When is a Tree Really a Truck? Exploring Mental Models of Encryption

Justin Wu
Department of Computer Science
Brigham Young University
Provo, Utah
Email: justinwu@byu.edu

Daniel Zappala
Department of Computer Science
Brigham Young University
Provo, Utah
Email: zappala@cs.byu.edu

I. Introduction

The adoption of encryption tools by the public has been advocated as a protective measure that would further both security and privacy aims. However, past work has shown that when users are actively involved in the encryption process, they can struggle to accomplish this task [1], [2], [3], [4]. This is a major obstacle to the practical adoption of encryption because mistakes involving encryption can have terrible consequences. Failures to use encryption tools correctly can result in a false sense of security or, perhaps worse still, unintentional and self-imposed denial of service when users lose access to precious accounts and data.

When the impact of user error is severe, a natural response is to circumvent users entirely by transparently incorporating complex mechanisms into the software itself. Indeed, in contexts where encryption has successfully achieved widespread deployment—TLS/HTTPS, secure messengers, and smartphone encryption—this has been the approach taken; most users are not even aware encryption occurs in these systems. Unfortunately, while indeed effective, this approach is not without limitations [5], [6]. Automation is not always perfect, and even the best programmed software will occasionally require user input. Further exacerbating the issue, when a process has been sufficiently automated such that the user is not even aware of its presence, they will lack the context necessary to enact the correct response when interaction is required. To this point, in two of the cases where encryption has been transparently applied, research has shown users are indeed confused by resulting errors [7], [8].

In this work, we conduct a study focused on understanding what users perceive about encryption tools in situations where interaction is required but in which their knowledge is limited to knowing that encryption is somehow involved. More specifically, we present the first directed effort to explore users' mental models—the representation of how one perceives something works—of encryption. We perform 19 semi-structured phone interviews with participants across the United States and examine three aspects of their mental models of encryption: what it is, how it works, and what role it plays in daily life.

We find that participants' models can be divided into four types which, while differing in structural details, boil down to functional abstractions of access control and symmetric encryption. We further observe highly varied opinions on the strength of encryption, opinions which do not appear to correlate with the detail or accuracy of participants' models. Finally, we note that effort must be made with respect to conveying the utility of the personal use of encryption. More specifically, participants felt that service providers routinely employ encryption to protect their sensitive data, while the personal use of encryption was viewed as the domain of either illegal or immoral activity, or the paranoid.

II. Methodology

We conducted an IRB-approved study consisting of 19 semi-structured phone interviews with participants from across the United States. Participants were recruited via the Prolific Academic research platform. Interviews were divided into two phases: the first half concerned the mechanics of encryption, what it is and how it works; the second half revolved around the role of encryption in daily life and presented participants with three specific use cases for discussion.

In the first half of the interview, participants were asked to explain what came to mind when they heard the word "encryption." Follow-up questions were asked as necessitated to expound upon these responses. Importantly, the diagramming phase of the study was performed as part of this first half. Participants were tasked with "encrypting" two entities: a provided sentence and a picture of their own devising, and to illustrate their vision of this process. No explicit instructions were given as to form to avoid influencing participants, and they were allotted as much time as needed to make their diagrams. When participants finished their diagrams, they photographed them and sent them to the study coordinator, whereupon discussion of its contents proceeded.

At the conclusion of the diagramming exercise, the second half of the interview began: the discussion of encryption's role in daily life. Participants were asked to explain what role, if any, they felt encryption played in their life. They were then presented with three examples of encryption—smartphone encryption, HTTPS, and secure messengers—and asked to discuss what utility they imagined such technologies might offer.

Responses were divided into two categories: those that we perceived as pertaining to mental models of encryption, and those to be explored as individual themes. From the former, we identified four properties which we used to categorize mental models. Each participants' responses were assessed with respect to these properties and then resulting models were analyzed for similarity, with four final models resulting.

III. Results

We identified four models of encryption: an access control model, a "black box" model, a cipher model, and an "iterative-encryption" model. The access control model was the most primitive, and did not even view encryption as transforming the source data, instead simply perceiving that it prevented access by undesired persons. The black box model is a straightforward extension of the previous model, continuing the abstraction of access control, although participants with this model now understood that encryption would transform data, though they did not have a sense for how. Those with the cipher model extends the black box model with a notion of what the encryption process entails: a cipher. Participants with the final model varied on details such as the types of operations performed by the encryption process, but all perceived encryption as an iterative process involving multiple passes.

Nearly all participants were quite confident that the service providers they dealt with—such as banks and online merchants—proactively encrypt their data. Encryption was largely associated with online activity, although interestingly, their model of how encryption was applied was one of data at-rest; participants simply did not have a model for encryption of data in-transit. When it came to the individual, as opposed to institutional, use of encryption, participants noted sensitive contexts, such as investment information or illegal activity. Privacy was also recognized as a potential motivating concern, although it was typically qualified as a "paranoid" one.

IV. Recommendations

The commonality of the view equating encryption with symmetric encryption and viewing its purpose as access control has potential. It is a useful and intuitive abstraction for certain forms of encryption, such as the encryption of data at rest on mobile devices. However, its corollary is that asymmetric encryption is *non*-intuitive, and thus presenting asymmetric encryption interaction mechanisms as "encryption" is perhaps counterproductive.

Because participants largely saw little personal utility in encryption, risk communication efforts must improve greatly. The implications of a negative perception of encryption are far-reaching; even if usability issues can be resolved, if users see no value in its adoption, the status quo will continue. Instead, perhaps a focus on conveying the benefits to the larger community—protecting those who need protection even if you personally do not feel a need for it—might prove helpful.

Relatedly, perceptions of the strength of encryption varied wildly, with many participants believing it to be well within the capability of potential attackers. Accordingly, in attempting to communicate to users what encryption can offer them, effort must be made to educate them on its strength within the context of the capability of attackers.

Finally, we offer a general recommendation that care be taken with the use of security warnings and indicators, that their design be considered within the context the user—not the designer—perceives. Specifically, we observed that TLS browser indicators were misinterpreted by participants, and thus were perceived as offering security guarantees that were not intended.

V. Conclusion

We find that despite varying details and complexity in mental models of encryption, the functional abstractions that people possess are essentially the same. Namely, perceptions of the interaction model of encryption are of access control and symmetric encryption. We observe that participants appear to lack a model of encryption of data in-transit, with remarks pointing almost unilaterally to a model where encryption always occurs on data at-rest. Furthermore, our findings reveal concerning views about the utility of encryption. We present recommendations based on our findings which largely focus on the need for improved risk communication efforts: more work is needed in crafting messages that resonate with users as well as discovering which communication mediums are most effective.

Acknowledgment

The authors would like to thank Rick Wash and Emilee Rader for their guidance in the early phases of this study.

References

[1] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (Special Agent) Johnny (still) can't encrypt: A security analysis of the APCO project 25 two-way radio system." in *USENIX Security Symposium 2011*, 2011, pp. 8–12.

[2] S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons, "We're on the same page: A usability study of secure email using pairs of novice users," in *SIGCHI Conference on Human Factors in Computing Systems (CHI 2016)*. ACM, 2016, pp. 4298–4308.

[3] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why Johnny still cant encrypt: evaluating the usability of email encryption software," in *Symposium On Usable Privacy and Security (SOUPS 2006)*. USENIX Association, 2006, pp. 3–4.

[4] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0." in *USENIX Security Symposium 1999*, vol. 1999. USENIX Association, 1999.

[5] W. K. Edwards, E. S. Poole, and J. Stoll, "Security automation considered harmful?" in *New Security Paradigms Workshop (NSPW 2008)*. ACM, 2008.

[6] S. Ruoti, N. Kim, B. Burgon, T. Van Der Horst, and K. Seamons, "Confused Johnny: when automatic encryption leads to confusion and mistakes," in *Symposium on Usable Privacy and Security (SOUPS 2013)*. USENIX Association, 2013.

[7] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *USENIX Security Symposium 2013*, vol. 13. USENIX Association, 2013.

[8] S. Schröder, M. Huber, D. Wind, and C. Rottermanner, "When SIGNAL hits the fan: On the usability and security of state-of-the-art secure mobile messaging," in *European Workshop on Usable Security (EuroUSEC 2016)*, 2016.