Erstellung eines Erklärvideos zur Verwendung von S/MIME (WIP)

Fabian Lucas Ballreich
fabian.ballreich@kit.edu
Karlsruher Institut für Technologie
Karlsruhe, Germany

Melanie Volkamer
melanie.volkamer@kit.edu
Karlsruhe Institut für Technologie
Karlsruhe, Germany

Figure 1: Standbild aus dem Videoentwurf zum Zeitpunkt der Erstellung der Arbeit

Abstract

Die Kommunikation mittels E-Mail spielt trotz der Verfügbarkeit anderer Nachrichtensysteme nach wie vor eine wesentliche Rolle im Alltag vieler Organisationen. Allerdings gibt es hierbei einige konzeptbedingte Sicherheitsprobleme. Die S/MIME-Technologie bietet als Sicherheitserweiterung eine Möglichkeit, die Schutzziele Vertraulichkeit und Integrität durch Verschlüsselung und Signierung zu erreichen. Diese Arbeit beschreibt die iterative Entwicklung und Evaluation eines Erklärvideos für die Verwendung von S/MIME-Zertifikaten an einer deutschen Universität. Dabei werden die Grundlagen, Entwurfsentscheidungen und der Entwicklungsprozess thematisiert sowie die Inhalte des Videos beschrieben. Es handelt es sich um *work in progress*. Der Inhalt bezieht sich auf den Stand Anfang Juni 2024.

Mensch und Computer 2024 – Workshopband, Gesellschaft für Informatik e.V., 01.-04. September 2024, Karlsruhe, Germany

https://doi.org/10.18420/muc2024-mci-ws17-152

Keywords

E-Mail-Sicherheit, S/MIME, Verschlüsselung, Signierung

1 Einleitung

Die E-Mail bleibt trotz der Verfügbarkeit vieler neuartiger Kommunikationsdienste in zahlreichen Organisationen wie Universitäten, Forschungseinrichtungen und Unternehmen weiterhin von großer Bedeutung. Insbesondere an Universitäten, die oft sehr große Einrichtungen mit einer heterogenen IT-Landschaft darstellen, ist dies der Fall. Diese Heterogenität kann beispielsweise aus der Eigenverwaltung von einzelnen Organisationseinheiten wie beispielsweise Instituten entstehen. Eine Besonderheit ist, dass man an Universitäten häufig eine Nutzerschaft vorfindet, deren technische Expertise von Experten, über reine Anwender bis hin zu Laien reicht. Zwar können innerhalb einzelner Organisationseinheiten verschiedene andere Kommunikationskanäle verwendet werden, dennoch basiert die Kommunikation zwischen den Einheiten oder beispielsweise gegenüber Studierenden überwiegend auf E-Mails. Bei der Interaktion mit Studierenden werden hierbei häufig sehr sensible Informationen wie zur Anerkennungen von erbrachten

Leistungen, zu Problemen mit Noten, der Prüfungsan- und abmeldungen sowie Atteste ausgetauscht.

E-Mails haben konzeptbedingt grundlegende Sicherheitsprobleme, insbesondere hinsichtlich der Zusicherung von Schutzzielen wie Integrität und Vertraulichkeit. Um diese Probleme zu adressieren, existieren verschiedene Sicherheitserweiterungen wie beispielsweise die Secure Multipurpose Internet Mail Extension (S/MIME). Eine entscheidende Frage in diesem Zusammenhang ist, welche Schutzziele in einer Organisation überhaupt erforderlich oder gewünscht sind. In großen Organisationen mit lokalen Mail-Servern verlassen interne E-Mails beispielsweise niemals die eigene IT-Infrastruktur und durchlaufen daher keine externen Übertragungspunkte. Das Schutzziel der Vertraulichkeit kann folglich - abhängig von den getroffenen Annahmen - bereits ohne weitere Maßnahmen ausreichend gewährleistet sein, wodurch der Fokus auf Integrität gelegt werden sollte.

Das Ziel dieser Arbeit ist die iterative Konzeption, Entwicklung und Erstellung eines Erklärvideos zur Verwendung von S/MIME an einer deutschen Universität und die Evaluation dieses Videos mit Angehörigen der Universität. Das Video soll im Anschluss im Rahmen von Security Awareness Maßnahmen für Angehörige der Universität regulär eingesetzt werden.

Bei dieser Arbeit handelt es sich um *work in progress*. Der Inhalt bezieht sich auf den Stand Anfang Juni 2024.

2 Technische Grundlagen

Im folgenden werden die Grundlagen der E-Mail Kommunikation sowie die konzeptbedingten Sicherheitsprobleme beschrieben. Im Anschluss wird die S/MIME-Technologie eingeführt und deren Schutzmöglichkeiten erläutert.

2.1 E-Mail Technologie

Innerhalb des E-Mail-Dienstes hat jeder Teilnehmender eine individuelle Adresse, die aus einem lokalen Teil (vor dem @-Zeichen) und einem domainbezogenen Teil (nach dem @-Zeichen) besteht. Der domainbezogene Teil muss auf eine gültige Domain verweisen, die über das Domain Name System (DNS) aufgelöst werden kann. Der lokale Teil einer E-Mail-Adresse beeinflusst die Übertragung der Nachricht über das Internet nicht und kann vom Server des Empfängers beliebig verarbeitet werden. Er dient in der Regel zur Unterscheidung und Verteilung auf die jeweiligen Empfängerpostfächer.[5, S. 375-376]

Versand, Transport und Empfang einer E-Mail basieren auf den folgenden Hauptkomponenten: Mail User Agents (MUA) erstellen die E-Mail im geeigneten Format, bereiten den Versand vor und sind im Mail-Client des Absenders integriert. Mail Transfer Agents (MTA) haben als Übertragungspunkte die Aufgabe, eine Nachricht über das Internet in Richtung des Empfängers weiterzureichen und finden sich in der Regel in Gestalt von Mail-Servern wieder. Das Simple Mail Transfer Protocol (SMTP) dient als Netzwerkprotokoll der Einspeisung und Weitervermittlung von E-Mail-Nachrichten über Rechnernetze hinweg. Das Post Office Protocol Version 3 (POP3) und das Internet Message Access Protocol (IMAP) dienen dem Abruf einer Nachricht aus dem Postfach durch den Mail-Client des Empfängers. Bei POP3 werden die E-Mails hierbei vom Server heruntergeladen, wohingegen sie bei IMAP auf dem Server verbleiben und dort verwaltet werden.[5, S. 375-376]

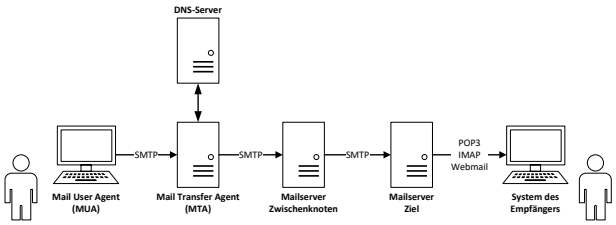

Figure 2: Vereinfachter Prozess des Versands einer E-Mail.

2.2 Erfüllung von Schutzzielen bei der Übertragung

Nachrichten werden bei SMTP standardmäßig unverschlüsselt übertragen, wodurch für die Inhalte das Schutzziel der Vertraulichkeit nicht gewährleistet ist. Weiterhin werden Nachrichten konzeptbedingt auf den beteiligten Übertragungspunkten offen zwischengespeichert, wodurch die Verletzung des Schutzziels bei nicht ordnungsgemäßer Löschung nach der Übertragung noch verstärkt wird. Ebenfalls stellt SMTP keinen ausreichenden Integriätsschutz sicher, weswegen ein Angreifer beispielsweise den Inhalt einer Nachricht oder Teile des Headers unerkannt verändern kann. Unter anderem aus diesem Grund kann auch die Authentizität des Absenders nicht gewährleistet werden, da ein Angreifer mittels Mail-Spoofing beliebige Absenderadressen eintragen kann. Derartige Maskierungsangriffe sind sowohl während der Übertragung als auch direkt durch den Angreifer als Absender möglich.[3, S. 146-147]

2.3 Einsatz von Sicherheitserweiterungen

SMTP, POP3 und IMAP basieren auf TCP als Transportprotokoll, wodurch in jedem Fall die Absicherung mittels Transport Layer Security (TLS) möglich ist. Eine gesicherte TLS-Verbindung mittels SMTP wird in Abbildung 3 vereinfacht dargestellt. Im Gegensatz zu POP3 und IMAP bietet SMTP durch TLS aber nur begrenzten Schutz der Vertraulichkeit. Dies liegt daran, dass ein Client zwar die Sicherheit der Verbindung zum eigenen Mailserver, aber nicht die Absicherung zwischen den nachfolgenden Übertragungspunkten beeinflussen kann. Zudem ist die Absicherung der nachfolgenden Verbindung für den Client nicht unmittelbar erkenn- und beurteilbar.[5, S. 422]

Neben den genannten Erweiterungen zu den verwendeten Protokollen existieren mit DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF) und Domain based Message Authentication, Reporting and Conformance (DMARC) verschiedene weitere Ansätze zur Stärkung von Schutzzielen bei der E-Mail Kommunikation, auf die an dieser Stelle jedoch nicht weiter eingegangen wird.

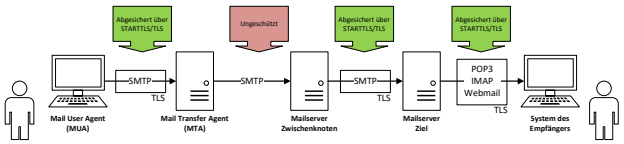

Figure 3: Begrenzte Schutzwirkung durch TLS bei SMTP-Verbindungen

2.4 Ende-zu-Ende-Absicherung

Für die Ende-zu-Ende-Absicherung der E-Mail-Kommunikation existieren mit OpenPGP und S/MIME zwei grundsätzlich unterschiedliche Ansätze, wobei im folgenden lediglich S/MIME thematisiert wird.

Secure Multipurpose Internet Mail Extensions (S/MIME) ist als Sicherheitserweiterung zum MIME-Standard mit Fokus auf Verschlüsselung und Signierung von E-Mails entwickelt worden und basiert auf einem hybriden Verfahren zur Nachrichtenverschlüsselung.[5, S. 373] Der Inhalt wird mittels symmetrischem Sitzungsschlüssel verschlüsselt, wobei auch nur einzelne MIME-Datenobjekte gesichert werden können. Der Sitzungsschlüssel wird anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und der Nachricht beigefügt.[5, S. 393]

S/MIME erscheint gut geeignet zu sein, zukünftig der dominante Standard zur Absicherung der E-Mail Kommunikation zu sein. Gründe hierfür sind die Integration in zahlreiche kommerziellen und freien Anwendungen sowie die Möglichkeit, beliebige Inhalte (als MIME-Datenobjekte) zu verschlüsseln und zu signieren.[3, S. 806] Weiterhin ermöglicht S/MIME one-pass-processing, da alle zur Bearbeitung benötigten Daten direkt in einer gesicherten E-Mail integriert sind.[3, S. 801]

S/MIME basiert auf dem Vertrauensmodell einer hierarchischen Zertifizierungsinfrastruktur, wobei die Authentizität eines öffentlichen Schlüssels anhand von X.509-Nutzerzertifikaten zugesichert wird.[3, S. 805-806] Die Certification Authority (CA) erstellt hierbei als Zertifizierungsstelle die Zertifikate und widerruft diese im Bedarfsfall. Verschiedene Zertifizierungsstellen können hierarchisch angeordnet sein, wobei die höchste als Root-CA bezeichnet wird und als Vertrauensanker dient. Die Registration Authority (RA) prüft als Registrierungsstelle die Verbindung zwischen öffentlichem Schlüssel und eindeutigen Identitätsmerkmalen (z.B. Name, Organisation, E-Mail Adresse) des Antragstellers und bestätigt diese gegenüber der CA. Eine Certification Policy umfasst hierbei als Zertifikatsrichtlinie alle Regeln, nach denen eine CA Zertifikate ausstellen und verwalten kann sowie Maßnahmen zum sicheren Betrieb der CA-Infrastruktur. Die Certificate Revocation List (CRL) dient als Sperrliste für - beispielsweise wegen Kompromittierung - widerrufene Zertifikate und kann über verschiedene Verfahren abgefragt werden. Die Validierung eines S/MIME-Zertifikats erfolgt ausgehend vom fraglichen Zertifikat entlang der Vertrauenskette bis zur jeweiligen Root-CA, wobei jedes Zertifikat einzeln auf Gültigkeit geprüft werden muss.[3, S. 404]

Das Schlüsselmanagement kann bei S/MIME allein über E-Mails abgewickelt werden, wenn initial eine signierte und unverschlüsselte Nachricht versendet wird. Das System des Empfängers kann hierdurch automatisch eine Zertifikatsdatenbank der persönlichen Kontakte erstellen. Alternativ ist es, beispielsweise in größeren Organisationen möglich, Zertifikate von zentralen Verzeichnisdiensten (z.B. LDAP) bei Bedarf nachzuladen. Weiterhin existieren Ansätze, Zertifikate in Rahmen einer DNSSEC-Abfrage[1] abrufbar zu machen. [5, S. 403-404]

Ende-zu-Ende-Verschlüsselung hat konzeptbedingt den Nachteil, dass verschlüsselte Nachrichten durch Sicherheitsanwendungen inhaltlich nicht auf Schadsoftware, Phishing oder andere Angriffe geprüft werden können. Dieses Problem kann beispielsweise mit E-Mail Gateway Lösungen adressiert werden, bei denen E-Mails durch eine zentrale Komponente entschlüsselt, geprüft und wieder verschlüsselt werden. Beim Einsatz derartiger Lösungen ergibt sich jedoch wiederum ein Risiko für den Absender beziehungsweise Empfänger, dessen Privatsphäre hierdurch beeinträchtigt wird.[5, S. 392]

3 Literatur

Zur Erklärung der Konzepte von Verschlüsselung und Signierung wurden von Forschenden verschiedene Metaphern für unterschiedliche Zwecke vorgeschlagen und evaluiert. Häufig fanden diese Untersuchungen beispielsweise im Kontext der Gestaltung von Benutzeroberflächen von Mail-Clients statt. In 2005 untersuchten Roth et al.[4] allgemeine menschliche Einflussfaktoren bei der Absicherung von E-Mail Kommunikation. In diesem Zusammenhang wurde der Vorschlag einer Metapher mit Postkarte und Briefumschlag formuliert, mit Interviews evaluiert und im Ergebnis als gut geeignet bewertet, um den Sachverhalt der Verschlüsselung zu vermitteln. Bai et al.[1] machten den Vorschlag, ein Vorhängeschloss und den zugehörigen Schlüssel als Metapher für den privaten und öffentlichen Schlüssel zu verwenden, wohingegen Tong et al.[6] historische Bilder wie das einer verschlossenen Schatztruhe wählten. Lausch et al. untersuchten in 2017 existierende Indikatoren, die im Kontext von E-Mail Verschlüsselung verwendet werden. Hierbei wurde der Vergleich eines Vorhängeschlosses mit zugehörigem Schlüssel kritisch bewertet, da ein normales Schloss mit dem selben Schlüssel ver- und aufgeschlossen werden kann. Dies steht gerade dem Prinzip asymmetrischer Verschlüsselung entgegen und kann somit Anwender verwirren oder sogar falsche mentale Modelle fördern. Die Forschenden sprechen sich unter Anderem aus dem Grund für die Verwendung der Metapher eines analogen Briefumschlages aus, da zwischen diesem und der elektronischen Mail ein direkt vergleichbarer Anwendungsbezug besteht. Delgado Rodriguez et al. [2] leiten aus Interviews verschiedene Symbole und Metaphern für Privacy und Security bezogene Themen ab und schlagen eine Kategorisierung vor, die beispielsweise Entwicklern als Grundlage dienen kann. Im Bereich der Authentifizierung wird hier beispielsweise der Fingerabdruck oder eine händische Unterschrift als Metapher vorgeschlagen. Tong et al.[6] schlagen für Signaturen das Bild eines Stempels und Kopien von Stempelabdrücken vor. Analog hierzu kann auch die Metapher Siegel und Siegelabdruck gewählt werden.

[1] Domain Name System Security Extensions als Sicherheitserweiterung zu DNS

4 Konzeption und Implementierung

In diesem Kapitel werden Grundlagen und Annahmen sowie der eingesetzte Entwicklungsprozess beschrieben. Im Anschluss werden einzelne Entwurfsentscheidungen erläutert und der Aufbau des Videos vorgestellt.

4.1 Grundlagen und Annahmen

Die Universität, bei der das Video eingesetzt werden soll, stellt allen Angehörigen individuelle E-Mail-Konten zur Verfügung, womit neben Mitarbeitern, auch Gäste, Partner und Studierende eingeschlossen sind. Interne E-Mails werden ausschließlich über lokal betriebene Mail-Server versendet, wodurch sie das interne Netzwerk nie verlassen und somit nicht über externe Übertragungswege geleitet werden. Es wird angenommmen, dass die Infrastruktur der Universität nicht kompromittiert ist und es keine internen Angreifer gibt. Die Universität betreibt eine eigene Zertifizierungsstelle, die unterhalb von *GÉANT*[2] *Trusted Certificate Services* angesiedelt ist und unter Anderem die Ausstellung von S/MIME-Zertifikaten ermöglicht. Die Beantragung der Zertifikate erfolgt über ein Online-Portal, wobei für die Authentifizierung gegenüber der Zertifizierungsstelle auf die Nutzerkonten der Angehörigen zurückgegriffen wird. Der Prozess ist daher vollständig digital und im Rahmen der Universität beliebig skalierbar. Aktuell gibt es an der Universität keine einheitliche oder verbindliche Vorgaben bezüglich des Verwendens von S/MIME zur Absicherung der Kommunikation.

4.2 Entwicklungsprozess

Zur Entwicklung des Videos wurden ein iterativer Prozess eingesetzt, bei dem verschiedene Stellen der Universität einbezogen wurden. Forschende aus dem Bereichen Informationssicherheit trugen ihr Fachwissen bei, um den Inhalte korrekt und wissenschaftlich fundiert zu gestalten. Hierbei wurde eng mit dem Informationssicherheitsbeauftragten der Universität kooperiert. Durch die Einbeziehung von Mitarbeitern der Verwaltung (insb. Mitarbeiter des Rechenzentrums, des Computernotfallteams und des IT-Sicherheitsmanagements) wurde sichergestellt, dass organisatorische Aspekte berücksichtigt wurden. Zur Bearbeitung des Skripts und für die grafische Umsetzung des Videos wurde ein externer Dienstleister beauftragt.

Der Entwicklungsprozess gliedert sich in mehrere Schritte. Zunächst wurden die geplanten Grundinhalte formuliert und anschließend in mehreren Iterationsschritten überarbeitet. Diese Überarbeitungen umfassten sowohl die Skriptentwürfe (Sprechertext), als auch hierauf aufbauend die Entwürfe zur Bildbeschreibung (Videoinhalt). Der Entwurf des Videos (Kombination Sprechertext mit Videoinhalt) durchlief eine Feedbackschleife, um sicherzustellen, dass alle relevanten Aspekte berücksichtigt und die Inhalte korrekt und verständlich dargestellt wurden.

Im weiteren Verlauf sind hierzu zusätzliche Feedbackschleifen geplant, die zum gegenwärtigen Zeitpunkt noch nicht begonnen wurden. Zur Begleitung von Security Awareness Maßnahmen wurden an der Universität eine Mailingliste eingerichtet, für die sich interessierte Angehörige freiwillig registrieren können und über die Evaluationen bzw. die Sammlung von Feedback möglich ist. Derzeit sind rund 30 Angehörige aus verschiedenen Bereichen der Universität hierfür registriert. Es ist geplant, diese Mailingliste zur Durchführung einer Feedbackschleife zu verwenden.

[2] Zusammenschluss der europäischen nationalen Forschungs- und Bildungsnetze

4.3 Entwurfsentscheidungen

4.3.1 Fokus auf Signierung. Die Universität betreibt, wie viele andere große Organisation, ihre eigenen lokalen Mailserver. Die interne Kommunikation zwischen den verschiedenen Gruppen von Angehörigen (z.B. zwischen Studierenden und Lehrenden oder Beschäftigten und Verwaltung) macht einen großen Teil der Gesamtkommunikation aus und muss daher in den Fokus genommen werden. Da interne E-Mails niemals die organisationseigene Infrastruktur verlassen, wird die Verschlüsselung im Vergleich zur Signierung als weniger relevant angesehen. Vielmehr ist es in allen Fällen entscheidend, eine Möglichkeit zur haben, die Integrität des Inhaltes und die Authentizität des Absender aller eingehenden E-Mails prüfen zu können. In diesem Zusammenhang erweist sich die Signierung mittels S/MIME als äußerst hilfreich und wichtig, da sie Informationen darüber liefert, ob eine E-Mail tatsächlich vom angegebenen Absender stammt und ob der Inhalt manipuliert wurde. Ein entscheidender Vorteil der Signierung im Vergleich zur Verschlüsselung besteht darin, dass der Empfänger, unabhängig davon, ob er intern oder extern ist, kein eigenes S/MIME-Zertifikat besitzen muss. Das Zertifikat des Absenders genügt. Dies bedeutet, dass jeder sich dafür entscheiden kann, alle E-Mails in Zukunft zu signieren, ohne Nachteile zu erwarten. Durch einen flächendeckenden Einsatz von Signierung lässt sich bereits relativ viel erreichen und das Sicherheitsniveau innerhalb der Organisation steigern. Das Video thematisiert zwar beide Themen Verschlüsselung und Signierung mit ihren jeweiligen Auswirkungen, legt den Fokus aus den genannten Erwägungen jedoch auf Signierung.

4.3.2 Einbettung in Zusatzmaterialien. Das Video soll nicht isoliert stehen, sondern durch geeignete Zusatzmaterialien unterstützt werden. Konkret behandelt das Video die Sicherheitsprobleme von E-Mail Kommunikation und beschreibt Verschlüsselung und Signierung mittels S/MIME als eine mögliche Lösung. Dabei bleibt das Niveau abstrakt, ohne beispielsweise echte E-Mail-Clients zu zeigen und deutet entsprechende Benutzeroberflächen lediglich an. Informationen zur konkreten Beantragung oder dem Backup von Zertifikaten und Schlüsselpaar sowie zur Einrichtung in verschiedenen Clients werden auf anderem Weg - beispielsweise als Schritt-für-Schritt-Anleitungen - bereitgestellt. Diese Informationen sind nur dann hilfreich, wenn sie sehr detailliert sind und auf jedes verwendete Betriebssystem und jeden E-Mail-Client eingehen. Auch der Aspekt der Aktualisierung und Wartbarkeit muss berücksichtigt werden, da die Benutzeroberflächen von Clients regelmäßig angepasst werden oder es zu Veränderung beim Prozess der Zertifizierungsstelle kommen kann. Aus diesen Gründen eignen sich schriftliche Anleitungen besser im Vergleich zu Videos, deren Änderung mit einem hohen Zeit- und Kostenaufwand verbunden ist. Detailinformationen zur Kryptografie und ihrer Funktionsweise werden ebenfalls nicht im Video behandelt. Stattdessen wird auf weiterführende Informationsquellen verlinkt, für diejenigen, die sich für dieses Thema vertieft interessieren. Ein detailliertes Eingehen darauf würde den Umfang des Videos sowie der Zusatzmaterialien übersteigen. Eingefasst werden die unterschiedlichen Materialien durch die Bereitstellung einer zentralen Ansprechstelle

(Service Desk) für weitergehende Fragen oder Probleme. Aufgrund dieser Gliederung könnte das Video unverändert auch in einer anderen Organisation verwendet werden und müsste lediglich mit unterschiedlichen Zusatzmaterialien ergänzt werden.

4.3.3 Wahl von Metaphern. Zur Verbesserung der Verständlichkeit soll das Video die Themengebiete Signierung und Verschlüsselung anhand von bildlichen Metaphern erklären. Zunächst wurde eine Recherche durchgeführt, um festzustellen, welche Metaphern und Bilder für Verschlüsselung und Signierung verwendet werden könnten. Dabei wurden sowohl etablierte und häufig verwendete als auch neuere Vorschläge berücksichtigt. Trotz der erkannten Nachteile wurde sich letztendlich für die Nutzung etablierter Metaphern entschieden. Ein Beispiel für eine verwendete Metapher ist das "Siegel" als Repräsentation für Signierung: Hierbei wird veranschaulicht, dass nur der Inhaber eines Siegelstempels ein Siegel erstellen kann. Der Empfänger kann wiederum beurteilen, ob es sich um das authentische Siegel handelt. Allerdings besteht das Problem, dass der Inhalt eines Dokuments mit einem Siegel verändert werden kann, ohne das Siegel zu beschädigen. Insbesondere dann, wenn das Siegel nur unterhalb des Textes angebracht ist, kann die Echtheit des Textes vom Siegelinhaber nicht eindeutig festgestellt werden. Weiterhin kann die Frage gestellt werden, ob ein Dokument mit Siegel heutzutage überhaupt noch einer Alltagsrealität entspricht. Möglicherweise ist eine ungeöffnete Flasche eher vergleichbar. Man kann von Außen erkennen, was sich innerhalb der Flasche befindet, und ebenfalls anhand des Siegels (Kunststoffverschluss, Papierstreifen, etc.) feststellen, ob sie bereits geöffnet wurde. Für die Verschlüsselung wurde die Metapher mit der Unterscheidung zwischen einer Postkarte und einem Umschlag gewählt. Hier wird veranschaulicht, dass der Inhalt und die Metadaten einer Postkarte für jeden sichtbar sind. Sobald der Inhalt jedoch in einem Umschlag verschlossen und dieser beschriftet ist, sind nur noch die Metadaten erkennbar, die für die Zustellung notwendig sind. Diese Metapher funktioniert besonders gut, da sie eine Alltagssituation widerspiegelt. Jedoch besteht ein Problem darin, dass der Schutz, den ein Briefumschlag bietet, nicht mit dem der Verschlüsselung vergleichbar ist. Ein Umschlag kann in der Realität ohne nennenswerten Aufwand leicht geöffnet werden. Insgesamt wurden bekannte Metaphern trotz ihrer Nachteile gewählt, da sie allgemein gebräuchlich sind und ein breiteres Anwendungsspektrum bieten.

4.3.4 Reduktion der Komplexität. Ausgangspunkte für die Gestaltung des Videoinhaltes war die Frage, was Anwendende tatsächlich wissen müssen. Das Thema muss so reduziert werden, dass es verständlich ist, jedoch inhaltlich korrekt dargestellt wird und keine Fehlvorstellungen fördert. Um die eingesetzten Verfahren der Kryptografie umfassend zu beschreiben, müsste man weit ausholen. Dies würde private und öffentliche Schlüssel, deren Zusammenhang, den Einsatz hybrider Verfahren und weitere Aspekte umfassen. Eine oberflächliche Erklärung dieser Themen würde den Sachverhalt jedoch nicht angemessen vermitteln. Beispielsweise benötigt die Erläuterung der CA-Infrastruktur (Certificate Authority) mit einer Root-CA (Root Certificate Authority) einen gewissen Umfang an Text, um korrekt und verständlich zu sein. Für die Anwendenden bringt es jedoch nur einen geringen Mehrwert, wenn sie beispielsweise wissen, dass man die Zertifizierungsstelle prüfen kann, aber nicht erklärt bekommen, wie dies genau funktioniert.

Die Mitglieder einer Universität haben teils sehr unterschiedliche technische Hintergründe – von IT-Experten bis hin zu Laien. Das Video sollte so gestaltet sein, dass es für jeden verständlich ist, ohne zu überfordern oder zu langweilen. Ein weiterer wichtiger Aspekt ist der Kompromiss zwischen Detaillierungsgrad und Aufmerksamkeit des Zuschauers. Hierbei war das Ziel, ein Video mit einer maximalen Dauer von 5 Minuten zu erstellen.

4.4 Aufbau des Videos

Das erstellte Video gliedert sich in vier Abschnitte, die jeweils unterschiedliche Aspekte betrachten und aufeinander aufbauen.

4.4.1 Abschnitt 1: Erklärung des Problems. Der erste Abschnitt dient der Erläuterung des eigentlichen Problems: E-Mails werden trotz zunehmender Bedeutung anderer Dienste noch häufig für die Kommunikation oder den Austausch von zum Teil sensiblen Informationen verwendet. Obwohl sie auf dem Übertragungsweg in der Regel geschützt sind, können E-Mails an den Übertragungspunkten im Klartext eingesehen werden, was ein Problem für die Vertraulichkeit darstellt. Außerdem kann der Empfänger nicht mit Sicherheit feststellen, ob die angegebene Absenderinformation wahr ist oder ob der Inhalt auf dem Übertragungsweg verändert wurde, was die Integrität der E-Mail in Frage stellt.

4.4.2 Abschnitt 2: Einführung von S/MIME. Der zweite Abschnitt verfolgt das Ziel, S/MIME als eine mögliche Lösung für die Probleme der Vertraulichkeit und Integrität vorzustellen und die einzelnen Komponenten sowie den Prozess zu erläutern: Das digitale S/MIME-Zertifikat wird für ein kryptografisches Schlüsselpaar (privater und öffentlicher Schlüssel) von einem Anbieter ausgestellt, was in der Regel nur wenige Sekunden dauert. Mit S/MIME werden der E-Mail Technologie zwei neue Sicherheitsfunktionen hinzugefügt: Signierung und Verschlüsselung. Die Einrichtung des S/MIME-Zertifikats samt Schlüsselpaar kann auf beliebig vielen Geräten bzw. E-Mail-Clients erfolgen. Die Technik zur Verschlüsselung und Signierung arbeitet nach Einrichtung bequem im Hintergrund.

4.4.3 Abschnitt 3: Erläuterung von Signierung. Der dritte Abschnitt des Videos führt das Konzept der Signierung und die hierdurch erreichten Schutzwirkung ein: Die Signierung kann man sich wie das Hinzufügen eines Siegels vorstellen, das aus dem Inhalt der Nachricht und den Absenderinformationen mit dem privaten Schlüssel des Absenders erzeugt wird. Wenn die E-Mail nun auf dem Übertragungsweg verändert wird, ist das Siegel gebrochen und der Empfänger kann feststellen, dass es nicht mehr passt. Das bedeutet, dass eine E-Mail mit gültiger Signatur genauso vom Absender verschickt wurde, der Inhaber des Zertifikats zum verwendenten Schlüssel ist. Obwohl der Inhalt auf dem Übertragungsweg nicht manipuliert wurde, bleibt das Mitlesen und Speichern der Nachricht hiervon unverändert möglich.

4.4.4 Abschnitt 4: Erläuterung von Verschlüsselung. Der vierte Abschnitt geht auf das Konzept der Verschlüsselung und der hierdurch erreichten Schutzwirkung ein: Die Verschlüsselung bei S/MIME basiert auf einem komplexen asymmetrischen Kryptosystem, weswegen hier eine vereinfachte Darstellung gewählt wird. Bei S/MIME verwendet der Absender den öffentlichen Schlüssel des Empfängers zur Verschlüsselung der E-Mail. Diese kann dann nur noch mit dem

zugehörigen privaten Schlüssel durch den Empfänger entschlüsselt werden. Hierdurch wird die E-Mail von einer offen lesbaren Postkarte zu einem geschlossenen Briefumschlag, wodurch das Problem der Vertraulichkeit adressiert wird. Das bedeutet, wenn eine Nachricht verschlüsselt ist, kann sie auf dem Transportweg nicht von Dritten gelesen werden und ist von Ende zu Ende abgesichert. Durch die Kombination von Verschlüsselung und Signierung lassen sich beide genannten Sicherheitsprobleme der E-Mail-Kommunikation adressieren.

5 Diskussion und Ausblick

Im folgenden wird ein kurzer Überblick über die Einschränkungen dieser Arbeit, die Lessons Learned sowie ein Ausblick auf die weiteren Schritte gegeben.

5.1 Einschränkungen

Bei der Entwicklung des Videoskripts wurde aktuell lediglich die Deutsche Sprache berücksichtigt, wodurch die Verwendung im internationalen Umfeld einer Universtität nicht vollständig möglich ist. Nach Abschluss der Entwicklung ist perspektivisch auch eine englischsprachige Version geplant. Das Thema Barrierefreiheit wird durch das Video aktuell nur begrenzt adressiert. Zwar steht der Sprechertext aktuell nicht in Gebärdensprache zur Verfügung, jedoch ist die Bereitstellung einer Version mit Untertiteln geplant. In jedem Fall sollten betroffene Personen zur Schaffung größtmöglicher Barrierefreiheit mit umfangreichen und speziell angepassten Zusatzmaterialien unterstützt werden.

Um die Komplexität zu reduzieren, wurde der Umfang des Inhalts beschränkt. Die gewählten Metaphern für Verschlüsselung und Signierung sind zwar weit verbreitet und etabliert, jedoch bringen sie - wie erläutert - auch Nachteile mit sich. Eine systematische Suche und Evaluation geeigneter alternativer Metaphern wäre daher von großem Nutzen für derartige Vorhaben.

5.2 Lessons Learned

Eine umfassende Beteiligung von Personen aus verschiedenen Bereichen (Forschende, Verwaltung, Techniker, Informationssicherheitsbeauftragter, etc.) ist ausgesprochen sinnvoll, um die Qualität der Ergebnisse wesentlich zu steigern. Beispielsweise können Formulierungen, die für manche Personen selbsterklärend sind, für andere unverständlich sein oder gar falsche Vorstellungen hervorrufen. Weiterhin hat sich die Anwendung eines iterativen Prozesses als sinnvoll dargestellt. Hierbei zeigte sich, dass tendenziell die Durchführung von mehreren kleineren Iterationsschritten gegenüber wenigen großen Schritten vorteilhaft ist. Das Feedback einer oder weniger Personen sollte adressiert werden, bevor der Entwurf weiteren Personen vorgelegt wird, um doppeltes Feedback und damit unnötigen Aufwand für die Personen zu reduzieren. Der Abstraktionsgrad des für Laien komplexen Inhalts muss sorgfältig in Anbetracht der Einsatzumgebung und Zielgruppe gewählt werden. Insbesondere Kryptografie ist ein äußerst umfassendes Thema, das nicht in wenigen Minuten vollständig und korrekt erklärt werden kann. Daher ist eine Reduktion der Komplexität und Länge erforderlich, auch wenn dies eine gewisse Ungenauigkeit mit sich bringt. Hierbei muss beachtet werden, dass formulierte Aussagen dennoch korrekt und für den Anwender nicht irreführend sind.

5.3 Ausblick

Zur Fertigstellung des Videos befinden wir uns derzeit in der Phase des internen Feedbacks zum Videoentwurf. Nach Abschluss ist ebenfalls die Untersuchung der Effektivität geplant. Darüber hinaus sind gegebenenfalls weitergehende Evaluationen möglich.

References

[1] Wei Bai, Moses Namara, Yichen Qian, Patrick Gage Kelley, Michelle L Mazurek, and Doowon Kim. 2016. An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for {Key-Directory} Encryption Systems. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 113–130.

[2] Sarah Delgado Rodriguez, Anh Dao Phuong, Franziska Bumiller, Lukas Mecke, Felix Dietz, Florian Alt, and Mariam Hassib. 2023. Padlock, the Universal Security Symbol?-Exploring Symbols and Metaphors for Privacy and Security. In *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia*. 10–24.

[3] Claudia Eckert. [n. d.]. *Konzepte – Verfahren – Protokolle*. De Gruyter Oldenbourg, Berlin, Boston. https://doi.org/10.1515/9783110985115

[4] Volker Roth, Tobias Straub, and Kai Richter. 2005. Security and usability engineering with particular attention to electronic mail. *International Journal of Human-Computer Studies* 63, 1-2 (2005), 51–73. https://doi.org/10.1016/j.ijhcs.2005.04.015

[5] Jörg Schwenk. 2020. Sicherheit und Kryptographie im Internet, Theorie und Praxis. (2020). https://doi.org/10.1007/978-3-658-29260-7

[6] Wenley Tong, Sebastian Gold, Samuel Gichohi, Mihai Roman, and Jonathan Frankle. 2014. Why king george III can encrypt. *Freedom to Tinker* (2014).