THREAT MODELING IN SOCIAL NETWORKS

Molulaqhooa Maoyi
Rotondwa Ratshidaho
Sanele Macanda

INTRODUCTION

- Social Networks popular web service.
- 62% adults worldwide use social media
- 65% of world top companies have an active Twitter profile.
- 137.6 Million unique visitors per month on Facebook

INTRODUCTION continued.

- Prone to vulnerabilities
- Social Engineering attacks: Identity theft and Phishing.
- Threat Modelling approach to identify threats and vulnerabilities.

What is Threat Modelling ?

- "A systematic, non provable, internally consistent method of modelling a system, enumerating risks against it, and prioritising them." (SensePost,2011)

- Defines the security of the application which helps to scope and set boundaries and constraints for the system

Threat Modeling Approaches

- Attack centric model

  -How does an attacker think?

  -What does an attacker look for?

- Software centric model

  - How to better protect resources

  - How to mitigate risks

Division of Work

- Attack Centric Model :

- Rotondwa
- - Insecured direct object reference
- -Unvalidated redirects and fowards

- Molulaqhooa
  - Injections
  - Cross-Site Scripting (XSS)

- Software Centric Model :
- Sanele
- How to mitigate four risks

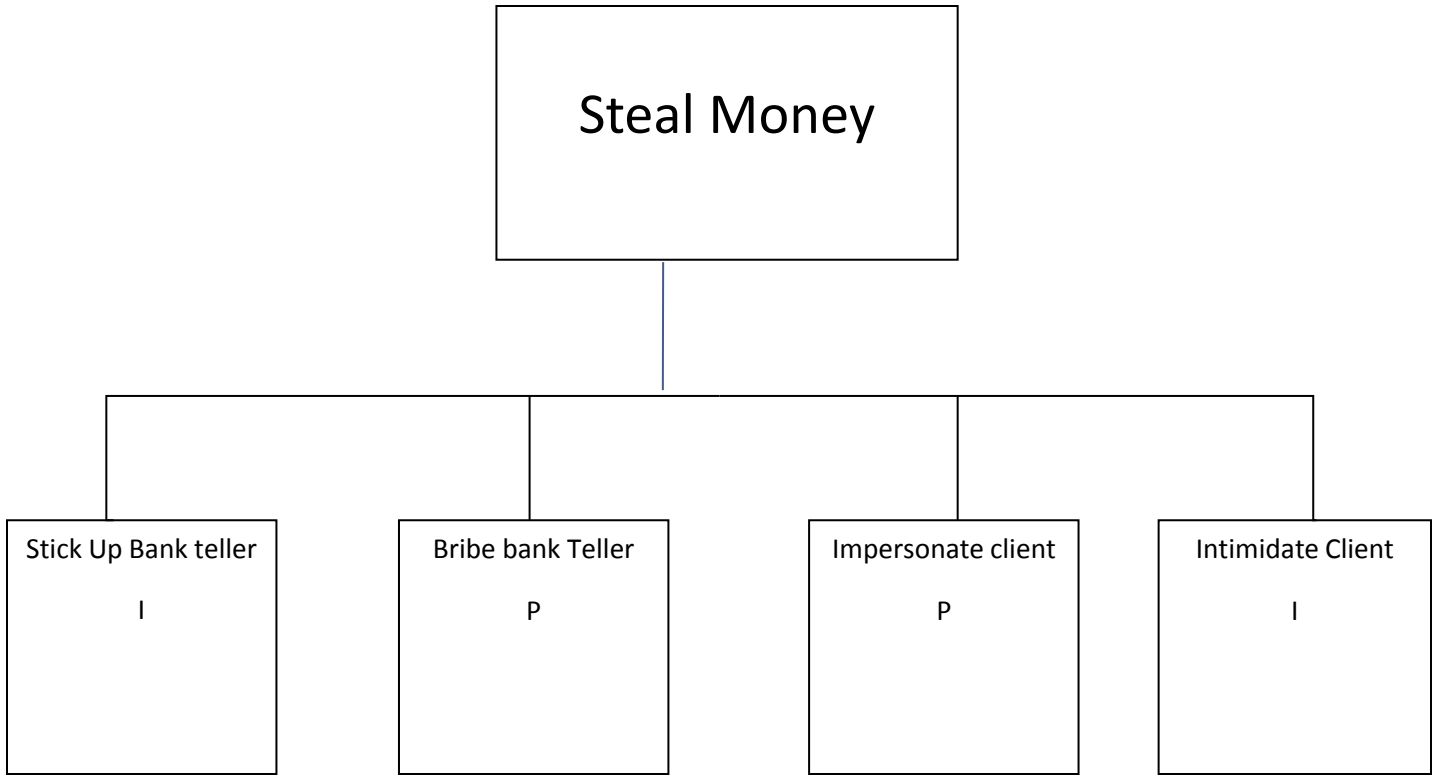
Social Network

- Build one using Social Network Platform.
- Elgg Social Networking Engine
- Create simple profile to mimic real social network

Attack centric Approach

- Focuses on the identification of all possible access points to the system and the possible adversary aims.
- Uses attack trees to show how and why the security of a system can be compromised.

Attack Tree


Steal Money
Stick Up Bank teller
I
Bribe bank Teller
P
Impersonate client
P
Intimidate Client
I

Research Questions

- Can threat models be used from an attackers point of view?
- How good is the Microsoft threat modeling tool in exposing threats from attack centric approach as opposed to Sensepost model from Software centric approach?

Microsoft STRIDE threat model

- Use Microsoft STRIDE model to identify systems vulnerability.

Attack grouping in STRIDE

- STRIDE model groups attackers aim into one or more of the following groups
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of services
  - Elevation of privileges

Restricting the scope

- To limit the scope of our project, we will put our focus on OWASP ten most critical web application security.
- Two security risk each (Attack centric).

Division

Rotondwa	Linda
Insecure direct object references	Injection
Invalidated redirects and Forwards	Cross-Site Scripting

Insecure direct object references

- A developer exposes a reference to an internal object, (file, directory or database key)
- I will try to manipulate these reference so that I can get access to some internal data.
- Can compromise all the data that can be referenced.
- E.g http://www.12robots.com/getfile.cfm?filename=jasonsLittleBlackbook.txt

Invalidated redirects and Forwards

- Links invalidated redirect and tricks the user into clicking it.
- Redirects the users to other pages and websites or use internal forwards
  - May attempt to install malware
  - Trick the user into disclosing passwords and other sensitive data.

Injections

- "From an attack centric perspective, is the software centric approach used by Sensepost (Sanele's) effective in mitigating SQL ...attacks?"
- Most common vulnerabilities (OWASP, 2010)
- Types : SQL, OS, LDAP
- Untrusted data is sent to an interpreter as part of command or query.

Technical Impacts

- Data corruption or loss
- Lack of accountability
- Denial of Service attack
  - Service Crashing.
  - Service Flooding.

Business Impacts

- Data could be stolen, modified or deleted.
- Reputation harmed .
- Profit loss for business.

Cross-Site Scripting (XSS)

- Number 2 (OWASP, 2010)
- Application takes untrusted data and sends to a browser without proper validation and escaping.

Technical Impacts

- Execute Scripts in Browser :

- Hijack user sessions
- Deface websites
- Insert hostile content
- Redirect users

Business Impacts

- Spread from victims browser to other users.

  Case study : Sammy XXS Worm which carried a payload that will display " but most of all, Sammy is my hero".
- View infected profile, payload will be planted on their page.
- Execution of payload resulted in an automatic "Friend Request" to the author.

Research Questions

- Are threat models helpful in preventing attacks in a system?

- How successful are these models in identifying the threats in a system

Background work

- Open Web Application Security Project (10 most critical web application security risks)
- Microsoft STRIDE model to categorize threats (injection, cross-site scripting, Insecure Direct object reference)
- Attack trees (that hackers use to attack the system)

Background work

OWASP 10 most critical security risks

- Injection
- Cross-Site scripting
- Broken Authentication
- Insecure Direct Object Reference
- Cross-Site Request Forgery
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL access
- Insufficient Transport Layer Protection
- Invalidated Redirects and Forwards

Software Centric Approach

- The software centric approach:
  - Evaluates the system's design and attempts to step through a model of the system checking for attacks against each element of the model.
  - Applying security only once during development might allow for some vulnerabilities to be undetected.

Software Centric Approach

- Use the SensePost Threat modeling tool
  - AIM: Look for vulnerabilities and threats in the social network
- I will use the threat modeling tool to identify attacks (injection, cross-site scripting, Insecure Direct Object Reference, Invalidated Redirects and Forwards) on the social network

Why SensePost threat model

sensepost

- Is a hybrid approach, a combination of attack centric, software centric and asset centric (highly flexible)

Evaluating the Solution

- Apply SensePost threat modeling tool on the social network identifying threats and vulnerabilities
- I will use the OWASP categorisation to prioritise and design solutions to prevent the vulnerabilities from being exploited.
- Then will let Linda+ Rotondwa attack the social network again. To see if this threat modeling tool will prevent these attacks. (answer to Q1)

Conclusion

- We will use the two threat models to they identify vulnerabilities in a the social network
- Then compare the two threat models (see if they identify the same threats and vulnerabilities, also which is better
- Write a solutions to countermeasure attacks identified on the social network

Deliverables

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

Risks associated to the project

- Not meeting project milestone

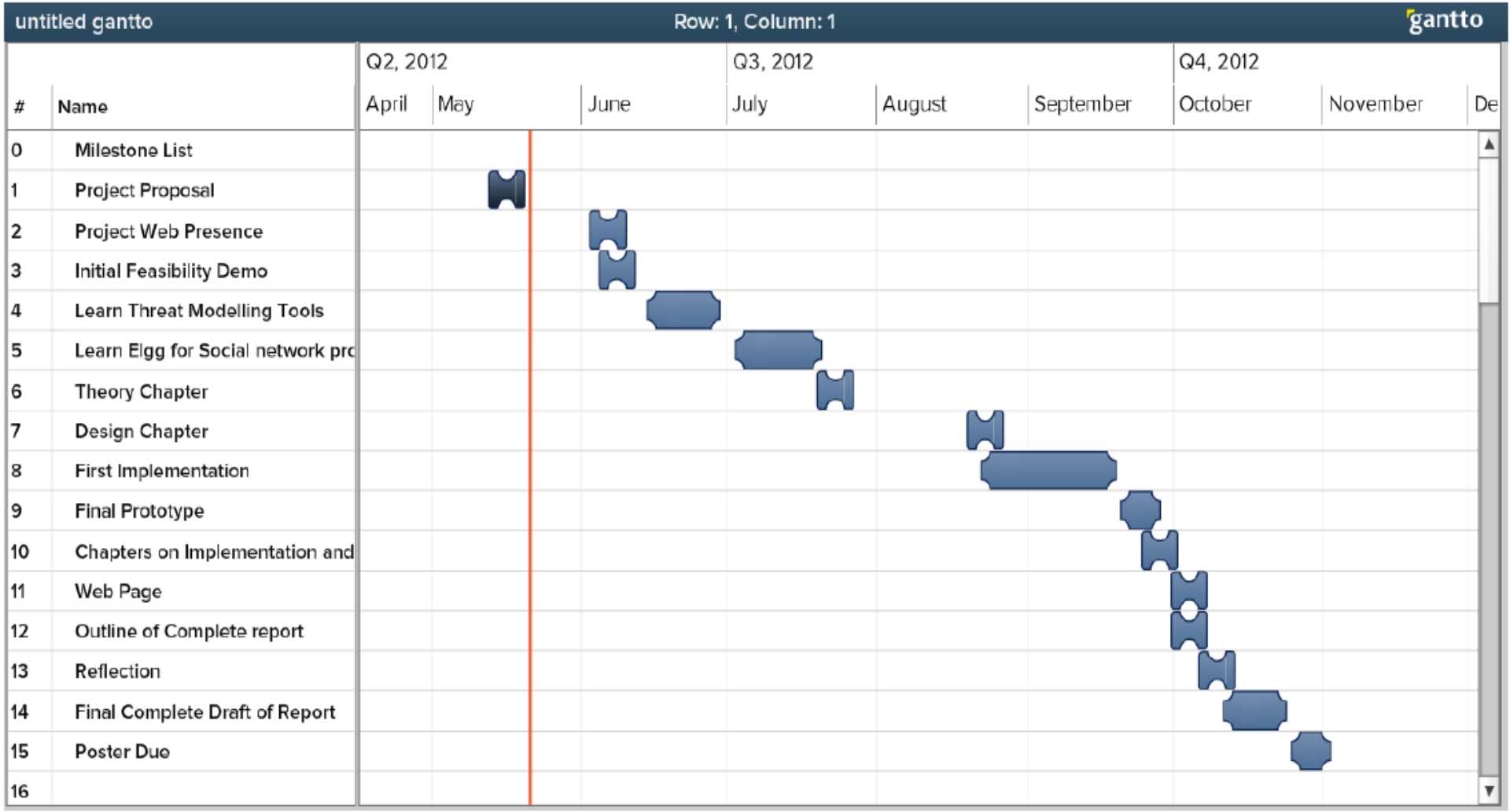
  Impact: May affect future tasks that need to be done because less time will be allocated to them which might cause the project fail.

- Member leaves the group

  impact:

- Knowledge of subject

Gantt Chart


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 pro
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

THANK YOU

?