National Research
Council Canada

Conseil national
de recherches Canada

Institute for
Information Technology

Institut de technologie
de l'information

NRC·CNRC

HCI and Security Systems *

Patrick, A.S., Long, A.C., and Flinn, S.
April 2003

Canada

HCI and Security Systems

Andrew S. Patrick
National Research Council of
Canada
1200 Montreal Rd.
Ottawa, ON K1A 0R6
CANADA
+1 613 991 3374
Andrew.Patrick@nrc-cnrc.gc.ca

A Chris Long
Parallel Data Laboratory
ECE Department
Carnegie Mellon University
Pittsburgh, PA 15213
+1 412 268 6658
chrislong@acm.org

Scott Flinn
National Research Council of
Canada
46 Dineen Drive
Fredericton, NB E3B 9W4
CANADA
+1 506 451 2567
Scott.Flinn@nrc-cnrc.gc.ca

THE TOPIC: HCI AND SECURITY SYSTEMS

The human factor is often described as the weakest part of a security system and users are often described as the weakest link in the security chain. This workshop will seek to understand the roles and demands placed on users of security systems, and explore design solutions that can assist in making security systems usable and effective. In addition to examining end-users, this workshop will also examine the issues faced by security system developers and operators. The primary motivation for the workshop is that previous research on HCI and Security (HCISEC) has been scattered in different conferences and journals, and information sharing has been difficult. The goal of the workshop is to build a more cohesive and active HCISEC community of researchers and practitioners. This will be done by building a network of interested people, sharing research activities and results, discussing high priority areas for research and development, and exploring opportunities for collaboration.

Scope of the Topic

Security is a large topic so there are many areas where HCI is important. Three obvious areas of interest are authentication (passwords, biometrics, etc.), security operations (intrusion detection, vigilance, policies and practices, etc.), and developing secure systems (developing for security, understanding users, installation and operation support, etc.). Some previous research has been done in each of these areas, but there are many open issues.

Authentication

The most common authentication procedure is for the user to provide a user ID and a shared secret password that they have chosen. Users have been described as the weakest link in security systems because of their behavior when using user ID/password systems. Many studies have shown, for example, that users tend to choose short and/or guessable passwords [1]. Another very common problem is that users forget their passwords. One estimate is that 50

percent of all help desk calls are password-related, and most of these are because a password has been forgotten (Murrer, cited in [3]).

Probably because of the difficulty remembering, users also have a tendency to write their passwords down. In one study, 50 percent of the users surveyed admitted to writing down their passwords, and the other 50 percent did not answer the question [1]. Other notorious password behaviors are: (1) users share their passwords with their friends and colleagues, (2) users fail to change their passwords on a regular basis even when instructed to, (3) users may choose the same password (or closely related passwords) for multiple systems, and (4) users are often willing to tell their passwords to strangers who asked for them. (Asking was the most common technique used by Kevin Mitnick in his infamous security exploits [10].)

There are solutions to the security issues caused by the behavior of users, but they are not commonly used (see [1] for an excellent review). To alleviate the problem of a remembering multiple passwords, for example, organizations can support synchronized passwords across systems. A related solution is a single-sign-on system where users are authenticated once and then they are allowed to access multiple systems. Another technique is to reduce the memory load placed on users. It is well known that cued recall, where users are prompted for the information they must remember, is more accurate than free recall [4]. This can be used in security systems by requiring personal associates for passwords, such as "dear - god, "black - white", "spring - garden". Performance can also be improved by not asking users to recall at all, but rather to recognize certain material. Recognition is much easier and more accurate than recall [8]. There is some evidence, for example, that Passfaces are easier to remember than passwords, especially after long intervals with no use [3].

There has been much interest recently in using biometrics, such as fingerprints or voice patterns, for user identification [5] [9], but these systems can have their own problems. Biometrics can be hard to forge but easy to steal [11]. For example, fingerprints can be lifted from objects and used when the owner is not present. Also, the master file of biometric templates can be compromised so that an intruder

could replace a legitimate thumbprint file with their own. If the integrity of a biometric has been compromised (e.g., a thumbprint file has been widely distributed) it makes the biometric system unusable forever. Also, a biometric security network can be compromised by packet sniffing and insertion, where an illegitimate biometrics file is inserted in place of a legitimate one that is being transmitted.

Biometrics systems can be based on physical characteristics, such as fingerprints, or behavioral characteristics, such as voice patterns [7] or typing styles [6]. The performance of behavioral biometrics (in terms of correction rejections and false acceptances) can be affected by circumstances such as health, stress, and other factors. Also, at least one behavioral biometric system, the one based on typing styles, appears to be less acceptable to users, who are afraid that their work performance may be monitored in some way [3].

Security Operations
Human factors problems are not restricted to end-users. System operators are also human and therefore have limitations and the potential to make mistakes. Perhaps the most serious behavioral problem of system operators is poor implementation of the system. This may be due to failure to understand the security technology, and/or failure to implement all of the necessary features. In one study, failures during installation and feature selection were the most common sources of security problems in the banking and government sectors [2].

System operators of large installations also face the problem encountered in other domains of monitoring and controlling large complex systems. Tools such as distributed firewalls promise to improve security, but configuring, monitoring, and controlling these systems is difficult. Operators would benefit from better interfaces for these systems.

Another problem seen with system operators is poor operating procedures. This includes not keeping the system up-to-date, not responding to security notices, badly managing their own passwords, cost-cutting, and simple laziness. An interesting research area might be an analysis of factors that contribute to inappropriate system operator behaviors. Finally, operator fraud can be a serious problem in situations where security compromises can lead to financial gain [2].

Developing Secure Systems
Developers of secure systems face a serious challenge. If a security system is not user-friendly, developers face failure in the marketplace, or users that circumvent or ignore the security features. Although it often appears that security and usability are contrary product attributes, it need not be that way. For example, Yee [12] has recently laid out ten

HCI design principles that can be used to improve the usability of security systems.

In addition, tools are emerging to assist developers when checking for security vulnerabilities. Often the results and implications of the code scans can be complex and difficult to interpret. The field of HCI can likely contribute to improvement of security-enhancing development tools.

Another development issue is design philosophy. Especially in the realm of Web applications and services, design typically proceeds from the bottom up, driven by well established Web application design patterns and the constraints imposed by underlying technologies, such as public key cryptography. However, it is often difficult to retrofit these design patterns with acceptable security architectures. An alternative approach begins with a user-centered analysis of workflow and information flow (with emphasis on the boundaries), followed by a design approach that is driven from the top, taking care to use well established security models to enforce access control and data separation where appropriate.

REFERENCES
1. Adams, A., & Sasse, M.A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM, 42*, 41–46.
2. Anderson, R. (1994). Why cryptosystems fail. *Communications of the ACM, 37*, 32–40.
3. Brostoff, S., & Sasse, M.A. (2000). Are Passfaces more usable than passwords? A field trial investigation. *In Proceedings of HCI 2000*, Sept. 5–8, Sunderland, U.K., 405-424 Springer.
4. Crowder, R.G. (1976). *Principles of learning and memory*. Hillsdale, NJ: Lawrence Elrbaum Associates.
5. Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*, 91–98.
6. Joyce, R., & Gupta, G. (1990). Identity authentication based on keystroke latencies. *Communications of the ACM, 33*, 168–176.
7. Markowitz, J.A., (2000). Voice biometrics. *Communications of the ACM, 43*, 66–73.
8. Preece, J. (1994). *Human-computer interaction*. NY: Addison-Wesley.
9. Rejman-Greene, M. (2001). Biometrics—Real identities for a virtual world. *BT Technology Journal, 19*, 115–121.
10. Sasse, M.A., Brostoff, S., & Weirich, D. (2001). Transformng the 'weakest link': A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*, 122–131.
11. Schneier, B. (1999). Biometrics: Uses and abuses. *Communications of the ACM*, 42 (8), 58.
12. Yee, K.-P. (2002). User Interaction Design for Secure Systems. http://zesty.ca/sid/uidss-may-28.pdf