Chapter 8.5
Cyber Security and Privacy in the Age of Social Networks

Babar Bhatti
MutualMind, Inc., USA

ABSTRACT

Social media is transforming the way we find, create, and share information during the course of our personal life and work. The rapid growth of social media and the ubiquitous sharing and access of information through various digital channels has created new vulnerabilities and cyber threats. This chapter will provide an overview of the security and privacy implications of social networks and communities. The goal of this chapter is to examine and raise awareness about cyber security threats from social media, to describe the state of technology to mitigate security risks introduced by social networks, to shed light on standards for identity and information sharing or lack thereof, and to present new research and development. The chapter will serve as a reference to students, researchers, practitioners, and consultants in the area of social media, cyber security, and Information and Communication technologies (ICT).

INTRODUCTION

The goal of this chapter is to provide information about online social networks and the security and privacy issues which are associated with them. The chapter talks about online social networks, their scale and reach in the society, what actions are taken on these networks and what are the consequences for security and privacy. This chapter also includes recent examples of security and privacy issues associated with online social networks.

The chapter also looks at what efforts have been made to control and solve the problems and provides references for related research. It provides references to research papers, blogs and other media articles related to social media security and privacy.

DOI: 10.4018/978-1-61350-323-2.ch8.5

BACKGROUND

The proliferation of social networks is a relatively new phenomenon. Social media and digital content is getting embedded in our private lives and work culture. The novelty, scale and velocity of this change introduce a multitude of issues including security and privacy. It is against this background that we review the current state of cyber security and privacy.

The rapidly shifting nature of social networks and web 2.0 has made it difficult to define standards, boundaries and mechanisms to secure identities and information for individuals and groups. There is active research going on to identify and address various facets of security and privacy issues related to social networks. Industry practices and literature review shows novel approaches and experimentation to address public, business and government concerns. The references section at the end of the chapter is a good starting point. We expect new tools and industry standards for security and privacy to emerge in the next few years.

Further sections in the chapter provide information about the specific social networks and their vulnerabilities, how and where social networks are accessed and used and what all of this means for lay persons and security practitioners.

IMPACT OF SOCIAL MEDIA ON CYBER SECURITY AND PRIVACY

As described in introduction section above, the new modes of communication and sharing introduced by social media necessitates that we re-examine security and privacy. This section looks at the impact of social media. We start with some numbers which give an idea of the scale of social media, discuss the core security and privacy issues related to social media and provide examples of recent security and privacy breaches in the realm of social media.

Social Media Growth

The rapid growth of social media over the last few years has changed the way people create, share and distribute digital content, whether it is messages, photos or other items.

Here are a few statistics for 3 popular social networks – the numbers will surely have changed by the time you read this:

- Facebook has more than 500 million active users
- LinkedIn has over 75 million members
- Twitter has over 150 million registered users and 180 million unique visitors every month

The growth of user generated content is staggering: an average user of Facebook creates 70 pieces of content each month. Estimates by (Rao, 2010) suggest that Twitter users create about 70 million messages – known as Tweets in social media speak – a day.

Most of the growth has taken place in the last 5 years or less, causing disruptions in the way communication and information flows. For instance, breaking news can spread fast due to the viral sharing characteristic of Twitter. In same way, malware can be transmitted rapidly through Twitter. This proliferation of social media and the accompanied user generated content and sharing changes the landscape of privacy and security. In many cases, the standards and recommendations have not kept up with the changes brought up by social media. This environment provides new opportunities for those with malicious intent to exploit user information or to use the viral nature of social media to disperse viruses and malware.

Security concerns of social media applications include Phishing, Scams, Social engineering attacks and Identity Spoofing. There are a number of well-documented incidents related to social media security or privacy. These incidents include phishing, scams, direct hacks, bugs which reveal