Scramble

[Short Abstract]

Ero Balsa, Filipe Beato, Claudia Diaz, Bart Preneel
ESAT/COSIC - KU Leuven
Leuven, Belgium
{first.lastname}@esat.kuleuven.be

1. SHORT ABSTRACT

Scramble is a Firefox Extension whose main security goal is to allow Online Social Network (OSN) users to enforce their own *privacy settings* without depending on the OSN provider [3]. Scramble uses *end-to-end encryption*, relying on the OpenPGP to encrypt messages and posts such that only the members of a user-defined recipient set are able to decrypt.

We have set two main usability goals: ease of privacy settings definition and transparent cryptography. To facilitate the definition of privacy settings, Scramble allows users to define groups of (frequent) recipients. In order to streamline cryptographic operations and key management, Scramble automatically parses encrypted messages, decrypting or hiding them depending on whether or not the user is an intended recipient. To speed up the cryptographic operations Scramble uses Java rather than Javascript. While for key management, Scramble automatically uploads, searches for, and downloads keys from public key servers. Besides, we are extending Scramble to support identity based broadcast encryption [4] to further unburden users of key management.

In addition, to facilitate user adoption Scramble was set up as an open-source project, and aims to be OSN-independent. It has been successfully tested for Facebook and Twitter, and its interface is implemented in Javascript for easy portability to other browsers, e.g., Chrome. We have aimed to comply with terms of service that may forbid posting encrypted content. Thus, Scramble allows users to post a link to an external server (freely available and potentially managed by the user) hosting the encrypted messages. These operations are automatically managed by Scramble. When posting, Scramble publishes a link to the encrypted message, stored in the external server. Upon retrieving content, Scramble replaces the links with the decrypted messages if the user is an intended recipient, hiding the links otherwise [2].

Despite the aforementioned goals and strategies, usability remains a major challenge. Scramble hitherto features an interface that, even if it follows "standard" interface design formulae, was not designed for people unfamiliar with cryptography, as highlighted in a recent user study [1]. Participants of this study acknowledged that Scramble was difficult to use, unintuitive, slow or unnecessarily complex, suggesting that more automation is needed.

Beyond interface weaknesses, more fundamental issues emerged. Users showed mistrust on Scramble due to a lack of understanding of cryptography, failing to grasp that no additional trusted third party is required to enforce access control, or no data is collected by Scramble. They pointed out that the government or Facebook could be behind Scramble. They seemed unconvinced by the security afforded by cryptography and thought that encryption was too heavyweight a protection means for the data they share on Facebook, which they consider to be "not that sensitive". This demonstrates that more usability studies on cryptographic tools are needed in order to find out how to properly communicate to users the benefits and operation of these tools.

All in all, participants praised Scramble's security goal, applauding the initiative of providing more robust privacy protections against network providers, governments and any other unintended recipients.

2. REFERENCES

[1] E. Balsa, L. Brandimarte, A. Acquisti, C. Diaz, and S. Gürses. Spiny cactos: Osn users attitudes and perceptions towards cryptographic access control tools. In *USEC*, page 10, 2014.

[2] F. Beato, I. Ion, S. Capkun, B. Preneel, and M. Langheinrich. For some eyes only: protecting online information sharing. In E. Bertino, R. S. Sandhu, L. Bauer, and J. Park, editors, *CODASPY*, pages 1–12. ACM, 2013.

[3] F. Beato, M. Kohlweiss, and K. Wouters. Scramble! your social network data. In S. Fischer-Hübner and N. Hopper, editors, *PETS*, volume 6794 of *Lecture Notes in Computer Science*, pages 211–225. Springer, 2011.

[4] R. Sakai and J. Furukawa. Identity-based broadcast encryption. *IACR Cryptology ePrint Archive*, 2007:217, 2007.