Shouldn't All Security Be Usable?

MARY FRANCES THEOFANOS
National Institute of Standards and Technology

SHARI LAWRENCE PFLEEGER
Dartmouth College

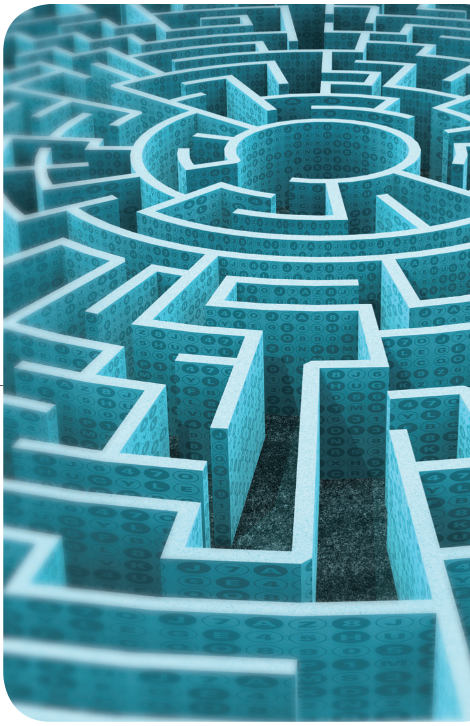
Usability—"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use"[1]—is more than a well-designed user interface. Consider the following examples of usability and security.

A handheld fingerprint identification device for law enforcement is currently being field-tested in several local jurisdictions.[2] The unit captures suspects' fingerprints and takes a photo. The officer can send this information to the local police department and federal databases, and if it generates a database hit, the officer can view the suspect's history and a photo.

For security, the officers must log in to the device with a user ID, password, and fingerprint. Unfortunately, the small interface and keyboard make it difficult to enter text, and because an asterisk is displayed for each input character, users have no indication that they selected the correct characters. In addition, no input device is supplied, so users must use a pen or stylus from another device. During observation, officers often tried to log in three or four times before they were successful. Most stopped using the device in the field because they couldn't log in quickly enough.

Usability testing should have rooted out these interface problems during design or testing, but testing the usability of security mechanisms isn't always straightforward. For example, in the medical field, to protect patient data, access control and traceability are traditionally managed using password-protected accounts. Medical professionals trying to administer patient care might perceive this type of access control as an impediment, particularly when many people access a single machine during the day. Anne Adams and Ann Blandford reported that, in one UK hospital, staff members often remain logged in throughout the day, providing unfettered access to the computing systems.[3] Circumventing security controls allows swift and efficient patient care, but it destroys the audit trail.

In this example, the interface isn't the problem. Even though passwords are easy to use and not particularly technologically complex, they impede the primary task. Thus, system designers face the challenge of providing adequate security without interrupting performance.



A Short History of Usable Security

Jerome H. Saltzer and Michael D. Schroder's "The Protection of Information in Computer Systems"—an early and influential paper on computer security—addressed usability and defined the 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."[4]

However, little additional cybersecurity research considered usability's role until 20 years later. In the late 1990s, three classic pa-

1540-7993/11/$26.00 © 2011 IEEE

pers put security usability back in the spotlight:

- "User-Centered Security," by Mary Ellen Zurko and Richard T. Simon, introduced the phrase *user-centered security*;[5]
- Anne Adams and Angela Sasse's "Users Are Not the Enemy" reclassified users as potential parts of the solution, not the problem;[6] and
- "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," by Alma Whitten and Doug Tygar, demonstrated that even when security software developers strive to make their software useful, profound usability problems might still exist.[7]

Zurko and Simon observed that "as computing power becomes more prevalent on the office desktop and in the home, usability becomes increasingly important in determining which software will be deployed and which software will not."[5] This comment reflects a growing, 21st-century recognition of the user's role as a key component in large and complex software systems. User perceptions, characteristics, needs, and abilities are essential inputs to an effective and robust system design.

These papers were followed by several important workshops:

- The first formal meeting of the human-computer interaction (HCI) community focusing on security—the HCI and Security Systems (HCI-Sec) workshop—was held in conjunction with the ACM Computer-Human Interaction Conference in 2003.
- A birds-of-a-feather session examining security usability was held at the Usenix Security Conference in 2003.
- The first Workshop on Usable Privacy and Security Software was held at Rutgers University in July 2004.

Workshop attendees formed a critical mass of interested researchers in this fledgling field and eventually initiated an annual Symposium on Usable Privacy and Security (SOUPS) in 2005. The SOUPS organizers also published a usability and security reference text, *Security and Usability: Designing Secure Systems that People Can Use*.[8] Since then, interest has grown steadily, and attendance at the sixth SOUPS conference was double that of the original meeting.

Research Focus Areas

The 2010 SOUPS workshop's program indicates current research areas:

- passwords and accounts;
- authentication for mobile devices;
- privacy, security, and public policy;
- institutional review boards and HCI-Sec research;
- integrating usability with security education;
- usability of health security and privacy; and
- security models and decision-making.

Paper topics offer a broader picture of key research areas. The "word cloud" in Figure 1—generated from the titles of references in several HCI-Sec bibliographies (for example, http://gaudior.net/alma/biblio.html)—reveals the popularity of studies involving authentication (especially passwords), access controls, encryption, models, phishing, privacy, trust, and general security. The publication year was included in forming the cloud; its size represents the number of papers. It's clear that the research literature on security usability is growing at an accelerating rate.

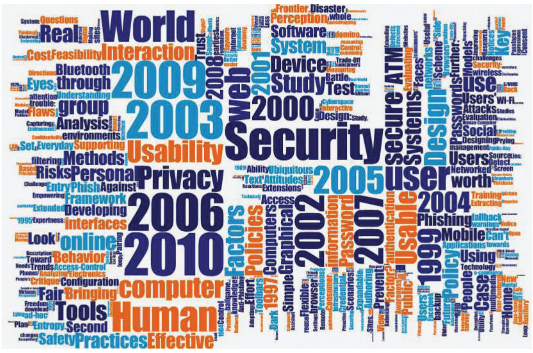


Figure 1. Word cloud of security usability studies topics. The publication year was included in forming the cloud; its size represents the number of papers.

The cloud provides the big picture, but scrutiny of the details reveals a variety of types of investigation. In 2009, Colin Birge analyzed the existing usable security literature, partitioning studies into five general categories:[9]

- usability and design studies that apply traditional usability evaluation methods to user interfaces with security or privacy implications (see the "Traditional Usability Evaluation Methods" sidebar);
- security feature studies that examine specific security or privacy risks and their mitigations;
- trust and ethical studies that explore definitions and concepts of trust and privacy from multiple perspectives;
- security and privacy experience studies that investigate users' attitudes about security and privacy; and
- modeling and guidelines that attempt to create models demonstrating how trust interactions work. (We can expand this category to include models that define HCI related to computer security.[10–14])

M. Eric Johnson and Eric Goetz documented the concerns of security experts at several Fortune 500 companies.[15] They reported that customers expect security to be usable and demonstrably effective. Researchers are starting to pay attention to these needs. When a

Traditional Usability Evaluation Methods

Usability tests share five distinguishing characteristics:[1]

- The test's primary goal is to improve a product's usability. This characteristic differentiates usability testing from a number of other types of testing, such as quality assurance and conformance tests, which focus on determining whether the product works according to specifications. It also distinguishes usability testing from hypothesis-based research studies.
- Test participants represent real users. User demographics are critical to the test's success. Testing more or less experienced users than the actual user population might result in changes that cause the product to fail in the marketplace.
- Test participants perform real tasks. The tasks must be realistic and relevant to real users and should relate to the usability team's goals and concerns about the product.
- Test facilitators observe and record what participants say and do. This characteristic differentiates usability tests from focus groups, surveys, and beta tests. Focus groups gather information on users' opinions, preferences, and even self reports about performance, but usually don't extend to observing how they actually perform with the product. The same is true with surveys. Beta tests have been found to provide little useful information on usability. In general, they're "too little, too unsystematic, and much too late to be the primary test of usability."[1]
- Test facilitators analyze the data, diagnose the problems, and recommend changes to address the identified problems. Usability tests result in both quantitative and qualitative data presented with the test facilitators' observations and test participants' comments.

Although testing with real users and real tasks is the gold standard, many have realized that recruiting real users to iteratively test multiple design aspects is often difficult or expensive. Therefore discount methods—called *usability inspection methods*—have emerged based on rules of thumb and the evaluator's experience, skill, and knowledge.[2]

References

1. J. Dumas and J. Redish, *A Practical Guide to Usability Testing*, Ablex, 1994.
2. J. Nielsen and R.L. Mack, eds., *Usability Inspection Methods*, John Wiley & Sons, 1994.

July 2009 workshop in Washington, DC, brought together key international usable security researchers, the workshop identified three overarching challenges to advancing usability, security, and privacy research[16]:

- inconsistent terminology and definitions, including terms such as *usable security* or *privacy*;
- limited data access—the need for more and better empirical data; and
- scarceness of expertise and unfamiliarity with each other's work—many are working in the field but in distinct and separate disciplines that don't share information.

Researchers now present usable security papers at mainstream conferences in both security and HCI. Governments have initiated programs, and universities have begun to offer courses, some establishing focused research programs (see the "Usable Security Programs" sidebar).

Is Security Becoming More Usable?

Has research improved the quality of a user's experience interacting with security technologies? A simple but telling example—passwords—illustrates the tension between competing goals. Usability requirements suggest that passwords should be easy to remember, reused across multiple systems, and changed infrequently.[6] But security requirements suggest the opposite: longer passwords with seemingly random characters, numbers, and special characters are more secure; each system should have a unique password; and passwords should be changed frequently. Table 1 contrasts security and usability goals.

In a recent study of half a million Microsoft Windows Live Toolbar customers who opted to respond, the average user had 25 accounts that require passwords, and a typical user typed an average of eight passwords per day.[17] Moreover, the password policies about length and frequency of change often vary widely across these accounts, adding to the user's cognitive load; the result is a kind of "access amnesia"[18] and password interference.[19] These password examples also illustrate the problem of scale[20]: distinguishing usability in the small—using a single access mechanism for a single application—from usability in the large—handling many and varied access mechanisms at once.[21] Zurko and Simon suggested that, even when a single password is strong, the collection of almost all forms of deployed security using passwords is weak in terms of both usability and security.[5]

Moreover, brute-force attacks are no longer the preferred means of gaining passwords.[20,22] Instead, the human in the loop is the largest vulnerability; social engineering and phishing attacks are the primary vehicles for entry. According to *The Economist*, 90 percent of the 140 billion emails sent daily are spam. Of them, 16 percent are phishing attacks aimed at collecting passwords—an attack for which a complex password offers no defense.[22]

One challenge for security professionals is moving usability research results into practice. For example, password guidelines are readily available but aren't always implemented in an application's design. Like many quality attributes, both usability and security have been poor step-children during system development, often added to an application only at the end of the development process. Understanding that these attributes must be built as an integral part of a system's design, experts in both security and usability have developed methodologies to do just that. Interdisciplinary research or development teams—such as the Institute for Information Infrastructure Protection's Leveraging Human Behavior to Reduce Cyber Security Risk—are essential; security improvements are more likely to be realized only when experts in usability, security, and privacy work together collaboratively throughout product design, development, testing, and deployment.

Usable Security Programs

Recognizing the importance of usable security, many universities are creating special curricula and programs to educate students in its principles:

- The University of Arkansas at Little Rock created a center of excellence called Assure (Assurance, Security, and Software Usability, Research, and Education), which aims to improve the existing curricula, develop new ones, and support research activities that will increase the number and skills of information assurance professionals (http://technologize.ualr.edu/computerscience/assure).
- Carnegie Mellon University's CyLab Usable Privacy and Security Laboratory is a hub for researchers studying diverse aspects of understanding and improving privacy and security software and systems' usability. The lab uses "three high-level strategies to make secure systems more usable: building systems that 'just work' without involving humans in security-critical functions; making secure systems intuitive and easy to use; and teaching humans how to perform security-critical tasks" (http://cups.cs.cmu.edu).
- University College London's Human-Centred Systems Group works closely with the Computer Security Group to address usable security problems. In addition to biometrics, CCTV, and general computer security, the group examines issues in mobile systems, e-government, social networks, and intelligent interfaces (http://hornbeam.cs.ucl.ac.uk/hcs).
- The new research-led Indraprastha Institute of Information Technology, Delhi, has a security and privacy research program in which one of the stated research areas is security and usability (www.iiitd.edu.in/security/research.html).

Many governments have also recognized the need for usable security. The US has initiated several programs:

- The Comprehensive National Cybersecurity Initiative (CNCI) includes usable security research in Initiative 9, which defines and develops enduring "leap-ahead" technology, strategies, and programs (www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative).
- The US National Science Foundation's (NSF's) Trustworthy Computing program includes usability as a research area: "Of particular interest are proposals that address foundations of trustworthy computing (e.g., 'science of security' and privacy-preserving algorithms), privacy, and usability" (www.nsf.gov/funding/pgm_summ.jsp?pims_id=503326&org=CNS).
- The National Institute of Standards and Technology (NIST) established a research program in usable security currently focusing on passwords, password policies, and identity and biometrics, with the goal of providing usability data to improve security policy decisions (www.nist.gov/itl/usability.cfm).
- In July 2009, the National Academy of Science convened a workshop, sponsored by the NSF and NIST, to "identify promising research directions to advance usability, security, and privacy" (www.nap.edu/openbook.php?record_id=12998&page=R1).

The European Union's Security Research Call 4 included usable security opportunities as well as privacy and societal impacts of technologies (http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=322), and the UK funded the Privacy Value Networks project (http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/G002606/1).

Steps toward More Usable Security

The definition of usability, in concert with the psychological acceptability principle, provides hints for effective usability testing and research based on understanding users and their goals:

- Who are the users? Determining who the users are isn't a trivial task. Bill Curtis, Herb Krasner, and Neil Iscoe pointed out that "users" can include end users, system administrators, system developers, and even the people or organizations that pay for the system but don't actually use it.[23] Moreover, each type of user has (sometimes competing) goals for the system's security and privacy.
- How do we evaluate usability? As the world moves to include a profusion of independent devices, such as mobile phones and medical sensors, that are networked together in myriad ways, we must determine not only how to evaluate such a system's security but also how to evaluate its usability in the vast number of contexts in which it will be used.
- How do we model usable security? Psychological acceptability relies on mental images or models. Currently, we have well-accepted mental models for many computer constructs, such as a computer "file system" with

Table 1. Password characteristics.

Password characteristic	Security focus	Usability focus
Length	Longer	Shorter
Composition	Heterogeneous characters	Homogeneous characters
Uniqueness	Forbid reuse	Common passwords
Change frequency	Often	Seldom

files stored in "folders." We need similarly effective mental models for user perceptions of security, trust, and risk.

- How do we maintain good security as complexity grows? Matt Bishop noted that, "A fundamental precept of designing security mechanisms is that, as the mechanisms grow more complex, they become harder to configure, to manage, to maintain, and indeed even to implement correctly. Errors become more probable, thereby increasing the chances that mechanisms will be configured erroneously, mismanaged, maintained improperly, or implemented incorrectly."[24] Evidence of increasing complexity and decreasing security abounds. For example, according to the most recent Verizon data breach report, "loosely defined, error is a contributing factor in nearly all data breaches."[25] Thus, complexity has great potential to weaken not only usability but also security.

As Birge said, "usability is necessary to a secure system."[9] Usability and security complement one another. We need to make it easy for the user to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens anyway. This special issue moves us in that direction in several ways.

In "Bridging the Gap in Computer Security Warnings: A Mental Model Approach," Cristian Bravo-Lillo and his colleagues examine how novice and advanced users understand warnings to determine whether users' security expertise affects how they assess warnings. The authors show that understanding users' behaviors is critical to designing effective security solutions.

In "Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client," Kristin S. Fuglerud and Øystein Dale remind us that many identification and authentication methods aren't necessarily usable by users with disabilities. Yet, online services are vital to this population. The authors provide lessons learned from creating and performing user testing of an accessible, usable, and secure authentication mechanism.

The migration to electronic health records and the passage of the Health Information Technology for Economic and Clinical Health legislation spotlight the importance of usable security in health information technology. In "Usability Failures and Healthcare Data Hemorrhages," M. Eric Johnson and Nicholas D. Willey provide insight into the types of healthcare information being breached as well as the root causes.

When users forget passwords, systems must provide a secondary mechanism to reestablish access. In "When the Password Doesn't Work: Secondary Authentication for Websites," Robert W. Reeder and Stuart Schechter review popular secondary authentication mechanisms and provide a strategy for assembling an effective secondary authentication system.

We invite *IEEE Security & Privacy* readers to enjoy these articles. We hope that, whether performing research or designing secure systems, you ensure that usability is a nonnegotiable and welcome consideration. □

References

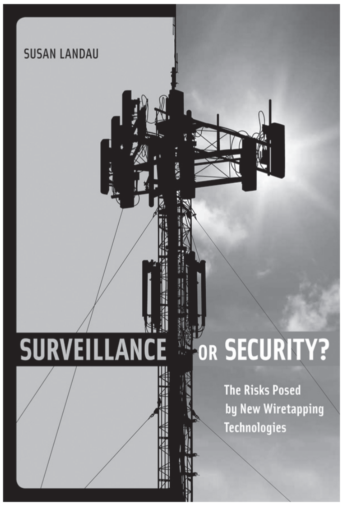
1. ISO 9241-11:1998, "Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)—Part 11: Guidance on Usability," Int'l Standards Org., 1998; www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=16883.
2. M. Theofanos and S. Furman, "Houston PD Handheld Finger Printing Device Project," NIST-IR, Nat'l Inst. Standards and Technology, Oct. 2010.
3. A. Adams and A. Blandford, "Bridging the Gap between Organizational and User Perspectives of Security in the Clinical Domain," *Int'l J. Human-Computer Studies*, vol. 63, nos. 1–2, 2005, pp. 175–202.
4. J.H. Saltzer and M.D. Schroeder, "The Protection of Information in Computer Systems," *Proc. IEEE*, vol. 63, no. 9, 1975, pp. 1278–1308.
5. M.E. Zurko and R.T. Simon, "User-Centered Security," *Workshop on New Security Paradigms*, ACM Press, 1996, pp. 27–33.
6. A. Adams and M.A. Sasse, "Users Are Not the Enemy," *Comm. ACM*, vol. 42, no. 12, 1999, pp. 41–46.
7. A. Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," Usenix Assoc., 1999, pp. 169–184.
8. L.F. Cranor and S. Garfinkel, eds., *Security and Usability: Designing Secure Systems that People Can Use*, O'Reilly and Assoc., 2005.
9. C. Birge, "Enhancing Research into Usable Privacy and Security," *24th ACM Int'l Conf. Design of Communication* (SIGDOC 09), ACM Press, 2009, pp. 221–225.

10. L.J. Camp, "Mental Models of Privacy and Security," *IEEE Technology and Society*, vol. 28, no. 3, 2009, pp. 37–46.
11. P. Dourish, J. Delgado de la Flor, and M. Joseph, "Security as a Practical Problem: Some Preliminary Observations of Everyday Mental Models," *CHI 2003 Workshop on Human-Computer Interaction and Security Systems*, 2003; www.andrewpatrick.ca/CHI2003/HCISEC/hcisec-workshop-dourish.pdf.
12. S. Brostoff and M.A. Sasse, "Safe and Sound: A Safety-Critical Design Approach to Security," *Proc. New Security Paradigms Workshop*, ACM Press, 2001, pp. 41–50.
13. L.F. Cranor, "A Framework for Reasoning about the Human in the Loop," *Proc. Usability, Psychology, and Security* (UPSEC 08), Usenix Assoc., 2008.
14. L. Hoffman, K. Lawson-Jenkins, and J. Blum, "Trust Beyond Security: An Expanded Trust Model," *Comm. ACM*, vol. 49, no. 7, 2006, pp. 95–101.
15. M.E. Johnson and E. Goetz, "Embedding Information Security into the Organization," *IEEE Security & Privacy*, vol. 5, no. 3, 2007, pp. 16–24.
16. Nat'l Research Council, "Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop," Nat'l Academies Press, 2010.
17. D. Florencio and C. Herley, "A Large-Scale Study of Web Password Habits," *Proc. 16th Int'l Conf. World Wide Web* (WWW 07), ACM Press, 2007, pp. 657–666.
18. J. Zhang et al., "Improving Multiple-Password Recall: An Empirical Study," *European J. Information Systems*, vol. 18, no. 2, 2009, pp. 165–176.
19. A. Adams, M.A. Sasse, and P. Lunt, "Making Passwords Secure and Usable," *Proc. HCI on People and Computers*, Springer-Verlag, 1997; http://hornbeam.cs.ucl.ac.uk/hcs/people/documents/Angela%20Publications/1997/HCI%201997.pdf.
20. D. Norman, "When Security Gets in the Way," *Interactions*, vol. 16, no. 6, 2009, pp. 60–63.
21. D. Hix, H.R. Hartson, and Jakob Nielsen, "A Taxonomy for Developing High Impact Formative Usability Evaluation Methods," *SIGCHI Bulletin*, vol. 26, no. 4, 1994, pp. 20–22.
22. "War in the Fifth Domain," *The Economist*, 3 July 2010; www.economist.com/node/16478792?story_id=16478792.
23. B. Curtis, H. Krasner, and N. Iscoe, "A Field Study of the Software Design Process for Large Systems," *Comm. ACM*, vol. 31, no. 11, 1988, pp. 1268–1287.
24. M. Bishop, "Psychological Acceptability Revisited," *Security and Usability: Designing Secure Systems that People Can Use*, O'Reilly and Assoc., 2005, pp. 1–11.
25. Verizon Business RISK Team, 2009 Data Breach Investigations Report, Verizon business, 2009; www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

***Mary Frances Theofanos** is a computer scientist at the National Institute of Standards and Technology's Visualization and Usability Group. Contact her at mary.theofanos@nist.gov.*

***Shari Lawrence Pfleeger** is director of research at Dartmouth College's Institute for Information Infrastructure Protection. Contact her at shari.l.pfleeger@dartmouth.edu.*

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*



SUSAN LANDAU
SURVEILLANCE OR SECURITY?
The Risks Posed by New Wiretapping Technologies