Poster: A Framework for Comparative Usability Studies on Secure Device Pairing

Achal Channarasappa, Pranita Ramakrishnan, Joshua Tan, Jeremy Thomas
Carnegie Mellon University
Pittsburgh, PA
{achannar,pranitar,jstan,thomasjm}@andrew.cmu.edu

1. INTRODUCTION

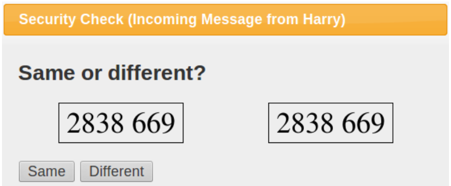
Secure communications may be desired in situations in which there is no trusted thirty party or prior security context. In these cases, device pairing methods can be used to establish a secure communication channel and to protect against Man-in-the-Middle attacks. Prior research has proposed pairing methods that vary with respect to required device features (e.g., cameras, accelerometers), communication channels (e.g., visual, audio), and level of automation.

Researchers have compared the usability of device pairing methods and techniques primarily using lab studies [2] [3] [4]. Lab studies are useful as a preliminary step to determine which approaches warrant further investigation. However, due to the high cost of large sample sizes, it is difficult to perform quantitative analysis on data collected in lab studies. In an online study of more than 400 participants, Hsiao et al. performed a comparative usability study of 9 visual fingerprint representations. In this study, participants were shown approximately the same number of matching and non-matching items and asked to compare them as the primary task [1].

A potential issue with prior usability studies on device pairing methods lies in their ecological validity; in most real-world settings, security is a secondary task and Man-in-the-Middle attacks are rare. Thus, it is important to see how the security and usability of device pairing methods are affected in cases where participants are habituated to benign pairing scenarios and in which device pairing is a secondary task. We have designed and implemented a framework that can be used to extend prior work to additionally examine the extent to which habituation and framing the security task as a secondary task affect the security and usability of device pairing approaches.

2. EXPERIMENTAL FRAMEWORK

Our experimental framework consists of two components: an interactive online activity and a follow-up questionnaire. In the online activity, participants must complete a series of distraction tasks in the context of a role-playing scenario. Within each of these tasks, the participant must perform device pairing as a secondary task. Our current implementation focuses on device pairing methods involving comparison of two visual fingerprints. The follow-up questionnaire is used to gather additional usability data on subjective satisfaction with the device pairing method, as well as demographic information.



Security Check (Incoming Message from Harry)

Same or different?

2838 669

2838 669

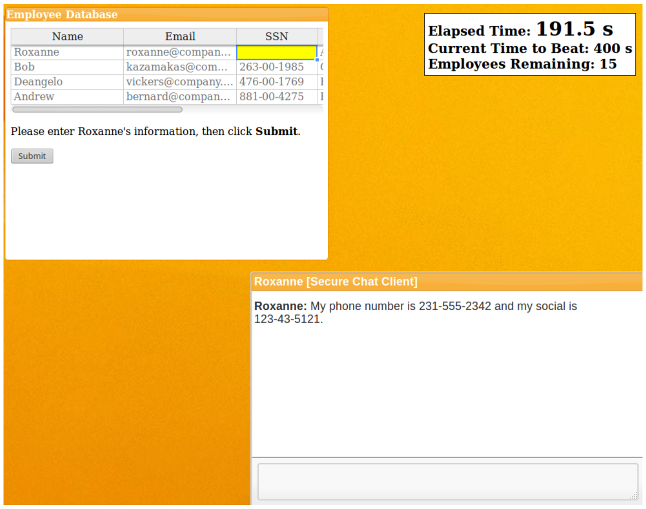
Figure 1: Comparison dialog shown for each of the 30 employees. This example is for a numeric fingerprint representation.

Participants are randomly assigned to an experimental treatment, which affects the particular version of the activity they see. For all conditions, participants are first shown a page describing the role in which they are asked to complete the activity. Participants are asked to imagine that they work as an administrative assistant and that they need to update their company's employee database. To complete this update, they must communicate with 30 employees using an instant messaging system, retrieve the employees' social security numbers (SSN) from the messages, and enter them into the database.

Participants are told that, given the sensitive nature of the communicated information, they will need to perform a security check before talking with each employee. This security check involves comparing two items, shown side-by-side, and correctly determining whether they are the same or different (Figure 1). If participants click the "Same" button, a message from the employee will be shown containing that employee's SSN (Figure 2). If they instead click "Different," a system message will be shown that instructs them to enter "ERROR" in place of the SSN. In both cases, participants must manually type the required information into the database field (copy/paste is disabled) and click the "Submit" button. To increase focus on the database task instead of the item comparison task, we vary the text for each simulated employee's message. In addition, the SSN is sometimes spelled out in words or placed alongside other similar, but incorrect information (e.g., a telephone number).

Our framework is currently designed for a between-subjects experiment testing the security and usability of device pairing methods involving visual comparison. We record usability metrics such as the amount of time participants spend on each comparison task, accuracy of comparisons, and subjective satisfaction (via our post-activity questionnaire). In our current implementation, experimental treatments vary based on two conditions: representation and type of "attack."

Representation. Our framework allows for easy substi-



Employee Database

Name	Email	SSN
Roxanne	roxanne@compan...	
Bob	kazamakas@com...	263-00-1985
Deangelo	vickers@company....	476-00-1769
Andrew	bernard@compan...	881-00-4275

Please enter Roxanne's information, then click **Submit**.

Elapsed Time: 191.5 s
Current Time to Beat: 400 s
Employees Remaining: 15

Roxanne [Secure Chat Client]

Roxanne: My phone number is 231-555-2342 and my social is 123-43-5121.

Figure 2: Database task when participant chooses "Same." The participant must enter the SSN displayed in the chat message into the highlighted database field and click "Submit."

tution of any visual hash representation. Our current implementation includes 7-digit numbers, 3-word phrases, and T-Flag images [5]. In addition to different types of representations, the entropy contained in the representation can be varied by modifying the length or complexity of the chosen representation (e.g., by increasing the number of digits for numeric representations).

Attack. In order to test the security and usability of device pairing methods while under attack, our framework supports conditions based on the type of attack. Example attacks for numeric representations include two different fingerprints that match in the beginning and/or end, or where a '1' in one fingerprint has been substituted with a '7' in the other.

3. SECURITY AS A SECONDARY TASK

Often in the real world, users perform security tasks only in order to accomplish some other primary task. In our role-playing description and in the activity itself, we emphasize the database (distraction) task over the security task. While engaging in a security task, users may additionally be burdened by distractions such as stress and time pressure. We attempt to simulate these conditions using bonus incentives; in our recruitment and activity description, we explain that the fastest 15% of participants who perform their tasks without making any mistakes will receive an additional $1 bonus payment. An on-screen stopwatch is prominently displayed during the entirety of the online activity to remind participants of the need to act quickly (Figure 2).

4. HABITUATION

Participants that perform many security-related tasks may experience habituation that reduces their attention towards these tasks over time. This is especially true if the majority of security tasks involve benign situations.

In our framework, researchers can control the length the habituation period (initial series of benign device pairing tasks). For example, participants could be shown identical pairs for the first 20 out of 30 comparison tasks, with 2 tasks randomly chosen from the last 10 to be an attack. This would allow researchers to compare the security and usability of pairing methods under high levels of habituation. Alternatively, researchers could vary the length of the habituation period as an independent variable. This approach could be used to explore the ability of different representations to resist habituation effects.

5. CONCLUSION

Our framework can be used to facilitate comparative studies of secure device pairing schemes in conditions where security is a secondary task and in which user habituation is a factor. Although our current implementation is targeted towards pairing methods in which users must visually compare two fingerprints, future work could extend its scope to support additional types of pairing methods and fingerprint representations. Some pairing methods may require the use of a smartphone device, such as methods in which the user uses a smartphone to take a picture of a barcode. Future work could explore ways to incorporate these pairing methods into our framework.

6. REFERENCES

[1] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang. A Study of User-Friendly Hash Comparison Schemes. In *2009 Annual Computer Security Applications Conference*, pages 105–114. IEEE, Dec. 2009.

[2] R. Kainda, I. Flechais, and A. W. Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, page 1, New York, New York, USA, July 2009. ACM Press.

[3] A. Kobsa, R. Sonawalla, G. Tsudik, E. Uzun, and Y. Wang. Serial hook-ups: a comparative usability study of secure device pairing methods. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, page 1, New York, New York, USA, July 2009. ACM Press.

[4] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun. Caveat eptor: A comparative study of secure device pairing methods. In *2009 IEEE International Conference on Pervasive Computing and Communications*, pages 1–10. IEEE, Mar. 2009.

[5] Y.-H. Lin, B.-Y. Yang, A. Studer, H.-C. Hsiao, J. M. McCune, K.-H. Wang, M. Krohn, P.-L. Lin, A. Perrig, and H.-M. Sun. SPATE: small-group PKI-less authenticated trust establishment. In *Proceedings of the 7th international conference on Mobile systems, applications, and services - Mobisys '09*, page 1, New York, New York, USA, June 2009. ACM Press.