A Risk Analysis Framework for Social Engineering Attack Based on User Profiling

Ziwei Ye, State Key Laboratory of Mathematical Engineering and Advanced Computing, China
Yuanbo Guo, State Key Laboratory of Mathematical Engineering and Advanced Computing, China
Ankang Gu, State Key Laboratory of Mathematical Engineering and Advanced Computing, China
Fushan Wei, State Key Laboratory of Mathematical Engineering and Advanced Computing, China
Ruijie Zhang, State Key Laboratory of Mathematical Engineering and Advanced Computing, China
Jun Ma, State Key Laboratory of Mathematical Engineering and Advanced Computing, China

ABSTRACT

Social engineering attacks are becoming serious threats to cloud service. Social engineering attackers could get Cloud service custom privacy information or attack virtual machine images directly. Existing security analysis instruments are difficult to quantify the social engineering attack risk, resulting in invalid defense guidance for social engineering attacks. In this article, a risk analysis framework for social engineering attack is proposed based on user profiling. The framework provides a pathway to quantitatively calculate the possibility of being compromised by social engineering attack and potential loss, so as to effectively complement current security assessment instruments. The frequency of related operations is used to profile and group users for respective risk calculation, and other features such as security awareness and capability of protection mechanism are also considered. Finally, examples are given to illustrate how to use the framework in actual scenario and apply it to security assessment.

KEYWORDS

Authority, Cloud Security, Network Security Assessment, Operating Frequency, Risk Analysis, Social Engineering, User Profiling, Vulnerability

INTRODUCTION

With the development of cloud security, social engineering attacks have been paid more and more attention because of the outstanding capability of penetrating cloud service which is difficult to the conventional techniques. However, the awareness for social engineering of cloud service customs and providers is relatively low (Krombholz et al., 2015; Kuyoro et al., 2011). Improving awareness and ability of prevention to social engineering attacks is of great significance for the accuracy of cloud security assessment and anti-attack capability.

Current researches on social engineering attacks are mainly of classification and qualitative analysis based on known cases. Chandra et al., (2015) treats social engineering attack as a feature of APT and discuss how to deploy defense system in cloud. A case is given to show how to run a malicious

DOI: 10.4018/JOEUC.2020070104

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
virtual machine in Amazon EC2 by social engineering (Meer et al., 2009). Some researchers summed up the existing social engineering attack classification achievements (Foozy et al., 2011) and frequently used social engineering malwares (Abraham & Chengalur-Smith, 2010). In Mouton et al. (2014) the writers extracted a social engineering attack framework based on Kevin Mitnick’s book “The art of deception: Controlling the human element of security” (Mitnick & Simon, 2001). A multi-layered model was presented for assessing possible social engineering exploits (Jaafor & Birregah, 2016). How educational and technological means can be used to reduce social engineering risk which the social media users faced was discussed (Tayouri 2015). Sheng et al. (2010) used a roleplay survey instrument to assess user’s vulnerability of phishing. However, there is little quantitative evaluation of possibility of being compromised by social engineer attacker and potential loss expect (Sheng et al., 2010), so that it is impossible to compare risks between social engineering attacks and technical attacks without social factors. Social engineering attack risk couldn’t be taken into account in network security assessment, resulting in negative effects on network reinforcement.

User profiling is an important application of big data. By adding descriptive tags to users, it can depict users from multiple dimensions, and reflect users’ behaviors, hobbies, jobs, etc. In recent years, user profiling has been widely used in network security research. An automated insider threat detection system was realized user profiling (Legg et al., 2017). Nurse et al. (2016) the writers studied how to distinguish online identify falsification. A framework was proposed to analyze users’ attributes and recognize accounts which belong to the same user from different social networks (Monika et al., 2016). As social engineering attack is the exploitation of human weaknesses, and the object of user profiling is also human, user model can be built by user profiling to find possible social engineering attack surface. It will be more pertinence comparing with techniques whose objects are networks or computers.

Aiming at the problem that existing network security assessment techniques cannot quantify the risk of social engineering attack, the authors present a risk analysis framework for social engineering attack based on user profiling. By extracting the relevant features, the possibility of being compromised and potential loss caused by social engineering attack could be quantified. The framework can be applied to various network security assessment instruments to optimize results and guide the employment of protection mechanisms against social engineering attack.

**SOCIAL ENGINEERING VULNERABILITY AND RISK**

Social engineering attacks are becoming more and more complicated with the development of information technology. According to the classification summary on social engineering attacks (Foozy et al., 2011), it is recognized that social engineering attacks can be classified into two categories according to their correlation with computer and network: human-based attacks and technical-based attacks. Aiming at introducing social engineering risk analysis into network security assessment, the framework mainly directs at the technical-based social engineering attacks which are more dependent on computer and network. Within the instances of technical-based social engineering attacks, related operation frequencies of phishing, waterholing, malware and pop-up windows are obvious and easy to extract by user profiling. On this account the authors choose the above four attack types as objects. In future works, our work would be extended to human-based attacks, and other emerging attacks.

**Typical Social Engineering Attacks**

*Phishing*

Phishing is one of the most common forms of cyber-attacks. Usually the attacker sends e-mails or SMS with malicious link or attachment containing malicious code, to induce victims to open attachment or click on the link, so as to realize remote control or get information.
A Proposed Framework Factors of the Acceptance of Recommender Systems in E Learning for Saudi Universities
www.igi-global.com/chapter/a-proposed-framework-factors-of-the-acceptance-of-recommender-systems-in-e-learning-for-saudi-universities/173968?camid=4v1a

Knowledge Appraisal and Knowledge Management Systems: Judging What We Know
www.igi-global.com/chapter/knowledge-appraisal-knowledge-management-systems/38084?camid=4v1a