Promoting Secure Email Communication and Authentication

Verena Zimmermann[1], Birgit Henhapl[2], Nina Gerber[1], Matthias Enzmann[3]

Research Group Work and Engineering Psychology, Technische Universität Darmstadt[1]
Research Group Security, Usability & Society, Technische Universität Darmstadt[2]
Dept. for Cloud Computing and Identity & Privacy, Fraunhofer SIT Darmstadt[3]

Abstract

Nowadays, the possibility to communicate securely is crucial for users in the private as well as in the business context. However, to do so they have to face problems regarding mismatching mental models of encryption and bad usability not only concerning the encryption, but also the authentication process. To solve this problem, we evaluate users' perception on encryption and authentication schemes in order to (1) derive a process, which is more in line with their expectations and (2) use authentication schemes which provide security but also achieve a high acceptance rate from users. We plan to integrate our findings into a prototypical software in order to evaluate users' acceptance for our technical approach.

1 Introduction

The use of email and instant messaging is constantly increasing for both business and private use. However, privacy aspects like confidentiality of trade secrets or personal data are all too often disregarded and hence encryption is rarely used in person-to-person communication.

Several studies have been conducted to analyse this dilemma (Whitten & Tygar, 1999; Kapadia, 2007; Renaud, Volkamer & Renkema-Padmos, 2014). One problem surely originates from the fact that the setup for encryption can be complex for laypersons. For instance, one of the two dominating standards for email encryption, S/MIME, requires much preparation on behalf of users, is often cumbersome, and usually costs money too. Therefore, this standard is seldom used by individuals in open environments – even so S/MIME is supported by major email clients. The second most widely spread standard, PGP/OpenPGP, relies on a rather complex trust network, the so called "web of trust". While laypersons already have problems to understand the concept of encryption, PGP's web of trust only adds to this. Moreover, existing implementations still have usability issues. On top, some email clients offering encryption do not extend their service to key generation – keys have to be generated elsewhere

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2017 in
M. Burghardt, R. Wimmer, C. Wolff, C. Womser-Hacker (Hrsg.):
Mensch und Computer 2017 – Workshopband, 10.–13. September 2017, Regensburg.
Copyright (C) 2017 bei den Autoren. https://doi.org/10.18420/muc2017-ws05-0404

and imported into the email clients. This is an additional challenge for many people. But even after one has managed to overcome these problems, one cannot start sending encrypted emails until the recipient has overcome these problems, too. This seriously hinders the proliferation of encryption because a user's initial enthusiasm for using encrypted email may quickly erode when s/he realises that none of her/his friends will be able to process encrypted messages.

Additionally, communication partners – along with their keys – have to be authenticated to ensure that s/he is the person s/he claims to be. The dominating schemes for authentication today are password-based, although other methods such as biometrics or tokens have been around for a while. However, passwords suffer from several shortcomings that are well acknowledged in the literature: Users often choose weak passwords, re-use them, or write them down to increase memorability (Inglesant & Sasse, 2010). Furthermore, studies by Ur et al. (2015) showed that the users' perception of a secure password differs from its actual security. Thus, to provide secure authentication for encryption, alternatives have to be considered.

Within the module *User-friendly Confidential and Authentic Communication* of the CRISP 2 project we plan to remedy these drawbacks. Our goal is to provide a framework for easy to use encrypted email where encryption keys only need to have been setup at the sender's end.

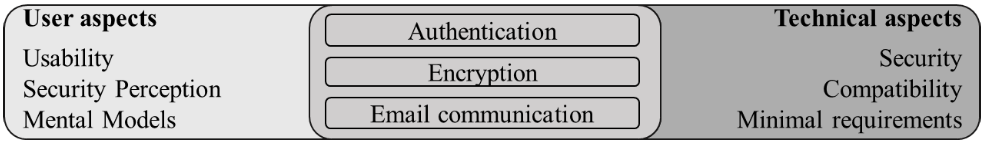

Figure 1: Framework for secure email communication and authentication

To pursue this objective, the project started with the evaluation of current authentication and encryption solutions with the focus on their acceptance by users, their usability flaws, and existing mental models with respect to encryption, i.e. the users' conception of how encryption works. Based on these results, requirements for authentication, and encryption were formulated. Currently, the evaluation of solutions for the requirements is in progress. The project's current state is described in the next sections.

2 Encryption

With email encryption users can send private data to one or more recipients without fear of being eavesdropped. For this, the communicating parties simply generate their respective key pairs (public and private key), exchange their public keys, and start encrypting messages – in theory. However, the first arising problem in practice is that many people do not have the means or knowledge to encrypt messages, let alone to generate the keys required for this.

One of the most citied papers with respect to usability of encryption software is "Why Johnny can't encrypt" (Whitten & Tygar, 1999). Analysing the widely used email client Thunderbird together with its PGP encryption plugin "Enigmail", we found that problems like automated key exchange and feedback on encryption had been resolved (Zimmermann et al, 2017).

However, the major problem – lack of understanding or misunderstanding – can still be observed according to recent studies on user mental models of encryption (Renaud, Volkamer & Renkema-Padmos, 2014; Emeröz, 2017). Thus, unintended actions may occur and users might not know how to react to error messages. Even worse, they might publish their private keys instead of their public ones.

Moreover, the study from Emeröz (2017) revealed that some of the test persons did not have any understanding at all of what encryption actually means. Some of them simply could not understand the concept of end-to-end encryption. And most of them did not care enough to involve themselves, either arguing that they did not have secrets or that even encrypted messages could surely be deciphered by the service providers and/or legal authorities.

It will go way beyond the scope of this project to catch up on the users' sense for data privacy. However, we propose to construct a framework for encryption that will release the user from the most challenging problems. For this reason, we focus on user aspects, since the technical requirements with regard to encryption are straight forward: Email encryption must ensure that only the intended recipient will be able to decrypt the message. Many existing algorithms, protocols, and solutions satisfy this requirement. However, to bridge the gap between users and non-users of email encryption, our evaluation of existing solutions shows that the challenge will be in meeting the following requirements:

- The recipient need not have a key pair, the sender must have a key pair.
- The recipient should be able to authenticate the sender's key as well as the sender.
- The recipient need not have cryptographic software readily available.
- Both recipient and sender shall be able to use their own key pairs in the future.

3 Authentication

Authentication is a process to verify the claimed identity of a person, typically to protect valuable information from unauthorized access. In the context of encryption, keys are also subject to authentication in order to correctly attribute encryption keys to their true holder. Since password-based schemes are still most commonly used, we regard them as a reference in our task to find alternative authentication schemes, which are both secure and usable.

Among the alternatives to password-based authentication schemes are biometric schemes, making use of a person's individual characteristics (e.g. fingerprints), tokens (e.g., RFID-chips)and graphical passwords, which make use of the fact that people are better at memorising pictures than random strings. These schemes have certain advantages compared to passwords, e.g., they are easier to memorise or do not need memorisation at all. Bonneau et al. (2012) systematically evaluated about thirty different authentication schemes and compared them to password-based schemes. They showed that no authentication scheme scored high in all analysed usability, deployability, and security categories. For instance, tokens prove resilient against many security threats and hence achieve a high score in the security category.

However, deploying them is more complex compared to passwords and hence they score low in deployability. Thus, it is important to consider the scenario in which the schemes are used to be able to weigh requirements and to identify the most suitable authentication scheme or schemes for the intended purpose.

The users' security perception plays an important role for the acceptance and use of authentication technologies. If the users' perception is low, independent of the actual security, users might reject the scheme and thus the encryption solution as well. If the users' perception is higher than the actual security, users might unintentionally act insecurely. Several studies showed that the users' perception of security differs from the actual security. For instance, in a study by Bhagavatula et al. (2015) users lacked the understanding that an authentication scheme is only as secure as its fall-back mechanism and hence overestimated the security of Android's face recognition scheme "Facelock". A study by Ion et al. (2010) showed that the security perception was not only influenced by the actual security but also by the operability of and feedback within an application.

We conducted an explorative study to evaluate eight different authentication schemes in a within-subject design, namely the knowledge-based password and graphical password schemes as well as gesture recognition, and biometric schemes using fingerprint, facial, speech, ear shape, and iris recognition (Zimmermann & Gerber, 2017). The results revealed that nearly as many of the 35 participants preferred the classic password for privacy reasons as did prefer biometric authentication via fingerprint for its uniqueness. This result showed that even though biometric authentication schemes are on the rise, passwords are still popular with about 1/3 of the participants preferring them. It further indicates that two user groups may exist preferring either passwords or biometrics. Since participants rated fingerprint data as more sensitive than password data, this decision may be influenced by privacy concerns. Another interesting result from our study was that several statements in the follow-up interview indicated that people preferred not to use gesture, speech, or face recognition due to proneness to shoulder-surfing and a feeling of awkwardness when used in public. This shows that the users' evaluation might also depend on the context of authentication. Thus, to provide a secure authentication scheme that users are actually willing to use it is important to consider the scenario as well as the users' perceptions in terms of usability and security.

For our framework, we derived the following requirements from our study:

- The authentication mechanism should be suitable for the scenario secure email authentication in terms of deployability, cost, duration, and effort of the authentication process, e.g. the scheme should be cost-free for the user and compatible to current browsers.
- The authentication mechanism should fulfil the security criteria after Bonneau et al. (2012) covering a broad range of possible security threats to provide actual security and also be perceived as secure to increase the users' willingness to use the scheme
- The authentication scheme should fulfil objective usability criteria in accordance with Bonneau et al. (2012) and also be perceived as usable to increase the users' acceptance and satisfaction.

4 Challenges to the Framework

An important task within our project is the development of a framework for secure, usable and authentic email communication. This framework is supposed to incorporate the findings outlined before and should naturally satisfy the derived requirements. However, the road to a prototype framework is paved with additional practical challenges which we outline next along with our planned approaches to deal with them.

Rating of authentication schemes. To identify schemes that meet certain objective security, usability and deployability criteria, appropriate evaluation criteria need to be defined. Next, an assessment of each authentication scheme must be made in the face of incomplete information with respect to security, usability, or performance as some concepts have not been implemented or well investigated, yet.

Approach: From a literature review, we identified 84 authentication schemes. For determining the most suitable schemes for our scenario, we plan to conduct an evaluation followed by a rating based on the Usability-Security-Deployability (USD)-framework proposed by Bonneau et al. (2012). To deal with the challenge of evaluating concepts instead of implementations in some cases, we plan to rely on the published literature and compare the assessment to existing schemes with related features, e.g., password space or resilience against physical observation.

Fulfilling the needs of different user groups. Our study to explore user perceptions of authentication schemes indicated that two user groups may exist, one preferring passwords for privacy reasons and another one preferring biometrics. This finding might pose a challenge in accommodating the perhaps conflicting needs of two different user groups.

Approach: The assumption of different user groups and the possible influence of privacy aspects need to be further investigated and, if verified, addressed in the choice or design of the authentication scheme within our framework. Thus, we conducted a subsequent online survey with 95 participants to shed light on the factors influencing user preferences (Gerber & Zimmermann, 2017). We found that, for the purpose of email authentication, about 63% preferred passwords compared to 37% preferring biometrics. Furthermore, the purpose, e.g., authenticating for access to email vs. social networks, seems to influence user preference. Since there seem to be two large groups preferring either scheme a possible solution to this might be to consider two schemes instead of one to satisfy both user groups.

Providing authentication for different situations. One of our requirements states that the recipient need not have a key pair but the sender must have one. Thus, the authentication scheme needs to adapt to cases with and without key pairs and the purpose at hand, e.g., authentication of a person’s key or authentication to a server/Web site. The challenge will be to identify one suitable scheme for several purposes or a combination of schemes that do not overly increase the burden on the user, e.g., by having to memorise many secrets.

Approach: To deal with this challenge we plan to evaluate the authentication schemes scoring highest in the rating described above in terms of user perceptions in a laboratory study. The study context will be email communication to assure the applicability of the schemes for our scenario. The results will serve to sort out schemes and to evaluate the suitability of others for different authentication tasks within our scenario. Follow-up studies using mock-ups will then be used to verify the findings and explore the interplay of possible combinations of schemes.

Asymmetric capability. Public key cryptography requires symmetric cryptographic capability, e.g., key pairs and appropriate software components at both communication ends. Our goal is to support asymmetric capability for encrypted messages, requiring only the sender to have cryptographic capability.

Approach: We start with the sender *A* having some cryptographic capability, i.e., access to software for key generation, key management, encryption, and handling of custom protocol data. The recipient *B*, unlike *A*, only needs to have access to common communication software like an email client and/or Web browser which do not necessarily have built-in cryptographic capabilities. Although not perfect, the latter can be compensated by using portable cryptographic code, which can be implemented in, e.g., JavaScript and interpreted by modern Web browsers. This, however, requires some kind of media change as our goal is to support encrypted email and email clients typically do not execute portable code which is a prerequisite for our approach. To make this change less painful for users, a (Web) server can be used to store the message encrypted by the sender *A* and provide the recipient *B* with a unique Web link (URL) to the encrypted message. Once the "linked message" is loaded into *B*'s browser, the decryption will be made locally by the browser such that the server's provider does not learn the message content. The portable code for decryption may come from the message server or from another (Web) resource such that the recipient need not have any cryptographic capability beforehand. The key used for the decryption comes with the URL given to the recipient as a so called fragment identifier, see below.

$$\underbrace{\text{http://host.domain.tld/path/page.html}}_{\text{URL}}\underbrace{\text{\#someID}}_{\text{fragment identifier}}$$

The trick with the fragment identifier is that it is omitted by the browser when the URL's content is requested from the server, i.e., the browser only sends the URL part and thus the server provider does not learn the decryption key. Services implementing the Web server side already exist, e.g., ZeroBin (see https://zerobin.net/). This approach is close to what we want to achieve. However, we additionally plan to make use of the sender *A*'s existing cryptographic keys, such that the recipient *B* can address *A* as if he had cryptographic capability himself.

Promoting existing cryptographic capability. Privacy sensitive users having mastered the sometimes "painful" process of generating and deploying key pairs in their own software should be rewarded and not (further) frustrated if communication partners do not have cryptographic capability (yet). We want to support and include existing (certified) key pairs such that entities without cryptographic capability can use their communication partners' *existing* public keys for encryption.

Approach: We want to make use of the sender *A*'s public key to allow the recipient *B* to send his *encrypted response* using *A*'s public key. Similar to the ZeroBin approach, we want to make use of portable cryptographic code to process public keys at the recipient *B*'s end and use them to form an encrypted response to *A*. For this, *A* has to include her public key in the encrypted message, similar to S/MIME messages, such that the portable code at *B*'s end can extract the key and use it for the encrypted response.

Key transport. The URL pointing to *A*'s encrypted message together with the decryption key in the fragment identifier might be given to the recipient *B* in clear, e.g., in an unencrypted email. Thus, an eavesdropper, observing *B*'s communication, could learn everything required to download and decrypt the message from the server.

Approach: The encrypted message stored at the server could be made "read once", i.e., the URL pointing to the message will become invalid once it was accessed and the message will also be deleted from the server – such an option already exists with ZeroBin and is called "burn after reading". This does not save *A* and *B* from being eavesdropped but at least the privacy breach would be noticeable by the recipient who could then act accordingly. A solution to transport the decryption key from *A* to *B* in a manner that is resilient to observation –and user friendly too– should also respect our usability requirements, e.g., it should not increase users' burdens. Hence, common solutions like pre-shared passwords/keys or online key agreement schemes will not help here and thus, this issue will be subject to further work in our project.

5 Outlook

Our next steps include the continued development of our technical approach and the process design. We need to tackle questions such as: What does the process look like for a user having a key pair compared to a user having none? How can the users' mental models of encryption be taken into account? For what purpose and how often do users have to authenticate?

Meanwhile, we will conduct further studies to explore the users' perceptions of encryption and authentication. For instance, we plan to conduct another laboratory study with selected authentication schemes to examine the users' security and usability perception as described in the challenge section. Other studies will focus on the evaluation and re-design of usability aspects in currently available encryption software. The results of the studies will serve as a base for the design of integrated interface mock-ups that combine the technological requirements with the user aspects in terms of encryption and authentication. These mock-ups will iteratively be developed with the feedback provided by experts and users.

The major challenge we are facing is the integration of the partially conflicting technical and user requirements. For example, users may prefer an authentication scheme that requires a costly device or which is not easily browser-compatible if they do not have to remember passwords or fulfill complex interactions in return. Such results would pose a challenge for the requirements cost-free use and browser-compatibility. Also, users might want feedback and information on the encryption and authentication process but at the same time demand efficiency. Thus, the users' perceptions and needs have to be considered and weighed for each design decision, having in mind that fulfilling one requirement might negatively affect others. Similar to the challenge of dealing with people either preferring the password or biometrics (privacy aspects), one possibility to deal with these trade-offs might be to provide the users with adaptive features and choices.

Acknowledgement

This work was supported by the German Federal Ministry of Education and Research (BMBF) within CRISP.

Literature

Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F., & Savvides, M. (2015, February). Biometric authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In *Proc. USEC 2015* (pp. 1-2). Internet Society.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012, May). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *In IEEE Symposium on Security and Privacy (SP) 2012* (pp. 553-567). IEEE.

Emeröz, S. (2017). Mentale Modelle von Endnutzern zur Ende-zu-Ende-Verschlüsselung im MessagingKontext. Master Thesis, to appear.

Gerber, N., & Zimmermann, V. (in press). Security vs. privacy? User preferences regarding text passwords and biometric authentication. In proceedings *Mensch und Computer 2017.*

Inglesant, P.G. & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems 2010* (pp. 383392) ACM.

Ion, I., Langheinrich, M., Kumaraguru, P., & Čapkun, S. (2010, July). Influence of user perception, security needs, and social factors on device pairing method choices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 6). ACM.

Kapadia, A. (2007).A Case (Study) For Usability in Secure Email Communication. In S.W. Smith (eds) *IEEE SECURITY & PRIVACY* (p. 80-84)

Renaud, K., Volkamer, M. & Renkema-Padmos, A. (2014). Why Doesn't Jane Protect Her Privacy?. In De Cristofaro E., Murdoch S.J. (eds) *Privacy Enhancing Technologies. PETS 2014. Lecture Notes in Computer Science*, vol 8555. Springer, Cham.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N. & Cranor, L. F. (2015, July). "I added '!'at the end to make it secure": Observing password creation in the lab. In *Proc. SOUPS Symposium on Usable Privacy and Security 2015*, USENIX Association.

Whitten, A. & Tygar, J. T. (1999, July). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proc. 8th USENIX Security Symposium 1999*, ACM..

Zimmermann, V., Henhapl, B., Volkamer, M. & Vogt, J. (2017). Ende zu Ende Sichere E-Mail Kommunikation. In *DuD • Datenschutz und Datensicherheit 5 |2017***.**

Zimmermann, V. & Gerber, N. (in press). "If It Wasn't Secure, They Would Not Use It in the Movies" – Security Perceptions and User Acceptance of Authentication Technologies. In *International Conference on Human Aspects of Information Security, Privacy, and Trust 2017*. Springer, Cham.

Authors

Zimmermann, Verena

Verena Zimmermann finished her studies of Psychology at the Technische Universität Darmstadt in 2015. After a research stay at Griffith University, Brisbane, she started working as a researcher and PhD student in the Department of Psychology back in Darmstadt in the group Work and Engineering Psychology in 2016. Her research interests cover Usable IT Security, Human-Computer-Interaction and Human Factors in Safety and Security.

Henhapl, Birgit

Birgit Henhapl is a postdoctoral researcher in the group of Prof. Dr. Melanie Volkamer at the Department of Computer Science of the Technische Universität Darmstadt since November 2016. She is team member in the CRISP - Delegated Privacy and Security Settings project and responsible for HiWi contracts at SECUSO. She received her PhD on: "On the Efficiency of Elliptic Curve Cryptography" from the Technische Universität Darmstadt in November 2003, supervised by Prof. Dr. Johannes Buchmann. Before this appointment, she worked as Information Security Consultant and PCI DSS Auditor at usd AG.

Gerber, Nina

Nina Gerber studierte Psychologie an der Technischen Universität Darmstadt. Seit Anfang 2015 ist sie dort am Institut für Psychologie als wissenschaftliche Mitarbeiterin in der Forschungsgruppe für Arbeits- und Ingenieurpsychologie tätig. Ihre Forschungsinteressen liegen hauptsächlich im Bereich der Mensch-Maschine-Interaktion. In mehreren Kooperationsprojekten mit dem Fachbereich Informatik beschäftigt sie sich aktuell damit, wie Nutzer im Technikkontext mit privatsphäre-kritischen Daten umgehen.

Enzmann, Matthias

Matthias Enzmann is a Senior Researcher at the Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT). He works on privacy-friendly authentication and identification technologies as well as on privacy-friendly data processing. He is constantly striving to make his work more accessible for laypersons, still hoping that it will eventually be usable.