The Security–Usability Tradeoff Myth

M. Angela Sasse | University College London
Matthew Smith | University of Bonn and Fraunhofer FKIE

Usability problems are the root cause of many of today's IT security incidents. Security mechanisms are often too time consuming for people to bother with, or so complex that even those willing to use them make mistakes. For more than a decade, usable security researchers and practitioners have tried to address this problem by creating more usable security solutions. Retailers, banks, and communications providers have learned that security that gets in the way of their customers is bad for business. Some organizations—especially those who were "born digital" and have a large customer base—have managed to increase security without impacting business, for instance, by introducing low-effort two-factor authentication and using the data they have to identify unusual behavior patterns. But researchers still identify a disconcerting number of security mechanisms today that induce mistakes or noncompliance, and ultimately put individuals and organizations at risk—or cause consumers to walk away. This not only damages digital business but also fosters the unhelpful perception among non–security experts that online security isn't worth bothering with. As the value of digital transactions continues to increase, so will the number and sophistication of attacks—if the bank robber Willie Sutton Jr. were alive today, he would turn to cybercrime, because "that's where the money is" now. To successfully defend digital business, we need to engage with consumers and offer them simple and effective security solutions.

This special issue of *IEEE Security & Privacy* features three articles and a roundtable discussion that examine the relationship between security and usability in detail to identify the perceptions, processes, and practices that underlie these continuing problems and to identify what needs to change to move the field forward.

When we examine published usable security research to date, we find that most studies have been performed in laboratories with a limited number of participants (often students) who were

1540-7993/16/$33.00 © 2016 IEEE Copublished by the IEEE Computer and Reliability Societies

observed on one occasion using a security mechanism. Over the past few years, we've seen a growing number of studies with hundreds or thousands of participants recruited via crowdsourcing platforms. In these studies, participants receive very small payments in return for interacting with a security mechanism and completing surveys. But they use the security mechanisms only once or twice, within a couple of days, in the context of a fictional task that isn't their own and where their money or data isn't at risk. There's a lack of field studies in real environments to understand the impact that security mechanisms have on individuals and businesses. The article, "Secure and Usable Enterprise Authentication: Lessons from the Field," by Mary Theofanos and her colleagues, makes a notable contribution because it surveyed more than 30,000 employees of two US government departments on their day-to-day experiences with two-factor authentication. The authors found that different implementations of the same two-factor technology produced significantly different experiences—reminding us that sometimes small differences in implementation can make a big difference to those who have to use the security.

> **Retailers, banks, and communications providers have learned that security that gets in the way of their customers is bad for business.**

"Barriers to Usable Security? Three Organizational Case Studies," by Deanna D. Caputo and her colleagues, reports on three software development organizations that wanted to provide usable security solutions. A multidisciplinary team interviewed developers, management, and security and usability experts who had been involved in the development of a certain product from each company. However, the researchers found no tangible evidence that the products were usable. The companies didn't perform empirical or analytic usability testing and had no criteria or measurements. Similarly, there was little or no formal security evaluation—and certainly no metrics. The interviews showed that many developers and security experts didn't understand usability and its contribution to the business process. In the absence of formal testing and measurements, usability was mostly a *grudge sale*: it became a concern only when the company experienced significant problems, such as a drop in sales or a significant rise in help-desk calls. At the same time, security experts keep bemoaning the fact that security is a grudge sale, as far as users are concerned.

Software-engineering research established 20 years ago that the later in the process you have to "fix" fundamental problems, the more expensive it will be to do so. But Caputo and her colleagues' studies found that, nevertheless, the companies didn't consider the requirement for security to work in the context of business tasks upfront. Many security experts and developers in these studies invoked the security–usability tradeoff, which is insidious because it reinforces the perception that it's not necessary to engage with users or to understand the tasks users are engaged in. As Cormac Herley points out in the roundtable discussion, "Debunking Security–Usability Tradeoff Myths," this is "phon[ing] in" an excuse. Very few participants in Caputo and her colleagues' studies had engaged sufficiently with usability to realize it would increase security—because if the security is usable, users will do the security tasks, rather than ignore or circumvent them.

As Herley points out, the insidiousness of the purported tradeoff is that, in the absence of measurements, it's hard to disprove. The tendency has been to use any hypothetical reduction in security as an excuse for users to have to bear the cross of workload and complexity that a security mechanism puts on them. The roundtable discussion, which also featured Heather Lipford and Kami Vaniea, revealed that this attitude squanders user attention and effort that will be needed as the number and sophistication of attacks increase. Vaniea points out that communication about risks and what consumers need to do needs improvement—for instance, users aren't aware that software updates are key to security.

Although usable security researchers see the value of engaging with end users when designing security mechanisms, many experts do not. It's common for experts to believe that they know best and that users should invest whatever time and effort they believe is necessary. Vaniea offered this quote from a study concerning the Windows 10's update process: "the audacity of a user to question the opinion of the expert who put this update in there is shocking." This kind of attitude is of course harmful and needs to be studied. We must find ways to help experts engage with users.

A further and as yet unstudied area of usable security research is the mistakes made by experts. Many of the most catastrophic security incidents weren't caused by consumers or employees, but by developers or administrators. Heartbleed and Shellshock were both caused by single developers and had global consequences. The recent Sony hack compromised an entire multinational IT infrastructure and misappropriated more than 100 Tbytes of data—unnoticed. Fundamentally, every

software vulnerability and misconfigured system is caused by developer or administrator mistakes, but very little research has studied the underlying causalities and possible mitigation strategies. A multitude of factors play into this problem. The first is the myth that experts are infallible. Similar to Anne Adams and M. Angela Sasse's seminal work and call to action, "Users Are Not the Enemy," we need to rethink our stance concerning experts and recognize that they too are only human and should receive as much if not more assistance than end users because their mistakes are just as natural but often more critical.

The article "Developers Are Not the Enemy! The Need for Usable Security APIs," by Matthew Green and Matthew Smith, explores this issue in the context of usability of cryptographic APIs. What makes this area of research particularly challenging is that it's far harder to recruit experts for usability studies, compared to the relative ease of recruiting end users. Consequently, we haven't seen many studies involving experts and this area remains largely unexplored, leaving many more myths to find and bust.

This is an exciting time for security research—a time to examine long-held beliefs about how to manage security. We need to use scientific research methods to put countermeasures that pass the test on sounder footing, and use measurements to check if we're doing better or worse when we make changes. And of course, we need to be prepared to bury the beliefs that turn out to be incorrect. The security–usability tradeoff myth is only the first to bite the dust. ■

M. Angela Sasse is a computer science professor at University College London. Contact her at a.sasse@ucl.ac.uk.

Matthew Smith is a computer science professor at the University of Bonn and the Fraunhofer FKIE. Contact him at smith@cs.uni-bonn.de.

Letters for the editor? Please email your comments or feedback to editor Christine Anthony (canthony@computer.org). All letters will be edited for brevity, clarity, and language.