Social Network Security: A Brief Overview of Risks and Solutions

Edward Wang, ekwl@cec.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract

In this study, we present the various aspects of social, network and physical security related with the use of social networks, by introducing the mechanisms behind each and summarizing relevant security studies and events related to each topic. It has been long understood that the widespread use of social networking sites can provide attackers with new and devastating attack vectors. In this study we attempt to dive deeper into each mode of security threat, as well as confirm the security risk associated with each topic by providing real world financial / social consequences. We recognize that while organizations and individuals may have legitimate business / personal uses for social networks, we recommend specific actions be taken to bolster stronger user awareness, more secure software designs as well as better organizational accountability.

Keywords

Social network security, social engineering, XSS, CSRF, DoS, stalking, OpenID, Facebook, twitter, LinkedIn, phishing, information theft, identity, identity hijacking, malware, worms, firewall, corporate security

---

Contents

Introduction

For a newcomer to the internet arena, social networking sites are an ever more popular way for people to stay connected. Some might even venture to say business opportunities are formed and lost online, as our web presence becomes an integral part of our personal lives. In an era where our online identity not only overshadows our actual identity, but other key financial and personal systems as well, the potential security risks associated with these social networks cannot be stressed enough.

Over the years, researchers and hackers alike have identified a handful of security risks ranging from people, process to application. The purpose of this study is to give a sweeping overview of the major security topics surrounding social networks today, and introduce the underlying mechanisms behind each. We follow up with some tangible consequences that each risk might have, and finally provide a direction to look at in terms of solutions.

Social Engineering

Information Leakage & Theft

Mechanism

Scope of Visibility

Most people when asked will agree that not everyone they know is their best friend; there are the mere acquaintances all the way to those with whom we share our deepest secrets, along with many shades in between. However the widespread phenomena of social networking sites has added new meaning to friends: two people are often "friends or not" (D, 2004). While social networks may not necessarily increase strong ties, it certainly does very little for weak ties. One may have a couple of close friends and thousands of distant friends, and a social network may simply categorize them all as "friends."

More contacts aren't necessarily a bad thing; the problem is who has access to our information? Social networking sites provide a certain level of access control, but most people do not take the effort to configure

these properly. As a result, everyone ends up with equal access rights. To make matters worse, oftentimes information travels through several hops of "friends," and by the idea of six degrees of separation it seems unreasonable to assume we are far from the bad guys.

Use of Real Names and Personal Information

As an added bonus, social networking sites contain information that is either mostly real or easily identified as fake. For the sole purpose of keeping up with friends in a seemingly trustworthy domain, people have very little incentive to falsify information on Facebook. The same idea goes for sites like MySpace and LinkedIn. See figure 1 for a recent study at Carnegie Melon University (Gross & Acquisti, 2005).

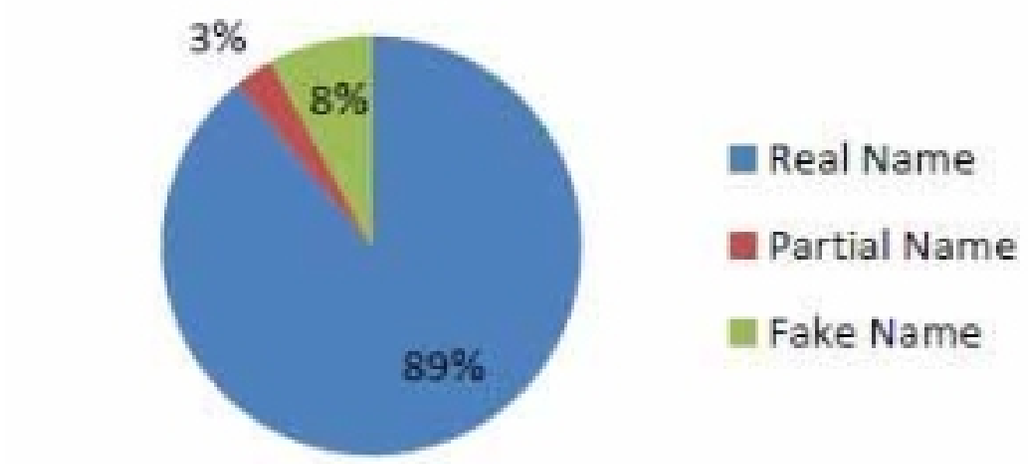

Figure 1: Percentage of CMU Facebook profiles and their respective name authenticity

Similar results exist for other sensitive information, such as birthdates, education history and hometown. In fact, a group of Taiwanese researchers have gone on to propose automated identification systems for name, age and education record inference on a different social network with good results (Lam, Chen, & Chen, 2008)

Breadth of Available Information

In the same CMU study, Gross and Acquisti go on to show the sheer amount of information available simply within the CMU Facebook realm. (Gross & Acquisti, 2005) Again, most users make very little effort to subdivide access privileges to different parts of their profile. By the same line of logic as names and birthdates, we have very little reason to doubt the validity of this information.