1. Threat Modeling Overview

In many applications, security is typically incorporated at the end of the design cycle. The consequence is that many systems are deployed with security mechanisms that have not been checked as rigorously as the rest of the system. Scandals such as the one that occurred in July of 2011, where security consultant (Ron Bowles) used a piece of code to collect personal data off Facebook and publish it on Pirate Bay (a popular file sharing site), only serve to emphasize the need for more thorough security and privacy verifications [1].

Threat modeling is useful in applying a structured approach to system security. With threat modeling one can identify and categorize potential security vulnerabilities in a system and then develop countermeasures accordingly.

2. Project Synopsis

In this project, we will look at two threat modeling approaches to social networks, the attack centric model and the software centric model [2].On the one hand, the attack centric model is centered on the attacker's goals and motivations for breaking into a system. In the case of the attack centric model, we want to evaluate how the attacker would achieve this and why. On the other hand, the software centric model is aimed at detecting vulnerabilities in the system's design. In the case of the software centric model, the idea is to step through the different components of the system and find the weaknesses that an attacker might exploit.

Having a blueprint of potential threats is useful, from the system designer's view point, because potential attack scenarios as well as the countermeasures can be simulated before the application is deployed. However, until recently, not much consideration has been given to comparing threat models or evaluating their efficacy in dealing with threats. This project is aimed at developing a framework to compare and evaluate different threat modelling approaches, attack and software centric. We will use an open source social network as a case study for evaluating the threat modeling approaches and implement an "intelligent" multi-agent system to provide countermeasures for potential attacks.

3. Problem statement

3.1 Research Questions

The main research questions of this project fall under the following categories:

- What are the social network security risks?

  Attackers can use many paths in a social network to exploit vulnerabilities that can be used to do harm to businesses, organizations or users. Each of these paths represents a risk that may, or may not be serious enough to warrant attention and so we need to identify and categorize the risks in terms of importance or danger [2].

- What sort of attacks on social networks can be perpetrated by malicious code and how does one model these attacks in order to mitigate them?

- What counter measures could be employed by the software centric model to identify threats and mitigate them?

- How do the attack centric and software centric models differ with respect to identifying threats and vulnerabilities?”

In the next preceding sections we will see how to tackle the above questions methodically throughout the project.

4. Procedures and Methods

4.1 System

The major challenge that the group will face will be to build a social network and get it running with a minimum number of 20 users.

4.1.1 Building the social network

An open source social network will be created using Elgg social network engines. The social network will be powered by the apache server using the Xamp tool. In ordered to have this social network up and running, the group will need a fast computer with at least 100 GB of free space which will be used to store user's data and will be running throughout the project duration. Getting such a computer will be one of the major challenges in building the social network since without it nothing with regard to the social network development will be done. People and Students from different faculties will be recruited to register as users and use this social network for the duration of the project. The group members will take the initiative to go and approach people and ask them to join the social network. At least 20 registered users will sufficient to get the social network ready to be used for the project. Although this is a small number, it will be a challenge to get all these users to use this social network throughout the entire project life time without getting something useful out of it. Another challenge the group might face is to keep this users interested in using this social network. One of the solution that have been proposed is to get at least 100 students to register, and from those 100 students registered, about 60% of them won't really put some effort into maintaining their profile or home page, so that 40% left will be enough for the social network to be useful for the project. To keep users active on the social network, it was proposed that each user will gain points depending on how much they interact with the system, the more the user is active, the more points the user earn. Since the social network will be used more during the mid-sections of the project, to get more people active at that time, we can raise the incrementation of points, say double the points earned a day if a user at least 20% of the day. The user with the highest points in the end will get a prize.

There are social networks like Facebook, twitter, LinkedIn, just to mention a few, that if we use for our project, the research would be much more interesting. However, due to this social networks "Statement of Rights and Responsibilities" [6], we have limited rights on how we use them. Social networks mentioned above are not open source; they limit the group from exploiting information about their users without their permission, hence the group won't be able to evaluate the security these social networks.

4.2 Procedures

The hackers will use different methods; which can also be a piece of code, to try and exploit as much information as they can about the registered users on the social network created. Methods used to exploit data will be those that threat modeling tools either do not pick up or assigned a low probability. The focus of hackers will be based on the attack centric model. After each method, the hackers will also create an antidote to quickly detect and counteract the actions of the piece of code used. The attacks that hackers are to implement will be amongst one of the following categories:

1. Injection: Injection flaws such as SQL, OS, and LDAP injection.
2. Cross-site-Scripting (XSS): The attacker will try to execute scripts in a victim's browser which will hijack the user's session or send some sensitive information to the attacker.
3. Broken authentication and session management: The attacker will try to get the user's password using faults on application functions related to authentication and session management.
4. Insecure direct object references: The attacker will use the exposed reference of an object, such as directory, file, and database key to try and access unauthorized data.
5. Cross-site request forgery: The attacker will user the logged in victim's browser to send a forged HTTP request.
6. Security misconfiguration: The attacker will try to find a weakness in the security configuration and use it his advantage.
7. Insecure cryptographic storage: The attacker will try to get sensitive data stored as plaintext.
8. Failure to restrict URL access: The attacker will try to forge URLs to access hidden pages.
9. Insufficient transport layer protection: The attacker will try to get sensitive data being sent from one end to the other in plaintext. This can include password and other secret information.
10. Invalidated redirects and forwards: The attacker will try and redirect users to a phishing site to get user's logging information.

The social network security administrator will use threat modeling tools to identify possible attacks as well as the reason behind their possibility. The model that the security administrator will use will be based on software centric approach. The security administrator will focus on the implementation of different components that make-up the social network. After this, the security administrator will all come up with strategies to close these loopholes.

4.3 Ethical, Professional and Legal Issues

This project requires people or students to register on the social network as. The social network will require the following information about the user in order to get the user registered:

1. Name and surname
2. Information about their studies
3. E-mail address
4. *Home language
5. *Date of birth
6. *Residential information
7. *User's picture

Items marked with * are optional. The e-mail address is vital since it will be used to contact the users to encourage them to keep on using the social network. Hence the group will need ethical clearance from the ethics Committee. All the users will be informed that the information they give to us will only be visible to the people they interact with on the social network, and that their information will only be kept for the duration of the social network life time, after that, all information will be removed. They will also be asked to sign a form stating that they understand the terms and give this group permission to use their information.

5. Related work

Web applications are quite popular and environments such as social networks that encourage data sharing and seamless user interaction facilitate the use of internet. This makes them one of the prime targets to attack because these web applications typically handle considerable amount of personal information. Social networks can be exposed to different types of attacks which weaken the security of the application which makes the information the application manipulates vulnerable. The Open Web Application OWASP provides the ten most critical web application security risks. So it is worth looking at OWASP security risks because these security risks are the most damaging to a system, and will be used to attack our social network. If we can find a way of preventing these attacks, then we will be taking a huge step towards securing an application. We will also look at threat modeling which is a tool to model threats and vulnerabilities on a system. A threat modeling is a tool typically used to proactively identify threats that can be classified as potential vulnerabilities in a system and provide countermeasures to prevent these attacks from being exploited to cause damage to the system.

5.1. An approach to web application threat modeling

Akash [5] suggested that to design a secure web application, it is important to analyze potential threats and model them. This defense centric approach can be applied using threat modeling, which is a process for optimizing application security by identifying threats and vulnerabilities, then defining countermeasures to prevent or mitigate the effects of them on the web application. Threat modeling helps shape your application design to meet security objectives such as confidentiality, privacy and integrity. Entry points to the system are typically used to attack web applications. Entry points are places/access points where data enters or exits the application, be it authorized or unauthorized. This is where users get access to the application by authenticating themselves to the application by using their username and passwords. SQL injection attacks are ranked 1st on the OWASP ten most critical web application security risk and these attacks are applied at the entry point of the application. So it makes sense in looking threat modeling from both the attack and defense software centric perspectives.

5.2 Attack centric approach

Threat modeling will help identify threats in our social network so we will use this approach to look at our social network from the attack software centric perspective. We will be more concern with the security threats on web application and how they are applied to it, since we will be looking at threat modeling on social networks. It is important to look at typical threats on web applications as we will try and prevent them from perpetrating. We will also look at SQL injection attacks as they are ranked 1st from the OWASP's ten most critical web application security risks. It is important on looking at the most damaging attack to web applications and see how it can damage your application and finding ways of stopping it from perpetrating.

5.2.1. Security threats on web applications

Open Web Application Security Project (OWASP) has released a list of the top ten most common vulnerabilities in web applications [6]. OWASP rank threats according to the severity of its impact. They provide ways on how these attacks are used and how to countermeasure them. 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. Insecure direct objects whereby an attacker manipulates a reference to an internal implementation object such as a file to access unauthorized data.

5.2.2. SQL injection attack

This type of an attack focuses on the database of a system. The security threat this attack poses on a web based application would be the built-in database access. SQL injection attacks are caused by attackers who insert a malicious SQL query into the web application to manipulate data or even gain access to the back end of the database [7]. This can be prevented if developers model the application which would give them a better understanding of the system and help identify bugs in the system.

5.3. Defense Software Centric

After looking at the social network from the attack software centric perspective, we will look at the social network from the defense software centric perspective. We will be more concern with shielding against SQL injection attacks. As mention earlier SQL injections are ranked 1st on the OWASP top ten application security risks. Therefore it is important to protect the social network against the attack. Also look at Microsoft STRIDE model. As this 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.

5.3.1. Shielding against SQL attacks

Madan at el [8] provided a method that would protect web applications from SQL injection attacks. This method models the security of an application by first analyzing the security objectives, then dividing the application, marking the vulnerabilities in the system, identifying, rank and then eliminates threats. However, a lot of work has been done on preventing SQL injection attacks. We were interested in this paper as it uses the Microsoft STRIDE model to categorize threats before modeling them [9]. This is important because each category has a specific set of mitigations. Once threats are analyzed and categorized you can mitigate them. Below shows the STRIDE model.

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

6. Anticipated Outcomes

6.1. System

The social network will be built without security implementation hence it will be vulnerable to attacks. We plan on finding these attacks, analyze them and find a solution to solve these problems using threat modeling tools. The anticipated outcome is that the social network will provide a strong information security to the users. The social network will provide a strong security to the confidentiality, integrity and the availability of data. The social network will resist all the attacks applied to it; however if it becomes vulnerable to an attack an antidote will be developed so that the social network becomes resisted to that attack.

6.2. Expected Impact

Should this project be a success then the techniques discovered to countermeasure attacks and protect data on the social network can be implemented to other social networks like Facebook, tweeter,

MySpace, LinkedIn and other web applications. This project can have a major impact on social networks and web applications security in general.

6.3. Key success factors

The success factor is to make sure that the social network we have created is secured. If the social network can resist attacks then the goal of our project will be a success. This does not mean that the social network is 100% guarantee free from threats, but the threats discovered during the project research have been circumvented.

7. Project Plan

7.1 Risks

1- Low2- Medium3- high

Not meeting project milestones

Risk: Expected deliverables may not be met due to time constraints.

Impact: May effect future tasks that need to be done because less time will be allocated to them which might cause the project fail.

Likelihood: 2.5

Contingency Plan: Weekly scheduled milestones that are submitted to the client for marks and progress reports between the developers to track work done and outstanding. Planning early for project deliverables. Task distribution and parallel task sets throughout.

Member leaves the Group

Risk: Team member decides to leave the group project due to circumstances

Impact: Certain project deliverables may not be met resulting in the overall failure of the project

Likelihood: 1

Contingency Plan: Separate tasks such that tasks can be worked on separately by each member while there is interdependency between them for the final product.

Knowledge on subject

Risk: The team members not having enough knowledge in threat modelling tools that will be used throughout the project.

Impact: Most of the scheduled functions are not going to be implemented. The final product will exhibit poor quality

Likelihood: 2

Contingency plan: Spend more time learning the underlying technologies and reviewing examples of how most of the things are done. Ask more questions and try doing the work early.

8. Timeline (see Appendix A)

9. Resources Required

9.1 Hardware

Minimum of four standard computer workstations, one to run the social network server and three to test the social network for threats and vulnerabilities.

9.2 Software

Microsoft Threat Modelling tool.

SensePost Threat Modelling tool.

Elgg Software for Social Network development.

Apache webserver for hosting the social network.

PHP SDK.

MySQL for Database storage of user information on the social network.

10. Deliverables

- Project Proposal
- Project Proposal presentation
- Project web presence
- Theory Chapter
- Design Chapter
- Project webpage
- Project Poster
- Project Report
- Project Software

11. Milestones

Milestones	Date
Project Proposal	21-May
Project Proposal Presentation	24-May
Revised Proposal Finalized	11-June
Project web Presence	12-june
Initial Feasibility Demonstration	13-June/29-July
Theory Chapter	29-July
Design Chapter	29-August
First Implementation	19-September
Final Prototype	28-Sep
Chapters on Implementation and Testing	3-October
Outline of complete report	10-October
Final complete draft of report	24-October
Poster due	03-November
Web Page	7-October
Reflection	11-October

12. Work allocation to team

Due to the scale of the project the work has been divided accordingly amongst the group members based on experience and expertise of the research area. Though some parts of the project will be worked on collaboratively to prevent absolute separation of the whole project. For the project to be successful and on time, each of the group member's sections" has to be completed.

The following tasks will be carried out collaboratively

- Feasibility study
- Project report
- Testing and Verification of threat modelling tools.

Molulaqhooa and Rotondwa are responsible for using the Microsoft threat modelling tool to analyze threats the attack centric approach. Sanele will use the Sensepost threat modelling tool to analyze threats using the defense centric approach.

13. References

[1] 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

[2] N.Sportsman, Threat Modeling (2011)

URL:http://www.praetorian.com/presentations/Praetorian_Threat_Modeling_ Presentation.pdf

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

[4] Facebook, "Statement of Rights and Responsibilities," 2011

[5]. An Approach to Web Application Threat Modeling By Akash Shrivastava April 2008

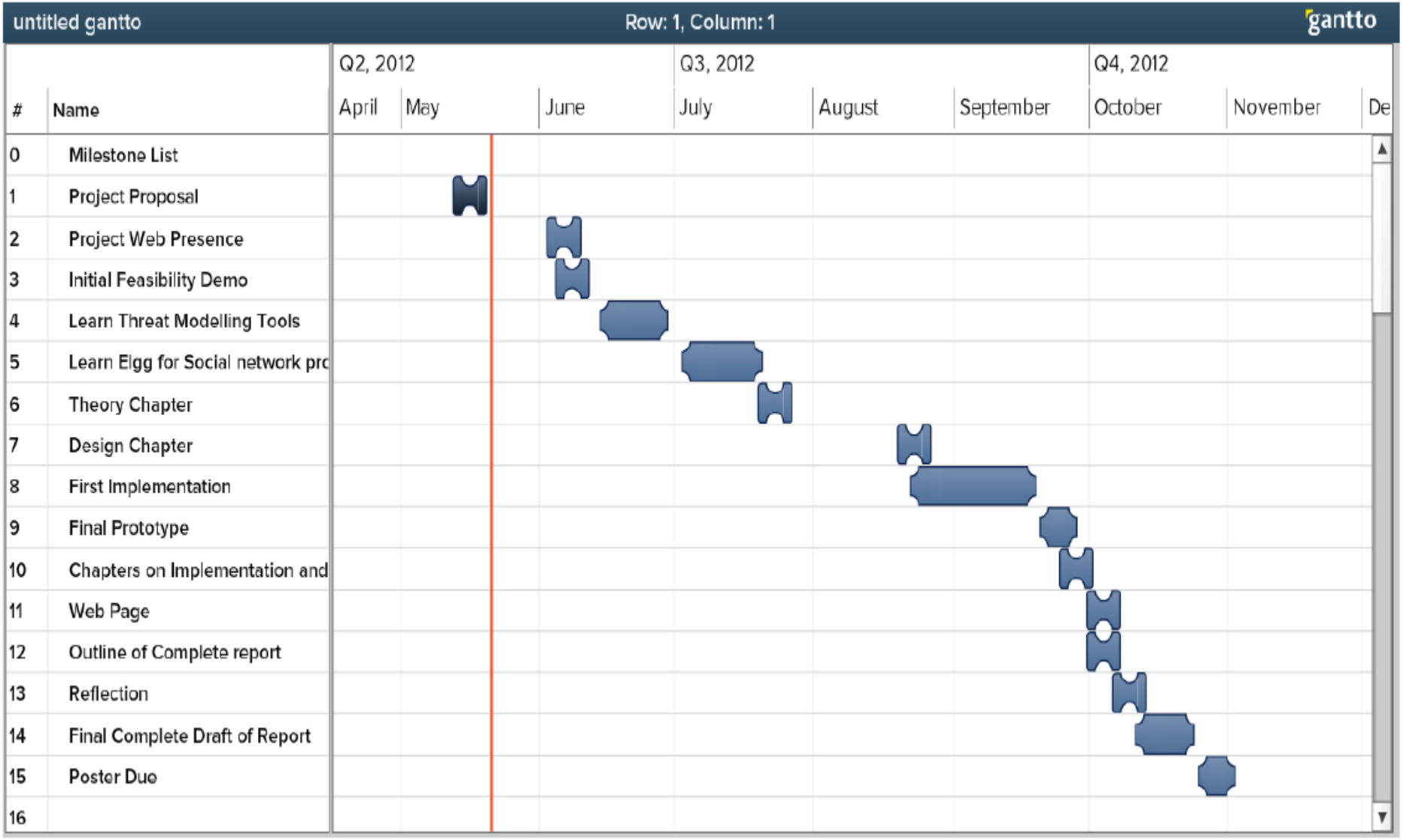
[6] https://www.owasp.org/index.php/Top_10_2010-Main

[7] Augmented Attack Tree Modeling of SQL Injection Attacks

[8] S. Madan and S. Madan. Shielding Against SQL Injection Attacks Using ADMIRE Model. In First International Conference on Computational Intelligence, Communication Systems

[9] http://blogs.msdn.com/b/larryosterman/archive/2007/09/04/threat-modeling-again-stride.aspx

Appendix A


untitled gantto
Row: 1, Column: 1
gantto
Q2, 2012
Q3, 2012
Q4, 2012
April
May
June
July
August
September
October
November
De
Name
0 Milestone List
1 Project Proposal
2 Project Web Presence
3 Initial Feasibility Demo
4 Learn Threat Modelling Tools
5 Learn Elgg for Social network prc
6 Theory Chapter
7 Design Chapter
8 First Implementation
9 Final Prototype
10 Chapters on Implementation and
11 Web Page
12 Outline of Complete report
13 Reflection
14 Final Complete Draft of Report
15 Poster Duo
16