Helping Johnny 2.0 to Encrypt His Facebook Conversations

Sascha Fahl, Marian Harbach,
Thomas Muders, Matthew Smith
Dept. of Computer Science
Leibniz Universitaet Hannover
Hannover, Germany
fahl, harbach, muders,
smith@dcsec.uni-hannover.de

Uwe Sander
Dept. of Information and Communication
University of Applied Sciences and Arts
Hannover, Germany
uwe.sander@fh-hannover.de

ABSTRACT

Several billion Facebook messages are sent every day. While there are many solutions to email security whose usability has been extensively studied, little work has been done in the area of message security for Facebook and even less on the usability aspects in this area. To evaluate the need for such a mechanism, we conducted a screening study with 514 participants, which showed a clear desire to protect private messages on Facebook. We therefore proceeded to analyse the usability of existing approaches and extracted key design decisions for further evaluation. Based on this analysis, we conducted a laboratory study with 96 participants to analyse different usability aspects and requirements of a Facebook message encryption mechanism. Two key findings of our study are that automatic key management and key recovery capabilities are important features for such a mechanism. Following on from these studies, we designed and implemented a usable service-based encryption mechanism for Facebook conversations. In a final study with 15 participants, we analysed the usability of our solution. All participants were capable of successfully encrypting their Facebook conversations without error when using our service, and the mechanism was perceived as usable and useful. The results of our work suggest that in the context of the social web, new security/usability trade-offs can be explored to protect users more effectively.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation (e.g. HCI)**]: User Interfaces - Input Devices and Strategies, Evaluation.; D.6.m [**Security and Protection**]: Miscellaneous

General Terms

Security, Human Factors, Measurement

Symposium on Usable Privacy and Security (SOUPS) 2012, July 11-13, 2012, Washington, DC, USA., ACM 978-1-4503-1532-6/12/07

Keywords

Usable Security, Social Networks, Message Encryption

1. INTRODUCTION

The usability of email security has been the subject of research for more than a decade. Whitten and Tygar [22] conducted the first Johnny study in 1999, analysing the usability of PGP5, followed by the more recent evaluations of S/MIME in Outlook Express in Garfinkel and Miller's Johnny 2 study [10] and the re-evaluation of the original Johnny study using PGP9 by Sheng et. al. [20]. In this paper, we address the issue of message security in the context of Online Social Networks (OSN) in general and Facebook in particular. Even though the Web 2.0 paradigm is now a decade old and OSN sites such as Facebook play a major role in many people's online lives, there has been very little work on the usability of message security in this domain.

As of April 2012, Facebook had over 900 million users[1]. In 2010, when Facebook had only 500 million users, Facebook published internal statistics showing that more than 4 billion private messages (including chat messages) were sent every day[2]. Also in 2010, a Gartner study predicted that social networking services would replace emails as the primary vehicle for interpersonal communications for 20 percent of business users in the near future[3]. To put these numbers into perspective, Google announced that Gmail had 350 million users in January 2012[4].

While there are some solutions available to cryptographically protect Facebook conversations, to the best of the authors' knowledge, there is no widespread use of them. Thus, the aim of our work was to find out why this might be the case and what could be done to help OSN users to encrypt their Facebook conversations. While mechanisms to protect email messaging could in principle be adapted to Facebook conversations in a straightforward manner, previous usability studies show significant problems with the existing email encryption mechanisms. One of our goals was therefore to

[1] http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2012/04/23/businessinsiderfacebook-now-has-900.DTL
[2] http://techcrunch.com/2010/11/15/facebook-350m-people-using-messaging-more-than-4b-messages-sent-daily/
[3] http://www.gartner.com/it/page.jsp?id=1467313
[4] http://www.email-marketing-reports.com/metrics/email-statistics.htm

see if the changes brought about by the OSN paradigm might open up new possibilities for a usable security mechanism protecting private OSN messages.

To answer these questions, we conducted multiple studies to evaluate needs surrounding the protection of users' conversations on Facebook and then compared different existing solutions for conversation encryption. Based on these intermediate results, we developed an approach to encrypt Facebook conversations which we tested in two user studies to ascertain whether the solution provided good usability characteristics while at the same time protecting user privacy. The results of the final study show that the OSN paradigm does indeed offer new ways of simplifying security and finding security/usability trade-offs which are acceptable to users.

This paper is organised as follows: Firstly, Section 2 introduces related work, followed by a more detailed description of existing protection mechanisms for Facebook conversations in Section 3. Next, Section 4 describes the prototypes we built as mockups to be used in the lab study detailed in Section 5. These results led to the development of an encryption service for Facebook conversations, outlined in Section 6. Sections 7 and 8 present the evaluation of our solution in two further studies. Finally, Section 9 discusses limitations of our approach and Section 10 outlines future work and concludes this paper.

2. RELATED WORK

In 1999, Whitten and Tygar's Johnny study [22] raised awareness of the usability problems in email encryption with PGP 5. Only one third of their twelve participants was able to send encrypted and signed emails in their 90-minute test. 25% of the participants accidentally sent confidential information without encryption. Whitten and Tygar found significant problems with the user interface and questioned PGP's analogy between cryptographic and physical keys. They concluded that the interface *"does not come even reasonably close to achieving our usability standard"* and that it *"does not make [exchanging secure email] manageable for average computer users"*.

Garfinkel and Miller [10] built and evaluated a system based on key continuity management (KCM). Their prototype, CoPilot, addressed the problem of finding other users' public keys by automatically extracting senders' keys from incoming messages. Their study revealed that after using CoPilot for less than an hour, users generally understood the advantages of securing their emails. They found that while the KCM approach generally improved security, only a third of the participants chose encryption for confidential data and most sent information in an unprotected fashion. Some participants expected their email program to protect them from making mistakes and said that if encryption was important, a system administrator would have configured the email program to send only encrypted messages. This is a strong indicator that message encryption systems need to provide clear information about the security of the outgoing messages and apply security mechanisms automatically whenever possible [14].

Sheng et al. [20] conducted a follow-up pilot study to Whitten and Tygar's Johnny study with six novice users in order to understand the usability of PGP 9 and Outlook Express 6.0. Compared to the prior study of PGP 5, Sheng et al. found that PGP 9 made improvements in automatically encrypting emails, but the key verification process was still problematic and signatures in PGP 9 were actually more problematic than in PGP 5.

Outside of the messaging realm, there are several user studies that deal with Facebook privacy issues. Egelman et al. [5] ran a user study to examine how Facebook users cope with limitations of the Facebook privacy settings interface. King et al. [13] study the interaction of Facebook app users with the apps they use, what they understand of the apps' access and profile information exchange behaviour and how this relates to their privacy concerns. Wang et al. [21] identified problems in the authentication dialogs for third-party apps on Facebook, proposed their own interface designs and conducted a qualitative study evaluating their designs.

3. INITIAL EXPLORATION

Before exploring how users could protect their Facebook conversations, we conducted a screening study to gain an overview of the level of interest in protecting these conversations. We invited 16,915 students at the Leibniz University Hannover via email to participate in the study. It was introduced as a poll on Facebook privacy. We did not attempt to hide the fact that we were interested in Facebook message privacy, since we explicitly wanted to study those users who would like to protect their conversations. There was no direct reward for completing the poll, however the possibility of a paid follow-up study was stated.

In the poll, we queried some Facebook usage statistics and asked whether or not the participants thought that Facebook could read their private messages as well as whether or not this would be a cause for concern for them. We received 514 responses. Of these, 413 (80.35%) were aware that Facebook was able to access their private messages. When asked whether this concerned them, 263 (63.68%) answered "yes", 78 (18.88%) answered "no" and 72 (17.43%) stated they didn't care. The other 101 (19.65%) participants stated they were not aware that Facebook could read their private messages. When asked whether it would concern them if Facebook could read their private messages, 79 (78.21%) answered "yes", 12 (11.88%) answered "no" and 10 (9.90%) stated they did not care. In total, 342 (66.53%) of the 514 participants stated that they were or would be concerned by Facebook being able to read their private messages.

Since there were users who were concerned that Facebook could read their conversations, we used Google, Bing and Yahoo (in September 2011) and searched for products which could be used to encrypt private messages on Facebook. Encipher.it[5] and uProtect.it[6] were the top hits which could also be installed. The discontinued product FireGPG was not compatible with current browsers[7], so we did not consider it a viable solution that normal users could currently install.

3.1 Encipher.it

Encipher.it provides a *bookmarklet* for Firefox, Chrome and Internet Explorer (IE) that is capable of encrypting text in any HTML text area. Thus, to encrypt a Facebook message, the user writes the message text into the Facebook

[5] `http://encipher.it`
[6] `http://uprotect.it`
[7] `http://blog.getfiregpg.org/2010/06/07/firegpg-discontinued/`

message composer as usual and then has to click on the Encipher.it bookmarklet in the upper browser bar. Next, a popup in the centre of the screen appears and asks the user to "Enter encryption key". Internally, Encipher.it uses AES [18] in Counter Mode [19] for encryption, i. e. the same symmetric key is used for encryption and decryption. To derive a secure symmetric key from the user's input, PBKDF2[8] is used. After a key is entered, the user must press the "Encrypt" button. The bookmarklet then replaces the clear text in the Facebook message box with an enciphered version that can be sent as normal with Facebook's "Send" button. Key management is left entirely to the user, which means the user must find a secure way of sharing the encryption key with the receiving party.

3.2 uProtect.it

Unlike the generic Encipher.it solution, uProtect.it is a third-party service specifically designed for Facebook. The user has to create a uProtect.it account and needs to install the uProtect.it browser plugin. Plugins are provided for Firefox and Google Chrome as well as a bookmarklet for other browsers. After the user has created a new uProtect.it account and installed the plugin, a green bar appears at the top of the browser window and asks the user to log into uProtect.it when the user is on Facebook. Subsequently, orange encryption buttons are placed next to text areas. Messages are encrypted and decrypted by pushing the orange button.

Unlike Encipher.it, key management is handled automatically by the service. Unfortunately, uProtect.it does not provide any information concerning their internal security mechanisms. They do however state that they store the user content on their servers alongside the encryption keys. Thus, they are able to eavesdrop on the users' data, as stated in their Terms of Services[9].

3.3 Academic Solutions

Apart from the approaches above, which the average user can easily find on search engines, there are also several academic solutions such as flyByNight by Lucas et al. [16], Scramble! by Beato et al. [2], Musubi by Dodson et al. [4] and concept work by Anderson et al. [1]. These works mainly focus on the cryptographic aspects of their solutions and do not study the usability of their approaches. For more detail on these solutions, the reader is referred to Appendix A.

3.4 Extraction

Unlike in the related email-based studies, where relatively mature and stable implementations of PGP and S/MIME were available and could be studied directly, the solutions for Facebook are partly general purpose encryption products which can also be used with Facebook or early academic prototypes and niche products with usability issues which stem more from implementation limitations than design issues. For this reason, we decided to extract the design decisions and build mockups to study the basic building blocks and their usability issues. A further reason for choosing this abstract approach over a direct product evaluation was that the two available solutions, Encipher.it and uProtect.it, differ in several key areas, which would have made it very difficult to judge which features made the one more usable than the other. Thus, we extracted core features of the above solutions to study the usability of encryption for Facebook conversations.

Three features are particularly well suited to distinguish the above approaches: encryption UI, key management and integration. For the encryption UI, some solutions require the user to trigger the encryption process manually by activating a bookmarklet or pressing a button, others trigger encryption automatically. The different key management options require the user to get involved in the key management process by manually sharing or selecting keys, while other solutions automate this issue. A further feature is integration. Some solutions require the user to send private messages via a completely separate UI instead of Facebook's standard UI, while others integrate their solution into Facebook. In order to keep the study design as simple as possible, we chose to focus on integrated solutions, because we believe it is better not to force the user to leave the normal Facebook UI. Table 1 gives an overview of the values for the two remaining variables in the two real-world solutions. Based on this extraction, we built four mockups, described in the following section, which were then used for the laboratory study.

Table 1: A comparison of key management and encryption/decryption concepts applied by Encipher.it and uProtect.it.

	Encipher.it	uProtect.it
Key Management	manual	automatic
Encryption	manual	manual

4. FIRST PROTOTYPES

To evaluate the different interface and workflow concepts for sending encrypted Facebook messages as discussed above, we built mockups using Greasemonkey[10]. The mockups allowed us to test the independent variables shown in Table 1 in the context of sending encrypted private Facebook messages. Screenshots of the mockups are shown in Figures 1 and 2.

4.1 Mockups

Figure 1 shows mockups 2 and 4 corresponding to manual encryption combined with both manual and automatic key management. In the case of manual encryption with manual key management, the user enters the message text as usual (Step 1). The user must then click the new "Encrypt" button. A popup asks the user for an encryption password with which the message is encrypted (Step 2) and the resulting ciphertext is placed in the message box. The user can then send the message using the original "Send" button (Step 3). The encryption password must be shared with the recipient manually. This corresponds to the Encipher.it workflow. All steps are repeated for every message sent.

In the case of manual encryption with automatic key management, the key management model from uProtect.it is used to replace the manual key management of Encipher.it. This means that Step 2 only needs to be executed once per Facebook session, since the password can be cached locally and the entered password does not need to be shared manually with the recipients.

[8] `http://www.ietf.org/rfc/rfc2898.txt`
[9] `https://uProtect.it/terms`
[10] `http://www.greasespot.net/`

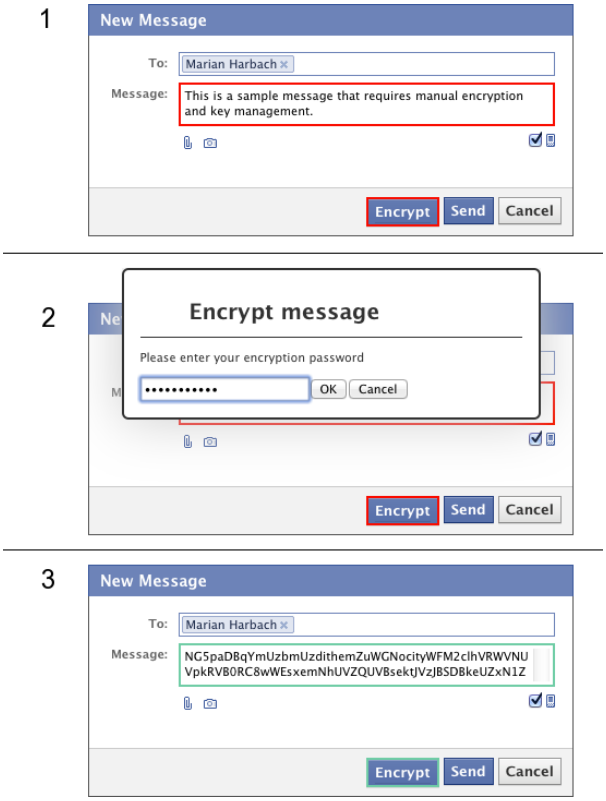

Figure 1: The three steps in mockups 2 & 4

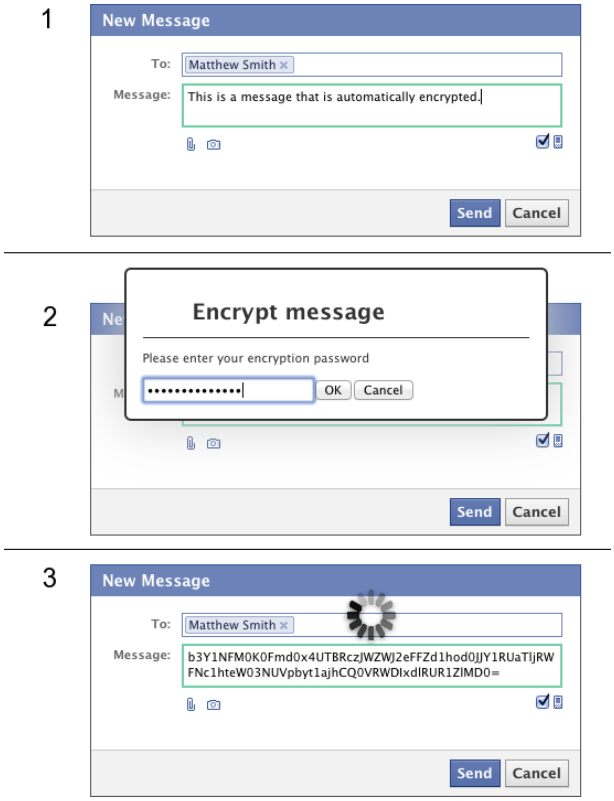

Figure 2: The three steps in mockups 3 & 5

Figure 2 shows mockups 3 and 5 corresponding to automatic encryption combined with both manual and automatic key management. With these mockups, the user does not need to manually trigger encryption. Rather, when the Facebook "Send" button is pressed (Step 1), encryption is triggered automatically. In the case of manual key management, the user needs to choose an encryption password for each message to be sent and share it with the message recipient manually (Step 2). In the case of automatic key management, the user only needs to enter the password once per Facebook session, as in the uProtect.it workflow. In order to offer a similar amount of visual feedback as in mockups 2 and 4, the message is not sent instantly after completion of Step 2. Instead the ciphertext is shown in the message composer's text area with a spinner animation for two seconds to visually indicate successful encryption after which the message is sent (Step 3).

We also added red and green visual security indicators to the text area and the "Send" button of mockups 2-5 as a visual aid, as suggested by Egelman et. al. [6] and Maurer et. al. [17].

In addition to mockups 2 to 5 described above, we built mockup 1 without any modifications of the Facebook message composer to serve as control condition.

5. LABORATORY STUDY

Based on the concepts and mockups presented above, we conducted a laboratory study. The goal of the study was to evaluate the basic building blocks of a message protection mechanism. We therefore tested the influence of manual vs. automatic encryption and manual vs. automatic key-management on usability, acceptance and perceived security. We also wished to find out what role password or key recovery plays in the acceptance of an encryption mechanism. Depending on the cryptographic principle used, the loss of the encryption key can result in complete loss of the encrypted data in case the key cannot be recovered and as a result decreases both the acceptance and the utility of a solution.

During the study, each condition (cf. Table 1) was dealt with in a separate task with a separate mockup. Table 2 gives an overview of which condition is dealt with in which task.

Table 2: Properties of the tasks in the lab study.

Task	Interface	Encryption	Key Management
T01	Facebook	None	None
T02	Mockup 2	Manual	Manual
T03	Mockup 3	Automatic	Manual
T04	Mockup 4	Manual	Automatic
T05	Mockup 5	Automatic	Automatic

5.1 Technical Setup

The study took place in our usability lab, where we had set up a PC with Firefox 9, Greasemonkey, the mockups and a webmail interface for each participant. We created artificial Facebook accounts and email addresses, so that the participants did not have to use their real accounts and data. The mockups simulated sending private messages, rather than actually sending the messages which might have accidentally triggered the anti-spam protection of Facebook, resulting in blocked accounts. However, we did ensure that we simulated the behaviour of Facebook's standard message composer, so

that participants would not notice that messages were not actually sent.

5.2 Participants

For this study, we were interested in participants who would potentially want to use an encryption mechanism to protect their Facebook conversations. Educating or motivating participants who are not worried about their conversation's privacy is outside the scope of this work. We randomly selected test candidates from the poll participants (cf. Section 3), who met the following criteria: they needed to be concerned that Facebook could access their private messages and needed to use Facebook at least on a weekly basis. We excluded infrequent Facebook users to minimise the risk of technical difficulties when using Facebook. Finally, we excluded computer science students to avoid bias based on technical skills and possible familiarity with encryption mechanisms.

This left us with 291 possible candidates, from whom 100 were randomly selected for the study. 96 of these attended their appointed slot. Each participant received a compensation of 10 Euros. All participants were students from the Leibniz University Hannover. Appendix B gives demographics for the participants.

5.3 Ethical Considerations

The study was conducted in Germany and thus was not required to pass an IRB review. Nevertheless, our studies complied with the strict German privacy regulations. We did not use the participants' real Facebook accounts and all data was collected anonymously. After the study, the participants were debriefed and any questions regarding the study were answered.

5.4 Procedure

The participants were informed that they would be testing five different technologies to encrypt Facebook conversations. To avoid bias, we explained that the technologies were not built by us and that we were testing the technologies, not the participants. Each participant was watched by a study monitor, who measured the time needed to complete each task and noted errors. The monitor was allowed to assist with the browser tabs and the webmail program, but no help or information was given concerning the mockups or the tasks themselves. The next section outlines the basic structure of each task (cf. Table 2).

5.4.1 Tasks

To keep the design simple, all tasks were focused on encrypting and sending private Facebook messages to three different friends (Jan, Vanessa and Heike). The decryption process is analogous to encryption and was therefore not tested explicitly.

Handouts were given to the participants which explained the procedure of sending an encrypted message with the given technology. The messages to be sent were as follows:

To Jan: Hello Jan. Please transfer the money to my bank account, account number 123456 and sort code 100200.

To Vanessa: Jan has transferred the money to my bank account.

To Heike: Hi Heike. Have you transferred the money yet?

Since all participants had a self-reported interest in protecting their Facebook conversations from unauthorised access, we chose sample messages which contained financial information with the aim of inducing a similar wish for privacy in all participants.

T01 was the control group task. Participants were asked to send the messages using the normal Facebook message composer. The task was used to get a baseline for error rates and speed of the individual participants. Like in the other tasks, the participants were told that their messages were encrypted. In contrast to T02 to T05, message encryption was not featured explicitly, but included in the regular sending process without visual indicator or actions. The control task therefore additionally lends itself to examine whether or not the participants would accept and trust a mechanism that provides "invisible" security.

During the manual key management tasks (T02 and T03), the participants needed to use the webmailer to send an arbitrarily chosen key to the corresponding recipients out-of-band. Using webmail is of course not the optimal out-of-band solution in terms of security. However, since the study's focus was on the Facebook UI and not the out-of-band communication capabilities of the participants, it was used as a mechanism which would cause little technical trouble during the study. In a real world setting additional problems could arise here.

In the automatic key management tasks (T04 and T05), only the first message required the participants to enter their password. The password was cached for the rest of the session.

The only difference between the manual and automatic encryption tasks is that the "Encrypt" button needs to be pushed before sending the message.

5.5 Study Design

Since the study encompassed reading and comprehension, we chose a within-subjects design [15]. To minimise the bias of the learning effect, we also chose a random latin square setup, so that each task was equally distributed over each position in the within-subjects design.

In the post-task questionnaires for each of the five tasks (cf. Section 5.4 and Appendix D.2), we collected the system usability score (SUS, ten items addressing multiple facets of general system usability [3], see Appendix D.2) as well as additional items concerning the users' willingness to use the corresponding mechanism in the future for private and general messaging ("acceptance"). A final item gauged how well the users felt their messages were protected.

After completing the tasks, the participants were given a final questionnaire (cf. Appendix D.3). Apart from gathering demographic information, the questionnaire also presented a hypothetical question, asking whether or not the participants would use an encryption method which would render all previous encrypted messages unreadable if they forgot their password. We also asked supporting questions to ascertain the reasoning behind this decision.

5.6 Results

Across all cases, we found the highest mean system usability score (SUS) in T04 (86.51) and T05 (89.79), as well as in the control T01 (88.20, cf. Table 3). T04 and T05 also received the highest acceptance ratings for both private and general messaging. However, the users felt best protected

in T02 and T03. Additionally, Appendix C describes who or what was perceived to be the biggest threat for the privacy of the users' Facebook conversations.

Table 3: Mean usability (SUS) and acceptance for private (a_{priv}) and all messages (a_{all}), as well as security feeling (sf) across tasks.

Task	SUS	sd_{SUS}
T01	88.20	15.32
T02	64.27	18.56
T03	65.86	18.43
T04	86.51	11.43
T05	89.79	14.20

Task	a_{priv}	sd_{priv}	a_{all}	sd_{all}	sf	sd_{sf}
T01	2.62	1.438	2.67	1.449	1.57	0.778
T02	3.19	1.439	1.87	1.136	3.49	1.133
T03	3.35	1.421	1.87	1.117	3.42	1.158
T04	3.87	1.259	2.91	1.437	3.20	1.148
T05	3.92	1.319	3.30	1.415	3.23	1.174

We aggregated the SUS and acceptance ratings for tasks with (non-)automatic key management (T02-T03 and T04-T05) and encryption (T02-T04 and T03-T05) respectively. Normality tests indicated significant or almost significant deviations for these scores and ratings, since the distributions were cut off at the upper score-interval boundary. Therefore, we used the non-parametric Wilcoxon Signed Ranks test to analyse the scores and ratings. We found a significant difference in SUS for automatic key management ($Z = -8.102$, $p < .01$) and automatic encryption ($Z = -3.230$, $p < .01$). We found similarly significant differences in acceptance ratings for all messages with respect to automatic key-management ($Z = -6.884$, $p < .01$) and automatic encryption ($Z = -2.692$, $p < .01$). Acceptance for sending private messages differed significantly for automatic key-management ($Z = -3.644$, $p < .01$) but not for automatic encryption ($Z = -1.637$, $p = .102$). We therefore conclude that an optimal workflow would use automatic key management while automatic encryption did not have a significant impact in the study.

To test how fear of losing data influences the need for password recovery, we divided the participants into those who stated that they were worried or very worried about losing all their old messages or forgetting their password (group A, $n = 49$) and those who were not (group B, $n = 47$), using top-2-box scores of a 5-point Likert scale. We found a significant difference between group A and group B using a Chi-Square Test concerning whether or not they would use a mechanism without password recovery ($\chi^2_1 = 18.383$, $p < .001$) and whether or not they would prefer a mechanism with password recovery ($\chi^2_1 = 10.341$, $p < .001$). In group A, 72.3% would not use a mechanism without recovery and 78.7% would prefer a mechanism with password recovery, while in Group B these figures were 28.6% and 46.9% respectively. Hence, we believe that password recovery is desirable for users, especially for those who worry about forgetting their password.

To test the correlation between the perceived usability and the stated acceptance of a message protection mechanism, we used Spearman's rho and found significant values in all five tasks (see Table 4). However, the correlations are only weak to medium and therefore merely suggest that higher usability correlates with higher acceptance. We investigated this issue further in the interviews (cf. Section 8).

Table 4: Spearman's correlation between usability and acceptance for private/all messages across tasks.

Task	$\rho_{private}$	p	ρ_{all}	p
T01	.253	$< .05$	.260	$< .05$
T02	.554	$< .01$	.361	$< .01$
T03	.466	$< .01$	.249	$< .05$
T04	.533	$< .01$	.407	$< .01$
T05	.530	$< .01$	.507	$< .01$

In order to investigate the perceived level of protection across mechanisms, we ran a Friedman test on the participants' answers concerning their perceived protection in tasks T02 through T05. We found a highly significant difference in the mean ranks ($\chi^2_3 = 15.947$, $p < .001$). The top-2-box scores show that in tasks T02 and T03 54.2% of the participants felt well protected and in T04 and T05 only 41.7% and 40.6% felt the same way. We therefore suspect that the complexity of a mechanism – in this case creating individual encryption keys for each recipient and distributing them manually – heightens a user's subjective sense of security. However, we could not find any meaningful correlations to support this.

It is noteworthy that only 2% of the participants felt well protected in the control task. Even though they had been told that the mechanism presented in T01 would protect their message, they apparently placed little faith in this statement. While this could be due to their familiarity with Facebook, we also suspect that an entirely invisible and effortless protection mechanism does not generate a feeling of security and is not trusted by users. This is an interesting question, since "invisible" security is often claimed to be a desirable feature. However, our results suggest that trust in the mechanism could be a problematic issue. This study was not set up to analyse this observation further, but this issue might be worth a dedicated investigation in the future.

6. USABLE FACEBOOK CONVERSATION ENCRYPTION

Our aim was to create a security system with good usability which addressed the concern that Facebook and potentially other third parties could read private messages sent via Facebook. Considering the findings of the lab study, we based our design on the interface and workflow of mockup 5. While the manual key management mockups 2 and 3 created a higher security feeling, they also had significantly lower acceptance and usability scores. We chose mockup 5 over mockup 4 due to the higher acceptance and usability scores of 5. While mockup 4 included some manual operations, there was no significant difference in the perceived level of protection between mockup 4 and 5.

In a work-in-progress poster [11], we presented some preliminary work on our solution, which we expanded in the following. One of the key decisions for our implementation concerns the use of a PKI. Based on the fact that previous Johnny studies have shown that PKI based key management and message protection has severe usability problems, we decided to avoid the use of a PKI and opt for a simpler approach. Hence, our implementation of message

encryption for Facebook addresses confidentiality and integrity, using the non-cryptographic message authentication offered by Facebook. By dispensing with digital signatures, it was possible to create a simpler overall system. This is a security/usability tradeoff. Since the main aim of protecting users' private messages from entities which are currently able to read them can be achieved with confidentially alone, the reduction in complexity was the deciding factor in this matter.

However, we would like to briefly discuss message authentication in the social web. The use of Facebook brings about some interesting changes in certain aspects of the message authentication landscape. While emails can be easily forged and are also used to initiate communication with unknown communication partners, in the social network context much of the communication over Facebook is conducted in the context of "friendship-connections" which are established a priori and filled with additional information. This reduces the need for authentication on the message level to a certain extent. While there are social-engineering-based attacks, in which users can be duped into falsely believing a message originated from a friend, we believe these are currently less relevant than for example email-spoofing attacks. This makes the lack of message level authentication less problematic for a social web context than for emails. However, this last statement is speculative and needs to be the focus of a separate study.

The choice to offer only confidentially also enabled us to offer a key recovery feature that allows users to recover their encryption passwords. For this, we opted for a service-based approach offering confidentiality as a service which we named FBMCrypt. Special attention was paid to creating a service that does not enable the FBMCrypt provider to access the private messages, but allows automated key management at the same time. To enrol in the service, a user needs to register and bind his Facebook account to FBMCrypt. This will be illustrated in the following.

6.1 Registration

For registration with the FBMCrypt provider, we chose a simple username/password authentication scheme, since this method is a well-known scheme to Web 2.0 users. Although passwords are not the strongest authentication credentials, they enjoy widespread application and are the most widely accepted concept by online users [12]. The registration process relies on Email-Based Authentication and Identification (EBIA) [9], the most prevalent authentication scheme for online accounts.

6.2 Account Binding & Browser Plugin

Once the registration process is complete, the user needs to bind his Facebook account to the newly created FBMCrypt account. This is initiated by clicking a button to log into Facebook using Facebook's Social Plugin API.
After Facebook has confirmed the authentication – through Facebook's OAuth mechanism – the user agrees to allow the FBMCrypt provider to see the email address registered with Facebook. The FBMCrypt provider uses this email address to send a second validation link, which establishes that the currently logged-in FBMCrypt user also has access to the Facebook account in question and can furthermore read email sent to that account. This process only proves that the current FBMCrypt user has access to the Facebook account, but does not give the FBMCrypt provider access to the Facebook account. After the successful binding of a Facebook identity to a FBMCrypt account, the user is subsequently able to use the FBMCrypt provider's services with the bound Facebook identity.

The user finally needs to install a browser plugin which handles the actual encryption and decryption of the messages. Similar to the mockups, our prototype plugin uses a Greasemonkey user-script, which is easy to install. The plugin communicates transparently with the FBMCrypt provider and handles all the cryptographic operations for encryption and decryption without requiring any further user involvement, apart from entering the FBMCrypt password once per session.

6.3 Sending an Encrypted Message

The FBMCrypt plugin automatically checks if the recipients of a message are registered with the FBMCrypt service. If they are not, the message cannot be encrypted and can only be sent in the clear. We modified the message composer to make the user aware of an unencrypted message exchange, as illustrated in Figure 3.

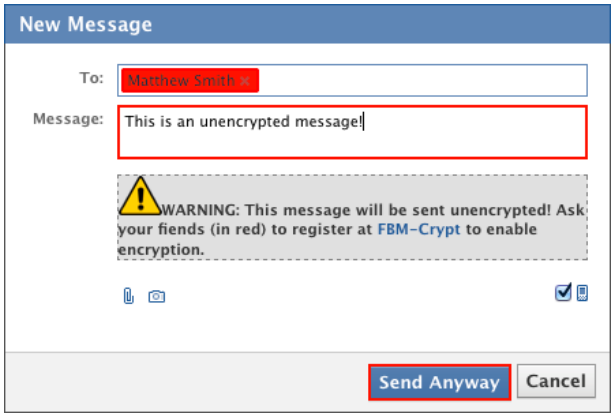

Figure 3: The modified message composer in case a message will be sent unencrypted.

If the recipients are enrolled with the FBMCrypt service and the "Send" button is clicked, the FBMCrypt plugin connects to the FBMCrypt service over a secure HTTPS connection. The plugin authenticates the user to FBMCrypt by sending the previously bound Facebook ID and the user's hashed FBMCrypt password. The plugin then triggers FBMCrypt' automatic key management (cf. [8]) procedure and encrypts the message.

Before actually sending the encrypted message via Facebook, the plugin prefixes *##caasfb##* to the message to allow for automatic decryption on the recipient's side.

6.4 Reading an Encrypted Message

To read an encrypted message, decryption is integrated into the usual workflow as transparently as possible. The plugin automatically analyses the messages site and searches for FBMCrypt-encrypted ciphertexts. If one is detected, the plugin checks the user's credentials, authenticates him to the FBMCrypt service and triggers automatic decryption. Figure 4 shows the message view with a decrypted and encrypted message.

Figure 4: Cleartext and ciphertext of a FBMCrypt protected message

A more detailed technical description of the confidentiality as a service backend and the encryption mechanism as well as a security discussion can be found in [7, 8]. The following focuses mainly on the usability aspects of the message protection mechanism.

7. SETUP PROCESS EVALUATION

The registration and account binding procedure (cf. Sections 6.1 and 6.2) was designed to enable FBMCrypt to fulfil the requirements derived from the laboratory study. Since these steps form the basis for the rest of the system and poor design could potentially deter users from the outset and make further development unnecessary, we conducted an initial study of the registration and binding design to ensure the usability of our concept, before proceeding with the development of the rest of the system.

We ran a field study with 20 participants (all undergraduate students, 9 females, 11 males, with an average age of 23) and asked them to register an FBMCrypt account, bind that to a Facebook account and install the plugin. Since this was only a simple ten minute task to eliminate early issues in the design phase, we recruited students randomly on campus. We asked them if they were Facebook users and interested in participating in a ten minute scientific study that was about a security mechanism for their private Facebook messages in exchange for some candy bars.

The technical setup was similar to the lab study: we provided a laptop with Firefox 9 and Greasemonkey and asked them to log into their Facebook and email account. We deleted all browsing data after the experiment ended. For this initial study, we were interested in the time needed to set up a working FBMCrypt plugin installation and corresponding error rates.

All participants were able to successfully create an FBMCrypt account, bind the account to Facebook and install the FBMCrypt plugin for Facebook. On average, the entire process took 3 minutes and 8 seconds, with a range of 90 seconds to 6 minutes and 18 seconds. Since no problems with the installation and binding process were identified, the design was integrated into the rest of our approach.

8. FINAL STUDY

To evaluate the usability of the proposed FBMCrypt service (c. f. Section 6) as a whole, we conducted a final study with 15 participants in which the entire process was evaluated in conjunction with an online survey and a semi-structured interview. During the study, one interviewer and one assistant were present.

8.1 Participants

We randomly recruited the participants from the same pool of users that we used for the laboratory study, excluding those that had already taken part. There were 6 male and 9 female participants. On average, their age was 22 ($sd = 3.39$) and 13 of them had been using Facebook for more than a year. Three of them had forgotten their Facebook password at least once and 14 used Facebook for at least one hour per day. They had 233 Facebook friends on average ($sd = 125$) and all of them sent at least five private Facebook messages per week. More detailed demographics can be found in Appendix E.

The technical setup and procedure was analogous to the laboratory study, except that during the task participants were audio recorded and asked to "think aloud". To test our encryption mechanism for Facebook conversations, all participants were asked to fill out an online survey, complete a task involving three subtasks and participate in a semi-structured interview. The entire study lasted between 28 and 44 minutes ($mean = 33$, $sd = 4$).

8.1.1 Task

Firstly, the participants were asked to register for the FBMCrypt service. After the EBIA procedure (cf. Section 6.1) was completed and a new FBMCrypt account created, this account had to be bound to the Facebook account provided for the participants (cf Section 6.2). Successfully binding the accounts allowed the participants to install the encryption plugin as the last step of the first subtask. After the plugin was installed and operational, they started with the second subtask.

Here, the participants were asked to have an encrypted Facebook conversation with the assistant. The conversation was initiated by the assistant, who sent the following message: *Hi <participant's first name>, what is your major at university?* Next, the participant was asked to answer the question as he would usually do when sending a Facebook message. The assistant sent a new encrypted message: *Sounds interesting. Do you happen to know what AES is?* Depending on the participant's answer, the assistant either answered: *No problem, thanks anyway and have a nice day!* or *Thank you very much, you really helped me. Have a nice day!*

Finally the last subtask was to send another pre-defined Facebook friend an arbitrary message. This friend, however, was not yet registered with FBMCrypt. In order not to bias the participants, we did not indicate that this message would be sent in an unencrypted fashion.

8.1.2 Interview

The interview component of the final study was conducted as a semi-structured interview. The framework of themes to be explored during the interview encompassed a usability evaluation of the encryption service registration, binding and plugin installation, sending/reading an encrypted message, the perceived security and reasons for or against the proposed password recovery mechanism (c. f. Appendix F).

8.2 Data Analysis

We transcribed the audio recordings of the interviews. Trends were identified and answers grouped into categories for each question in the interview.

8.3 Results

This section presents the findings of our final study. Firstly, we describe the reception of the FBMCrypt registration, binding and installation process, such as how users feel about creating an extra FBMCrypt service account, choosing a different password than the one for their Facebook account and installing the plugin. Section 8.3.2 describes usability findings while sending and receiving encrypted Facebook messages. Section 8.3.3 describes the perceived security while using FBMCrypt. The last subsection discusses the participants' attitudes to the key recovery feature.

We refer to the participants as $P01, P02, \ldots, P15$. $P14$ stated that he already used a mechanism to encrypt his Facebook messages. No participant used any encryption for their email, though $P02$ and $P06$ already had experience with software to encrypt their hard disks. $P05$ and $P07$ did not know whether they used any software to encrypt their data and the rest stated they did not use any encryption mechanism. We asked the participants to rate their computer expertise by telling us how they handle computer problems they or their friends have. $P02$ and $P15$ self-reported their computer expertise as high, $P06, P09$ and $P13$ as medium and the rest as low.

Table 5: Case study post-task survey. (1=Strongly disagree; 5=Strongly agree)

$N = 15$	*avg*	*sd*
I'm sure that I used the mechanism correctly	3.93	1.03
I would send sensitive messages with this mechanism in the future	4.06	0.96
I would send all my messages with this mechanism in the future	3.46	1.06
I have the feeling that my messages are now well protected	3.53	1.06
I found applying the encryption mechanism irksome	1.67	0.89

The mean values we found using the post-task survey were slightly better than those in the lab study (cf. Section 5.6), but there were no statistically significant differences. Table 5 gives a descriptive overview of the survey answers.

In general, after creating a new FBMCrypt account, installing the browser plugin and actually encrypting messages, participants were confident that they were using the system correctly, would like to send future messages protected by the FBMCrypt mechanism and did not perceive the encryption as obstructing their workflows. The following subsections will discuss the results of individual aspects of our final study.

8.3.1 The Setup Process

We asked our participants about their impressions of the registration, binding and installation process of the FBMCrypt service and plugin. Additionally, we asked the participants to compare the process with creating a Facebook or an email account. During the task, all 15 participants were able to successfully register an FBMCrypt account, bind this account to the provided Facebook account and download and install the plugin. On average, the complete setup phase took 3:51 minutes ($sd = 51s$).

In the interview, we first asked the users to rate the account registration process itself. Overall, the registration process was described as *"easy"* and *"appropriate"* in the context of online service accounts. P02 said *"I would describe the effort involved in setting up such an account as relatively small. I think it took me about 30 seconds – if it really helps to protect my messages this is definitely worthwhile."* Only P07 described the registration process as *"complex – just like setting up my Facebook account. For that I asked my boyfriend to help me to setup the account."* and described the registration effort as *"too high"*. Two participants added a condition to their rating and said the effort would be acceptable if the service really provided protection for their data and was not a subsidiary of Facebook. Eight participants described the FBMCrypt registration process as *"more pleasant"* than creating a new Facebook account, because *"they did not want to know so much information, such as my birthday or phone number"*.

All participants described the fact that the FBMCrypt password needed to be different to the user's Facebook account as *"understandable and unproblematic"*. P10 said *"using two different passwords for Facebook and the encryption service is obvious, because every hacker that knows my Facebook password also would try this password to login to my FBMCrypt account to read my conversations. And if both passwords are the same the encryption would be pointless."* 11 participants stated they used different passwords for online services that they either memorise or write down. The rest used three to six different passwords for all their online accounts. In general, the participants stated that they rarely forgot or lost their passwords – only *"passwords for services I rarely use"* (P06, P08, P10, P12) were liable to be forgotten. P12 added: *"but in this case there is this great 'lost password' button I already had to use a couple of times"*. In contrast to other online services, Facebook passwords were forgotten less frequently. Only P06 had once forgotten her Facebook password. The participants estimated that their FBMCrypt password would be as *"safe"* as their Facebook password, because encryption service is so *"closely linked"* to their Facebook account: *"If I have to enter my FBMCrypt password each time I read my Facebook messages, I am pretty sure not to forget it [because I use Facebook so often]"*.

The account binding process was rated as *"coherent"* and *"appropriate"* in general. Three participants had security concerns during the binding process. Two participants (P02 and P12) falsely identified the binding process as a Facebook App, which they distrusted in general and did not use. P02 said: *"in general I have an aversion to Facebook apps, because I don't know what information they secretly use"*. During the "think aloud" phase, P05 said she would not have downloaded and installed the plugin on her own laptop because *"my boyfriend told me not to download anything from the Internet"*.

8.3.2 Encryption/Decryption

We asked the participants to rate the process of sending and receiving encrypted as well as unencrypted private Facebook messages. Two participants (P11 and P14) would use FBMCrypt to send *"sensitive"* messages but not *"smalltalk messages that are not very private"* (P11). The other participants said they would like to send *"all messages with FBMCrypt enabled, if possible"*. The *"if possible"* condition had two different manifestations – two participants (P01 and P08) would use it for all their messages if they felt that the

service *"really was secure"* and the second group of participants would send all their messages with FBMCrypt if the service gained widespread adoption and their friends used it as well.

We asked the participants to attribute properties to the process of sending and reading (un-)encrypted messages with the FBMCrypt plugin. The participants gave answers such as *"uncomplicated, simple, secure"* and *"as easy as without the service"*. P15 stated: *"I thought there would be annoying popups and I really liked that none appeared."*. P10 described it as an *"invisible assistant"*. Next, the participants were asked to describe the interface for sending and reading (un-)encrypted messages. Two participants (P04 and P14) did not perceive any difference compared to the normal interface.

The green and red borders, indicating encrypted and unencrypted messages respectively, were thought to have two different meanings. Six participants interpreted the different border colours as *"a green border stands for secure messages"* and *"a red border stands for insecure messages"*. Four participants said the green border indicates their conversation partner *"also has the programme installed"* while a red border indicates the conversation partner is not an FBMCrypt user. Six participants noticed that the ciphertext was displayed before an encrypted message is sent or an encrypted message is decrypted. Five participants stated they saw that the messages were encrypted *"because of the jumbled up text that was displayed"*. Four other participants described the ciphertext as *"jumbled up text"* but did not recognise it as ciphertext. However, the presence of ciphertext did not disturb them in their workflow or caused concern.

All but one participant (P13) would recommend FBMCrypt to their friends to enlarge the group of people they can securely communicate with. We also asked the participants if they would be willing to pay money to encrypt their Facebook conversations. Four participants said no – while P01 would not pay money for such a service for herself she said: *"if I had children who used Facebook, I would pay money to protect their privacy."* All the others were willing to pay *"a small amount of money"*. Five participants preferred a single payment: *"the price should be similar to an iPhone App"*. Seven participants stated that they could imagine paying a *"monthly fee"* ranging from 5 to 10 Euros.

8.3.3 Perceived Security

We were interested to see if the application of FBMCrypt affected the perceived security of the participants. Firstly, we asked the participants whether they would send messages which are more confidential via Facebook if FBMCrypt were used. None of the participants affirmed this. All of them said they could not sufficiently *"trust"* the encryption mechanism at this point because they could not verify if it was functioning properly. So while they were all satisfied with the usability and would use FBMCrypt for their current messages, messages with a higher level of confidentiality would still not be sent over Facebook.

Participants' views on this can be divided into two groups: Four participants were sceptical by default and would not trust computer systems in terms of data security without more detailed knowledge. P06 said: *"in the Internet, you can download a program to crack everything, so I do not trust computer systems in general. This is similar to online banking. Although I see this little lock in my browser, I am not really sure that no one can steal my data [because I think anyone could put a lock like that in my browser bar]"*. The second group of 11 participants did not trust the mechanism because they did not know *"if it really works"*. P02 (who also falsely identified the FBMCrypt plugin as a Facebook App) said: *"I really cannot say if the program does what it purports to do. I mean, any app could probably draw a green border around my message to simulate security. I would need some proof of security."*.

To investigate why the participants were so sceptical and to ascertain what could be done to alleviate their doubts, we asked why they did not trust the mechanism. They all said they could not verify whether or not the mechanism really did what it said and needed *"proof"*. When we asked what kind of proof that might be, there were three types of answer. Three participants said they would trust *"reports in specialist magazines"*. Participant P10 said his trust would depend on the operator of the FBMCrypt service: *"I would trust the encryption service if it was operated by a university or a nonprofit organisation that campaigned for privacy on the Internet."*. The remaining participants would trust the judgement of *"friends that know computers well"*.

We also asked the participants if the application of FBMCrypt influenced their perception of privacy. Eight participants stated that they had a more positive perception of their message privacy when using FBMCrypt. Two participants (P04 and P09) referred to the displayed ciphertext before sending a Facebook message as the reason for their changed perception. P15 said that *"installing the extra program made me feel better"*. P05 said: *"entering a second password results in a double protection for my messages which makes me feel more secure."*. The rest of the participants said that applying FBMCrypt did not improve their perception of privacy.

8.3.4 Password Recovery

To get a better understanding of the trend towards preferring a mechanism that allows for key recovery (cf. Section 5), we asked the participants if they would use the FBMCrypt mechanism if *"losing the password resulted in not being able to access messages that were encrypted with the FBMCrypt mechanism"*. Eleven of the participants would not use the service if losing the password resulted in losing their messages. P15 said: *"I sometimes use Facebook to share important job-related information. [...] I would definitely need a recovery mechanism because losing access to my data would be disastrous."*. Five participants suggested integrating a password recovery mechanism similar to Facebook's. P15 wanted a *"more secure recovery mechanism with telephone verification in addition to a confirmation email."* Only one participant stated that she would not use a mechanism with password recovery because of security concerns (P12): *"This would be much less secure, because a hacker who has access to my email and Facebook account can then also decrypt my Facebook messages."* Three participants of this group said they *"never read old Facebook messages"* (P05 and P03) or they would ask the conversation partner about the content (P6), hence they were unconcerned about losing access to their previous conversations.

We also asked the participants if they would prefer a password recovery mechanism. Twelve participants would prefer a password recovery mechanism. Most said that they could not guarantee that they would never forget their password

(even if *"from an empirical point of view, my risk is very low"* – P05) but they did rely on being able to access their archived messages. Again, P12 would not chose a password recovery mechanism because of security concerns.

8.4 Discussion

During the task, we focused on the usability of the FBMCrypt service and the participants' willingness to use the mechanism. The results show that most participants rated the registration, binding and installation process as appropriate and easy in terms of usability. The few participants who found it too complex or had other concerns described themselves as *"untalented"* computer users who often asked others for help. All participants described the process of sending encrypted messages and reading encrypted messages as *"normal"* and non-disruptive and most would use FBMCrypt to send all their private Facebook messages if their friends were using it as well.

All but one participant noticed the visual security indicators and most of the participants connected them to *"message security"*. An interesting finding during the interviews was that the displayed ciphertext was perceived as a trustworthy indicator for functioning encryption while the green and red borders were not. This aspect should be explored in more detail in further studies. A second interesting finding is that while the participants confirmed good usability attributes, the problem of establishing trust was described as something FBMCrypt itself could not provide. Instead, third parties were described as sources of information and trust. Some participants seemed to expect more overhead when encrypting a message. While Whitten and Tygar [22] as well as Garfinkel and Miller [10] showed that too complex a system results in rejection, the question of whether an appropriate amount of overhead could improve the perceived privacy and hence increase acceptance is an interesting one.

9. LIMITATIONS

The work presented in this paper has the following limitations. Precision: due to the within-subjects design of our lab study, carry-over and fatigue effects could have affected the study results. While a brief between-subject analysis based on the latin square setup did not show any worrying trends, a larger dedicated between-subjects study would be needed to rule out these effects.

Generalisability: Participants were all university students, selected for their frequent use of Facebook and their desire for Facebook message privacy. We believe the two selection criteria are valid, since this is the target group of our Facebook encryption mechanism. However, future studies of participants outside the university's demographic is of course desirable. Additionally, extending the sample to include non-privacy-aware users could also yield interesting insights into why people do or do not wish to protect their messages and how technology affects this.

Realism: The participants were restricted to using the computer provided for them during the study and using dummy Facebook and email accounts. Furthermore, only the first-time user experience was studied; we did not examine daily usage behaviour. Long-term studies using real Facebook accounts would address this.

10. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented several user studies concerning conversation security on Facebook. In an initial screening study with 514 participants, we showed that within our student population, there is a desire to protect Facebook conversations. We identified two key design features of existing solutions: automatic or manual key-management and encryption. In a laboratory study with 96 participants, we tested the four combinations of these features using mockups and found highly significant preferences for automatic key-management and automatic encryption. Furthermore, participants who were worried about forgetting their password or losing access to their previous conversations stated that they would not use a mechanism without password recovery. Even though the automatic mechanisms had the higher acceptance rate, we also found that the two more complicated encryption mechanisms generally made the participants feel better protected.

As a result of our findings in the user studies, we designed and implemented an encryption mechanism for Facebook conversations. Several key design decisions were made to provide good usability. A service-based approach was chosen, providing confidentiality and integrity with automatic key management and recovery instead of burdening the user with complex cryptographic details. Security/usability trade-offs in this paper were made considering the context of the Web 2.0 and Online Social Networks. For cases where these trade-offs are acceptable, our solution offers better usability than the email encryption systems tested in previous Johnny studies: All our study participants successfully encrypted their Facebook conversations without making any mistakes.

The interviews conducted during the final study revealed that usability alone is not a sufficient incentive for accepting a mechanism for message security on Facebook. Many interviewees stated that actually seeing the mechanism do something – displaying ciphertext for example – heightened their perceived protection. However, we also found considerable distrust of security software in general. Participants stated that they would need to be convinced of the correctness by friends or trusted third parties, such as computer magazines before entrusting sensitive information to a message security mechanism. While this last statement was made after using the presented mechanism for Facebook conversations encryption, the interviewees often stated that this was a general attitude they had towards unknown security software.

The issue of trust is a particularly interesting area for future work. Further studies should analyse how users develop trust in a solution and what can be done to support this process. We also plan to analyse the impact of key recovery features in more detail, especially over a longer timespan. Furthermore, the study in this paper did not handle the visual security indicators as an independent variable. While the visual indicators were well received, a dedicated study to optimise their effect is planned. Another question that arose is when and why users would actually care enough to encrypt their Facebook conversations. Hence, it would be interesting to study the sociological implications of confidentiality for Facebook conversations in more detail.

11. REFERENCES

[1] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano. Privacy-enabling Social Networking over Untrusted Networks. In *Proceedings of the 2nd ACM Workshop on Online Social Networks*, pages 1–6, 2009.

[2] F. Beato, M. Kohlweiss, and K. Wouters. Scramble! Your Social Network Data. In *Proceedings of the 11th International Conference on Privacy Enhancing Technologies*, pages 211–225. Springer, 2011.

[3] J. Brooke. SUS: A "Quick and Dirty" Usability Scale. In P. Jordan, B. Thomas, B. Weerdmeester, and A. McClelland, editors, *Usability Evaluation in Industry*. Taylor and Francis, 1996.

[4] B. Dodson, I. Vo, T. J. Purtell, A. Cannon, and M. S. Lam. Musubi: Disintermediated Interactive Social Feeds for Mobile Devices. In *Proceedings of the 21st International Conference on World Wide Web*, pages 211 – 220, 2012.

[5] S. Egelman, A. Oates, and S. Krishnamurthi. Oops, I Did it Again: Mitigating Repeated Access Control Errors on Facebook. In *Proceedings of the 29th International Conference on Human Factors in Computing Systems*. ACM, May 2011.

[6] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti. Timing is Everything?: The Effects of Timing and Placement of Online Privacy Indicators. In *Proceedings of the 27th International Conference on Human Factors in Computing Systems*, pages 319–328. ACM, 2009.

[7] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service - Usable Security for the Cloud. In *Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2012.

[8] S. Fahl, M. Harbach, T. Muders, and M. Smith. TrustSplit: Usable Confidentiality for Social Network Messaging. In *Proceedings of the ACM Conference on Hypertext and Hypermedia*, 2012.

[9] S. Garfinkel. Email-based Identification and Authentication: An Alternative to PKI? *IEEE Security & Privacy*, 1(6):20–26, Nov. 2003.

[10] S. L. Garfinkel and R. C. Miller. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In *Proceedings of the First Symposium on Usable Privacy and Security*. ACM, July 2005.

[11] M. Harbach, S. Fahl, T. Muders, and M. Smith. POSTER: All Our Messages Are Belong to Us: Usable Confidentiality in Social Networks. In *Proceedings Companion of the 21st International Conference on World Wide Web*, Apr. 2012.

[12] C. Herley and P. Van Oorschot. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy*, 10(1):28–36, 2012.

[13] J. King, A. Lampinen, and A. Smolen. Privacy: Is There an App for That? In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, July 2011.

[14] A. P. Lambert, S. M. Bezek, and K. G. Karahalios. Waterhouse: Enabling Secure E-mail With Social Networking. In *Proceedings of the International Conference On Human Factors In Computing Systems*. ACM, Apr. 2009.

[15] J. Lazar, J. H. Feng, and H. Hochheiser. *Resarch Methods in Human-Computer Interaction*. Wiley, 2010.

[16] M. M. Lucas and N. Borisov. FlyByNight: Mitigating the Privacy Risks of Social Networking. In *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society*, pages 1–8, 2008.

[17] M.-E. Maurer, A. De Luca, and S. Kempe. Using Data Type Based Security Alert Dialogs To Raise Online Security Awareness. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011.

[18] National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES) (FIPS PUB 197), October 2001.

[19] P. Rogaway and D. Wagner. Comments to NIST concerning AES Modes of Operations: CTR-Mode Encryption. National Institute of Standards and Technologies, 2000.

[20] S. Sheng, C. Koranda, J. Hyland, and L. Broderick. Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *Proceedings of the Second Symposium on Usable Privacy and Security, Poster*, 2006.

[21] N. Wang, H. Xu, and J. Grossklags. Third-party Apps on Facebook: Privacy and the Illusion of Control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, 2011.

[22] A. Whitten and J. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, 1999.

APPENDIX

A. ACADEMIC SOLUTIONS

There are several academic solutions which propose security for Facebook conversations. Even though these publications focus mainly on the cryptographic aspects of their solutions, each is briefly outlined in the following.

In 2008, Lucas et al. [16] proposed flyByNight, a prototype Facebook app that encrypts and decrypts messages using public key cryptography. The flyByNight server handles the key management and uses its own database to store the encrypted messages. This is a standalone app which does not protect messages sent via the standard Facebook messaging centre, but rather requires the user to send all messages via the app. Lucas et al. noted that usability would be an issue for future work.

Scramble! [2] is a PKI-based Firefox plugin that can store encrypted social network content either on a third-party TinyLink server or directly at the SN provider. However, as with most PKI solutions, key management is an issue, since it relies on PGP mechanisms and must be dealt with by the user. When sending encrypted content, the user composes a message with the Facebook UI and selects the text he wants to encrypt, whereupon Scramble! requires the user to choose the contacts to encrypt the content for manually. The encrypted text or a TinyLink URL is then placed into the message composer and can be sent through the regular UI.

Anderson et al. [1] and Dodson et al. [4] present concepts to use rich-clients as a way to improve privacy. The SN provider is reduced to a mere content distribution server while the client handles cryptography and information semantics. This approach would require a user to migrate to another SN and change the interaction patterns, which is a different scenario from that this paper addresses.

B. LAB STUDY DEMOGRAPHICS

	N=96
Gender	
Male	44
Female	52
Age	M=22,SD=2
< 20	12
20 - 25	69
> 25	15
Facebook Membership	
6 months	7
1 year	16
2 years	37
longer	34
don't know	2
Facebook Password Loss in The Last 12 Months	
not once	79
once	9
twice	3
three times	2
more than three times	3
Facebook use	
several times per week	10
< 1 hour per day	27
1 - 2 hours per day	41
2 - 4 hours per day	15
more than hours per day	2
Facebook Friends	M=207,SD=130
50 - 100	20
101 - 150	24
151 - 250	28
251 - 350	13
> 350	11
Facebook Messages / Week	M=24.35,SD=46.68
< 10	45
10 - 20	27
21 - 30	8
> 30	16

Facebook Chat Use	
several times a day	15
daily	23
weekly	28
less frequent	17
not at all	13
Prior contact with encryption mechanisms	
yes	33
no or don't know	63

C. LAB STUDY: PERCEIVED PRIVACY THREATS

To analyse who was perceived to be the biggest privacy threat, we also asked participants to rate how easy it would be for different entities to access their Facebook conversations on a 5-point Likert scale. Facebook employees and hackers were perceived as having the easiest access to that information: 87.5% and 84.4% said that they thought it would be easy or very easy for these actors to access their private messages, followed by the government of the USA (62.5%), advertising agencies (49.0%) and the German government (35.4%). Only 12.5% believed that it was easy or very easy for their friends to access these messages. Additionally, we wanted to know how motivated the participants believed these entities would be to access their messages. Advertising agencies were believed to be the most eager (70.8%). Facebook (44.8%), Hackers (29.2%), the US government (28.1%) and the German government (25.0%) are believed to have less motivation to access private messages. Friends were believed to be the least motivated (18.2%). Finally, we asked how bad the participants would feel if these entities accessed their private messages. 55.2% would find it bad or very bad if friends could access private messages not intended for them. For all the remaining actors, the participants almost unanimously agreed that access to their private messages would be bad or very bad (82.3% to 90.6%).

D. LAB STUDY SURVEY

D.1 Pre-Test Items

Since when have you been using Facebook?
Choose one answer: For 1 month, For 6 months, For 1 year, For 2 years, Longer, I don't know, n/a.

How often have you forgetten your Facebook password in the last 12 months?
Choose one answer: Never, Once, Twice, Three times, More than three times, n/a, I don't know, Other.

How important is it to you that only you and the recipient can read private messages?
Rate from 1 (unimportant) to 5 (important).

How often do you normally use Facebook on average?
Choose one answer: Less than an hour per day, 1 to 2 hours per day, 2 to 4 hours per day, More than 4 hours per day, More than once per week, Once per week, Monthly, Less frequently than once per month, n/a.

Approximately how many friends do you have on Facebook?

How many Facebook messages do you send per week on average?

How many of these messages have more than one recipient?

How many of these messages do you consider worthy of protection?

How often do you use the chat on Facebook?
Choose one answer: More than once per day, On a daily basis, On a weekly basis, Less than once per week, Never, n/a.

How easy do you think it is for the following persons or organisations to read your private messages on Facebook?
Rate from 1 (very easy) to 5 (very hard) for the following: Friends, Hackers, Facebook employees, Advertising Companies, US government, German government.

How high do you think the motivation is for the following persons or organisations to read your private messages on Facebook?
Rate from 1 (very low) to 5 (very high) for the following: Friends, Hackers, Facebook employees, Advertising Companies, US

government, German government.

How much would it concern you if the following persons or organisations were able to read your private messages on Facebook?
Rate from 1 (very little) to 5 (very much) for the following: Friends, Hackers, Facebook employees, Advertising Companies, US government, German government.

How well do you feel you and your privacy are protected when communicating through Facebook messages?
Choose from 1 (not at all) to 5 (very well).

How well do you feel you and your privacy are protected when communicating through Facebook chat?
Choose from 1 (not at all) to 5 (very well).

D.2 Post Task Items

Please rate the following questions regarding the mechanism you just used.
Choose from 1 (strongly disagree) to 5 (strongly agree) for the following:

1. I think that I would like to use this system frequently;
2. I found the system unnecessarily complex;
3. I thought the system was easy to use;
4. I think I would need the support of a technical person to be able to use the system;
5. I found the various functions in this system well integrated;
6. I thought this system was too inconsistent;
7. I would imagine that most people could learn to use this system very quickly;
8. I found the system very cumbersome to use; I felt very confident using the system;
9. I needed to learn a lot of things before I could get going with this system.

Please rate the following questions regarding the mechanism you just used.
Choose from 1 (strongly disagree) to 5 (strongly agree) for the following:

1. I would send private messages using this mechanism in the future;
2. I would send all my messages using this mechanism in the future;
3. I feel that my messages are now well protected.

D.3 Final Questionnaire Items

Please enter your age.

Please specify your gender.

Please enter your major subject.

A password is needed to use an encryption mechanism. If losing or forgetting the password led to the loss of all previous private messages, would you use such an encryption mechanism?
Choose yes or no.

Please rate the following statements with regard to the previous question about password recovery.
Choose from 1 (strongly agree) to 5 (strongly disagree) for the following: I am worried about forgetting my password; I am worried about the potential loss of all my previous messages.

Would you prefer a mechanism that is able to recover your password like it is possible on the Facebook website?
Choose yes or no.

Do you use software to encrypt your data?
Choose one or more answers: Yes, for Facebook; Yes, for email; Yes, for my hard disk; I don't know; No; Yes, for: ...

When friends have computer problems, they often ask me for help.
Choose from 1 (strongly disagree) to 5 (strongly agree).

When I have computer problems, I often ask my friends for help.
Choose from 1 (strongly disagree) to 5 (strongly agree).

What is AES?
Choose one or more answers: A browser extension; A Facebook application to store images; An encryption mechanism; I don't know; Something else: ...

Do you have any comments on this study, the procedure, the technologies used or anything else?

E. FINAL STUDY DEMOGRAPHICS

	N=15
Gender	
Male	6
Female	9
Age	
< 20	3
20 - 25	9
> 25	3
Facebook Membership	
1 month	1
6 months	1
1 year	3
2 years	5
longer	5
Facebook Password Loss in The Last 12 Months	
not once	12
once	2
more than three times	1
Facebook use	
< 1 hour per day	6
1 - 2 hours per day	8
several times per week	1
Facebook Friends	
50 - 100	3
101 - 150	2
151 - 250	4
251 - 350	3
> 350	3
Facebook Messages / Week	
< 10	7
10 - 20	4
21 - 30	3
> 30	1
Use Harddisk Encryption	2
Heard of AES	1

F. FINAL STUDY INTERVIEW GUIDELINE

The following gives a brief overview of the questions we asked in the semi-structured interview in the final study.

F.1 FBMCrypt Account

1. Please rate the effort for creating a FBMCrypt account.
2. With respect to the application, please rate the appropriateness of creating an extra account for encrypting Facebook messages.
3. Please compare the account creation process with the creation of a new Facebook and webmail account.
4. Please rate the fact that your FBMCrypt password had to be different from your Facebook password.
5. How likely would it be that you forget your FBMCrypt password?
6. Have you ever forgotten a password? Your Facebook password?

7. Please attribute the FBMCrypt-to-Facebook account binding process.
8. Please rate the plugin installation procedure.

F.2 Facebook Messaging

1. How many private Facebook messages do you send per week?
2. Do these comprise – in your opinion – sensitive information? If not, what channel do you use to transport sensitive information? If yes, what is the amount of sensible messages?
3. Do you have reservations that an unauthorised third party could access your private Facebook messages? If yes, who do you think is able to do so? If not, why do you think your messages are secure?

F.3 FBMCrypt Workflow

1. Please attribute the process of sending a FBMCrypt-protected private Facebook message.
2. Please describe the message composer you used to send a FBMCrypt-protected private Facebook message.
3. Please describe the message composer you used to send a private Facebook message that was not encrypted.
4. Please attribute the reading of a FBMCrypt-protected private Facebook message.
5. Please describe the presentation of a FBMCrypt-protected private Facebook message when reading it.

F.4 Satisfaction/Perceived Security

1. Would you send all your private Facebook messages using the FBMCrypt service? If not, why and what messages would you not send using FBMCrypt?
2. Please compare your perceived feeling of security sending a private Facebook message the normal way to sending a message with FBMCrypt.
3. Would you recommend FBMCrypt to your friends?
4. Would you pay for the FBMCrypt service? If yes, what would you be willing to pay?

F.5 Key Recovery

1. Would you use FBMCrypt if loosing or forgetting the password would result in losing access to your private Facebook messages? If yes/no, why?
2. Would you prefer a mechanism that allows for recovery of the encryption password?