Kennesaw State University

DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education, Research and Practice

2016 KSU Conference on Cybersecurity Education, Research and Practice

“Not All FRIENDs are Equal”: Friendship Classification for Defending against Social Engineering Attacks

Munene W. Kanampiu
North Carolina A & T State University, wkanampiu@yahoo.com

Mohd Anwar
North Carolina A & T State University, manwar@ncat.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ccerp

 Part of the Information Security Commons, and the Technology and Innovation Commons

Kanampiu, Munene W. and Anwar, Mohd, ""Not All FRIENDs are Equal": Friendship Classification for Defending against Social Engineering Attacks" (2016). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 3.
https://digitalcommons.kennesaw.edu/ccerp/2016/Practice/3

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Abstract

Social engineering is a serious security threat to Online Social Networks (OSNs). Identity theft, impersonation, phishing, and deception are some of the social engineering-based attacks that exploit vulnerabilities of interpersonal relationships of online users. As a result, relationships in OSNs need to be thoroughly examined. In this vein, we propose a relationship categorization model to evaluate relationship strength based on graph-theoretic properties and social network analysis (SNA) methods. For example, in Facebook, users may be categorized into close-neighbors, distant-neighbors, celebrities (influential by admiration), authority (influential by power), and loners. Close-neighbors category will help identify a set of trustworthy actors while an actor of distant-neighbors category should not be trusted as much as the former. A celebrity category actor should be more accountable, while a loner category actor will probably be less accountable. This type of categorization will help users engage in proper cybersecurity behaviors to avoid social engineering-based attacks.

Disciplines

Information Security | Technology and Innovation

This event is available at DigitalCommons@Kennesaw State University: https://digitalcommons.kennesaw.edu/ccerp/2016/Practice/3

INTRODUCTION

Online social networks (OSNs) provide support for forming chains of relationships. For example, if T befriends X who in turn befriends Y then Y becomes a friend of T by way of X. Because of this friendship transitivity property such friendship chains can grow long with little if any participants' control. Unfortunately this long chain of relationships brings with it an increased danger involving user data security especially data privacy. For example, by exploiting the network's friend recommendation feature an ill-intended Facebook user can reach out to a large pool of unsuspecting users to conduct a social engineering attack. Unlike physical entities, e.g., organizations where data security enforcement can be applied through policy and accountability, the same is unlikely in OSNs. Even for organizations, social engineering could still pose a substantial problem even for disciplined employees since it involves the attacker capturing such employees' trust for waging the attack. Such reasons, coupled with the increase in data breach cases,

(E.g. the 2012 LinkedIn data breach case http://thehackernews.com/2016/05/linkedin-account-hack.html) make online data privacy threats increasingly worrisome. As a result, users' interpersonal relationships in OSNs need to be examined to curb social engineering attacks. Such action would not only benefit OSN users but also, if incorporated by organization, would complement their existing security controls.

The question addressed in our research is: *can we develop a mechanism that uses social network analysis (SNA) to extract network properties of an OSN user to aid in avoiding a potential social engineering attacker in the OSN?*

We propose developing algorithms that can aid an online social network (OSN) user to perceive social engineering posture of a fellow user based on the latter's network properties. The algorithms will categorize an OSN users' interpersonal relationships considering graph-theoretic centrality properties of nodes in their network (e.g., betweenness, closeness, and eccentricity). The tool will be able to categorize network actors into authority, celebrity, and loner classes, which according to literature (e.g., Algani and Xu (2013), Festinger, and Carlsmith, (1959), Mitnick, Williams, and Wozniak, (2002), Weatherly, Miller, and McDonald, (1999)) can be relied upon in inferring social behavior such as social engineering.

APPROACH

Our approach starts with extracting node and edge information of a social graph and defining its nodes characteristics based on their centrality. This is

followed by (a) translating these characteristics in graph theoretic and (b) inferring the node behavior based on studies in the literatures.

We implement a prototype of our approach through a Java program simulation that takes as input the nodes of a social network and classifies them into either celebrity, loner, or authority based on their extracted network characteristics. From this classification the program then infers these nodes status as potential social engineering attacker based on the studies in the literature.

RESULTS

As seen in Fig 1, our simulation results include the display of a sociomatrix showing all the vertices paths, sum of all shortest paths for each vertex of graph, number of all shortest paths of graph, closeness centrality of each vertex of graph, radius and diameter of graph, average betweenness centrality of graph, category of each vertex of graph (celebrity, loner, authority), and a warning of any possible social engineers.

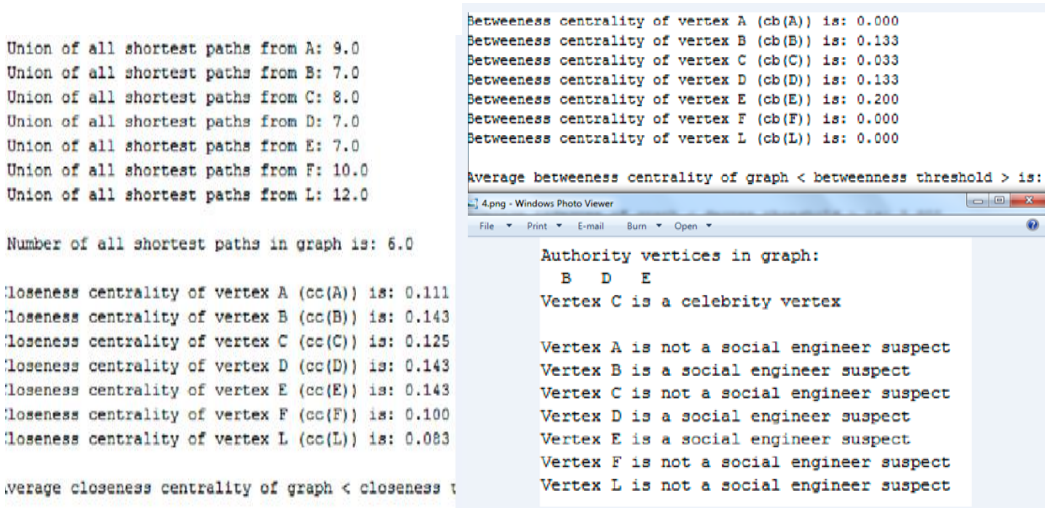

Fig. 1. A SNAPSHOT OF OUR SIMULATION OUTPUT WITH BLUEJ

RESEARCH LIMITATIONS

We observed that social graphs in OSNs can grow quickly. Just an extra one member added to the network n nodes can add up to n-1 new edges. For this reason we had to limit our simulated network size to just a few nodes. We plan to test a larger number and more realistic group of vertices from a real life OSN in order to represent a more real worldly situation.

REFERENCES

Algarni, A., and Xu, Y. "Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models," International Journal of e-Education, e-Business, e-Management and e-Learning. 2013, (3:6), p 7.

Festinger, L. and. Carlsmith, J. M. “Cognitive consequences of forced compliance”. The Journal of Abnormal and Social Psychology, 1959. 58(2), 203.

Mitnick, K. D. Williams, L. S. and Wozniak, S. “The art of deception” 2002.

Network Centrality [PDF Document]. Retrieved from http://cs.brynmawr.edu/Courses/cs380/spring2013/section02/slides/05_Centrality.pdf

Weatherly, J. N., Miller, K,.and McDonald, T. W. "Social influence as stimulus control." Behavior and Social Issues (1999)