Two-Factor Authentication, Usable or Not?
A Two-Phase Usability Study of the FIDO U2F Security Key

Sanchari Das, PhD Student, Indiana University Bloomington
Andrew C. Dingman, PhD Student, Indiana University Bloomington
Gianpaolo Russo, PhD Student, Indiana University Bloomington
Dr. L. Jean Camp, Associate Professor, Indiana University Bloomington
(Black Hat USA 2018)

Track

OS - Human Factors

Abstract

Why do people choose to use (or not use) Two Factor Authentication (2FA)? We report on some surprising results from a two-phase study on the Yubico Security Key working with Yubico. Despite the Yubico Security Key being among the best in class for usability among hardware tokens, participants in a think-aloud protocol encountered surprising difficulties, with none in the first round able to complete enrollment without guidance. For example, a website demo, built to make adoption simple, instead resulted in profound confusion when participants fell into an infinite loop of inadvertently only playacting the installation. We report on this and other findings of a two-phase experiment that analyzed acceptability and usability of the Yubico Security Key, a 2FA hardware token implementing Fast Identity Online (FIDO). We made recommendations, and then tested the new interaction. A repeat of the experiment showed that these recommendations enhanced ease of use but not necessarily acceptability. The second stage identified the remaining primary reasons for rejecting 2FA: fear of losing the device, illusions of personal immunity to risk on the internet, and confidence in personal risk perceptions. Being locked out of an account was something every participant had suffered while losing control of their account was a distant, remote, and heavily discounted risk. The presentation will surprise and inform the practitioners, showing them that usability is not just common sense, in fact, sometimes you need to think sideways to align yourself with your potential users.

Presentation Outline

1. Introduction to key terms (2FA)
- This will detail the basic state of research in usability and use of 2FA
- Show that Yubico is among best in class
- Introduce the two widely used evaluation checklists for 2FA

2. Acceptability and Usability
- “Installation precedes operation” is a core observation of usability. But acceptability precedes both, and is needed for continued enrollment
- It will include some remarkable changes in password content that show frustration with 2FA (literally from words of love to trash talk after adoption of 2FA)

3. Not All Those Who Wander Are Lost
-All those who wander around their drive looking for the USB storage device when trying to adopt 2FA are, however, completely lost
- List the sources of confusion, stoppage, and halting

4. From Stories to Telling
   - A slide describing the research steps, how to go from interviews and observations to quantifiable, testable findings
   - The qualitative process in a nutshell

5. Recommendations
-We illustrate the changes that were made

6. Results of Adoption
   - With fairly small changes, usability outcomes vastly improved
   - Yet acceptability was still a problem

7. Risk Communication
   - Examples of quick risk communication options for users, different conceptual models embedded into password risk information

8. Closing Remarks
   - Takeaways for local 2FA adoption

Attendee Takeaways

1. First, users bring some interesting conceptions to the table, and make mistakes we cannot predict without watching them in action.

2. Second, qualitative research can be quantified to provide actionable, testable ways to deal with the issues in the first.

3. Third, usability is achievable, but it is not enough. Messaging and methods to improve acceptability from risk communication and usable security

Also including a qualitative-research-in-a-nutshell, something to take away to understand how to bring this to your own product/deployment in order to get from the first qualitative impressions takeaway to the second quantitative testable result. Risk communications include short videos (short length but high impact), cartoons, and social communication that will be provided under Creative Commons.

Why Black Hat?

There is an immense need to adopt 2FA. If 2FA is not usable or unacceptable in practice, people use workarounds, including far riskier personal versions of Google Drive, free Azure, free emails, and others to just get work done. Making 2FA acceptable and usable for your own user base is a qualitatively different approach than strict compliance. It can result in increased safety and security in addition to greater user satisfaction, or at least, less user dissatisfaction.