EDITOR **JEFFREY VOAS**
IEEE Fellow; j.voas@ieee.org

Is Usable Security an Oxymoron?

Mary Theofanos, NIST

Current multipronged cybersecurity measures require the active support and participation of users for their successful deployment. Although no formal definition of usable security exists, it is time to make it a reality for users.

The field of usable security is nearly 25 years old. Despite an early, influential paper on computer security published in 1975 by Saltzer and Schroder[1] that defined the principle of "psychological acceptability," the fields of cybersecurity and usability continued to grow independently until the mid-1990s. Then, the authors of three seminal papers jumpstarted the research in usable security. First, in 1996, Zurko and Simon[2] introduced the phrase *user-centered security*. Soon after, Adams and Sasse[3] identified users as part of the solution, rather than the problem. Finally, in "Why Johnny Can't Encrypt,"[4] Whitten and Tygar applied usability testing to encryption software, demonstrating Saltzer and Schroder's principle of psychological acceptability:

> *It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized.*[1]

In the "Why Johnny Can't Encrypt"[4] case, the lack of understanding of the underlying models of public key cryptography and digital signatures interfered with using the interface.

Today, the field of usable security has an established body of research, with hundreds of papers in dozens of peer-reviewed venues across multiple domains, from human-centered interaction, cybersecurity, and usability to software engineering, economics, sociology, and psychology. Researchers span academia, industry, and government. The field has successfully raised awareness of the importance of the human element in meeting cybersecurity objectives. The awareness and recognition of the human element has been embraced by industry and spawned new businesses and major governmental initiatives in the United States and Europe.

Yet, users are still confused, frustrated, and overwhelmed and do not know how or what to do to keep themselves and their technology safe. The news is filled with stories of security breaches, identity theft, ransomware, and malware, which fuels fear and anxiety. Work at the National Institute of Standards and Technology (NIST) examining general users' perceptions and beliefs about cybersecurity and online privacy underscores the following sentiments:[5]

Digital Object Identifier 10.1109/MC.2019.2954075
Date of current version: 12 February 2020

There is a lot of information and there may be a lot of misinformation. And I tried—it is all behind me, and I cannot ever secure my computer. There is a lot to keep up with (participant 117).

There is the firewalls, and Norton, and there is this and antivirus, and run your checkup, and so many things that you can do—I just get overwhelmed (participant 108).

The phenomena the users in the study were describing and experiencing is called *security fatigue*, that is, "the psychological state one reaches when security decisions become too numerous and/or too complex, thus inhibiting good security practices."[6] With the pervasiveness of the Internet of Things (IoT), unfortunately, the number of cybersecurity decisions users must make is only getting worse. According to the Symantec Internet Security Threat Reports,[7] there are 25 connected devices per 100 inhabitants in the United States. An article in *The Economist*[8] predicts that there could be a trillion devices by 2035, at which point, IoT devices would outnumber humans by more than 100 to one.

What's a user to do? Maybe usable security is an oxymoron.

WHAT IS USABLE SECURITY?

As it turns out, usable security is hard to define. According to the International Organization for Standardization (ISO), *usability* is defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use."[9] And we know how to define *security*, now referred to as *cybersecurity*: "the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, to strengthen the confidentiality, integrity, and availability of these systems."[10] But how do we define *usable security*? To date, we have no formal definition of usable security; instead, the field has focused on applied problems and the interactions of cybersecurity and usability.

Since 1996, a body of research spanning five overarching themes has been published: authentication, encryption, security dialogs, social engineering, and privacy. The themes represent uniquely different constructs, user behaviors, and interactions. Authentication and encryption are tools that underpin the very foundation of cybersecurity. Security dialogs result from the need for human intervention when the system cannot determine the appropriate action. Social engineering is an attack or threat to cybersecurity through the use of deception. Finally, privacy is a right: "the right of a party to maintain control over, and confidentiality of, information about itself."[11] Assessing developments in the five themes provides a lens by which to evaluate the impact of the research on end users.

Authentication

Research studies on passwords and authentication represent the majority of papers in the field. Garfinkel and Lipford[12] group the study of text passwords into four categories: password policies, leaked stolen databases, users in laboratory settings choosing and using passwords, and password usage on operational systems. In addition to the heavy focus on text passwords, nearly every aspect of passwords has been examined, including password managers, graphical authentication, biometrics, token-based authentication, and multifactor authentication.

Yet, the main complaint about security is still passwords. Authentication and password management continue to paint a troubling picture for users and cybersecurity. LastPass,[13] a company which provides password managers that store encrypted passwords online, reported the following about the average employee:

- he/she juggles more than 100 passwords
- he/she types out credentials to authenticate to websites and apps 154 times per month
- he/she shares roughly four passwords with others
- more than half (61%) use the same or a similar password for everything, even though they know it is not a secure method.

Finally, multifactor authentication is not widely adopted, as only 27% of the businesses LastPass supports have enabled multifactor authentication to protect their password vaults.

Even conference reviewers, journal editors, and conference attendees have expressed fatigue with and for additional password and authentication research. Bonneau et al.[14] compared more than 30 authentication approaches with respect to usability, deployability, and security characteristics and found that, from a security perspective, most approaches outperform passwords. From a usability perspective, some perform better and others worse than passwords; however, none of the approaches could compete with passwords for deployability. The bottom line is that incumbent (passwords) will be around until the costs of remaining with passwords outweighs the cost of transitioning.

Encryption

As an enabling technology for cybersecurity, encryption plays a fundamental role in assuring confidentiality and integrity. Historically, cryptology and encryption in the form of ciphers have been used for centuries to send secret messages. Thus, it should not be surprising that encryption and digital signatures are the basis of secure messaging online. Unfortunately, the sending of secure email and messages is plagued by many usability challenges, including misleading and overloaded terminology, key management, the use of certificates and certificate pop-up messages, mismatches in conceptual models, complexity, and far too many steps.[15] Given that even seasoned software developers find it difficult to implement correctly,[16] what

hope does the typical user have? Since 1999, there has been a tremendous body of work focused on the usability challenges of encryption. But, despite this attention, the 2015 USENIX Test of Time Award was presented to "Why Johnny Can't Encrypt."

Social engineering

Social engineering can be defined as the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.[17] Phishing is the most publicized social engineering threat. In this respect, in particular, users have been categorized as the "weakest link." Although significant research on blacklists, whitelists, warnings (both active and passive), compliance-driven training, embedded training, fear, and punitive measures have been studied, the losses associated with phishing amounted to nearly US$1.3 billion in 2018,[18] double those of 2016, with an upward trend expected to continue.

Security dialogs/warnings

Security dialogs and warnings represent another major annoyance to users, much like authentication. In fact, we have conditioned users to ignore security indicators and just click through active browser pop-ups without any thought to the consequences. License agreements and privacy notices suffer the same fate; users click to eliminate the disruption and move on to their primary task. Security dialogs and warnings force users to make a decision about security, exacerbating security fatigue, and reinforcing that security is in the way.

Privacy

Privacy differs from the other constructs discussed in this article, as privacy is a human characteristic and right. As such, the technology of the World Wide Web, social media, mobile phones, and the IoT have highlighted the competing interests of organizations and consumers with respect to data collection and privacy. In a study of smart home technology usage, one participant recognized this discrepancy:

> *The manufacturer's desires are counter to the consumer, and I don't have much trust in what they say they collect and don't collect. I think they collect everything that they can and use it.*[19]

Given that business models and users' desires are in direct conflict, usability challenges abound in the privacy space. Research has examined user's perceptions, beliefs, and behaviors with respect to privacy, behavioral advertising, notice and choice, privacy policies, interfaces to address privacy settings, privacy tools, and location privacy to the risks of the shared data, among many others. The privacy space will continue to evolve as people's attitudes and social norms evolve with technology.

Given that business models and users' desires are in direct conflict, usability challenges abound in the privacy space.

In her 2019 keynote at the Usable Security Workshop, Angela Sasse wished the field of usable security, a "happy birthday" and followed with "It's time to grow up." Even though a substantial amount of research has been performed and reported over the last 25 years, the usable security community is "preaching to the choir." Consider a case study of three large companies (14,000–300,000 employees) that explored the organization's attempts to improve the usability of its security products.[20] Unfortunately, only one of the dozens of individuals interviewed described a user experience in which security didn't interrupt the user. Given this lack of understanding of the goal of usable security, it is not surprising that the developers had no concept of the importance of user capabilities and limitations, primary tasks, the context of use, and associated performance constraints.

It is time to move the theory into reality by codifying the best practices identified over the last 25 years to inform dialogue and decisions for those who implement cybersecurity. Although there are standards bodies, including ISO working groups that are actively producing standards in both usability and security, at this time, no working group is developing standards in usable security. As discussed previously, we do not even have a formal definition of usable security; however, we expect practitioners to intuit what it is and how best to implement it.

Several organizations have begun the process of documenting best practices, for example, the United Kingdom's Center for the Protection of National Infrastructure's Password Guidance[22] and the update of NIST's Special Publication 800-63 Identity Guidelines,[23] which specifically addresses usable security in the context of authentication. But we must formalize the documentation of best practices and guidelines into standards to systematically move from theory to practice. The convening of technical experts from academia, industry, and the public sector on an international stage to develop international standards in usable security provides the foundation for usable security to become a reality and debunk the oxymoron argument.

We need to stop thinking of users as adversaries. Today, cybersecurity requires a multipronged approach, which includes technological tools and organizational policies that support and encourage employees to actively participate. Consider phishing as just one example: providing easy reporting mechanisms and policies can encourage users to become an early warning system and

positions employees to play a major role in defending an organization's data.[21] Early detection can substantially reduce phishing recovery effort and cost.

It is time to make usable security a reality for users. Let's make it easy for users to do the right thing, difficult to do the wrong thing, and easy to recover gracefully when the wrong thing happens.

REFERENCES

1. J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proc. IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975. doi: 10.1109/PROC.1975.9939.
2. M. E. Zurko and R. T. Simon, "User -centered security," in *Proc. Workshop on New Security Paradigms* Lake Arrowhead, CA: ACM Press, 1996, pp. 27–33.
3. A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 41–46, 1999. doi: 10.1145/322796.322806.
4. A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proc. USENIX 1999*. Washington, D.C.: USENIX Press, 1999, pp. 169–184.
5. B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security fatigue," *IEEE IT Prof.*, vol. 18, no. 5, pp. 26–32, 2016. doi: 10.1109/MITP.2016.84.
6. M. F. Theofanos, "Vulnerabilities: Security fatigue," in *The Language of Cybersecurity*, 1st ed., M. A. Flores, Ed. Laguna Hills, CA: XML Press, 2018, pp. 16–17.
7. "2019 Internet security threat report," Symantec, vol. 24, 2019. Accessed on: Oct. 28, 2019. [Online]. www.symantec.com/security-center/threat-report
8. "Chips with everything: How the world will change as computers spread into everyday objects," *The Economist*, Sept. 12, 2019, pp. 1–13. [Online]. Available: https://www.economist.com/leaders/2019/09/12/how-the-world-will-change-as-computers-spread-into-everyday-objects
9. *Ergonomics of Human–System Interaction—Part 210: Human-Centred Design for Interactive Systems*, ISO 9241-210:2019.
10. NIST Computer Security Resource Center, "Glossary: Cybersecurity." Accessed on: Oct. 28, 2019. [Online]. https://csrc.nist.gov/glossary/term/cybersecurity
11. NIST Computer Security Resource Center, "Glossary: Privacy." Accessed on: Oct. 28, 2019. [Online]. https://csrc.nist.gov/glossary/term/privacy
12. S. Garfinkel and H. Lipford, *Usable Security: History, Themes, and Challenges*. San Rafael, CA: Morgan & Claypool, 2014. doi: 10.2200/S00594ED1V01Y201408SPT011.
13. "Average business user has 191 passwords," *Security Mag.*, Nov. 6, 2017. Accessed on: Oct. 28, 2019. [Online]. www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
14. J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Security and Privacy*, 2012, pp. 553–567.
15. R. Abu-Salma, M. Angela Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," in *Proc. IEEE Symp. Security and Privacy (SP)*, 2017, pp. 137–153.
16. J. M. Haney, M. Theofanos, Y. Acar, and S. S. Prettyman, "'We make it a big deal in the company': Security mindsets in organizations that develop cryptographic products," in *Proc. 14th Symp. Usable Privacy and Security (SOUPS 2018)*, 2018, pp. 357–373.
17. NIST Computer Security Resource Center, " Glossary: Social engineering." Accessed on: Oct. 28, 2019. [Online]. https://csrc.nist.gov/glossary/term/social-engineering
18. P. Muncaster, "FBI:BEC losses surged to 1.3bn in 2018," *InfoSecurity Mag.*, Apr. 24, 2019. Accessed on: Oct. 28, 2019. [Online]. https://www.infosecurity-magazine.com/news/fbi-bec-losses-surged-to-13bn-in-1-1
19. J. Haney, S. Furman, M. Theofanos, and Y. Acar, "Perceptions of smart home privacy and security responsibility, concerns, and mitigations," in *Proc. Symp. Usable Privacy and Security Poster*, Aug. 2019. [Online]. Available: https://www.usenix.org/sites/default/files/soups2019posters-haney.pdf
20. K. Greene, M. Steves, and M. Theofanos, "User context: An explanatory variable in phishing susceptibility," in *Proc. Workshop Usable Security (USEC 18)*, 2018. doi: 10.14722/usec.2018.23016. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2018/07/usec2018_01-2_Greene_paper.pdf
21. D. D. Caputo, S. L. Pfleeger, M. A. Sasse, P. Ammann, J. Offutt, and L. Deng, "Barriers to usable security? Three organizational case studies," *IEEE Security Privacy*, vol. 14, no. 5, pp. 22–32, 2016. doi: 10.1109/MSP.2016.95.
22. "Simplifying your approach: Password guidance," Centre for the Protection of National Infrastructure, National Technical Authority for Information Assurance, London, UK, 2015. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf
23. P. Grassi, M. Garcia, and J. Fenton, "Digital identity guidelines," NIST SP 800-63-3, 2017.

DISCLAIMER

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

MARY THEOFANOS is a computer scientist at NIST. Contact her at mary.theofanos@nist.gov.