Poster: What Are Usability Considerations in Developing Advanced Cryptographic Libraries?

Kenta Kodera[†,*], Masahiro Fujita[†], Hikaru Horigome[†], Aoto Takahashi[‡], Akira Kanaoka[‡]

† *Mitsubishi Electric Corporation, Kamakura, Kanagawa, Japan*

‡ *Toho University, Funabashi, Chiba, Japan*

* Kodera.Kenta@df.MitsubishiElectric.co.jp

***Abstract*—In recent years, advanced cryptography, such as attribute-based cryptography, has been widely adopted. Some libraries implementing advanced cryptography (hereinafter referred to as advanced cryptographic libraries) have also emerged. However, their usability remains unexplored. This study is the first step in evaluating the usability of advanced cryptographic libraries. The developers of an attribute-based cryptographic library participated an interview survey about the considerations they made to ensure usability when developing the library. The interview findings clarify the similarities and differences in considerations from a usability perspective between conventional and advanced cryptographic libraries. These findings can be applied to other advanced cryptographic libraries as well.**

Keywords— usable security, user interview, advanced cryptography, cryptographic libraries

I. Introduction

Software developers using cryptographic libraries often introduce vulnerabilities into their software by misusing the libraries [1][2] (hereafter these developers are referred to as "cryptographic library users"). Many studies have evaluated the usability of cryptographic libraries to ensure that the libraries are used as intended by their providers (hereafter these providers are referred to as "cryptographic library developers"). They have focused on libraries that contain conventional cryptographic algorithms such as RSA and AES (hereafter referred to as "conventional cryptographic libraries"). From a usability perspective, interviews and implementation-based experiments have been conducted considering both cryptographic library developers and users [3][4][5][6][7][8]. These studies have provided recommendations and suggestions for reducing misuse.

Recently, libraries containing advanced cryptographic algorithms (hereafter referred to as "advanced cryptographic libraries") have emerged [9][10]. Representative advanced cryptographic schemes include ID-based cryptography, attribute-based cryptography, group signatures, and searchable encryption. Advanced cryptography offers various added benefits compared to conventional cryptography. However, to the best of our knowledge, the usability of advanced cryptographic libraries is yet to be evaluated. Usability studies on advanced cryptographic libraries are essential to safely and widely promote advanced cryptography.

This study presents the first usability survey of advanced cryptographic libraries and answers the following research question: *What are usability considerations in developing advanced cryptographic libraries?* To answer this question, interview surveys were conducted with two advanced cryptographic library developers.

II. Study Design

This study focuses on attribute-based cryptography, an advanced cryptographic scheme. We conducted semi-structured interviews with two developers experienced in developing attribute-based cryptographic libraries. We directly recruited these two interviewees. The first participant had 8 years of experience in developing cryptographic algorithms, 8 years of experience in developing cryptographic libraries, but no experience in developing systems using cryptographic libraries. The second participant had 12 years of experience in developing cryptographic algorithms, 8 years of experience in developing cryptographic libraries, and 2 years of experience in developing systems using cryptographic libraries. Both participants belonged to the same organization.

The interviews were conducted by two authors specializing in the fields of cryptography and usable security. Before the interviews, the interviewers reviewed the specification document of the advanced cryptographic library developed by the participants and then prepared several questions. The interviews were conducted in a manner that allowed for an in-depth exploration of topics based on prepared questions, and each session lasted approximately 1 h. No compensation was provided to the participants. The interviews were conducted face-to-face, with audio recorded in Microsoft Teams. The interviewees were Japanese; therefore, the interviews were conducted in Japanese. The questions, responses, and coding results were translated from Japanese to English for this study.

Before starting the interviews, both participants completely understood and agreed on the purpose of the interview, the recording methods, and the data management procedures. After the interview, the participants requested that certain responses, containing confidential information within the library development team, not be displayed in this paper. For example, details about the organizational structure, internal information about the developed libraries, and organizational evaluation criteria should not be included this paper. Therefore, this information will be not included in the following sections.

The interview results were analyzed using NVivo 14, a qualitative analysis tool. The coding was performed by two authors following these steps:

1. Each coder independently conducted open coding.
2. The coders discussed their individual codebooks and created a common codebook.
3. Using the common codebook, each coder independently re-coded the data.
4. The inter-rater reliability was calculated.

5. If the inter-rater reliability was lower than the threshold, the coders discussed the similarities and differences in their coding results and returned to step 3.

Inter-rater reliability was calculated using Cohen's Kappa coefficient, obtained through the coding comparison query function in NVivo 14. The threshold was set at 0.75, based on the highest "very good" standard defined by Fleiss et al., as referenced in the NVivo 14 manual [11].

After steps 1 and 2, the common codebook contained nine codes. Using the codebook, steps 3 to 5 were performed twice, resulting in a Cohen's Kappa coefficient of 0.7883.

III. Discussion

A. Comparison with Related Works

Compared to the usability evaluation studies on conventional cryptographic libraries, the interview results revealed similar recommendations: simple design, secure default settings, comprehensive documentation, and clear error messages.

Additionally, the interview results also identify four issues and considerations specific to advanced cryptographic libraries that were not highlighted in the related works.

1) Increase in information to be provided to library users: Participants stated that they needed to explain many prerequisites to library users, such as the third party for key generation using a master secret key and concepts specific to attribute-based cryptography (e.g., attribute values and policies). Owing to the different parameters handled by each role, confusion may arise about the roles, parameters, and functions executed by each entity in the system.

2) Explanation through Mutual Communication: In addition to enhancing the content of the specification documents to prevent misuse by library users, participants also arranged opportunities for face-to-face explanations. These explanations were conducted using materials such as PowerPoint presentations.

3) Resolution of Cryptographic Algorithm Constraints through Operation: Advanced cryptography tends to impose more operational constraints on library users to achieve more features and security. Participants addressed algorithm constraints related to concurrent roles or changes in roles by requesting library users to manage attribute values appropriately in the operational phase of development.

4) Test Design for Advanced Cryptographic libraries: Experts in cryptographic algorithms also face difficulties in testing advanced cryptographic libraries. Participants mentioned that the dependency of test cases on the algorithm make it challenging to create general testing guidelines applicable to all advanced cryptography.

B. Recommendations

The interview results suggest that the challenges in using attribute-based cryptographic libraries stem from their complexity compared to conventional cryptography. In attribute-based cryptography, the potential for library misuse increases owing to many factors. For example, the library users need to know new concepts of attribute values and policies, the diverse roles and types of parameters associated with various entities, and the specific algorithms required to achieve advanced functionalities. The complexity observed in attribute-based cryptography is likely to extend to many other advanced cryptography. Therefore, it is essential to combine efforts in providing information to library users and designing the library to mitigate the impact of the complexity inherent in advanced cryptographic libraries. The trade-off between the versatility of the library and potential for misuse must be considered, along with the expected library users, to explore better design methods. Moreover, the potential for misuse must also be reduced by providing rich information to library users via graphic-rich documentation and various sample codes.

C. Limitations and Future Works

First, from an ethical standpoint, the interview results that the participants did not wish to reveal are not included in this paper. Analyzing those topics might yield more valuable insights. Second, the participants provided the advanced cryptographic library to users with experience in software development using cryptography. If library users had no cryptographic knowledge, new considerations not identified in this study need to be specified. Third, the number of cryptographic library developers interviewed was two. Individuals experienced in developing advanced cryptographic libraries are few; therefore, it is difficult to gather many participants. Future work should focus on identifying a way to generalize the results.

References

[1] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel, "An empirical study of cryptographic misuse in android applications", Proc. 2013 ACM SIGSAC Conference on Computer & Communications Security, 2013, No.12, pp.73-84.

[2] N. Meng, S. Nagy, D. Yao, W. Zhuang, and G.A. Argoty, "Secure coding practices in Java: challenges and vulnerabilities", Proc. 40th International Conference on Software Engineering, 2018, No.12, pp.372-383.

[3] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M.L. Mazurek, and C. Stransky, "Comparing the Usability of Cryptographic APIs", Proc. IEEE Symposium on Security and Privacy (SP), 2017, pp.154-171.

[4] M. Ukrop and V. Matyas, "Why Johnny the Developer Can't Work with Public Key Certificates: An Experimental Study of OpenSSL Usability", Proc. Topics in Cryptology CT-RSA 2018, 2018, pp.45-64.

[5] K. Mindermann, P. Keck, and S. Wagner, "How Usable are Rust Cryptography APIs?", Proc. IEEE International Conference on Software Quality, Reliability and Security, 2018, pp.143-154.

[6] D. Votipka, K.R. Fulton, J. Parker, M. Hou, M.L. Mazurek, and M. Hicks, "Understanding security mistakes developers make: qualitative analysis from build it, break it, fix it", Proc. 29th USENIX Security Symposium, 2020, pp.109–126.

[7] N. Patnaik, A. Dwyer, J. Hallett, and A. Rashid, "SLR: From Saltzer and Schroeder to 2021…47 Years of Research on the Development and Validation of Security API Recommendations", ACM Transactions on Software Engineering and Methodology, 2023, Volume 32, Issue 3, pp.1-31.

[8] K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, and A. Sasse, "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts", Proc. 33rd USENIX Security Symposium, 2024, pp.7213-7230.

[9] S. Mitsunari, "MCL: a Portable and Fast Pairing-Based Cryptography Library", [Online], Available: https://github.com/herumi/mcl.

[10] J. Bethencourt, A, Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", [Online], Available: https://acsc.cs.utexas.edu/cpabe.

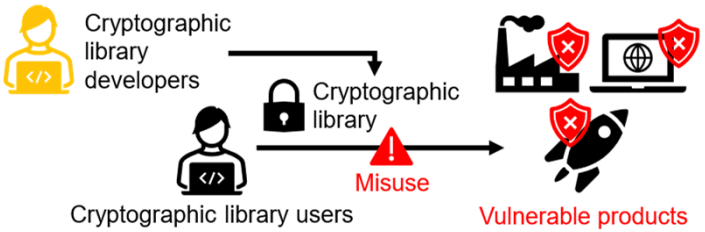
[11] J.L. Fleiss, B.A. Levin, and M.C. Paik, "Statistical Methods for Rates and Proportions(3rd Edition), 2003, John Wiley & Sons.

What Are Usability Considerations in Developing Advanced Cryptographic Libraries?

Kenta Kodera†, Masahiro Fujita†, Hikaru Horigome†, Aoto Takahashi‡, Akira Kanaoka‡
† Mitsubishi Electric Corporation, Kanagawa, Japan, ‡ Toho University, Chiba, Japan

Motivation

Preventing misuse in cryptographic libraries

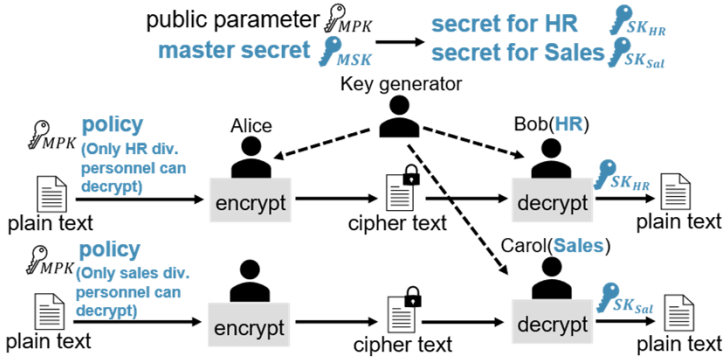


Research Positioning

	Conventional Crypto.	Advanced Crypto.
Scheme	RSA, ECC, AES, etc.	Attribute-based Crypto. etc.
Library	PyNaCL, OpenSSL, etc.	MCL, capbe, etc.
Usability study for prevention	Acar et al. [1], Mindermann et al. [2], Votipka et al. [3] , etc.	**Not yet researched**

RQ: What are usability considerations in developing advanced cryptographic libraries?

Target: Attribute-based Cryptography



Decryption can be controlled based on the attributes of the recipient.

Interview Design

Participants	Two developers of an attribute-based cryptographic library
Format	Face-to-face semi-structured interviews (in Japanese)
Recording	Audio recording in Microsoft Teams
Compensation	None
Ethical Consideration	• Prior agreement on interview purpose, recording method, and data management • Acceptance of participants' requests to exclude confidential information

Interview Analysis

Process	• Conducted by two authors using NVivo 14 • Created a codebook through open coding • Repeated independent coding until the inter-rater reliability exceeded 0.75
Coding Results	• Personal Experience • Development structure • Basic design • Detailed design • Requirements for operation • Test design • Knowledge of library users • Support for library users • Differences from conventional cryptographic libraries

Discussion

Comparison between conventional and advanced cryptographic libraries' design

Similarities	• Simple design • Secure default settings • Comprehensive documentation • Clear error messages
Differences	• Prevention of user's confusion about various roles and keys • Necessity of graphical explanation of new terms and behaviors • Handling cryptographic constraints operationally

Answer to RQ

- Addressing unique concepts such as attribute values, policies and diverse roles
- Considering the trade-off between the flexibility of the library and potential for misuse
- Providing rich information to library users via documentation and sample codes

Future works

- Conduct implementation experiments targeting cryptographic library users
- Develop the design guidelines and explanation methods of the library

[1] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M.L. Mazurek, and C. Stransky, "Comparing the Usability of Cryptographic APIs", Proc. IEEE Symposium on Security and Privacy (SP), 2017, pp.154-171.
[2] K. Mindermann, P. Keck, and S. Wagner, "How Usable are Rust Cryptography APIs?", Proc. IEEE International Conference on Software Quality, Reliability and Security, 2018, pp.143-154.
[3] D. Votipka, K.R. Fulton, J. Parker, M. Hou, M.L. Mazurek, and M. Hicks, "Understanding security mistakes developers make: qualitative analysis from build it, break it, fix it", Proc. 29th USENIX Security Symposium, 2020, pp.109–126.