Reading Response 1: Usable Security of PGP 5.0 and FBMCrypt

CSEC 759 - Mehul Sen

In their paper titled "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0"[1], Whitten and Tygar examine whether the design standards applied to general consumer software are sufficient for security software. The authors aimed to formulate a good usability evaluation for security software and better understand the design solutions required by security software. For their case study, they used PGP 5.0, considered the best candidate due to its good design per consumer software standards and advertised as easy to use, offering complex mathematical cryptography to inexperienced users. The authors evaluated the usability of PGP 5.0 through two methods. The first was an informal cognitive and heuristic evaluation, where they walked through each aspect of the software as if they were novice users to identify areas that might cause confusion or errors on the user's part. They also evaluated the software against a list of essential usability principles they believed it should adhere to. The second evaluation was a user test involving participants experienced in emails but without prior knowledge about public-key cryptography, where each participant was required to interact with PGP 5.0 and perform tasks involving encryption/decryption. The authors discovered that the software design for PGP 5.0 needed to be revised to make it usable for people unfamiliar with public-key cryptography. Additionally, they found that the standard usability evaluation methods do not apply to usable security because they treat security as a secondary rather than a primary goal. They suggested several design strategies for more usable security, such as clearly communicating the security model and technology with the users, providing accurate visual metaphors, making them aware of irreversible actions, and avoiding providing too much information.

In their paper titled "Helping Johnny 2.0 to Encrypt His Facebook Conversations"[2], Fahl et al. aimed to analyze the usable security for conversations on Facebook. They wanted to identify that the changes brought by online social networks could open new possibilities for a usable security mechanism to protect their conversations. They also wanted to understand why the current cryptographic solutions were not widely used and to design a new approach to encrypt Facebook messages. Fahl et al. conducted a poll to better understand users' privacy concerns on Facebook. Following this, they searched for products offering to encrypt private messages on Facebook to better understand their key management, encryption/decryption concepts, and usable security. After building several mockups that implemented the corresponding usable security concepts, they conducted a lab study involving participants interested in protecting their Facebook conversations, who frequently used Facebook and were unfamiliar with encryption mechanisms requiring them to interact with the security mechanism. This study was used to identify which mockup provided the best usable security. Based on the responses to the study, Fahl et al. designed their proposed security mechanism. They conducted another lab study involving the same pool of participants as before to evaluate the usability of their mechanism. Fahl et al. discovered that most of the people who participated in their initial poll knew that Facebook could read their messages, which was a point of concern for them. Their lab study found that participants preferred a solution that utilized automatic key encryption, while automatic encryption did not significantly impact their results. They also found that a password recovery solution was desirable to most people, and the complexity of a mechanism heightens a user's sense of security. Based on these findings and to keep their solution integrated with Facebook, they designed a service-based approach with automatic key encryption and recovery called FBMCrypt. In the final lab study, they found that the registration, binding, and installation process

for FBMCrypt was easy to perform. Additionally, the displayed ciphertext within the tool was a perceived indicator of functional encryption. However, FBMCrypt itself could not establish trust among users, and a trusted third party would be required to get users to start trusting and utilizing FBMCrypt.

These two papers discussed the usable security of security mechanisms. Whitten and Tygar evaluated the existing mechanism for PGP 5.0 and suggested potential changes. Meanwhile, Fahl et al. evaluated the existing security mechanisms to encrypt Facebook messages and proposed a new mechanism that addressed the shortcomings of the previous solutions.

Both papers involved user tests that required inexperienced users to understand and use the security mechanisms. However, Whitten and Tygar walked through each aspect of the software as if they were novice users. This method helped them identify areas that might cause confusion or errors, although this alone would not be sufficient to eliminate all errors. Fahl et al.'s research focused primarily on usability while providing little technical insight into their proposed solution. Additional information could shed light on how their encryption worked, their key management approach, and how they would address issues they did not reciprocate in their simulated lab study, such as interacting with Facebook accounts that utilize different languages or accessing accounts on different devices. Another interesting element of these evaluations was that, in their user tests, both papers involved participants unfamiliar with public key cryptography. Whitten and Tygar involved participants in the computer field, such as programmers, to get a diverse set of participants and an accurate assessment of how users might interact with the mechanism. Fahl et al. purposely excluded computer science students from their study to avoid bias based on technical skills and potential familiarity. While this is only partially accurate to the general public, it would increase the chances of finding non-technical errors and usability fallbacks. Considering these reasons, Whitten and Tygar performed a better heuristic evaluation of the paper and provided a solution that provided a better security solution. In contrast, the user tests and case studies performed by Fahl et al. were better designed to identify potential flaws and errors related to usable security within their corresponding mechanisms, providing a better usability solution.

References

[1]: "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" Alma Whitten, and J. D. Tygar, *USENIX Security Symposium*, Aug. 1999.

[2]: "Helping Johnny 2.0 to Encrypt His Facebook Conversations" Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander, *Symposium on Usable Privacy and Security*, July. 2012.