Usability Meets Access Control: Challenges and Research Opportunities

Konstantin Beznosov (moderator)
University of British Columbia
beznosov@ece.ubc.ca

Philip Inglesant
University College London
p.inglesant@cs.ucl.ac.uk

Jorge Lobo
IBM Research
jlobo@us.ibm.com

Rob Reeder
Microsoft Research
roreeder@microsoft.com

Mary Ellen Zurko
IBM Software Group
mzurko@us.ibm.com

ABSTRACT

This panel discusses specific challenges in the usability of access control technologies and new opportunities for research. The questions vary from "Why nobody, even experts, uses access control lists (ACLs)?" to "Shall access controls (and corresponding languages) be totally embedded and invisible and never, ever seen by the users?" to "What should be the user-study methodology for access control systems?".

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—*Access controls*; H.1.2 [**Models and Principles**]: User/Machine Systems—*Human factors*; H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*User-centered design*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Human Factors, Security, Design, Experimentation, Measurement

Keywords

usable security, HCISec, HCI, access control, security

1. PANEL DESCRIPTION

The recent resurgence of academic and industrial interest in usable security has led to an active re-examination of usability properties of wide range of security technologies, from the use of encryption in e-mail [12], to password managers [4], to authentication of users to web sites [3] and vice versa [11], anti-phishing approaches [5], CAPTCHAS [13], to name just few. The usability of access controls has so far received limited attention in both the HCISec and access control communities. At the same time, more and more new types of applications that require controlled sharing of resources or discrimination of information appear: social networks and other Web 2.0 applications, P2P and other ad hoc applications, Grid or "cloud" computing. This panel discusses specific challenges in the usability of access control technologies and new opportunities for research.

SACMAT'09, June 3–5, 2009, Stresa, Italy.
ACM 978-1-60558-537-6/09/06.

There are numerous practical and research challenges and questions, when it comes to the intersection of usability and access control. Here, we list just few.

Let us start with something close to home for everybody—access controls on the files accessed by users on their desktops and laptops. Almost nobody, even experts, uses access control lists (ACLs). Why? Reeder et al. [7, 10] discovered that end users cannot understand the implications of changes in ACLs when out-of-the-box user interface for managing ACLs is used.

Many agree that the needs of different audiences of access controls vary. How should the usability goals or approaches to improving usability for access controls be different for novices (e.g., average user from the street), intermediate (i.e., those who know what they are doing), power (e.g., IT professionals), and expert (e.g., system admins) users? Zooming in on novice users, what access controls, if any, should be exposed to them, under what circumstances? If system developers and owners must provide controls to the inexperienced, how can such controls be usable and secure at the same time? Raja et. al. [8] recently showed that the attempt by the designers of the interfaces for the Microsoft Vista Personal Firewall to make the firewall controls both usable and secure spectacularly failed, resulting in an interface that prevents end-users from developing adequate mental models of the controls.

Even for IT security practitioners and other experts, it turns out, access control and other security tasks are secondary, performed irregularly, and without necessarily proper training [1]. It is not surprising that even experts can make human errors, but failures arising from "human error" should be seen as design faults at a system level, rather than blamed on individuals [9]. What can be done to detect or prevent errors? Shall the researchers and developers work towards making access controls (and corresponding languages) more usable, or make access controls (and corresponding languages) totally embedded and invisible and never, ever let the user see them? If the former is the case, then should the focus be on improving visualization of controls or improving languages for representing them textually [6]?

New applications with new access control models pose new usability challenges. The management of ad hoc communities and coalitions, for example, diffuses the role of the security administrator, and access control decisions and policies authoring are moved closer to non-expert users. Grid computing, and other distributed computing, splits access control across administrative domains, making it hard to evaluate the effective permissions which a user or process has on an object. Information sharing among business partners of different trust levels also requires new access control models. Role-based access control and its variants are con-

ceptually hard for non-specialists to understand [2]. These new applications increase the relevance of usable controls.

New access control designs should take usability into account. How should the tension between low level enforcement (which is architecturally good, the closer to the object the better) and a higher level controls for users should be resolved?

When it comes to evaluating new access control systems, how are they evaluated today, and how could researchers and developers incorporate more usability testing into their evaluation? What should be the user-study methodology for access control systems? In particular, benefits of lab vs. field studies, and what each can teach us about the usability of access control systems?

2. REFERENCES

[1] BOTTA, D., WERLINGER, R., GAGNÉ, A., BEZNOSOV, K., IVERSON, L., FELS, S., AND FISHER, B. Towards understanding IT security professionals and their tools. In *Proc. of Symp. On Usable Privacy and Security (SOUPS)* (Pittsburgh, PA, July 18-20 2007), pp. 100–111.

[2] BROSTOFF, S., SASSE, M. A., CHADWICK, D., CUNNINGHAM, J., MBANASO, U., AND OTENKO, S. R-What?: Development of a role-based access control policy-writing tool for e-Scientists. *Software Practice and Experience 35*, 9 (2005), 835–856.

[3] CHIASSON, S., BIDDLE, R., AND VAN OORSCHOT, P. C. A second look at the usability of click-based graphical passwords. In *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security* (New York, NY, USA, 2007), ACM, pp. 1–12.

[4] CHIASSON, S., VAN OORSCHOT, P. C., AND BIDDLE, R. A usability study and critique of two password managers. In *Proceedings of 15th USENIX UNIX Security Symposium* (Vancouver, Canada, August 2-4 2006), USENIX, pp. 1–16.

[5] DHAMIJA, R., TYGAR, J. D., AND HEARST, M. Why phishing works. In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems* (New York, NY, USA, 2006), ACM, pp. 581–590.

[6] INGLESANT, P., SASSE, M. A., CHADWICK, D., AND SHI, L. L. Expressions of expertness: the virtuous circle of natural language for access control policy specification. In *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security* (New York, NY, USA, 2008), ACM, pp. 77–88.

[7] MAXION, R. A., AND REEDER, R. W. Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies 63*, 1-2 (2005), 25–50.

[8] RAJA, F., HAWKEY, K., AND BEZNOSOV, K. Towards improving mental models of personal firewall users. In *CHI '09 extended abstracts on Human factors in computing systems* (Boston, MA, USA, April 2009), ACM, p. 6.

[9] REASON, J. *Human error: causes and consequences*. Cambridge University Press, Cambridge, UK, 1990.

[10] REEDER, R. W., BAUER, L., CRANOR, L. F., REITER, M. K., BACON, K., HOW, K., AND STRONG, H. Expandable grids for visualizing and authoring computer security policies. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems* (New York, NY, USA, 2008), ACM, pp. 1473–1482.

[11] SCHECHTER, S. E., DHAMIJA, R., OZMENT, A., AND FISCHER, I. The emperor's new security indicators. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy* (Washington, DC, USA, 2007), IEEE Computer Society, pp. 51–65.

[12] WHITTEN, A., AND TYGAR, J. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *The 9th USENIX Security Symposium* (1999), pp. 169–183.

[13] YAN, J., AND EL AHMAD, A. S. Usability of CAPTCHAs or usability issues in CAPTCHA design. In *Proceedings of the 4th symposium on Usable privacy and security* (New York, NY, USA, 2008), ACM, pp. 44–52.