Proceedings of the Eighth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2014)

Shake Hands to Bedevil: Securing Email with Wearable Technology

A. Renkema-Padmos[1], J. Baum[2], K. Renaud[3] and M. Volkamer[1]

[1] SecUSo, CASED / TU Darmstadt, Germany
[2] Independent researcher, Germany
[3] School of Computer Science, University of Glasgow, UK
e-mail:arne@secuso.org; jerome@jeromebaum.com; karen.renaud@glasgow.ac.uk;
melanie.volkamer@cased.de

Abstract

Email users rarely use end-to-end encryption. It takes effort and requires explicit action. Users may not see the need for this, have access to the technology, possess the know-how, or may be faced with complex interfaces. To enable effortless exchange of encrypted emails we propose KeyRing, a design for a wearable device that builds on in-person trust establishment through device pairing. This pairing can be used to make the exchange of secure emails between the wearers easier. We discuss how the corresponding interactions of *handshake*, *seal*, and *unseal* can be implemented, and find that the most promising approaches are a ring communicating over infrared and a wristband communicating over Bluetooth. Issues around the human-device interface, user acceptance, feasibility, and deployment are discussed, but need further work.

Keywords

Tangible interaction, wearables, communications security

1. Introduction

Encryption can help prevent casual snooping and dragnet surveillance. After the Snowden leaks on the extent of NSA surveillance (Greenwald *et al.*, 2013), the public should know their emails are being monitored. Yet, few people use end-to-end email encryption. This may be due to users not seeing the need for this, not having access to the technology, not possessing the know how (Renaud *et al.*, 2014), or being faced with complex interfaces (Whitten and Tygar, 1999). Availability is especially problematic in webmail where simplicity and advertising income are key. If encryption is to be more widely used, all of the issues mentioned need to be taken care of. We address the usability aspect of end-to-end email encryption.

Our approach is tangible security, inspired by the historical use of seal rings in securing letters with wax, the modern practice of cryptographic handshakes, and people wearing cryptographic dongles around their neck, as well as the philosophy of industrial designer Naoto Fukusawa: “design dissolving into behaviour”. Bødker *et al.* (2012) identified tangible security as a fruitful area for security research. We look at the possibility of integrating secure email into existing

social activities through wear- able technology, applying human-human interaction principles to security interactions.

The contributions of our paper are:

- an overview of the research into wearable security tokens;
- identifying handshakes and sealing as interactions to support email security;
- suggestions for realising the proposed interactions in reality.

2. Related work

Given the increased interest in wearable technology in recent years, as well as the shift to mobile technologies, the area of wearable security is a interesting research area. A broad range of different wearable authentication technologies has been published, with application domains ranging from health to fashion, in form factors like pills (Fried, 2013), handbags (Yan *et al.*, 2012), and rings (Roth *et al.*, 2010). We are not aware of any work that uses wearables to make email security more usable for end-users.

Early work in the area of wearable user identification is that of contactless radio-frequency identification (RFID). Contact wearable user identification work was done by Matsushita *et al.* (2000), showing that capacitative touch (explored by Post *et al.*, 1997) can be used to signal a user's identify to the devices that they handle.

Various application areas for these kinds of technologies were explored. Ebringer *et al.* (2001) secured devices by connecting them to a secondary device with a virtual leash: if the leash breaks the primary device is locked. Another concept is the use of a wearable token for providing transparent encryption by Noble and Corner (2002; 2005). Using wearable technology for carrying messages and contraband was explored by Glance *et al.* (2001), and Schneider *et al.* (2000) and Satyanarayanan (2000) used wearables for transporting trust to replace the transport of content.

Different prototypes and products have been built based on the idea of wearable authentication. WearableKey (Matsushita *et al.*, 2000) prototyped user identification through physical contact, based on capacitive touch and a wristwatch. Contactless authentication was prototype by Motorola as an electronic tattoo (Arora and Ghaffari, 2013; Fried, 2013), and token for quickly unlocking phones (Motorola, 2014). Cryptographic tokens in the form factor of a bracelet were explored by the Singapore government (Gratzer and Naccache, 2007).

The form factor of rings has also been proposed and tested for identity applications. The Java Ring is an early example of a contact token in the form factor of a ring (Surendran, 2014). A concept for a contactless (Bluetooth) ring enbodying a social media contact was proposed by Labrune and Mackay (2006). Roth *et al.* (2010) prototyped a ring that can identify a user to an infrared touch table, and Vu *et al.* (2012; 2013) did the same for devices with a touch screen. A crowdsourced project succeeded in funding the production of a device that can authenticate the wearer via contactless (NFC) communication (Kickstarter, 2014).

Intellectual property rights are a potential issue for wearables. Various patents have been filed such as US 20030046228 A1, WO 2005117527 A2, and US 20090146947 A1. These describe ways of using wearable devices for authentication, how to build a trust network using such devices, and possible form factors such as bracelets, rings, and earrings. Whether these patents will hamper adoption remains to be seen.

3. Proposed interactions

To make secure email more usable we propose three interactions to support secure communications: *handshake*, *seal*, and *unseal*. The intention is to ease secure email communication by building on familiarity with in-person trust establishment and the centuries-old practice of sealing letters.

3.1. Handshake

This is the key exchange stage. Instead of having to find a way to securely exchange keys online, this protocol requires people to meet in person, in order to establish trust.

Two prospective email users will exchange an encryption key through a metaphorical or genuine handshake. In essence, their KeyRings will have to be in close enough proximity to each other, having been instructed by their owner to agree on a bespoke key for future email interactions. The wearable device will store the key for use in subsequent "Seal" and "Unseal" steps. Exchange of keys could happen automatically, but may be user directed to prevent malicious deception.

The protocol is as follows, when Tamara and Ted wish to send encrypted emails:

- Tamara and Ted meet in person;
- They activate their KeyRings and bring them close enough to each other so that the devices can communicate;
- The KeyRings generate a key *for this relationship* and store the key together with the other KeyRing's identifier and the email address of the other person.

3.2. Seal

Once users have paired their devices and successfully agreed a key, the aim is to make subsequent communications as simple as possible. The presence of the KeyRing indicates that encryption should be enabled. Alternatively, sealing can be made an explicit act through a physical sealing motion, involving gestures, another device, or clicking on an icon. The metaphor of sealing does not translate one-to-one to cryptographically secured communication, but it should be understandable enough for most users. It is thought to prevent confusion about the use of signing versus encryption, as the default setting for "sealing" would be to encrypt and sign.

When Tamara wishes to send an encrypted email to Ted, she:

1. Opens the KeyRing-Enabled Email Client;

2. Selects Ted's name as the email recipient;

3. Composes the email;

4. Seals the email either with a gesture, by clicking on an icon, or has KeyRing encryption enabled by default;

5. Clicks on the "Send" button.

3.3. Unseal

When the user receives an encrypted message he/she will be notified, and asked to signal that decryption should occur. The unsealing motion of traditional wax based seals can be employed. Optionally, all decryption and verification of email can be done automatically. Additionally, to represent the sender, an icon/symbol could be displayed on a trusted display.

When Ted receives an encrypted email from Tamara he:

1. Opens the KeyRing-enabled Email Client;

2. Clicks on the email in the inbox;

3. Clicks on the "unseal" icon or uses a gesture to signal that unsealing is required;

4. Opens and reads the plaintext email.

4. Physical realisation

Grosse and Upadhyay (2013) already identified the need for more appealing form-factors for authentication tokens, and highlighted jewellery as one potential candidate, possibly powered by RFCOMM/Bluetooth or NFC. In this section we propose a device that supports key exchange for bootstrapping trust for usable secure email communication. We do not know precisely how feasible the design is with current technology, or whether the protocols and algorithms are available to fully support the proposed interactions, but we provide preliminary ideas in this section.

4.1. Design considerations

The design space and solution space for such a device is large, and includes many aspects: communication design (e.g. antenna, body, light, sound), computational power, timing, algorithms, power, storage, cost, desirability, demand, safety, size, management. In a real-world implementation of the interaction patterns, trade-offs between all of these aspects will have to be made depending on where and how the

device will be used. Here we discuss these aspects in more detail, before describing concrete implementations proposals in the next section. While the full design space is likely to be intractable, general comments about promising directions can be made.

Model of the context of use. The threat model for the device is that the Internet backbone is monitored, hardware random number generators might be backdoored, and end-points could be compromised. The initial key exchange might be observed, but we see this as less of an issue. The utility model is that the device makes email encryption easier and safer by performing encryption on the wearable device, by making trust verification easier, and by allowing keys to be used across end-nodes (such as phones, tablets, and laptops). The usability model is a device that should make encrypted email as easy to use as non-encrypted email for a large class of use cases.

Form factor. The size of the device can be something like a ring, a wristband (i.e. KeyChain), or a smartwatch. When the handshaking motion is not directly observed by the device, form factors like a pendant or smart glasses are also possible. We think that a hand-worn device is best due to communication range considerations, and for preventing observability of the handshake.

Given the size of current microprocessors (e.g. low power ARM or ARV architectures) the patterns should be realisable in a ring-shaped device, although power constrains will be a real concern. A wristband will be more feasible, especially for a prototype version.

Key exchange. The key exchange and encryption can build on both public key cryptography and on symmetric encryption. If a secure way of sharing keys can be implemented, then public key encryption might not be necessary. Due to key sizes, power constraints, and ease of protecting the implementation against side-channel attacks, the use of symmetric keys seems most appropriate. A remaining issue is how to transfer keys securely. We propose transmitting them directly through some covert physical channel, possibly enhanced with input from sensors that are in similar physical locations, e.g. building on the speed with which hands are shaken. Due to privacy considerations it is important that the device not broadcast continuously, which is also important for battery savings.

Key management. Because the keys might be compromised through loss of the device or through theft, it is important that appropriate key management is in place. One approach that can limit the impact of key compromise is the use of ephemeral keys, although this is difficult to implement in existing email encryption solutions. Additionally, traditional techniques such as revocation certificates can be used, which could be provided as a third-party service to the user to increase usability. A remaining issue is how to protect against misuse of key material in case of theft of the device. Protection via a PIN, backed by a tamper-resistant smart card is one possible approach.

Communication channel. The communication between the two (or more) devices could take the form of ultrasound, infrared light, visible light, radio-frequency communication, capacitive sensing, haptics (vibrations), etcetera. Physical channels that seem fit for private transfer of information are ultrasound or infrared in the cupped hands of a handshake. Another option that seems appropriate is the use of capacitive touch, although a proper way of doing multiplexing within such an application would have to be developed and tested. Besides taking a contact or contactless approach, it is also possible to take a hybrid approach. An issue with any channel is the data rate that could be supported. Additionally, there may be issues with the availability of an interface between the PC and the KeyRing. Generally, different ways of communicating will have different security vulnerabilities, cost, accuracy, and power requirements.

Protocol. For the communication protocol we propose a simple tag-length-value protocol, along with a checksum, running over a serial line. It could be that different channels are needed for PC to ring communication. For half-duplex communication some form of collision detection is necessary. It is deemed important that the protocols are standardised, easy to implement (to reduce security holes), and freely available.

Device security. Securing the device against theft is not the primary goal, although this would certainly be possible by using something like a smart card combined with a PIN mechanism. Alternative mechanisms for user authentication may be fingerprints or other biometrics, device unlocking with the help of external input devices such as a laptop, or a trusted secondary device that is paired with the KeyRing.

End-user interaction. The interaction between the device and the user can work through different channels. One logical way of providing feedback to the user is through haptic feedback, i.e. vibrations. Another low-cost and visible way would be the use of LEDs for (colour) coding, which can also support crude animation. Alternatives are sound, smell, electrical signals, and shape-shifting interfaces.

Input from the user to the device can also take place in many different ways. The use of gesture recognition for the handshake, and automation for the decryption seems reasonable to us. To prevent decryption of messages forwarded by a malicious device, a simple pairing mechanism through a button press seems sufficient. Activation of the device might occur through an authenticated sequence from a PC, phone, or tablet, or maybe even be based on a gesture by the user.

Feasibility. Given current technology and the above considerations, it seems feasible to implement the proposed interaction patterns. A concrete description of how such a system might be implemented is given below. Note that an important aspect of the feasibility of the system is cost. We present both a system that might be built on top of existing devices as a software feature, as well as an approach that involves custom hardware design. The former may be cheaper, but can entail decreased flexibility.

4.2. Proposal for the System Design

Here we present and discuss a proposal for a high-level and low-level system design that implements the handshake, seal, and unseal interactions. Ideally we will reuse existing projects and infrastructure as much as possible. We can build the system on top of existing libraries that implement cryptographic standards such as AES (Advanced Encryption Standard) and SHA (Secure Hashing Algorithm), which can be used for key derivation and message authentication codes. From a high-level perspective, two KeyRings will create key material, which they exchange and use to derive a shared secret. This will be the basis for sessions keys used for encryption and authentication of email. Ideally, the KeyRing will provide a trusted cryptographic platform that can be used by a wide variety of services (e.g. PGP, TexSecure, Pond, etc) and support many identity providers (e.g. CAs, keybase.io, PGP key servers, etc).

The low-level view involves specific communication methods for transferring keys between the KeyRings, as well as for enabling KeyRing to PC and PC to KeyRing communication. For communication between the KeyRings the observability aspect is important, while for communication with the PC interoperability is paramount. We think there are several possible candidates that can serve as implementation of the KeyRing concept. A *smartwatch with Bluetooth* would have easy communication with PCs and phones, although observability of the key exchange might be a problem. *Rings with infrared* are better at hiding the key exchange, but the channel to and from a PC will be more difficult. Additionally data rates might be an issue. In order to communicate with the PC the use of ultrasound is a possibility. In either case, a hybrid scheme may be the most appropriate.

5. Discussion

Like all devices, our solution is not perfect, and there are several limitations and open questions related to the feasibility and usability of the protocols described in this paper. There are several specific aspects that need to be taken into account to make the tangible security patterns feasible. These can be summarised as the following questions: do users want it, can it be made, and will users buy it? We will pay special attention to these aspects in future work.

User acceptance. The acceptance of our proposed key management protocol and implementation is of vital importance if it is to be adopted by end-users. Various facets are likely to influence the acceptance of the device. Firstly, the device needs to be considered wearable, being comfortable and stylish/unobtrusive. Secondly, it needs to be socially acceptable: the handshake is an interaction pattern specific to Western cultures, and other cultures may not want to adopt it because of social norms (e.g. bowing is the norm in Japan, and shaking hands with the opposite sex is not the norm in many parts of the world). Thirdly, some way of dealing with lost or discharged devices may be needed, e.g. a backup solution. Users are prone to losing keys, and there is a risk that they will lose the KeyRing. Additionally, a fallback may be needed when the device has no power and urgent email need to be read or sent. Lastly, the impact on anonymity needs to be considered.

Technical feasibility. A big question is whether current technology allows for the interactions and form factors described in previous section, and if not, when we can expect the technology to be available. Major issues in a lot of wearable technologies are processing power and battery lifetime, the upgrading of devices, and their user interface. This is related to user acceptance: the device needs to be technically feasible from a power management perspective while at the same time falling within a comfortable size for the user. As we have described in the realisability section, a wristband form factor should be feasible for a prototype that will run for an average working day, and that can store an adequate number of contacts. With further improvements in technology and engineering, a ring form factor also seems feasible.

Besides the issue of manufacturing, there are other technical issues that are just as important. For a security device that stores keys for long-term communication with other users, compatibility is a major concern. Additionally, given a changing security landscape, some sort of upgrade potential seems wise. Balancing these may be difficult.

Deployment. Academic research is generally not directly interested in the economic viability of the research, or the ability of end-users to deploy the solution themselves. While the interactions might be applied in a limited contexts by individuals, for the interactions to have a bigger impact they will need to see widespread adoption. We have discussed the issue of people not using end-to-end email encryption in the introduction, and this remains a major open problem.

We see this paper as one step in the direction of enabling easier secure communication. We plan to further explore the barriers towards the adoption of encrypted communication in the future. Preliminary directions include the raising of awareness, finding a "killer application" for the device, and dealing with network effects.

Technology in use. There are various issues that come up when the device would be implemented in the field. As the device would be worn on the body, there is the risk of violence linked to theft of the KeyRing. Liveness detection is one possible way of decreasing the effectiveness of stealing the device. This is also the approach applied by Google Glass, which can be secured by a PIN code, while the device automatically locks when it is taken from the head of the wearer.

Related to user acceptance, the impact of ubiquitous authentication needs to be investigated. While the outcome might be hard to predict, a reasonable approach seems to be adding an element of user control.

6. Conclusions

We have presented an overview of prior work in wearable encryption and authentication technologies, showing that it is a promising research area. We have extended this work with our proposed interactions for making email encryption easier to use (hand-shake, seal, and unseal), and have provided thoughts on how these

protocols may be implemented (e.g. a ring communicating over infrared, or a wristband communicating over Bluetooth). Our proposal is a call for the usable security community to investigate contextualised interventions, and to review their practicality.

As described in the previous sections, we intend to build a prototype that supports the interactions, in order to make email security easier for the end-user. We plan to fine-tune and test it through participatory design and enactment (e.g. through Wizard of Oz experiments), inspired by Mathiasen and Bødker (2011). The expected miniaturisation of technology in the coming years should make the device easier to realise.

Additionally, we are looking to explore the kinds of interactions that could be supported when users wear multiple rings, as well as looking at the associated technical challenges. Also, interactions with the device itself need to be further explored, e.g. through gesture elicitation techniques. Another interesting avenue would be interacting with the device itself through, for example, deforming or combining rings. Other future work may look at extending the concepts to other situations and applications, for example cognitive augmentation by making the web of trust between people tangible, or tackling the problem of ATM security.

7. Acknowledgements

We would like to thank the anonymous reviewers of TEI 2014 and HAISA 2014. We would also like to thank the Horst Görtz Stiftung (horst-goertz.de) for funding this research through CASED (cased.de).

8. References

Arora, W. J. and Ghaffari, R. (2013), 'Extremely stretchable electronics'. US Patent 8,389,862.

Bødker, S., Mathiasen, N. R. and Petersen, M. G. (2012), 'Modeling is not the answer!: Designing for usable security', *Interactions* **19**(5), 54–57.

Corner, M. and Noble, B. (2005), 'Protecting file systems with transient authentica- tion', *Wireless Networks* **11**(1-2), 7–19.

Ebringer, T., Zheng, Y. and Thorne, P. (2001), Parasitic authentication, *in* 'Proc. Work- ing Conference on Smart Card Research and Advanced Applications', Kluwer Aca- demic Publishers, Norwell, MA, USA, pp. 307–326.

Fried, I. (2013), 'Motorola's Dennis Woodside and Regina Dugan'. URL: *http://allthingsd.com/20130529/motorolas-dennis-woodside-and-regina- dugan-talk-moto-x-tattoos-and-taking-big-risks-at-d11-full-video/*

Glance, N., Snowdon, D. and Meunier, J.-L. (2001), 'Pollen: Using people as a com-munication medium', *Computer Networks* **35**(4), 429 – 442.

Gratzer, V. and Naccache, D. (2007), 'Trust on a nationwide scale', *Security Privacy, IEEE* **5**(5), 69–71.

Greenwald, G., MacAskill, E. and Poitras, L. (2013), 'Edward Snowden: The whistle- blower behind the NSA surveillance revelations', *The Guardian* 9.

Grosse, E. and Upadhyay, M. (2013), 'Authentication at scale', *IEEE Security and Privacy* 11, 15–22.

Kickstarter (2014), 'NFC Ring by John McLear'. Accessed 2 June 2014. URL: *http://www.kickstarter.com/projects/mclear/nfc-ring*

Labrune, J.-B. and Mackay, W. (2006), Telebeads: Social network mnemonics for teenagers, *in* 'Proceedings of the 2006 Conference on Interaction Design and Chil- dren', IDC '06, ACM, New York, NY, USA, pp. 57–64.

Mathiasen, N. R. and Bødker, S. (2011), Experiencing security in interaction design, *in* 'Proc. CHI', CHI '11, ACM, New York, NY, USA, pp. 2325–2334.

Matsushita, N., Tajima, S., Ayatsuka, Y. and Rekimoto, J. (2000), Wearable key: De- vice for personalizing nearby environment, *in* 'Proc. ISWC', ISWC '00, IEEE Com- puter Society, Washington, DC, USA, pp. 119–.

Motorola (2014), 'Motorola Skip: Pins are for fashion not for phones'. Accessed 2 June 2014. URL: *http://www.motorola.com/us/motorola-skip-moto-x/Motorola-Skip-for-Moto-X/motorola-skip-moto-x.html*

Noble, B. D. and Corner, M. D. (2002), The case for transient authentication, *in* 'ACM SIGOPS European Workshop', EW 10, ACM, New York, NY, USA, pp. 24–29.

Post, E., Reynolds, M., Gray, M., Paradiso, J. and Gershenfeld, N. (1997), Intrabody buses for data and power, *in* 'Wearable Computers, 1997', pp. 52–55.

Renaud, K., Volkamer, M. and Renkema-Padmos, A. (2014), Why doesn't Jane protect her privacy?, *in* '14th Privacy Enhancing Technologies Symposium'.

Roth, V., Schmidt, P. and Güldenring, B. (2010), The IR ring: Authenticating users' touches on a multi-touch display, *in* 'Proceedings of the 23nd Annual ACM Sym- posium on User Interface Software and Technology', UIST '10, ACM, New York, NY, USA, pp. 259–262.

Satyanarayanan, M. (2000), Caching trust rather than content, *in* 'ACM SIGOPS Eu- ropean Workshop', EW 9, ACM, New York, NY, USA, pp. 245–246.

Schneider, J., Kortuem, G., Jager, J., Fickas, S. and Segall, Z. (2000), 'Dissemi- nating trust information in wearable communities', *Personal Ubiquitous Comput.* 4(4), 245–248.

Surendran, D. (2014), 'Knuckletop computing: The Java Ring'. Accessed 2 June 2014. URL: *http://people.cs.uchicago.edu/ dinoj/smartcard/javaring.html*

Vu, T., Baid, A., Gao, S., Gruteser, M., Howard, R., Lindqvist, J., Spasojevic, P. and Walling, J. (2012), Distinguishing users with capacitive touch communication, *in* 'Proc. Mobicom', Mobicom '12, ACM, New York, NY, USA, pp. 197–208.

Vu, T. and Gruteser, M. (2013), 'Personal touch-identification tokens', *Pervasive Computing, IEEE* **12**(2), 10–13.

Whitten, A. and Tygar, J. D. (1999), Why Johnny can't encrypt: A usability evaluation of PGP 5.0, *in* 'Proc. USENIX Sec', Vol. 99, McGraw-Hill.

Yan, Z., Chen, Y. and Zhang, P. (2012), An approach of secure and fashionable recognition for pervasive face-to-face social communications, *in* 'WiMob', pp. 853–860.