Article Review #1: Social Engineering in Cybersecurity

by

Galen Cole

A Review Paper

Submitted to CYSE 201S

Old Dominion University

Article Review #1

October, 2024

Introduction

The paper “Defining Social Engineering in Cybersecurity” addresses a significant issue in modern cybersecurity, focusing on the conceptual inconsistencies surrounding social engineering. The authors seek to resolve this issue by asking: What are the key conceptual inconsistencies in existing definitions of social engineering? and How can a more precise definition improve understanding and defense against these attacks? These questions aim to clarify the conceptual boundaries of social engineering while exploring the historical evolution of the term. By offering a new, precise definition, the paper strives to bridge the gap in understanding and defense and mitigate the overgeneralization of the term within cybersecurity.

Social Science Principles and Marginalized Groups

The significance of human vulnerabilities is often underestimated or not fully understood in cybersecurity. The article explores human vulnerabilities, psychological manipulation, and social interactions, all crucial to understanding cybersecurity risks. These principles highlight the importance of human behavior in cybersecurity and reinforce the need to understand social dynamics concerning technology use. Additionally, human factors engineering and psychology principles are paralleled in how attackers manipulate user behaviors, such as trust, in social engineering attacks. Marginalized groups, particularly those with limited access to cybersecurity education and resources, are disproportionately vulnerable to these attacks, which exacerbate existing social inequalities. The study stresses the need for more inclusive defense mechanisms to protect these groups.

Identifying Further Class Concepts

Several concepts already discussed in class are evident in this article, such as cyber victimization, where users unknowingly induce risk. The article emphasizes how social engineers exploit human behavior and how this aligns with victimization, showing that individuals with low self-control or high risk-seeking behavior are particularly susceptible. Cybersecurity, as an essential safety need, is central to social engineering, and the manipulation of this need mirrors Maslow's theory, where attackers exploit individuals' fear of losing security. Exploring human vulnerabilities connects directly to behavioral and cognitive theories of cyber offending, focusing on how social engineers exploit weaknesses in human psychology.

Research Methods and Findings

The paper utilizes a comprehensive literature review, analyzing existing definitions, case studies, and reports to trace the conceptual evolution of social engineering. The authors collect data through comparative analysis, using five tables that assess definitions based on clarity, scope, and precision. The study identifies that previous definitions of social engineering were inconsistent, overgeneralized, and unclear, leading to confusion in cybersecurity defenses (Defining Social Engineering in Cybersecurity, p. 2). Ultimately, the authors argue that a more precise and unified definition will enhance theoretical understanding and practical application in combating social engineering.

Conclusion

The study's primary contributions are the introduction of a refined definition of social engineering and a systematic analysis of its conceptual evolution. By addressing gaps in understanding and providing a more straightforward framework, this research strengthens the study of social sciences within cybersecurity. It highlights the critical role of social vulnerabilities in attack vectors, contributing to developing more effective, human-centric defenses against cyber attacks.

Works Cited

Z. Wang, L. Sun and H. Zhu, "Defining Social Engineering in Cybersecurity," in IEEE Access, vol. 8, pp. 85094-85115, 2020, doi: 10.1109/ACCESS.2020.2992807.

https://ieeexplore.ieee.org/abstract/document/9087851