WIRTSCHAFT
HOCHSCHULE MAINZ
UNIVERSITY OF
APPLIED SCIENCES

Evaluation of the Adherence of “Enhancing Predictive Analytics for Anti-Phishing by Exploiting Website Genre Information” to the Design Science Guidelines

Hochschule Mainz
University of Applied Sciences
Fachbereich Wirtschaft

Vorgelegt von:	Luise Bauer
	Matrikel-Nr: 940033
	Lars Jung
	Matrikel-Nr: 913727
Vorgelegt bei:	Prof. Dr. Gunther Piller
Eingereicht am:	15.07.2019

Table of Content

1 Introduction

1.1 Summary of given task

In the context of information systems design science plays a major role. It defines a framework for building and evaluating information systems. The approach of design science has been developed by Hevner et al. (2004) and was adopted by many other scientists for the development of new systems since then.

In this assignment the adherence of a scientific paper to the framework of design science is analyzed. The paper chosen was written by Abbasi et al. (2015) and deals with the topic of "Enhancing Predictive Analytics for Anti-Phishing by Exploiting Website Genre Information".

1.2 Summary of the research project

The paper by Abbasi et al. (2015) that will be analyzed describes the development of a new method for phishing website detection. Its objectives are to improve overall phishing website detection rates, generalizability across industries and categories of phishing attacks, performance of phishing website analysis and recommendations as well as accuracy and appropriateness of user security decisions. The study focuses on the most common categories of phishing websites which are concocted and spoof websites. "Concocted websites attempt to appear as unique, legitimate commercial entities in order to engage in failure-to-ship fraud" whereas "spoof websites engage in identity theft by mimicking legitimate websites and targeting those websites' customers" (Abbasi, et al., 2015, p. 113). Furthermore, the study discusses state-of-the-art anti-phishing methods which are lookup systems and content-based tools to develop its own genre tree kernel method for phishing website detection. The developed method is evaluated by conducting a series of different experiments.

2 Analysis according to the guidelines of Hevner et al.

In the following analysis an evaluation of the adherence of Abbasi et al. (2015) to the guidelines of design science is presented: design as an artifact, problem relevance, design evaluation, research contribution, research rigor, design as a search process as well as communication of research, according to Hevner et al. (2004).

2.1 Design as an Artifact

According to Hevner et al. (2004) “the result of design-science research in IS is […] a purposeful IT artifact created to address an important organizational problem” (p. 82). This includes constructs, models, methods or instantiations (p. 82).

The result of the study by Abbasi et al. (2015) is a new anti-phishing method achieving a more effective method regarding overall phishing website detection rates, generalizability across various industries and categories of phishing attacks and accuracy and appropriateness of user security decisions (p. 112). The authors focus on evaluating if their proposed IT artifact, a genre tree kernel-based method for detecting phishing websites, fulfills the given criteria. The aforementioned “approach leverages website genre composition and website design structure differences between legitimate and phishing websites” (p. 112). This approach emphasizes on differences in “business and operating models between legitimate and fraudulent websites” (p. 112).

In conclusion the new anti-phishing method developed by Abbasi et al. (2015) fits the definition of an artifact by Hevner et al. (2004) as it is a method aiming to improve the problem of phishing websites.

2.2 Problem Relevance

The guideline of problem relevance according to Hevner et al. (2004) requires the development of a technology-based solution to an unsolved and important business problem (p. 84).

The study by Abbasi et al. (2015) addresses the problem of phishing websites. This is not new but still a current problem. The study itself names some figures to prove the problem relevance. Numbers form Kaspersky are named, stating that phishing attacks increased by 87% from 2012 to 2013 and other scientific sources stating that phishing websites generate “billions of dollars in fraudulent revenue” (Abbasi, et al., 2015, p. 111).

To validate these statements and to check if phishing websites are still a current problem in 2019, we did some research on phishing websites as well. Current figures reveal that in December 2018 more than 45,000 phishing websites were discovered worldwide (Statista, 2019). Internet platforms, banking sector, payment services, social media platforms and online shops are mostly affected by phishing attacks (Gudkova, Vergelis, Shcherbakova, & Demidova, 2017). In Germany 1,425 cases of phishing in online banking with average damage of 4,000 € have been reported in 2017 (BKA, 2018, p. 2). Therefore, we conclude that the problem of phishing websites is still are current one and still relevant for many businesses.

But, other lookup systems and content-based tools already exist to detect phishing websites. That is why Abbasi et al. (2015) describe the shortcomings of existing methods as follows: they lack generalizability, lengthy run times are unsuitable for real-time environments and there is ineffectiveness in user environments. The new method aims to improve the usability of phishing website detection and thus aims to overcome the disadvantages of existing methods.

In conclusion, there is not only a business need for phishing website detection tools in general but also a methodological need to develop a new method to overcome existing shortcomings.

2.3 Design Evaluation

Concerning the guideline of design evaluation Hevner et al. (2004) "the utility, quality and efficacy of design artifact must be rigorously demonstrated via well-executed evaluation methods" (p. 85).

During development of the artifact appropriate research methods must be applied. Abbasi et al. (2015) used genre theory to develop the new method.

A series of experiments has been conducted to evaluate the new method for phishing website detection. A comparison with other content-based methods, existing phishing website detection tools as well as alternate genre- and tree-based methods has been conducted. Finally, an evaluation of user behavior using different anti-phishing tools, including an implementation of the proposed method, was carried out. The evaluation does not only include the construction of appropriate experiments, but the definition and application of appropriate performance measures as well. Abbasi et al. (2015) used overall accuracy and class-level precision, recall as well as F-measure to validate the developed method. Furthermore, the artifact must be tested within an appropriate context. To fulfill this requirement Abbasi et al. (2015) constructed a composition of a training data set of over 6,000 websites and a separate data set of 4,040 websites for evaluation. With this data set the new method was then applied to relevant website categories and industry sectors and compared with other content-based methods and existing tools. The evaluation revealed that the new method was more accurate in detecting phishing websites, showed a consistent performance across different website categories, had an enhanced performance and therefore led to better user security behavior.

In conclusion an extensive effort has been conducted by Abbasi et al. (2015) to rigorously evaluate and demonstrate the enhanced performance of the new method.

2.4 Research Contribution

According to Hevner et al. (2004) artifacts in design-science research must provide contributions in the areas of design artifact, foundations and/ or methodologies. These contributions can provide benefits based on novelty, generality or significance. (p. 87)

Abbasi et al. (2015) developed a new method by combining genre information and website design structure using a kernel-based classification technique. According to the knowledge of researchers, it is the largest anti-phishing benchmarking study conducted with respect to number of tools, types of phishing attacks and range of industry sectors examined. The study shows that more accurate security decision-support tools reduce user disregard rates and therefore enhance usability. Furthermore, other insights on user behavior can be derived. Although the new method improves existing tools, user-tool dissonance remains to some extent. This requires a multipronged approach, providing e.g. effective education and training.

Thus the artifact developed by Abbasi et al. (2015) creates various research contributions in the areas of design artifact, foundations and methodologies.

2.5 Research Rigor

The next guideline that is part of design-science research by Hevner et al. (2004) is about research rigor. Here “the application of rigorous methods in both the construction and evaluation of the designed artifact” (p. 87) is required.

The development of the new method is done by using different increments. It is mainly based on the construction of the tree structure for the genre tree kernel method, i.e. a folder/file structure on a server. A training data set was created for the method to learn a feature set for labeling files by genre. Next several hundred pages were tagged by independent annotators for a specific genre. A Process to label indexable files with genre information was used with different trees and tokens for different genres. Each node is classified by concatenating parent folder and filename as well as removing file extensions. These are matched against a learned feature set adding the tree to the genre label with most matches. This allows adaptation for complex structures by pruning to improve accuracy and computation times (limit maximum number of siblings in tree). To complete the process several random walk paths for trees have been created and compared by length. These steps are developed using a formal definition of the method written in a mathematical notation. This formal definition is based on variables and mathematical concepts from graph theory (trees), genre theory and kernel methods. These are combined for the new anti-phishing method, which is presented using mathematical formulas. For the evaluation, as discussed prior to this section, a series of experiments was conducted. For each experiment hypotheses were formulated and checked using a high variety of different measures including precision, recall and f-measure. Each measure, including its calculation, is presented in the appendix.

In conclusion, there is no obvious evidence to doubt the research rigor that has been carried throughout the development and evaluation of the method proposed by Abbasi et al. (2015).

2.6 Design as a Search Process

According to Hevner et al. (2004) “problem solving can be viewed as utilizing available means to reach desired ends while satisfying laws existing in the environment” (p. 88).

In the case of the development of a method for phishing website detection by Abbasi et al. (2015) the paper does not give any details regarding the development of the method. The reader solely knows that the method was created by combining genre theory and kernel-based methods and is proposed by the researchers. The origin of the requirements and development approaches is not mentioned, and the paper focuses on evaluating this proposed approach. More detailed information on any Generate/ Test Cycle cannot be found in the paper which limits the evaluation of the guideline on search process.

2.7 Communication of Research

The guideline on communication of research by Hevner et al. (2004) requires appropriate presentation of the research results for technology-oriented audience just as for management-oriented audience (p. 90).

The paper provides extensive background information on phishing website categories, phishing website detection tools including examples and their shortcomings. This helps especially management-oriented audiences to understand the basics and decisions made throughout the research process. The presentation for management-oriented audiences is mostly done in the introduction and conclusion where the implication of phishing websites on the costs for households and organizations is emphasized.

In general, the presentation focuses on technology-oriented audiences assuming the reader understands genre/ tree kernel theory and the associated mathematical backgrounds. Furthermore, a complete list of website genres that was used to construct the genre tree is included as well. By this the paper enables technology-oriented audiences to create an instantiation of the new developed and proposed method. Overall evaluation of the research approach.

In conclusion the paper by Abbasi et al. (2015) fulfills the requirements of the guideline on communication of research sufficiently.

3 Overall evaluation of the research approach

In summary, the proposed anti-phishing method is an IT artifact as defined by Hevner et al. (2004) and is designed as such. The problem of detecting phishing websites and improving user security decisions is as relevant today as it was in the past. This is due to a business need for such methods to avoid costs and expenses related to successful phishing attacks as well as a technological need for better methodologies to improve user acceptance and security decisions. The developed anti-phishing method contributes to existing research in various areas including a design artifact, foundations and methodologies. Research rigor is ensured by using various mathematical concepts in the development and definition of the anti-phishing method and experiments and statistical measures including precision, recall and f-measure in the evaluation phase. Since the artifact is already proposed at the beginning of the paper and not a result of a search process and multiple iterations the design is not done as a search process. Finally, the research results are communicated appropriately to a technical and managerial audience. Although the paper is focused on a technical audience, managerial aspects are mentioned and discussed, mostly in the introduction and conclusion. Overall the research paper adheres to the guidelines of design science as defined by Hevner et al. (2004).

References

Abbasi, A., Zahedi, F. "., Zeng, D., Chen, Y., Chen, H., & Nunamaker Jr., J. F. (2015). Enhancing Predictive Analytics for Anti-Phishing by Exploiting Website Genre Information. *Journal of Management Information Systems, 4*, pp. 109-157.

BKA. (2018). *Bundeslagebilder Cybercrime.* Retrieved June 23, 2019, from BKA.de: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

Gudkova, D., Vergelis, M., Shcherbakova, T., & Demidova, N. (2017). *Spam und Phishing im zweiten Quartal 2017*. Retrieved June 23, 2019, from Kaspersky: https://de.securelist.com/spam-and-phishing-in-q2-2017/73002/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 1*, pp. 75-105.

Statista. (2019). *Anzahl der entdeckten Phishing-Webseiten von Januar 2015 bis Dezember 2018*. Retrieved June 23, 2019, from Statista.com: https://de.statista.com/statistik/daten/studie/73876/umfrage/anzahl-der-gemeldeten-phishing-webseiten-weltweit/