Usable Cybersecurity

Levi Seibert

00086809

lseiber1@my.athens.edu

CS 484 Research Paper

Usable Security

It is well-known that we live in a world of convenience. Everyone carries around a computer in their pocket, groceries are delivered to people's porches, and work meetings are often held in the comforts of the bedroom. Today's culture is focused on how to please oneself with the least amount of work. As a consequence, there is a lackadaisical view of cybersecurity in society. Often, people are unwilling to take the extra steps necessary to protect themselves, their computer, and their workplace from the evils of the cyberworld. It is not all their fault, however. Cybersecurity can be tedious. In all fairness, it can at times seem unreasonable. Why waste so much time preparing for an attack that potentially may never come? It is easiest (and most convenient) to just ignore the issue. Unfortunately, ignorance is not bliss. But then again, people do not have all the time in the world to devote to protect themselves. Instead, a compromise must be reached; a compromise that makes cybersecurity more usable and doable.

Authors Nurse, Creese, Goldsmith, and Lamberts, from the University of Warwick, penned the article entitled, "Guidelines for Usable Cybersecurity: Past and Present", presented at the 3rd International Workshop on Cyberspace Safety and Security in 2011 (referenced throughout). This paper deals with the ongoing conflict between security and usability. An example of this tension that is presented in the article is that of password policies. From a security point of view, passwords should be unique, lengthy, and difficult to guess; however, from a usability view, users struggle to be able to meet these standards and their productivity suffers. Strict authentication methods can unnecessarily impede the capabilities (both mental and physical) and motivation of users. This is just a single example, but it is easy to observe the far-reaching consequence of the usability/security debate. In fact, it may seem unreasonable to be able to offer these two functions simultaneously; however, as the article discusses, the facilitation of these two properties is possible. The discussion of this concept is referred to as the Cybersecurity Usability and comparable Human-Computer Interaction and Security, abbreviated as HCISec or HCI-S.

After identifying and introducing the problem at hand, the authors of "Guidelines for Usable Cybersecurity", proceed to detail more specific examples of how the conflict is manifested in the real world. They break subdivide the field of cybersecurity into six categories: authentication, encryption, public key infrastructure, device paring, security, and security systems. Each of these facets of security tend to infringe upon the usability of the systems they are associated with. For instance, requiring users to have to authenticate themselves repeatedly impairs users from working to their full potential. As a result of reduced usefulness, a grave situation arises: security standards may be misconfigured. Unfortunately, most cybersecurity controls cannot be compromised. Security is vitally important, not only to just the user and their computer, but also to the network and the organization as a whole. A single point of failure can produce immense consequences.

Some of the reasons users may be willing to compromise on security include: security interfaces are not well designed, security is not a priority for users, security is hard to understand, there is a deficiency in feedback from security systems, and there is no way to ensure an attack has not occurred. In addition, the workloads required to implement cybersecurity often deter many users (even those trained in security). There is also the issue of "awkward" requirements involved with cybersecurity, such as always locking one's PC while not at the desk, a policy which many users find annoying and pointless. Often, it is the case that security is not even considered a priority in system design and is sort of tacked on at the end of the design phase, providing little actual usefulness to the system at all (if not impedance). In this case, usability is focused on security is practically forgotten. Not only does this lead to potential safety issues in the programs, but from an end-user's point of view, it may present a "lack of visibility" of security in user applications. Security features may be spread out too much, lack consistency, or even be marked as "advanced", thus discouraging use by common users. On the other side of the spectrum, there is a danger focusing too much on security, such that the usability is overshadowed. For example, systems may overwhelm users with industrial vocabulary, provide ambiguous functionality, or fail to deliver useful feedback. These issues, in addition to turning users against security, may also lead to unintentional and unplanned cybersecurity frameworks.

After discussing the problems between usability and security, "Guidelines for Usable Security" describes the methodologies used by researchers to evaluate the usability of cybersecurity systems. The two main approaches to usability research are user studies and expert input. When working with user studies, researchers meet with a representative portion of the users and perform experiments with them to gauge how usable a given systems is. These evaluations often take the form of lab-based testing, surveys, interviews, observations, and other forms of assessments. Researchers (either in a lab setting or using one-way mirrors) may observe users complete given tasks, in order to evaluate how usable the system is in real-life scenarios. It may also be useful to conduct pre- and post-assessments in order for the researchers to gather opinions and analysis from the users. Of course, simple user interviews may be used to gather direct input from those who currently use the cybersecurity systems. Since user studies provide researchers with very valuable information about the actual systems being studied, they are often the preferred method. Unfortunately, these studies do come a cost, namely, they can be expensive and take a lot of time (something that researchers may not have an abundance of).

In addition to user studies, Nurse, Creese, Goldsmith, and Lamberts suggest preforming usability evaluations based on input from experts. Experienced specialists are often consulted to assess how usable a system is. One of the benefits of this solution is that it helps researchers prioritize the different usability criteria during the assessment. Two of the main methods of expert evaluations are cognitive walkthroughs and heuristic evaluations. In walkthroughs, the experts mentally work through the system and consider the usability as they go along. Alternatively, in heuristic assessments, the experts compare the system to a set of rules (such as testing whether a specific tool meets given usability rules).

The implementation of user studies and expert analysis do not have to be distinct. Often, the best way of evaluating the usability of a system is to get input from both those who use the system (or will use the system) and those who are expertly trained in the knowledge of the workings of the system. One solution that has been presented consists of using expert-based assessments in the early stages of the evaluation and then later preforming user studies to verify the decisions made by the experts and to find any real-life problems that may exist in the proposed system.

After detailing how usability in cybersecurity systems is evaluated, "Guidelines for Usable Security" delineates the most significant recommendations that remediate the usability issues that are often faced. These guidelines are gathered by the authors from their own survey of literature, and the recommendations are analyzed. First of all, Nurse et al. conclude that the usability of cybersecurity solutions should be considered at an early stage in the design and development of systems. Cybersecurity usability also needs to accommodate any user who uses the product. Frameworks should be intuitive enough that they do not require an expert to understand how to use them. Systems also need to provide helpful feedback, troubleshooting, advice, and documentation, all of which should be understandable by all users. Along the same lines, systems should visibly display their current state, so that users are aware of the current situation of security. The functionality of the security also needs to clearly visible and easy to access. There also needs to be some mechanisms in place to guard against errors, and, if errors do occur, handle them properly and allow for ways to remedy them.

A very important concept that needs to be considered when creating cybersecurity systems is to design the features and functionalities to not be mentally tasking. That is, the elements of the system need to be designed with human limitations of cognition and memory in mind (do not require users to have memorize unreasonable amounts of information, make systems easy to understand, etc.). When presenting user decisions, the system should provide recommendations and guidance on what tasks to perform. The system designers need to strive to present a positive experience to the user. This design needs to as minimalistic and simple as possible, while not sacrificing functionality. In addition, the system, even if complex, and the content should be easy to learn. Part of the learnability of the system is achieved by removing any unnecessary jargon or technical vocabulary.

Users should be able to easily create a mental model of the system and understand its structure. This can be attained, in part, by separating distinct parts of the system (keeping policies and user values separate, for example). Since the purpose of a cybersecurity system is to provide protection, security needs to be implemented in all layers of the program (both the lower, technical levels and the upper, usable layers). This security, however, needs to be achieved without compromising performance. Failing to ensure this is true will lead to usability issues, thus conflicting with the ultimate goal of balancing security and usefulness. Finally, designers need to remember that the specific, individual tools of security are not complete solutions; the tools are necessary to implement the security but need to be made usable for consumers. While there are other potentially other security and usability considerations that may be needed in designing a system, Nurse, Creese, Goldsmith, and Lamberts felt that the aforementioned ones are the most important and will reliably produce a usable cybersecurity framework.

Further research needs to take place to create a complete template to balance security and usability; however, “Guidelines for Usable Cybersecurity: Past and Present” provides a general framework that seeks to alleviate the issues currently being faced. If an organization keeps these recommendations and principles in mind while designing their cybersecurity solutions, then security will be easier to accomplish, and users will be more willing to do their fare share of protecting an organization. Usable security is an attainable goal and, although it may be difficult to fully implement, it needs to be striven for.

Reference

Nurse, Jason & Creese, Sadie & Goldsmith, Michael & Lamberts, Koen. (2011). Guidelines for usable cybersecurity: Past and present. Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011. 21 - 26. 10.1109/CSS.2011.6058566.