Information and Password Attacks on Social Networks: An Argument for Cryptography

Enrico Franchi, Department of Information Engineering, University of Parma, Parma, Italy
Agostino Poggi, Department of Information Engineering, University of Parma, Parma, Italy
Michele Tomaiuolo, Department of Information Engineering, University of Parma, Parma, Italy

ABSTRACT

Online social networks have changed the way people interact, allowing them to stay in touch with their acquaintances, reconnect with old friends, and establish new relationships with other people based on hobbies, interests, and friendship circles. Unfortunately, the regrettable concurrence of the users’ carefree attitude in sharing information, the often sub-par security measures from the part of the system operators and, eventually, the high value of the published information make online social networks an interesting target for crackers and scammers alike. The information contained can be used to trigger attacks to even more sensible targets and the ultimate goal of sociability shared by the users allows sophisticated forms of social engineering inside the system. This work reviews some typical social attacks that are conducted on social networking systems, carrying real-world examples of such violations and analysing in particular the weakness of password mechanisms. It then presents some solutions that could improve the overall security of the systems.

Keywords: Cryptography, Information Security, Password Cracking, Social Engineering, Social Networks

1. INTRODUCTION

If we have to choose 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. Online social networks have already modified the way people interact. They allow users to reconnect with old friends, or to establish new connections with unknown people. In general, users are facilitated in maintaining and developing the relationships with their acquaintances, on the basis of common activities, interests, and contacts.
From a technological perspective, online social networks are mostly based on sets of web-based services that allow people to present themselves through a profile, to establish connections with other users in the system, and to publish resources. Moreover, these systems use common interests and the natural transitivity of some human relationships to suggest new contacts with whom to establish a connection. Although some of these aspects already appeared in other systems, online social networks represent an unprecedented cultural phenomenon. It is mainly characterised by the unceasing flow of information that users publish in such systems, and their relentless strive to increase the number of their virtual friends and acquaintances.

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.

This work reviews some typical social attacks that are conducted on social networking systems, carrying real-world examples of such violations and analysing in particular the weakness of password mechanisms. It then presents some solutions that could improve the overall security of the systems.

2. 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 (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 analysing these attacks, it is useful to identify the main abstract 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:

1. **The Social Networking Component**: It manages and protects access to the users’ personal profiles and the social relationships among users.
2. **The Content Management Component**: It manages and protects access to all user generated content, including personal
Development of an Information Kiosk for a Large Transport Company: Lessons Learned
Pieter Blignaut and Iann Cruywagen (2005). *Journal of Cases on Information Technology* (pp. 27-45).
www.igi-global.com/article/development-information-kiosk-large-transport/3160?camid=4v1a