und daher manipulierte E-Mails untergeschoben bekommen. Fällt dem Nutzer der Umschlag mit rotem Kreuz auf, wird dieses gut verständlich erläutert und eine Handlungsempfehlung gegeben. Für S/MIME sind K1, K2 und K6 daher nicht erfüllt. Er kann aber nach sorgfältigem Hinsehen selbstständig weitere Schritte unternehmen (K3 – K5).

4 Pilotstudie

Um einen ersten Eindruck für unsere Ergebnisse aus Kapitel 3 zu bekommen, baten wir eine Kollegin (Laie) dieselben Aufgaben durchzuführen und ihre Intentionen und Überlegungen laut zu äußern. Sie verwendet Thunderbird beruflich seit einiger Zeit und kennt E-Mailverschlüsselungen und -signaturen. Ihr wurde erklärt, dass Verschlüsselung das Mitlesen von E-Mails verhindern kann und mit digitalen Signaturen die Authentizität und Integrität (für sie in anderen Worten ausgedrückt) sichern kann.

Wir können im Rahmen dieser Publikation nur eine Kurzzusammenfassung der Ergebnisse darstellen. Die Kernerkenntnisse aus dieser Pilotstudie sind, dass die Notwendigkeit von Schlüsseln unbekannt und nicht von Interesse ist. Aus diesem Grund war ihre einzige Schwierigkeit auch das Versenden verschlüsselter E-Mails an Personen, deren Schlüssel/Zertifikate sie noch nicht hatte (s. A1). Bei PGP erkannte sie, dass es mit der Signatur Probleme gab, verstand diese bzw. deren Lösung aber nicht. Bei S/MIME erkannte sie die Signaturprobleme nicht. Erläuternde Texte las sie nur nach Aufforderung und stellte dann fest „Versteh ich nicht, ist ja auch egal“. Sie verwendete alle Menüs und Icons intuitiv, schnell und zügig. Nach eigener Aussage führte sie aber nur die Aufgaben aus und verstand nicht, welche Effekte diese haben. Dies bestätigt unsere Eindrücke vom Cognitive Walkthrough.

5 Diskussion und Verbesserungsvorschläge

Es wurde durch zwei CVs und eine Pilotstudie untersucht, ob S/MIME oder PGP in Thunderbird inzwischen im Alltag durch Laien nutzbar sind. Es ist ersichtlich, dass Signieren mit bereits eingerichteten Zertifikaten/Schlüsseln und das Verschlüsseln von E-Mails an oft kontaktierte Personen (A2 - A6) keine Probleme darstellen. Dies liegt in erster Linie daran, dass man zum „Knöpfe drücken“ (laut unserer Pilotstudie) keinerlei Verständnis für die darunterliegenden Mechanismen benötigt. Wenn erforderliche Aktionen zur Erreichung der Ziele *A1) verschlüsseltes Schreiben ohne bereits vorhandenes Zertifikat, A5) Überprüfen der Authentizität des Absenders, bzw. der A6) Integrität der Nachricht* das Anklicken von Icons übersteigen, sind Laien überfordert, da grundlegende technische Kenntnisse fehlen. Daher müsste es die Möglichkeit geben, diese Funktionen auch ohne dieses Wissen zu nutzen.

Laien bringen nicht nur wenig Wissen mit, sie können und wollen im Gegensatz zu Experten oft nicht alle Details verstehen. Sie begnügen sich mit der Zusicherung, alles sei sicher. Technische Fachbegriffe helfen nicht, lang umschreibende Texte möchte niemand im Alltag lesen (siehe Pilotstudie). Daher liegt es nahe, zwei unterschiedliche Modi anzubieten. Im Expertenmodus könnten dann alle Informationen gut sichtbar aufrufbar angeboten werden: Status *signiert*, *verschlüsselt*, Schlüssel-ID, Signatur-Fingerprint, etc. Für Laien dagegen automatisiert man so viel wie möglich: Signieren und Verschlüsseln ist standardmäßig aktiviert, im Hintergrund werden fehlende Schlüssel/Zertifikate heruntergeladen, E-Mails entschlüsselt und Signaturen überprüft. Wenn es Probleme mit einer Signatur gibt, wird aber deutlich darauf hingewiesen, das Problem mit einfachen Worten erklärt und Handlungsempfehlungen gegeben. Ist keine Verschlüsselung möglich, wird der Nutzer ebenfalls darauf hingewiesen und aufgeklärt, dass andere die E-Mail prinzipiell mitlesen können. Es wird aber nicht als Problem dargestellt.

Danksagung

Die in diesem Paper beschriebene Forschung wurde vom Bundesministerium für Bildung und Forschung (BMBF) und dem Hessischen Ministerium für Wissenschaft und Kunst innerhalb des Projekts CRISP (www.crisp-da.de/) gefördert.

Literaturverzeichnis

Benenson, Z. e. (2015). Maybe poor Johnny really cannot encrypt: The case for a complexity theory for usable security. *New Security Paradigms Workshop*. ACM.

Convios Consulting. (03 2017). Datenschutz und Verschlüsselung. *Repräsentative Umfrage im Auftrag von WEB.DE und GMX*. Convios Consulting. Abgerufen am 01. 06 2018 von http://docs.dpaq.de/12305-convios-datenschutz-2017-final.pdf

Ferreira, L., & Anacleto, J. (2017). Usability in Solutions of Secure Email – A Tools Review. *Human Aspects of Information Security, Privacy and Trust* (S. 57-73). Springer.

Lerner, A., Zeng, E., & Roesner, F. (2017). Confidante: Usable encrypted email: A case study with lawyers and journalists. *Security and Privacy*. IEEE.

Moecke, C. T., & Volkamer, M. (2013). Usable secure email communications: criteria and evaluation of existing approaches. *Information Management & Computer Security21.1*, S. 41-52.

Naiakshina, A., Danilova, A., Dechand, S., Krol, K., Sasse, M. A., & Smith, M. (2016). Poster: Mental Models – User understanding of messaging and encryption. *European Symposium on Security and Privacy.* IEEE.

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? *International Symposium on Privacy Enhancing Technologies Symposium.* Cham: Springer.

Ruoti, S. e. (2016). we're on the same page: A usability study of secure email using pairs of novice users. *Conference on Human Factors in Computing Systems.* ACM.

Schochlow, V. e. (2016). Bewertung der GMX/Mailvelope-Ende-zu-Ende-Verschlüsselung. *Datenschutz und Datensicherheit-DuD 40.5*, (S. 295-299).

TeleTrusT – Bundesverband IT-Sicherheit e.V. (15. 05 2018). *E-Mail-Verschlüsselung bleibt sicher - Angriff auf PGP- und S/MIME-Verschlüsselung nutzt Schwachstellen in E-Mail-Clients*. Von E-Mail-Verschlüsselung bleibt sicher - Angriff auf PGP- und S/MIME-Verschlüsselung nutzt Schwachstellen in E-Mail-Clients: https://www.teletrust.de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=1125&cHash=69758a095d6e222e80b9bd7121a4ae6d abgerufen

The Radicati Group. (2018). Prognose zur Anzahl der Nutzer von E-Mails weltweit in den Jahren 2018 bis 2022 (in Milliarden). Statista - Das Statistik-Portal. Abgerufen am 01. 06 2018 von https://de.statista.com/statistik/daten/studie/422274/umfrage/prognose-zur-anzahl-der-nutzer-von-e-mails-weltweit/

Wharton, C. e. (1994). *The cognitive walkthrough method: A practi-tioner's guide. In Usability inspection methods.* John Wiley & Sons, Inc.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can'T Encrypt: A Usability Evaluation of PGP 5.0. *USENIX Security Symposium - Volume 8* (S. 14). Washington, D.C.: USENIX Association.

Zimmermann, V., & Henhapl, B. (2017). Ende-zu-Ende sichere E-Mail-Kommunikation. *Datenschutz und Datensicherheit - DuD 41.5*, (S. 308-313).

Zimmermann, V., Henhapl, B., Gerber, N., & Enzmann, M. (2017). Promoting Secure Email Communication and Authentication. *Mensch & Computer 2017.* Regensburg: Gesellschaft für Informatik.

Autoren

Wenn Sie Fragen zur Einreichung Ihrer Beiträge haben, wenden Sie sich an die Organisatoren.

Gerber, Nina

Nina Gerber studierte Psychologie an der Technischen Universität Darmstadt. Seit 2018 ist sie als wissenschaftliche Mitarbeiterin in der Forschungsgruppe SECUSO am Karlsruher Institut für Technologie tätig. Ihre Forschungsinteressen liegen hauptsächlich im Bereich der Mensch-Maschine-Interaktion. In mehreren Projekten beschäftigt sie sich aktuell damit, wie Nutzer im Technikkontext mit privatsphäre-kritischen Daten umgehen.

Ghiglieri, Marco

Marco Ghiglieri ist seit Juni 2011 wissenschaftlicher Mitarbeiter an der Technischen Universität Darmstadt. Er arbeitet derzeit im Projekt CRISP mit Schwerpunkt E-Mail-Sicherheit. Seine Promotion drehte sich um Smart-TVs und deren Risiken für Endanwender. Vor der jetzigen Anstellung war er Berater in einem international tätigen IT-Beratungsunternehmen mit Fokus auf IT-Sicherheit. Dort hat er große Konzerne und auch mittelständige Unternehmen beraten.

Henhapl, Birgit

Birgit Henhapl ist seit November 2016 Postdoktorandin in der Arbeitsgruppe von Prof. Dr. Melanie Volkamer an der Technische Universität Darmstadt. Sie ist Mitglied im CRISP - Delegated Privacy and Security Settings Projekt. Ihren PhD erhielt sie für ihre Arbeit "On the Efficiency of Elliptic Curve Cryptography" von der Technischen Universität Darmstadt im November 2003 bei Prof. Dr. Johannes Buchmann. Vor ihrer jetzigen Anstellung arbeitete sie als Beraterin für Informationssicherheit und als Auditorin für PCI DSS in der usd AG.