Chapter 12

Information Attacks and Defenses on the Social Web

Agostino Poggi
University of Parma, Italy

Michele Tomaiuolo
University of Parma, Italy

ABSTRACT

Social web sites are used daily by many millions of users. They have attracted users with very weak interest in technology, including absolute neophytes of computers in general. Common users of social web sites often have a carefree attitude in sharing information. Moreover, some system operators offer sub-par security measures, which are not adequate for the high value of the published information. For all these reasons, online social networks suffer more and more attacks by sophisticated crackers and scammers. To make things worse, the information gathered from social web sites can trigger attacks to even more sensible targets. This work reviews some typical social attacks that are conducted on social networking systems, describing real-world examples of such violations and analyzing in particular the weakness of password mechanisms. It then presents some solutions that could improve the overall security of the systems.

INTRODUCTION

Nowadays, millions of people of any age and gender regularly access Online Social Networks (OSNs) and spend most of their online time social networking. In fact, if we have to chose among the innovations of the past decade just a single phenomenon because of its outstanding social impact, that would be the diffusion of online social networks. While some social networking services were already active in the nineties, the capillary diffusion and the sheer number of people involved transformed online social networking in an unprecedented revolution only recently.

Social web sites have attracted also users with very weak interest in technology, including people that before the social networking revolution were not even regular users of other popular Internet services and computers in general (Stroud, 2008). The phenomenon is so widespread that many people started
using social networking systems to ask questions to people instead of querying search engines and in place of regular email. Moreover, some of the largest social networking sites constitute a separate and closed network (Sabbag, 2011). After the huge success of the early social networking systems, many other players came in the social networking market and nowadays hundreds of different social networking systems exist.

According to Boyd and Ellison (2008), teenagers have a clear understanding of privacy related issues; however, the same does not apply to some adults that: (i) did not even use email and other basic Internet services before the social networking revolution (Stroud, 2008) and (ii) not only have limited computer-related technical skills, but they also lack risk consciousness about privacy issues. Moreover, many people are becoming uncomfortable with the presence of their employers in the same social networking systems, because some personal data may leak in their corporate environment due to privacy configuration errors (Skeels & Grudin, 2009).

Unfortunately, online social networks are becoming an interesting target for crackers and scammers alike. In fact, many factors concur to attract malicious actions: (i) the users’ carefree attitude in sharing information, (ii) the often sub-par security measures from the part of the system operators, and (iii) the high value of the published information. In particular, the information available through social media can be used to trigger attacks to even more sensible targets. Various forms of social engineering inside the system, including sophisticated and long-term attacks, may be facilitated by the general sense of sociability shared by users, which per se is an intrinsic objective of social media. However, while the only lasting solution to privacy and security issues would be increasing the users’ awareness, much can and shall be done at the system level in order to protect the data with cryptography and to decrease the impact of wrong choices and mistakes on the user’s part.

SECURITY THREATS ASSOCIATED WITH SOCIAL MEDIA

Nowadays, online social networks involve people from the entire world, of any age and with any kind of education. They also helped to increase computer usage among categories that previously showed little interest for it (Angiani et al., 2016; Franchi, Poggi & Tomaiuolo, 2016; Stroud, 2008). The users of information systems have various types of security requirements, including confidentiality, integrity, accountability, availability and anonymity. The same security requirements can be applied to social networking platforms, as well.

Unfortunately, while most users are aware that their profile and the information they publish is essentially public, they usually strengthen their privacy settings only after problems arise and tend to overlook the actual impact of the information they disclose (Stroud, 2008). Apparently, harmless information can be exploited, and the more information the attacker has, the more severe and sophisticated the attack can be. For example, name, location and age can be used to connect a profile to a real-world identity for more than half of the residents in the USA (Irani et al., 2011).

In fact, social networking platforms are susceptible to different types of attacks, targeting different components, conducted from different domains, using different techniques. For better analyzing these attacks, it is useful to identify the main components of a generic social networking platform, corresponding to different functional aspects of those systems. Attackers can target each of the different components, or they can target different levels, possibly with roughly the same logic. We identify four main components: