A

Project Report On

SOCIAL ENGINEERING ATTACK BY PROFILE HIJACKING AND USING HUMANS AS BOTNETS

Submitted By

Mayank Jain	**B8058578**
Rahul Patil	**B8058598**
Anjali Shira	**B8058622**

Under the guidance of

Prof. S.C. Dharmadhikari

In partial fulfilment of

Bachelor of Engineering

[B. E. Information Engineering]

[May 2012]

AT

Department of Information Technology

Pune Institute of Computer Technology

Dhankawadi, Pune 411043

Affiliated to

University of Pune

Pune Institute of Computer Technology

Department of Information Technology
Dhankawadi, Pune 411043

CERTIFICATE

This is certify that the Dissertation entitled **"Social Engineering Attack By Profile Hijacking and Using Humans as botnets",** submitted by **Mr. Mayank Jain** is a record of bonafide work carried out by him, in the partial fulfilment of the requirement for the award of Degree of Bachelor of Engineering (Information Technology) at Pune Institute of Computer Technology, Pune under the University of Pune. This work is done during year 2011-2012, under our guidance.

_____

(Prof. S.C. Dharmadhikari)

Project Guide

_____ _____-

Prof. Emmanual M. Dr. P. T. Kulkarni

HOD, IT Department **Principal PICT**

Examination:

Examiner _____

Date:

Acknowledgements

I am profoundly grateful to **Prof. S.C. Dharmadhikari** for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion.

I would like to express deepest appreciation towards **Dr. P. T. Kulkarni**, Principal PICT, Pune, **Prof. Emmanual M.** HOD Information Technology Department and **Prof. Manish R. Khodaskar** (Project Coordinator) whose invaluable guidance supported me in completing this project.

I am particularly grateful to **Dr. Navin Kabra** (Punetech) who allows me to work in the company.

At last I must express my sincere heartfelt gratitude to all the staff members of Information Technology Department who helped me directly or indirectly during this course of work.

Mayank Jain
Rahul Patil
Anjali Shira

CERTIFICATE

This is to certify that the project report entitled

Social Engineering Attack By Profile Hijacking and Using Humans as botnets

Submitted by

Mayank Jain B8058578
Rahul Patil B8058598
Anjali Shira B8058622

is a bonafide work carried out by them with the Sponsorship from ————————- under the supervision of Mr. ..... and has been completed successfully .

(Mr. .....)
(Designation)
External Guide

Place : Pune
Date:

Contents

List of Figures

Chapter 1

Introduction

1.1 Need

1.1.1 Social Engineering

Social Engineering is the act of manipulating a person to take an action that may or may not be in the targets best interest. This may include obtaining information, gaining access, or getting the target to take certain action[5]

1.1.2 Current Scneario

Businesses spend a significant portion of their annual information technology budgets on high-tech computer security. But the firewalls, vaults, bunkers, locks and biometrics those dollars buy can be pierced by attackers targeting untrained, uninformed or unmonitored users. Humans are the weakest link in any security system, according to KL-based organizers of the Hackers Halted Asia Pacific 2009 conference.[6]

The chief minister of Malacca, Datuk Seri Haji Mohd Ali Bin Mohd Rus- tam, said there is no perfect system in the world. Even if you have the best security devices and softwareyour organization still relies on humanswho are the weakest link in any security system. Public education and awareness is essential.

Figure 1.1 is a Data Security Breach Statistics of 2008 revealing that Malicious Insider and Careless/Untrained Insider is a bigger threat than an outside cracker.

Also, in the age of Social Networking Sites like Facebook, Twitter, Linkedin, Google+ information of companies internal hierarchy structure, employees,

personal information is readily available online for the information gathering phase to breach companies security perimeter by various social engineering ways like phishing links, Trojans, Backdoors, Password guessing, breaking security questions etc.

Is it possible to break into the circle of friends network on social networking sites and make them reveal certain information about them which can be used further to infiltrate the security perimeter of a company?

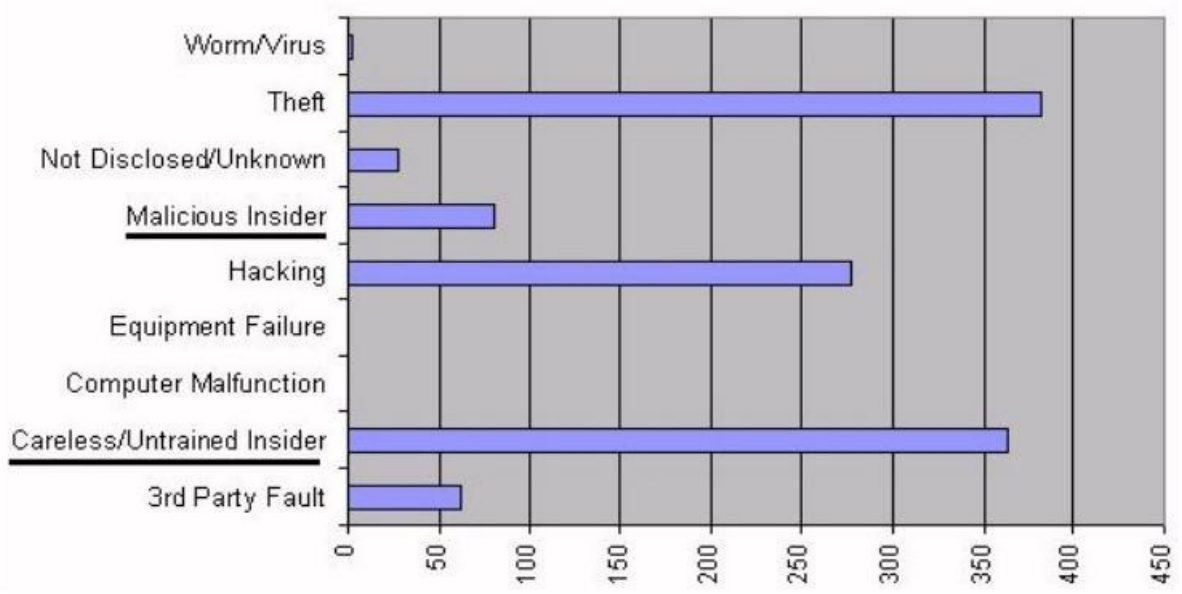

Figure 1.1: Figure 1.1: Data Security Breach Statistics of 2008

Our project is designed to answer this Question and provide a Proof of Con- cept that Yes, it can be done and without even raising any suspicion on the target for a long time.

1.2 Basic Concept

In this project we will use two main concepts:

1.2.1 Profile Hijacking

In Profile Hijacking, we will impersonate the target(s) profile on Social Net- working Sites like Facebook and use their identity to infiltrate the network of other targets friend to fit in the group. Profile Hijacking is important, to use them to reveal certain information without their knowledge.[2]

1.2.2 Using Humans as Botnets

We studied many AI based Chat Bots that are available on the web and we found that Using Chat Bots to chat with humans for Social Engineering Attack is not feasible as Humans detect that the other person is not a human but a program and hence the attack fails even before it is launched.[4]

Since developing a fully convincing AI based Chat Bot is not possible consid- ering the Scope, we will use another human to do the talking with our target while we sit in between, watch and modify the conversation towards the conversation which would reveal certain information which we are interested in.[1]

1.3 Application

Some of the best tools for fighting social engineering attacks are security awareness training and social engineering testing. The effectiveness of these controls will vary based on the quality of their

implementation, including follow-up and retraining.

Social engineering testing, by its very nature, can be difficult to conduct without third-party assistance. One option is to engage an information secu- rity organization to conduct testing. The testing can uncover areas in which an organization is most vulnerable so that risk can be assessed and mitigation strategies can be formulated and implemented.

Rolling social engineering testing into a larger security penetration engage- ment can reduce the cost of the social engineering component, says Jim Patterson, director of consulting for Rapid7.[6]

Main Application of this Project is to develop a tool that will aid in Do- ing Social Engineering Testing on Companies Employees, also it will provide as a live demonstration to employees under training on how social engineer- ing can be done and how by being cautious one can prevent serious damage not only to the company but also to their private life.

Chapter 2

Literature Survey

2.1 Towards Automating Social Engineering Using Social Networking Sites

2.1.1 Summary

In this paper, we saw the use of artificial intelligence to create a chat bot to do the automatic social engineering attack via social networking sites. Experiments were done on a small group of people on facebook.

2.1.2 Advantages

- Automatic tool, minimal input required from the user.
- If perfected, could be the best way to automate social engineering attack.

2.1.3 Disadvantages

- Fails to convince that the chat bot is a real human.
- Has no input of real world information.
- Chat algorithm is hard coded using regular expressions.
- No real world testing because of ethical issues.
- Building a real world chat bot is out of scope.

2.2 All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks

2.2.1 Summary

Presents a novel concept of profile hijacking and cloning, which laid the foundation for the proposed idea.

2.2.2 Advantages

- Works with all social networking sites which has no authentication mechanism of who you say is who you are in real world.
- Very Easy to do, as most of the data required is already available.

2.2.3 Disadvantages

- Does not give us information which is not available directly.
- Impersonating or Faking a human identity is a punishable act.
- Real world testing has ethical issues.

2.3 Honeybot, Your Man in the Middle for Automated Social Engineering

2.3.1 Summary

This paper presents the basic idea we can do man in the middle attack on two users. The testing was done on public IRCs but was suggested that it can be done by using profile hijacking on a social networking sites like Facebook.

2.3.2 Advantages

- Results of success is much higher than by using artificial intelligence via a chat bot.
- Easy to build compared to building artificial intelligence.

2.3.3 Disadvantages

- Required gender conversion in IRCs chat when impersonating a different gender.
- Testing was done on IRCs which is not targetted information gathering.

2.4 Eight Friends Are Enough Social Graph Approximation via Public Listings

2.4.1 Summary

Presents a novel idea of Publically available data of users on social networking sites. Also presents the idea of Dominating Sets. It was also mentioned that the facebook friends public data policy keeps changing, before it was 10 friends than it became 8 and now again its back to 10.

2.4.2 Advantages

- Avoids detection by Facebook.
- Presents a novel idea of using Dominating Sets.

2.4.3 Disadvantages

- Is not succesful in the current scenario where users are security concious.
- Has very low sucess rate as per our experiments.

Chapter 3

Proposed Work

3.1 Problem Statement

To develop a tool which can be used for automated social engineering attack on users of social networking sites using profile hijacking and man in the middle attack. Also test the tool via modified version of Turing test at basic conversation level

3.2 Passive Information Gathering Module

3.2.1 Social Networks

A social networking service is an online service, platform, or site that focuses on building and reflecting of social networks or social relations among people, who, for example, share interests and/or activities and people with similar or somewhat similar interests, backgrounds and/or activities make their own communities. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services.

According to ComScore, up to end of November 2011:[7]

Worldwide	Unique Visitors	Percentage
Facebook.com	792,999	55.1%
Twitter.com	167,903	11.7%
LinkedIn.com	94,823	6.6%
Google Plus	66,756	4.6%
MySpace	61,037	4.2%
Others	255,539	17.8%
Total	1,438,877	100%

Some statistics about Facebook from based on Alexa estimates, as of 20/04/2012 :-

daily page views 8.4 billion

daily visitors 650 million

views per visitor 12.9

site rank 2nd

traffic fraction 0.45% 1 in 220 of all web traffic

Your text explaining your project [**?**] contd explaining
This text is bold

3.3 Facebook Chat Attack Module

References

[1] *Honeybot, Your Man in the Middle for Automated Social Engineering*;Tobias Lauinger, Veikko Pankakoski, Davide Balzarotti, Engin Kirda; EURECOM Sophia-Antipolis, France. LEET10 Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats.

[2] *All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks*; Leyla Bilge, Thorsten Strufe, Davide Balzarotti, Engin Kirda EURECOM Sophia Antipolis, France. WWW 09 Proceedings of the 18th international conference on World Wide Web.

[3] *Eight Friends Are Enough Social Graph Approximation via Public Listings*; Joseph Bonneau, Jonathan Anderson, Frank Stajano, Ross Anderson. SNS 09: Proceedings of the Second ACM EuroSys Workshop on Social Network Systems.

[4] *Towards Automating Social Engineering Using Social Networking Sites*;Huber, M.; Kowalski, S.; Nohlberg, M.; Tjoa, S.; Computational Science and Engineering, 2009. CSE 09. International Conference.

[5] Social Engineering : The art of Human Hacking

[6] Link Name
`http://goliath.ecnext.com/coms2/gi_0199-7186209/ The-human-element-the-weakest`

[7] Market Share of Social Network Sites
`http://techcrunch.com/2011/12/22/googlesplus`