Human–Computer Interaction and Security

Kai Richter
Computer Graphics Centre (ZGDV), Germany

Volker Roth
OGM Laboratory LLC, USA

INTRODUCTION

Historically, computer security has its roots in the military domain with its hierarchical structures and clear and normative rules that are expected to be obeyed (Adams & Sasse, 1999). The technical expertise necessary to administer most security tools stems back to the time where security was the matter of trained system administrators and expert users. A considerable amount of money and expertise is invested by companies and institutions to set up and maintain powerful security infrastructures. However, in many cases, it is the user's behavior that enables security breaches rather than shortcomings of the technology. This has led to the notion of the user as the weakest link in the chain (Schneier, 2000), implying that the user was to blame instead of technology. The engineer's attitude toward the fallible human and the ignorance of the fact that technology's primary goal was to serve human turned out to be hard to overcome (Sasse, Brostoff, & Weirich, 2001).

BACKGROUND

With the spreading of online work and networked collaboration, the economic damage caused by security-related problems has increased considerably (Sacha, Brostoff, & Sasse, 2000). Also, the increasing application of personal computers, personal networks, and mobile devices with their support of individual security configuration can be seen as one reason for the increasing problems with security (e.g., virus attacks from personal notebooks, leaks in the network due to personal wireless LANs, etc.) (Kent, 1997). During the past decade, the security research community has begun to acknowledge the importance of the human factor and has started to take research on human-computer interaction into consideration. The attitude has changed from blaming the user as a source of error toward a more user-centered approach trying to persuade and convince the user that security is worth the effort (Ackerman, Cranor, & Reagle, 1999; Adams & Sasse, 1999; Markotten, 2002; Smetters & Grinter, 2002; Whitten & Tygar, 1999; Yee, 2002).

In the following section, current research results concerning the implications of user attitude and compliance toward security systems are introduced and discussed. In the subsequent three sections, security-related issues from the main application areas, such as authentication, email security, and system security, are discussed. Before the concluding remarks, an outlook on future challenges in the security of distributed context-aware computing environments is given.

USER ATTITUDE

The security of a system cannot be determined only by its technical aspects but also by the attitude of the users of such a system. Dourish et al. (2003) distinguish between theoretical security (e.g., what is technologically possible) and effective security (e.g., what is practically achievable). Theoretical security to their terms can be considered as the upper bound of effective security. In order to improve effective security, the everyday usage of security has to be improved. In two field studies, Weirich and Sasse (2001) and Dourish et al. (2003) explored users' attitudes to security in working practice. The findings of both studies can be summarized under the following categories: perception of security, perception of threat, attitude toward security-related issues, and the social context of security.

Perception of security frequently is very inaccurate. Security mechanisms often are perceived as holistic tools that provide protection against threats, without any detailed knowledge about the actual scope. Therefore, specialized tools often are considered as insufficient, as they do not offer general protection. On the other hand, people might feel protected by a tool that does not address the relevant issue and thus remain unprotected (e.g., firewall protects against e-mail virus).

Perception of threats also reveals clear misconceptions. None of the users asked considered themselves as really endangered by attacks. As potential victims, other persons in their organization or other organizations were identified, such as leading personnel, people with important information, or high-profile institutions. Only a few of them realized the fact that they, even though not being the target, could be used as a stepping stone for an attack. The general attitude was that no one could do anything with the information on my computer or with my e-mails.

Potential attackers mainly were expected to be hackers or computer kids, with no explicit malevolent intentions but rather seeking fun. Notorious and disturbing but not really dangerous offenders, such as vandals, spammers, and marketers, were perceived as a frequent threat, while on the other hand, substantially dangerous attackers such as criminals were expected mainly in the context of online banking.

The attitude toward security technology was rather reserved. Generally, several studies reported three major types of attitudes toward security: privacy fundamentalists, privacy pragmatists, and privacy unconcerned (Ackerman et al., 1999). Users' experiences played a considerable role in their attitude, as experienced users more often considered security as a hindrance and tried to circumvent it in a pragmatic fashion in order to reach their work objectives. Weirich and Sasse (2001) report that none of the users absolutely obeyed the prescribed rules, but all were convinced that they would do the best they could for security.

Additionally, users' individual practices are often in disagreement with security technology. People use legal statements in e-mail footers or cryptic e-mails, not giving explicit information but using contextual cues instead. In conjunction with such subsidiary methods and the fact that people often seem to switch to the telephone when talking about important things (Grinter & Palen, 2002) indicates the poor perception users have of security technology.

The feeling of futility was reported with respect to the need for constantly upgrading security mechanisms in a rather evolutionary struggle (i.e., if somebody really wants to break in, he or she will). As a result, personal accountability was not too high, as users believed that in a situation where someone misused his or her account, personal credibility would weigh more than computer-generated evidence, in spite of the fact that the fallibility of passwords is generally agreed.

The social context has been reported to play an important role in day-by-day security, as users are not permanently vigilant and aware of possible threats but rather considered with getting their work done. Therefore, it is no wonder that users try to delegate responsibility to technical systems (encryption, firewalls, etc.), colleagues and friends (the friend as expert), an organization (they know what they do), or institutions (the bank cares for secure transfers). Most people have a strong belief in the security of their company's infrastructure. Delegation brings security out of the focus of the user and results in security unawareness, as security is not a part of the working procedure anymore.

Whenever no clear guidelines are available, people often base their practice on the judgments of others, making the system vulnerable to social engineering methods (Mitnick, Simon, & Wozniak, 2002). In some cases, collaboration appears to make it necessary or socially opportune to disclose one's password to others for practical reasons, technical reasons, or as a consequence of social behavior, since sharing a secret can be interpreted as a sign of trust. Such sharing is a significant problem, as it is used in social engineering in order to obtain passwords and to gain access to systems.

Dourish et al. (2003) came to the conclusion that "where security research has typically focused on theoretical and technical capabilities and opportunities, for end users carrying out their work on computer systems, the problems are more prosaic" (p. 12). The authors make the following recommendations for the improvement of security mechanisms in the system and in the organizational context: