Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2011

Attack vectors against social networking systems: the Facebook example

Matthew Warren
Deakin University

Shona Leitch
Deakin University

Ian Rosewall
Deakin University

Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/131

ATTACK VECTORS AGAINST SOCIAL NETWORKING SYSTEMS: THE FACEBOOK EXAMPLE

Matthew Warren, Shona Leitch and Ian Rosewall,
School of Information Systems, Deakin University, Melbourne, Australia
mwarren@deakin.edu.au

Abstract

Social networking systems (SNS's) such as Facebook are an ever evolving and developing means of social interaction, which is not only being used to disseminate information to family, friends and colleagues but as a way of meeting and interacting with "strangers" through the advent of a large number of social applications. The attractiveness of such software has meant a dramatic increase in the number of frequent users of SNS's and the threats which were once common to the Internet have now been magnified, intensified and altered as the potential for criminal behaviour on SNS's increases. Social networking sites including Facebook contain a vast amount of personal information, that if obtained could be used for other purposes or to carry out other crimes such as identity theft. This paper will focus on the security threats posed to social networking sites and gain an understanding of these risks by using a security approach known as "attack trees". This will allow for a greater understanding of the complexity associated with protecting Social Networking systems with a particular focus on Facebook.

Keywords
Social Network Systems (SNS), Facebook, attack tree.

INTRODUCTION

The emergence of Web 2.0 and related Internet sites such as Facebook has had a major impact upon the Internet in recent years. One of the interesting aspects of Facebook is the use of third party applications and the interactions that this allows. This means that individual Facebook pages now act as a web page, blog, instant messenger, email system and the use of third party applications allows for real time functionality (DiMicco & Millen, 2007; Shuen, 2008).

In a generic context, social networking sites (SNS's) are virtual spaces where people congregate to discuss ideas, share information and communicate (Raacke & Bonds-Raacke, 2008). The reasons for the popularity of SNS's are varied and include (Lampe et al, 2007):

- To communicate and keep in touch with friends (as a way of supporting pre-existing friendships;
- To make new friends and build social relationships;
- To promote oneself.

This new way to communicate and share information has highlighted new and more profound security and privacy concerns than were encountered during the initial Internet boom period. This paper proposes the use of attack trees to understand the security threat of networks, in terms of this paper the focus will be upon Facebook. The paper will discuss the security issues of social networking, the security issues of Facebook, the development of attack trees and an analysis of the Facebook security example using attack tree analysis.

SOCIAL NETWORKING AND SECURITY ISSUES

In a SNS context there are of a number of key security and privacy issues, these are (Boyd, 2008; Dwyer et al, 2007; Shin, 2010):

- Security: In SNS's, security refers to users' perception on security; that is perceived security which is defined as the extent to which a user believes that using a SNS application will be risk-free;

- Privacy: In a SNS context privacy can be defined as control over the flow of one's personal information, including the transfer and exchange of that information. Privacy within SNS's is often not expected or is undefined;
- Trust: Trust in a SNS is defined as the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party. In a SNS, trust is a critical determinant of sharing information and developing new relationships.

The fabric of SNS's enable viruses, malware and Trojans to thrive on their ability to access personal information or cause password attacks leading to a breach of network security. SNS's also open the gates for cybercriminals and sexual predators and this is likely to become a major issue for the future. Increased use of SNS's such as Facebook increase the chance of malware or peer phishing attacks that can potentially cause serious damage to organisational data security (Socialman, 2009). For example there were concerns over a data leak after a hacker broke into the 'Top Friends' application on Facebook making users private information visible (Goldie, 2008). In 2009 a worm named Koobface spread quickly through Facebook; this particular worm stole personal information in a much more sophisticated way then has been seen before The worm could register itself on Facebook, add random strangers as friends and post messages on the their "walls" which would provide links to malware (Sophos, 2010). It continued its effect on the SNS's by spreading to other sites which compounded the effects (Luo et al, 2009).

PRIOR RESEARCH INTO FACEBOOK SECURITY CONCERNS

Earlier research into the security issues surrounding Facebook identified a number of unique security concerns (Leitch and Warren, 2009). Since that earlier research, a new key feature of Facebook has been developed, the federated login via Facebook connect. This means that logging in though Facebook gives users the ability to share information, in particular (Facebook, 2010):

Real Identity

Facebook users represent themselves with their real names and real identities. With Facebook Connect, users can take their real identity information with them wherever they go on the Internet including; basic profile information, profile picture, name, friends, photos, events, and groups.

Friends Access

Many people rely on Facebook to stay connected to their friends and family. With Facebook Connect, these users can continue to connect with their friends elsewhere on the Internet. Developers are able to add rich social context to their websites and can even dynamically show which of their Facebook friends already have accounts on their sites.

Dynamic Privacy

As a user moves around the open Internet, their privacy settings will follow, ensuring the users' information and privacy rules are always up-to-date. For example, if a user changes their profile picture, or removes a friend connection, this will be automatically updated in the external website. An example of the Facebook interconnection is shown in Figure 1.

Figure 1. Connecting to Digg via Facebook
According to Facebook (Facebook, 2011):

- Since Facebook connect plugins launched in April 2010 an average of 10,000 new websites integrate with Facebook every day;
- More than 2.5 million websites have integrated with Facebook (via Facebook Connect), including over 80 of comScore's U.S. Top 100 websites and over half of comScore's Global Top 100 websites.

This means that if Facebook user credentials are compromised then access to other sites is also enabled and that a user's online identity can be assumed. This is the driver for attacks on Facebook and attacks on Facebook user credentials.

ATTACK TREE DIAGRAMS

Attacks tree are a method of graphically representing the possible attacks against a system via the use of an attack tree diagram which is similar to a structured tree diagram. Prior research (Mauw and Oostdijk, 2005) determined that the graphical, structured tree diagram notation is appealing to practitioners, yet also seems promising for tool builders attempting to partially automate the threat analysis process. As such, attack trees may turn out to be of interest to the security community at large as a standard notation for threat analysis documents. The notion and concept of attack trees was introduced by a number of key researchs such as, Schneier (Schneier 1999; 2000) and (Amoroso, 1994).

Previous researchers (Dimitriadis, 2007; Schneier, 1999) have put forward a case that attack trees provide a formal methodology for analysing the security of systems and subsystems and that they provide a different way to think about security; which include security capture and the ability to reuse expertise about security as well as responding to changes in security. An attack tree has a root node and leaf nodes. The root node represents the target of the attack, while the leaf nodes represent the means for reaching the target, which are the events that comprise the attack.

The attack tree approach has been used in a number of different security situations, from the Critical Infrastructure (SCADA) (Byres et al, 2004) domain to commercial security environments (Internet banking) (Dimitriadis, 2007). The use of attack trees has been shown to be very flexible and is able to deal with complex situations, hence the authors decision to use this approach. The authors propose that the attack tree model may be one effective way of being able to clearly illustrate the attacks on SNS's.

FACEBOOK CASE STUDY

The case study used focused on the use of the social networking site, Facebook and draws attention to the particular security risks and issues of that SNS. The authors used the same approach when analysing Facebook that Dimitriadis (2007) applied in his study where attack trees were used to try and determine the particular security requirements of Internet Banking.

The stages of development were:

1. The identification of the known security risks that impact Facebook. Previous research by Leitch and Warren (2009) identified the security threat dimensions most commonly encountered in Facebook by modeling them in a Security Threat Matrix (STM); this was summarised later in the paper. The security risks identified were then used as the source information to be analysed in the current research to form the attack tree diagrams;
2. Development of the attack tree model to illustrate the high level security threats and issues that impact Facebook.

Eight security threat dimensions were considered based on the STM (Leitch and Warren, 2009) and an attack tree diagram was created for each threat.

One of the major issues that were identified as a security threat in Facebook was the compromising of user credentials (Leitch and Warren, 2009) to gain access to individuals Facebook pages (this may be related to the recent development of the federated login approach). These attacks occur because individuals either guessed, used technology or human means to compromise the credentials.

The attack tree modelling and implementation of the suggested countermeasures will help to mitigate the threat of the following security and misuse issues in relation to Facebook (Leitch and Warren, 2009):

Facebook Security Threat Dimension
I. Privacy & Confidentiality
II. Authentication & Identity Theft
IV. Vandalism, Harassment & Stalking
VII. Payment and Transaction Integrity
VIII. Malwares and Computer Virus

The attack tree diagram representing one of Facebook's main security risks is shown in Figure 2. The bull's-eye symbol in the figure is used to illustrate where suggested security countermeasures are linked to a particular threat, for example, security countermeasures that relate to vulnerability exploits relate to Malicious software installation.

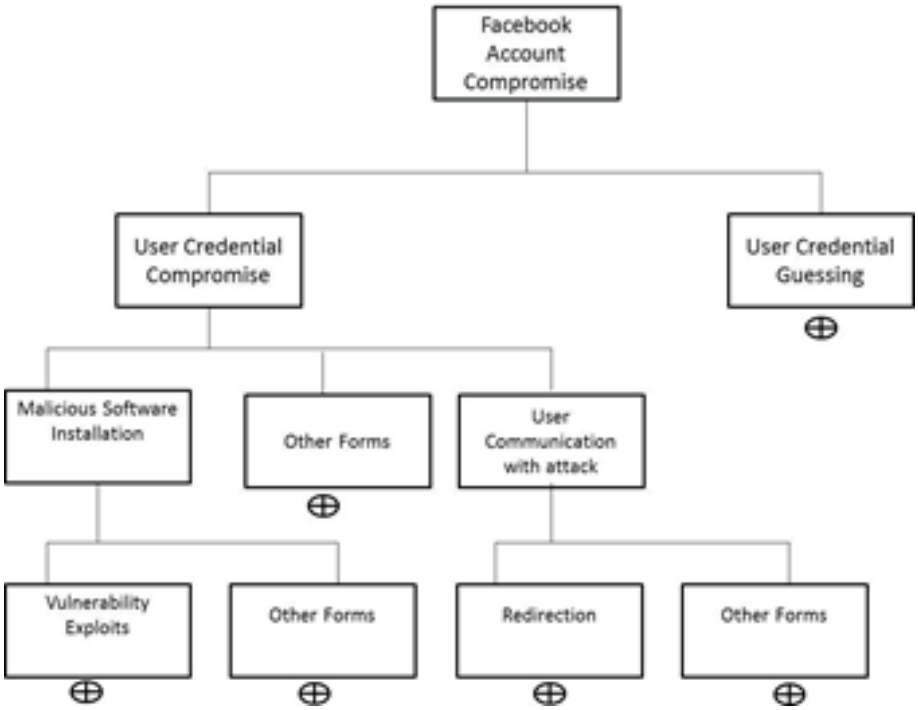

Figure 2.Attack Tree Matrix for Facebook

The abuse of user credentials as a means to compromise a Facebook account encompasses a number of different aspects and specific risks. These are outlined in Figure 2 (and explained below); these are the leaves of the attack tree diagram.

User Credential Compromise – Other Forms

The theft of handwritten notes containing password details, e.g. sticky notes on the computer.

User Credential Compromise – Malicious Software Installation – Vulnerability Exploits

The installation of software onto a computer to gain access to a user's credentials. This could compromise the user's login information and password, e g. through the use of keyboard loggers, screen capture, etc. This could also be a threat due to the third party applications used within Facebook.

Malicious Software Installation – Vulnerability Exploits

This is the use of hidden code within a webpage that exploits a known vulnerability to install malicious code. An alternative attack approach could be the use of worms that searches for vulnerabilities and exploits them automatically. This could also be an issue with the third party applications used with the Facebook system.

Malicious Software Installation – Other Forms

This relates to the installation of malicious code via email. The malicious code is sent as an attachment and the user accidently installs the code on their machine.

User Credential Compromise – User Communication with Attack - Redirection

A key issue is the manipulation of third party applications used with the Facebook system and the redirection of users to malicious sites and away from the Facebook environment.

User Credential Compromise –User Communication with Attack – Other Forms

These attacks could take the form of social engineering, such as fake Facebook friends trying to obtain information via emails, phone calls, etc. Another issue is the manipulation of third party applications used with the Facebook system and the communication and exchange of information through those channels.

User Credential Guessing

This is the use of technology to randomly generate usernames or passwords. In the Facebook example this could also include the accessing of the "secret question" in order to generate a new password and gain access to the Facebook account.

This part of the paper has defined the security threats that impact Facebook, the usage of the attack tree diagram approach to map those security threats and suitable security countermeasures that can assist in the mitigation of these threats.

DISCUSSION

Prior research into the most widely concerning security threats in Facebook and the subsequent use of the research to develop attack tree diagrams as a means to enhance understanding has helped to further highlight some of the unique security threats and risks that impact Facebook.

The attack tree diagrams provide a formalised method for understanding security threats and permits you to look beyond the high level threats and also consider the subsystems. This provides a greater understanding of the threats which is incredibly important, as noted by Schneier (1999), "Security is not a product -- it's a process. Attack trees form the basis of understanding that process". There are a number of advantages of the attack tree diagram approach, which include:

- The attack tree diagram allows the modelling of complex security threats to generate greater understanding;
- The attack tree diagram allows for security threats to be broken down into their sub- components, again enhancing understanding;
- The approach allows for the linkage between threats and security countermeasures and directly identifies the link between a countermeasure and the specific threat within the attack tree diagram.

The study has also identified some weaknesses in the attack tree approach, these include:

- The approach does not factor in the likelihood of an attack type, e.g. Pharming was not included in the analysis because of the extremely low likelihood of this being a threat related to the Facebook site;
- The approach does not factor in temporal issues, for example, a reflection of the time needed for social engineering attacks or the speed of online automated attacks.

Whilst SNS's continue to become the most powerful and popular Web 2.0 components, complex security threats will continue to increase. Not only are the traditional Internet based attacks still relevant but novel new techniques utilising social engineering tactics are also being observed. It is important that security professionals have the ability to develop organisational solutions. These solutions need to have the ability to understand security situations, the ability to map and react to complex security threats, and ensure that proposed security solutions are cohesive and comprehensive. Attack tree diagrams can go a long way to achieving this aim through their simple design, reusability and their ability to promote discussion not just on completion but as a part of the development process.

CONCLUSION

This study has identified that attack tree diagrams can be used to understand and model security issues of very complex systems, such as social networking systems. This study has also created opportunities for future research, e.g. the analysis and comparison of attack tree diagrams of other social networking sites such as Twitter or MySpace.

It is clear that SNS's have become a favorite target of hackers (Gostev, 2008) due to the potential for fraudulent earnings through the use of malware and spam. With the ever growing number of users availing themselves of the benefits of SNS's (Facebook (2011) reports its 500 millionth user in 2011) the need for a greater understanding and cohesive documenting of the attacks against SNS's is paramount to be able to progress further and plan countermeasures. By gaining an understanding of the security risks associated with social networking systems such as Facebook, it will allow for more effective decision making in regards to these issues.

REFERENCES

Amoroso, E. (1994). Fundamentals of Computer Security. Prentice Hall. ISBN 0-13-108929-3.

Boyd, D. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. Convergence, 14(1), 13–20.

Byres, E. J., Franz, M. & Miller, D. (2004). "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", International Infrastructure Survivability Workshop (IISW '04), Lisbon, Portugal.

Dimitriadis, C. (2007). Analyzing the Security of Internet Banking Authentication Mechanisms, Information Systems Control Journal, Vol 3.

Dwyer, C., Hiltz, S. & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09 -12, 2007.

Gostev, A, Zaitsev, O,Golovanov, S & Kamluk, V (2008). Kaspersky Security Bulletin: Malware evolution, URL: http://usa.kaspersky.com/threats/docs/KasperskySecurityBulletin_MalwareEvolution2008.pdf [Accessed 1/3/2011].

Facebook (2010). Announcing Facebook Connect, URL: http://developers.facebook.com/blog/post/108 [Accessed 1/3/2011].

Facebook (2011). Facebook statistics. URL: http://www.facebook.com/press/info.php?statistics [Accessed 1/3/2011].

Lampe, C., Ellison, N., & Steinfield, C. (2007). A face(book) in the crowd: Social searching versus social browsing. Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work, Banff, Canada.

Leitch, S. & Warren, M. (2009). Security Issue challenging facebook, Proceedings of the 7th Australian Information Security Management Conference, Edith Cowan University, Perth, W.A.

Luo, W., Liu, J. & Liu, J. (2009). An Analysis of security in social networks. 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

Mauw, S & Oostdijk, M. (2005). Foundations of Attack Trees, In proceedings In Conference on Information Security and Cryptology 2005, Beijing, China.

Schneier, B. (1999). Attack trees: Modelling security threats, Dr. Dobb's Journal, 1st December, URL: http://drdobbs.com/184411129 [Accessed 12/2/2011].

Schneier, B. (2000). Secrets & Lies: Digital Security in a Networked World, Wiley, USA.

Shin, D. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers, 3(5).

Sophos (2010) W32/Koobfa-Gen, URL: http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Koobfa-Gen/detailed-analysis.aspx [Accessed 12/2/2011].