# Usable Security

**Andrea Atzeni**
*Politecnico di Torino, Italy*

**Shamal Faily**
*Bournemouth University, UK*

**Ruggero Galloni**
*Square Reply S.r.l., Italy*

## INTRODUCTION

Recent decades have been characterized by the growth of information technologies in the private and public sectors. The positive impact that ICT has on job performance, as well as the expansion and creation of business opportunities for companies, count as the main drivers for this growth. This growth led to the proliferation of distributed applications and physical devices, and the diffusion of technologies that facilitate social participation and social interaction. All these applications, devices and interactions may contain important information, or give access to sensitive data, putting them at risk.

The rapid diffusion of technology has led to the reduction of active security monitoring, as well as the lack of technically competent people in control of applications and devices. Moreover, the increment in social interaction increases the damage other people can directly or indirectly cause.

Traditionally, security is only considered as strong as its weakest link, and people were considered as the weak links (Schneier, 2003). This thinking triggers a vicious circle. (Adam & Sasse, 1999) stated that users are informed as little as possible on security mechanisms took by IT departments, precisely because they are seen as inherently untrustworthy. Their work has shown that users were not sufficiently aware of security issues and tend to build their own (often inaccurate) models of possible security threats. Users have a low perception of threats because they lack the necessary information to understand their importance. According to (Sasse & al., 2001) blaming users for a security breach is like blaming human error rather than bad design. Security has, therefore, a human dimension that must be neither ignored nor neglected. The increase in the number of breaches may be attributed to designers who fail to sufficiently consider the human factor in their design techniques. Thus, to undo the Gordian knot of security, we must provide a human dimension to security.

## BACKGROUND

Human-Computer Interaction (HCI) is a field concerned with the interaction between people and technology, and how this supports humans in completing tasks to achieve one of more specific goals. Traditionally, it has been involved in analyzing and improving usability.

HCI has been an active area of research since the 1980s. It has focused on improving the design of user interfaces, and helping users transforming their goals into productive actions for the computers. Improving user interfaces and usability is important because poorly designed interfaces increase the potential for human error. In particular, human behavior is largely goal-driven, therefore the execution of activities which help the users to achieve their goals is the main key to create a

DOI: 10.4018/978-1-5225-2255-3.ch433

usable system. So, when a user "engages with a complex system of rules that change as the problem changes" (e.g. an interface does not present information clearly and coherently with a user mental model), it leads to "Cognitive Friction" (Cooper, 2004).

The "Cognitive Friction" is a by-product of the information age, and it is more evident in all the computing devices lacking a natural cause-effect relation between user input and device output, e.g. when similar inputs result in different outputs.

When a person is dealing with the cognitive friction, ancestral mechanisms of the human being come into play. As result, in this case, users cannot be modeled as purely rational beings. Thus, to understand users' behavior, and to appreciate how systems can be made usable, we need to consider the following factors:

- Users are driven by goals. People are naturally prone to pursuing goals. In achieving this, according to Krug "every question mark adds to our cognitive workload, distracting our attention from the task at hand" (Krug, 2005). This, according to Norman (Norman, 2002), creates usability issues, because it introduces the cognitive friction into play and leads users to make mistakes, which sometimes can also result into security flaws;
- Users do not read the instructions. Users proceed by trial and are not interested in reading manuals, instructions or documentation. For most of the users, it is not important to know how to do something, until the moment in which it is not necessary to use it (Krug, 2005);
- Users follow the path of least resistance. Several studies in the field of HCI have shown how users, in their task to accomplish a goal, tend to seek the path requiring them less effort (e.g. (Norman, 2002)). Once they find the first reasonable option allowing them to perform the desired action, it becomes irrelevant to them if it is not the most efficient and safe option. Furthermore, users have no incentive to improve. When users "find something that works - no matter how badly – they tend not to look for a better way" (Krug, 2005). Some operations can be inconvenient from the point of view of performance, others, in the long run, can cause damage to the system: users may be unaware of it until problems show up for the first time.

While many research studies in HCI has been focused in defining what usability is and, consequently, intervene in improving user interfaces, several studies have shown that the "ease of use" cannot be limited to those aspects alone (Whitten & Tygar, 1999) (Balfanz & al., 2004).

To increase the acceptance of the security mechanisms, conventional wisdom suggests it is sufficient to make them easier through a more usable user interface. In practice, however, it is not enough to provide a proper user interface, even in the case it is supported by specific configuration guidelines. This is what Whitten and Tygar argue, in their study "Why Johnny cannot encrypt" (Whitten & Tygar, 1999), which is a seminar paper in the usable security literature. This study focuses on analyzing data and email encryption of the security software Pretty Good Privacy 5.0 (PGP). They showed that user errors have not decreased, despite years of improvements to the graphical interface. This has led to additional studies looking beyond the interfaces.

This field of study, which deals with analyzing the usability issues related to security, is called HCI-Sec and was founded in 2000 by Whitten as a mailing list on Yahoo! Groups. It has been said that HCI-Sec "only rarely received significant attention as a primary subject for study" (Balfanz & al., 2004), this despite the fact that "usability remains one of the most pressing and challenging problems for computer security" (Whitten & Tygar, 1999).

Although HCI-Sec has only recently gained momentum, initial studies have their roots in 1975,

## Related Content