UISA: User Interface Security Assessment

Sarah Abdellahi, Heather Lipford *University of North Carolina Charlotte*
Carrie Gates, Jeremiah Fellows, *Bank of America*

Abstract

Human behavior can play a major role in many security breaches and issues within organizations. We propose the User Interface Security Assessment (UISA) method to allow application designers and developers to assess the security risks that result from user interaction with a particular application interface. UISA can help stakeholders to understand the implications of specific design decisions and identify areas for design and security improvements.

1. Introduction and Motivation

Most software designs, whether for external customers or internal employees, are evaluated based on the expected usability and user experience of the application. Many organizations have mature processes for assessing whether a design is intuitive, efficient to use, effective, and in line with the design patterns of the organization. Similarly, many applications with security implications can be evaluated by an application security team for vulnerabilities introduced by the software architecture or implementation. Yet, as the usable security community has long established, user behaviors and decisions play an important part in the overall security of an application, and the design of that application will directly impact those behaviors. As a consequence, a design that is faster to use may not, in fact, lead to the best security outcome. Similarly, if the most secure behaviors are time consuming, users will find less secure methods for accomplishing their goals.

Thus, what is missing from existing UI/UX methods are ways to consider the impact of the user interface and user experience design on application security outcomes. While there are myriad ways to measure how infrastructure, architecture, and code impacts the security of an application, there is not currently a way to measure the cybersecurity implications of a particular user interface. In this paper, we present a method, the User Interface Security Assessment (UISA), for assisting designers and developers in identifying and considering the security implications of a particular interface. Our research is inspired by human reliability measurement methods for safety critical systems, focusing in particular on the errors that people can make within any application [1,2]. Human error has been identified as a root cause of many security incidents [3]. Therefore, our method focuses on all the ways that users may not behave as expected, both from unintentional mistakes as well as intentionally avoiding unusable interactions. By identifying these errors, their implications and triggers, designers can evaluate the security risks of a particular design or application, prioritize aspects of a design that may need improvement, or compare different design ideas based on the potential impact on security.

2. Background

Human Reliability Assessment methods are a well-established research area within safety-critical systems. Numerous methods have been proposed for organizations to identify and measure the impact of human errors from several different aspects including process, psychology, response time, task and social-technical influence [4].

Since 2013, multiple researchers have suggested development of a systematic approach for prediction of data breaches caused by human error. For example, Gu et al, 2014, suggested use of the Technique for Human Error Rate Prediction (THERP), which is a mature technique in human reliability analysis, in the process of information security risk assessment [4]. Similarly, Evans et al suggested adopting HEARTS, another well-known human reliability assessment technique, as a systematic approach for human reliability and error assessment in the information security area [3].

While these two proposed techniques do focus on human errors, they do so at a very high level. For example, the methods outline several causes of human error as a mismatch between an operator's model of the world and that imagined by a designer, and high-level emotional stress [3, 4]. Thus, while these methods may identify that an interface design is a factor in human error, they do not help designers assess or target particular design or interface decisions and identify potential areas for improvement. We aim to fill this gap in our method.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020. August 9 -- 11, 2020, Boston, MA, USA.

3. User Interface Security Assessment

Our method was motivated from our own experiences and research results in usable security. While designers may be well trained in methods for considering and improving the user experience, they are rarely experienced in considering the security implications of those design choices. On the other hand, security engineers are likely to overlook the impact of human behavior within an application, and have unrealistic expectations as to what users are able or willing to do. Software developers may not be familiar with either usability or security engineering, and know how to consider both of those issues together. Thus, our aim is to provide sufficient assistance based on these varied backgrounds to help any particular stakeholder in assessing the security implications of design, as well as provide a way to structure conversations between stakeholders with different concerns regarding usability and security.

The method also focuses specifically on identifying the implications of interface and interaction design decisions, and in particular the ways in which users will behave in imperfect or unexpected ways. Our aim is to provide sufficient assistance to identify the errors that can occur within user interface designs, consider their security implications, and discuss the potential triggers for those errors based on common design guidelines.

The User Interface Security Assessment (UISA) method has 5 steps, which we outline below. Each step of the method is supported by a handbook to structure the assessment, and provide guidance to the variety of stakeholders with different levels of UI/UX design background or security knowledge who may perform the assessment.

1. *Identify application workflows*, to focus the assessment on particular tasks and screens of an applications. The evaluation process can be repeated multiple times to cover all the tasks and workflows in an application or only focus on a specific workflow.

2. *Elaborate all of the user interface elements* that are part of those workflows. This includes elaboration of every element where users provide input, navigate or perform activities, including navigation links and tabs, menus, text entry, and checkboxes and buttons. For the handbook, we developed a general list of these elements based upon a comparison of design component lists on UI design websites and an observation of common elements in interface designs.

3. *Identify all of the possible errors users* could make interacting with each of those individual elements, as well as possible errors they make interacting with a combination of elements in workflow level actions.

   We emphasize that users can make many kinds of mistakes, from unintentional slips and typos, to making the wrong choices due to misunderstandings, to higher level mistakes of finding ways of accomplishing tasks outside of the intended workflow. UISA emphasizes that no possible error should be overlooked during the assessment process, so that the short and long term security impacts of any possible error be considered. To support evaluators in identifying possible errors, as a part of the UISA handbook, we developed a list of possible user errors for each type of interface element, and a list of users common workflow-level mistakes. For example, element level errors are conditions such as when users click the wrong check box, menu option, or button. Users could also neglect to provide input, or provide the wrong input. At a higher level, as examples of workflow level errors, users could abandon the task before completing it, or find an alternative (and possibly less secure) way to accomplish a task.

4. *Determine the security consequences of each error*, and filter out those without security implications. To guide evaluators in thinking through these implications, we created a set of questions to ask for both element-level errors, and workflow-level errors. If the answer to any of these questions is positive, then evaluators should describe the security-related implication in their own words, to make the implications concrete for the particular application.

5. *Identify the potential triggers* for the errors based on usability and usable security guidelines. The final stage of the UISA process is identification of the underlying design choices which may increase the likelihood of the identified errors with security consequences. Users can make slips such as a typo in even the most well-designed textbox. Yet, users are more likely to intentionally or unintentionally provide the wrong input if the labels are poor or formatting of the text is unclear or not checked by the application.

   To reduce the overhead of identifying triggers, and help provide focus to those less familiar with interface design, UISA provides a set of triggers derived from common interface design guidelines, as well as usable security guidelines.

4. Improving and Using UISA

We intend for UISA to be used to identify and evaluate security risks from user errors in current or potential user interface designs. Our goal is to help guide designers in modifying design elements to eliminate or minimize the identified security risks. There are a number of future steps we are pursuing to improve the method. First, we are actively seeking feedback from researchers and practitioners. We will be conducting studies of the use of the method and handbook to ensure the method can be followed and improve the instructions and guidance provided by the handbook. We will be examining the outcomes and issues raised by the use of the method in case studies.

Additionally, we are extending our method to be utilized as part of a measure of security risk of interface and interaction designs. This security assessment metric will translate the UISA guideline findings into a numeric value that can be used for comparison of design alternatives and more structured conversation about usability and security preferences. Finally, we would like to build a tool to support assessors using and documenting the UISA Metric.

5. References

1. Bell, J., & Holroyd, J. (2009). Review of human reliability assessment methods. *Health & Safety Laboratory*, *78*.
2. Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667-4679.
3. Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, 74-89.
4. Gu, T., Li, L., Lu, M., & Li, J. (2014, August). Research on the calculation method of information security risk assessment considering human reliability. In *2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS)* (pp. 457-462). IEEE.