Chapter 10

Security and Privacy of Online Social Network Applications

Willem De Groef
iMinds–DistriNet, KU Leuven, Belgium

Dominique Devriese
iMinds–DistriNet, KU Leuven, Belgium

Tom Reynaert
iMinds–DistriNet, KU Leuven, Belgium

Frank Piessens
iMinds–DistriNet, KU Leuven, Belgium

ABSTRACT
An important recent innovation on social networking sites is the support for plugging in third-party social applications. Together with the ever-growing number of social network users, social applications come with privacy and security risks for those users. While basic mechanisms for isolating applications are well understood, these mechanisms fall short for social-enabled applications. It is an interesting challenge to design and develop application platforms for social networks that enable the necessary functionality of social applications without compromising both users’ security and privacy. This chapter will identify and discuss the current security and privacy problems related to social applications and their platforms. Next, it will zoom in on proposals on how to address those problems.

INTRODUCTION
Today social networking sites are ubiquitous and inseparable from the digital world. They host an important part of the online communication and contain the majority of people’s personal information that is available on the World Wide Web. The monetary worth of this huge amount of information is ever increasing, resulting in mind-blowing market values.

Ever since Facebook launched their application development environment, social application platforms – together with their applications itself - are ubiquitous in the context of social network-
ing sites. Almost every major social networking site nowadays provides means to consult personal user data from their social graph. Third-party social applications spread through the online communities and the popularity of these social applications keeps increasing. Support for such third-party applications is an important contributor to the overall success of social network sites (Pham, 2011).

Typical for these social-aware applications, is that the code provider typically is a third stakeholder, different from the social network site and the end user. Because an application has access to social data, also the application provider itself gets access. Given the growing amount of privacy-sensitive social data on social network sites, this becomes more and more an undesirable situation.

In this chapter we will focus on these privacy and security problems in the context of online social network applications. In this context, third-party application are typically developed in client-side scripting languages like JavaScript – which will be executed in the user’s browser - often in combination with server-side technologies like PHP or Java – fueling the back-end part of the application.

The first objective of this chapter is to introduce the details — both the architectural and technological - of the previous and current social application platforms. The second objective is to identify three different categories based on these security/privacy related problems. The third objective is to examine what recent scientific literature tries to do in order to address those problems.

BACKGROUND

According to Facebook, people install such applications more than 20 million times per day, day after day (Facebook, 2011). However, the use of such applications comes with privacy and security risk for the social network users.

SECURITY AND PRIVACY OF ONLINE SOCIAL NETWORK APPLICATION PLATFORMS

This section will cover two main implementation models for social network application platforms. Next it will dig into the different security and privacy issues resulting from the design choices.