Seminar Usability

Casper Kristiansson

January 31, 2024

1 Insights from Papers

When choosing the different papers to read, I decided to go for the ”Developer side” category. In this category, I will be reading and drawing conclusions from the two papers “Developers are not the enemy!: The need for usable security apis” by Green, Matthew, and Matthew Smith [1] and “Usability Smells: An Analysis of Developers’ Struggle With Crypto Libraries” by Patnaik, Nikhil, Joseph Hallett, and Awais Rashid [2].

1.1 Usability Smells: An Analysis of Developers’ Struggle With Crypto Libraries

- The paper concludes that there are a lot of usability issues with cryptographic libraries. The authors did a thematic analysis and related issues with these libraries. These issues were such as missing documentation or bad documentation.
- The paper finds what the common struggles are for a developer. Finding out what a developer is looking for or the common struggles that exist in libraries especially cryptographic libraries can be improved. Common struggles are missing documentation, confusion of API usage, and the overall lack of cryptographic knowledge.

1.2 Developers are not the enemy!: The need for usable security apis

- It highlights the importance of user-friendliness in security and privacy API for developers.
- APIs need to be well-designed in order to enhance the effectiveness of security systems by helping developers implement security features the correct way (lack of knowledge).

2 Technology: End-to-End Encrypted Email Service

2.1 What is it

I chose the technology of End-To-End Encrypted Email Service [3]. It is a type of email platform that provides improved security by encrypting emails from both the sender and receiver.

2.2 What it is used for

The service is used for secure communication. Ensuring that all messages that are sent between the sender and receiver are encrypted on both sides will ensure that only the intended recipient can read the content of an email.

2.3 How it works

The service encrypts the content of an email at the sender's end and then decrypts it only at the recipient's end. This will prevent any interception or unauthorized access during transmission.

3 Applied Insights from Papers

- Both papers mention the struggle of poorly documented and developed APIs in cryptographic libraries. Because these APIs have these flaws it might lead to the developers of the End-To-End Encrypted Email Services implementing security features in the wrong way. Because of this, it could lead to the application losing its main purpose.

- If the End-to-End Encrypted Email Service will serve its API service the API must be built in the best way possible. This means that it should be user-friendly in terms of cryptographic knowledge and well-documented. Doing this will allow developers that use the End-To-End Encrypted Email Service APIs to utilize them in the correct and best way.

References

[1] M. Green and M. Smith, “Developers are not the enemy!: The need for usable security apis,” *IEEE Security & Privacy*, vol. 14, no. 5, pp. 40–46, 2016.

[2] N. Patnaik, J. Hallett, and A. Rashid, “Usability smells: An analysis of {developers’} struggle with crypto libraries,” in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 245–257.

[3] *What is end-to-end encryption? — ibm*, https://www.ibm.com/topics/end-to-end-encryption, (Accessed on 01/31/2024).