Attack Centric Threat Modelling Approach to Social Networks: Hacking and Counter Measures.

Computer Science Honours

Research Methods Literature Synthesis

By: Molulaqhooa Linda Maoyi

Supervisor: Dr Anne Kayem

Submitted to:

Department of Computer Science

University of Cape Town

14 May 2012

ABSTRACT

Social networks are becoming ubiquitous nowadays as one of the most used internet services. As with every new web technology, they are prone to vulnerabilities that might compromise on the security of the system and lead to privacy concerns such as identity theft. In addition to these concerns, there are many other vulnerabilities that exist that might be potentially dangerous to the overall security of the social network. In this literature synthesis, we look at Threat Modelling approaches in social networks, which focus on the attack centric model in order to identify threats and vulnerabilities that could be exploited by an attacker.

Keywords: Social network, web technology, threat modelling, privacy

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

GLOSSARY

DFD	A Data Flow Diagram is a graphical representation of data flows, data stores, and relationships between data sources and destinations
SDLC	Software Development Life Cycle
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service and Elevation of privilege

.

1. INTRODUCTION

Social networks emerged in the 21st century because of the information technology boom and world globalization through the Internet [1]. This started in 1997 with the advent of SixDegrees.com and since then, this has resulted in the establishment of many social networking sites which were based on the "Social-circle model" [2] depicted in Figure 1. The notable ones are MySpace, LinkedIn, YouTube, Twitter and Facebook. These social networks provide users with options of personalizing their profiles where they can post personal data, sharing information with friends, chatting and uploading multimedia information. While these may have many benefits, there are also underlying security threats that can be exploited maliciously by hackers and cybercriminals to compromise the system.

Figure 1: Social-Circle Model

Social Networks have become a channel through which several security violations, such as identity theft and information leaking, occur. This literature synthesis starts by exploring what *Threat modelling* is and why it is important. The synthesis continues with a classification of the common threats that affect Social networks and then explains the vulnerabilities corresponding to these threats in detail. We use the words attacker and adversary to denote the same thing. The last section will conclude and outline future work.

2. THREAT MODELLING

2.1 Introduction

This section looks at the threat modelling approach in order to understand how to better exploit threats and vulnerabilities in a system. This is important because many systems have assets of value such as user passwords that are protected. However, there are vulnerabilities associated with these assets and therefore the threat modelling approach looks at the security vulnerabilities from the attackers view in order to understand how to design better security mechanisms and countermeasures.

2.2 What is Threat Modelling

A threat model is "A systematic, non-provable, internally consistent method of modelling a system, enumerating risks against it, and prioritising them." [3]. As it is an attack focused risk assessment [3], threat modelling is usually implemented during the design phase of the Software Development Life Cycle (SDLC) in order to identify the methods an attacker might use to exploit vulnerabilities in a system. The benefits associated with such a model are the ability to identify and investigate potential threats that could be mitigated early, this helps to prioritise threats and identify high impact vulnerabilities. In addition, threat modelling exposes logical or architectural vulnerabilities in a system, which helps to validate the security design of the system before development.

Threat modelling defines the security of the application which helps to scope and set boundaries and constraints for the system. decision making use of scenario modelling can be employed by a threat model whereby key issues that represent the risks such as authentication and authorization are highlighted since the scenario modelling is a skeletal overview of the before and after picture.

2.3 Modelling Approaches

There are three main approaches to threat modelling and depending on who is evaluating the system. According to N. Sportsman [4] one could look at the system in any of the following ways:

- **Asset Centric**

  Evaluating the system from asset classification such as personal information.
- **Defence centric**

  Evaluates weakness in security controls and looks for attacks against each element of the model.
- **Attack Centric**

  This where the system is evaluated from the point of view of an attacker and how they will go about exploiting the system and what they could possibly try to attack. For the purpose of this paper, we will be studying the attack centric model in depth.

2.4 Threat Modelling Process

The threat modelling process needs to be an iterative process because it is highly improbable that one can identify all possible vulnerabilities in a single pass. According to J.D. Meier et al [5] applications rarely stay the same forever and so, as an application evolves, the threat modelling process should be repeated to account for that change. In essence, the attacker should identify the security objectives of the system, look at the application overview, decompose the application, identify threats, identify vulnerabilities and repeat the threat modelling process. An outline of the threat modelling process is shown in Figure 2.

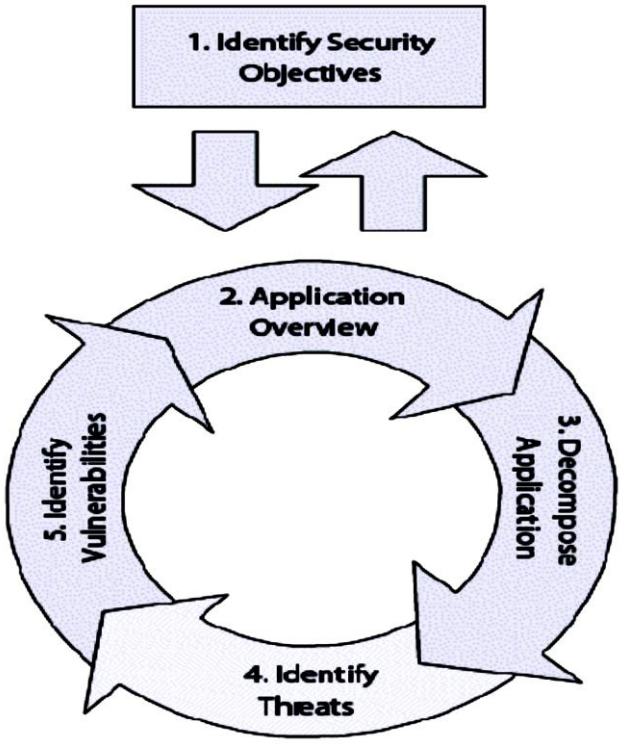


Figure 2 : Threat modelling Process

2.3.1 Security objectives

With reference to Figure 2 of the threat modelling process, from an attacker's point of view the first step would be to identify the assets that need to be exploited, this could be confidential data such as names, email addresses on user databases.

2.3.2 Application overview

Figure 2 number 2, Here the adversary will investigate what the system does and how it uses or accesses resources. This is a very important step as it analyses how certain resources can be misused.

2.3.3 Decompose the application

Looking at Figure 2 number 3, the attacker decomposes the application to create an attack profile for the system based on known vulnerabilities. There are also certain steps that an attacker might want to take such as identifying data flow between the social network and the server using Data Flow Diagrams (DFD's). DFD's could help in decomposing the system by providing detailed representation of the system components complete with boundaries and connections to other systems. In Addition, it is also vital to identify entry points in the system that might serve as entry points for any attack. Entry points are where data enters or exists the application; these may include authentication forms, web applications listening for HTTP request, profile-related web pages and searching.

2.3.4 Identifying threats and Vulnerabilities

Looking at Figure 2 number 4 and 5 of the threat modelling process The attacker identifies the threats associated with the system and must supply data to launch an attack this could be in the form of injections, cross-site scripting etc. [8].

2.4 Microsoft STRIDE Model

The Microsoft STRIDE model, just like attack trees that we will discuss later, can be used by an attacker to identify the types of threats that exist in a system such as changing authentication data, reading user profile data and what happens if access is denied to the user profile database. The STRIDE model threats are categorized as follows:

Spoofing – an attack on authentication whereby there is an impersonation of something or someone else.
For example, since session identifiers are incremental, it is possible to guess what another user's session ID will be and generate this session ID in order to impersonate the user.

Tampering – an attack on integrity whereby there is modification of data.
For example, database entries can be modified using SQL injections.

Repudiation – an attack on non-repudiation whereby one claims to not have performed an action.
For example, a system that does not have an audit functionality to monitor user operations in order to trace improper requests.

Information Disclosure - an attack on confidentiality by exposing information to someone not authorized to see.
For example, error messages that reveals the database schema.

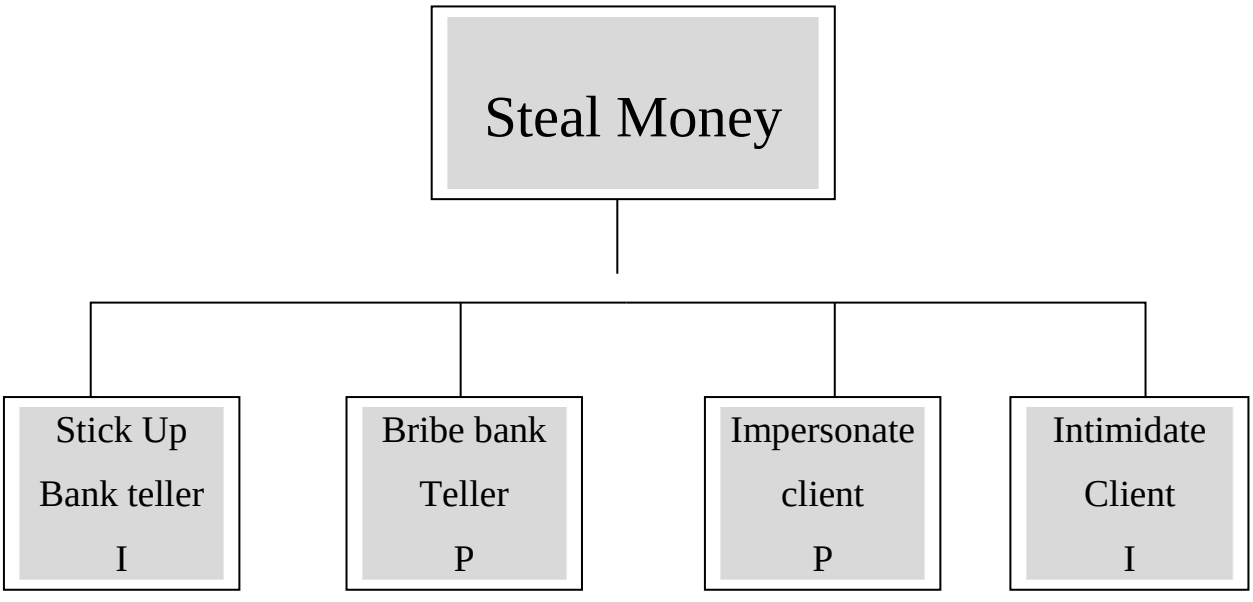
Denial of service – an attack on availability where there is a denial of service to users.
For example, system crashes from unexpected input.

Elevation of Privilege: an attack on the authorization policy whereby an attacker gains capabilities without proper authorization.

For example, a user is able to get administrator rights through variable changes using buffer overflow attacks

2.5 Attack Trees

Another way of modelling attacks or threats could be the use of attack trees as explained by Bruce Schneier [6]. These are methodical ways of describing the security of a system. The attacks are represented with tree like structure with goals of exploiting the root/parent node through one or more ways through the leaf/children nodes. For example, an attacker may want to steal money from a bank, he/she then plans out an attack tree like the one shown in Figure 3, of how he/she is going to go about stealing the money, and label the different plans with either P where the attack is probable or I where the attack is improbable.



P – Probable

I – Improbable

Figure 3 : Attack Tree to steal money from a bank

Attack trees are quite easy to be constructed and flexible and give a great overview on the attacks that might be made to a system. These trees can be used to understand the process of security for an attacker. While the STRIDE model helps to identify and categorize threats and vulnerabilities, attack trees determine which threats or vulnerabilities should be addressed and in what order. This can be useful in understanding attack patterns that require events to occur in a certain sequence.

3. VULNERABILITIES IN SOCIAL NETWORKS

3.1 Introduction

This section shows the different vulnerabilities exploited by attackers on social networks as pointed out by C. Laorden et al [7]. Most of These vulnerabilities can be exposed using the STRIDE model and attack trees from the previous section.

3.2 Vulnerabilities associated with platform

The most common vulnerability is associated with the difficulty of removing all user information when deleting an account. This is due to the licence agreement clauses which appear when a user tries to leave a social network, rights which were transferred to the Social network when the content was uploaded. So in order to delete uploaded contents permanently, one has to manually delete content one by one.

Weak authentication methods are a downfall for most web services, users are tempted to use easy to remember username and passwords which can be cracked easily. Another vulnerability is poor authentication of users, the social network just checks for a valid email address thus can populate the social network with fake profiles.

3.3 Vulnerabilities associated with data

Chat programs and many other social networking sites indicate when a user has logged off a particular application/site. This can provide attackers with time to exploit previously found vulnerabilities when the user is out of sight, for example, a user logs off a social network, the attacker having maliciously obtained the users login details previously, might login using the victims credentials and post explicit material that might bring embarrassment to the user

3.4 Application security risk

Attackers can use many ways to infiltrate a system and according to the Open Web Application Security Project (OWASP), there are 10 critical security risks associated with web applications [8]. These include injection flaws whereby an attacker can input SQL commands that access unauthorized data. Broken authentication and session management whereby an attacker is able to compromise passwords, keys and session tokens. Cross-Site scripting is when a perpetrator executes scripts in the victims' browser, which can be used to deface websites, hijack user sessions. For example, security consultant Ron Bowles who took publicly available information of over 100 million Facebook users, which included user ID,'s, Names and created a 2.8 GB file of this information for anyone to download from Pirate Bay [9].

4. CONCLUSION

As the world continues to depend on social networking for communication, the chances of the social networks to be attacked also increases. Security alone on the network layer is not sufficient unless security is implemented during the design phase of the application to minimise attacks. Threat modelling is very useful in discovering the vulnerabilities in a system. However, as we have noted this is a process that must be repeated and evolved over time, changing to adapt to new type of attacks and threats.

5. REFERENCES

[1] Z.Minchev, M. Petkova, information processes and threats in social networks. A case study, in: ACM Computing Classification System (1998). H.5, I.2.4, I.6.5, K.4.2, K.6.5

[2] Social circle, Wikipedia the Free Encyclopaedia (2012).
URL: http://en.wikipedia.org/wiki/Social_circle

[3] D.White, SensePost Threat Modeling Metricon 6, Usenix Workshop (2011)
URL: http://www.slideshare.net/sensepost/corporate-threat-modelling

[4] N.Sportsman, Threat Modeling (2011)
URL:http://www.praetorian.com/presentations/Praetorian_Threat_ Modeling_ Presentation.pdf

[5] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan, Improving Web Application Security: Threats and Countermeasures (2003)
URL: http://msdn.microsoft.com/en-us/library/ff648644.aspx

[6] B.Schneier , Attack Trees: Modeling security threats,
in : Dr. Dobbs's Journal (1999)
URL: http://www.schneier.com/paper-attacktrees-ddj-ft.html

[7] C.Laorden, B.Sanz, G.Alvarez, P.G.Bringas, A threat model approach to threats and vulnerabilities in On-line social networks, in: A.Herrero et al. (Eds.):CISIS (2010). AISC 85, pp. 135-142

[8] OWASP Foundation, OWASP Top 10 -2010: The ten most critical web application Security risks (2010).

[9] M.Chacksfield, Facebook 'hack' puts public data into the public domain (2010)
URL:http://www.techradar.com/news/internet/facebook-hack-puts-public-data-into-the-public-domain-706396

[10] MSDN Library, The STRIDE Threat Model (2005)
URL: http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[11] WindowSecurity.com, Analysis of Buffer Overflow Attacks (2004)
URL:http://www.windowsecurity.com/articles/
analysis_of_buffer_overflow attacks.html