CS563: Advanced Computer Security
Research Proposal

Cassandra Jacobs and James Smith
csjacobs2@illinois.edu
smith152@illinois.edu

October 10, 2016

Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

1 Introduction

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

2 Background

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

3 Related Work

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language. [**peskin1995introduction**]

4 Proposed Approach

To achieve our goal in helping to protect the scope of a user's posted content on Facebook we propose a two pronged approach. The first prong of this approach is a Facebook application that will intelligently control the audience of a user's post based off of security guidelines set in place by the user. When a user downloads our chrome extension for the first time he/she will be prompted to perform an initial setup. The setup will consist of the user creating different mappings or rather rules that link a given Friend List (e.g. Family) to a given category and action (e.g. politics, do not share). The categories will be predefined to begin with but the application will allow for custom categories to be created by the user later on. The application will be using the Graph API provided by Facebook to grab the valid set of Friend Lists for the user[1].

Once a user has established an initial set of rules they will then be presented with a dialog box. That dialog box will allow them to type in the contents of a post. It will also display the set of Friend Lists that the post will be visible to, a button to validate that list, and a button to post the content. When the user clicks 'post' the content will be published out to the shown Friend Lists. That list will be generated by our algorithm upon the user clicking the validate button. The algorithm to generate that list consists of two main parts: a weight function that assigns categories and their given weights to the given content and a decision function that takes the assigned categories and the user's rules to spit out a

recommend set of Friend Lists. Here the categories for a post will be assigned using a dictionary that will be preloaded with words that are mapped to a given category.

The second prong is a set of guidelines that will outline best practices for the user to take when setting up security zones in Facebook through the use of Friend Lists. This will take the form of a set of rules to be given to the user that will be used to assess the risk of a given friend based off of the information disclosed on the friend's profile[2]. Facebook no longer allows this information to be collected through the APIs; therefore this piece of our research has become a more manual process for the user. The guidelines will also include suggestions for different over-arching social privacy zones that are clearly defined and will get the user up and running quickly. The Friend Lists defined here will then be used by the application described above when a user is requesting advice for the specific Friend Lists a post should be sent to.

5 Research Plan

The overall goal of this research is to establish a mechanized way to intelligently protect the dissemination of a user's Facebook posts to a specific group of friends that is visible and transparent to the user in a simple and easy to understand fashion. Through the use of our application the user will be alleviated from having to tediously choose what friends a given post will be visible to and can instead follow the recommendations provided to them by the app. The application will provide a clean and easy to read interface that gives full transparency to the user on who his/her posts will be visible to. This functionality will help keep the posted content of a user confined to parties that have been verified as trustworthy for the given category of the content.

The second goal of this research is to provide a clear recommendation for users to use when setting up Friend Lists in Facebook and to provide them with the tools needed to use these lists as personal privacy security zones. The goal here is to educate users on how to be more conscientious of their social information and how to prevent privacy leaks into the social web. This will accomplished through the startup rules that will be laid out in the guidelines for creating Friend Lists (security zones) and how to best use these lists when posting content.

The two goals above have been presented separately but in all actuality they are closely related. The efficacy of the primary goal is very much dependent on the successful setup of meaningful and accurate Friend Lists. That is why making the manual part of our research process easy to implement by the user is important. We would like to automate this process but due to restrictions on the information that is publicly available from the Facebook Graph APIs this is not feasible at the current time. The guidelines that we will lay out could later be considered for developing an automated protocol for bucketing users into security zones.

References

[1] Jesse Weaver and Paul Tarjan. "Facebook linked data via the graph API". In: *Semantic Web* 4.3 (2013), pp. 245–250.

[2] Kambiz Ghazinour, Stan Matwin, and Marina Sokolova. "YOURPRIVACYPROTECTOR, A recommender system for privacy settings in social networks". In: *arXiv preprint arXiv:1602.01937* (2016).