Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 110 (2017) 492–497

Procedia Computer Science

www.elsevier.com/locate/procedia

The 4th International Symposium on Emerging Inter-networks, Communication and Mobility (EICM 2017)

A Multi-Agent Case-Based Reasoning Architecture for Phishing Detection

Hassan Y. A. Abutair* and Abdelfettah Belghith

Computer Science Department, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

Abstract

Security threats are becoming very sophisticated and pervasive everywhere. Phishing threats in particular has a changeable nature and short life cycle that complicates the detection process. In this paper, we introduce a Multi-Agent System (MAS) as an adaptive intelligent technique that acts on top of distributed Case-Based Reasoning (CBR) Phishing Detection Systems (CBR-PDSs) as a Phishing Detection System Architecture (PDSA) that runs on large scale globally to constitute a robust worldwide Phishing Threat Intelligence (PTI) environment. The global collaborations of PTI introduces a proactive phishing detection technique, quarantines phishing threats via global threats sharing, and minimizes users' susceptibilities to hard-to-detect spear or advanced phishing attacks. Also, combining two intelligent systems in a unified interactive architecture facilitates the prediction process, increases the accuracy rate, easily tackles the dynamic and changeable behaviors of advanced phishing threats, and minimizes the false negative rate as well. The proposed architecture illustrates the consolidated interaction between intelligent agents and distributed CBR-PDSs in a PTI framework.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Phishing Detection; Agents Technology; Case-Based Reasoning; Distributed Systems.

1. Introduction

Phishing attacks are inevitable and targeting organizations anytime and everywhere. Phishers are striving for devising new advanced phishing techniques by leveraging social engineering tactics and technology to launch their attacks. Moreover, Jakobsson and Young [1] were identified a new type of phishing attacks known as a Distributed Phishing

* Corresponding author. Tel.: +966-11-4697353 ; fax: +966-11-4696452.
E-mail addresses: habualteer.c@ksu.edu.sa and abelghith@ksu.edu.sa

1877-0509
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.06.131

Attack (DPA) that can bypass the most phishing detection techniques and defences. Advanced cyber security attacks span over different machines and gather sensitive information towards dedicated destructive attacks as most of these attacks are initiated by phishing attacks. In addition to that, users' anti-phishing immune system will never reach the point of perfection to detect and report phishing attacks as needed.

Most of phishing detection systems that work offline or online stay short to cover all the subtleties needed to draw the right conclusion about potential phishing threats by flagging them to legitimate or malicious. This because of (1) the lack of knowledge that a single phishing system can provide as phishing attacks are increasing dramatically (2) most of phishing detection techniques need a prior training to effectively detect phishing attacks. To address the above challenges, an integrated and cooperative distributed system should be existed in which, it can (1) adapt to tackle the changeable nature of phishing attacks and their complicated structures, (2) share new discovered phishing threats globally in order to avoid zero-hour phishing attacks (3) decide cooperatively and proactively on certain indecisive cases as different parties (agents) participate in making the final decision based on the knowledge they have.

In this study, we integrate our previous work that is CBR-PDS system[2] with Multi-Agent System to act as a cooperative intelligent architecture. Encompassing Multi-Agent system with the adaptive and dynamic CBR-PDS system brings a distributed phishing detection system that tackles phishing attacks on large-scale environment and allow different parties (Agents) to participate in drawing the final decision about suspicious phishing cases. We call our proposed system as Phishing Threat Intelligence.

2. Related Work

There are plenty of phishing detection studies that have been introduced to the tackle the phishing attacks locally without peers' cooperation and participation in deciding whether the current website for example is a fake website leveraged to deliver phishing attacks or not. Some Phishing attacks detections studies[3, 4] tried to detect phishing attacks as standalone systems or locally. Those systems have a high percentage of false positive and false negative because of one system decider. As phishing attacks getting sophisticated, there is a need to engage more participants to decide on a certain phishing attack or website that is there is a need to distributed phishing detection systems to deal with phishing attacks on large scale for better collaboration, prediction, and detection accuracy.

Singh, et al. [5] proposed a Uniform Resource Locator (URL) classification method that is suited for large scale streaming of URLs. They used seven different datasets to examine their method by training 70 percent of the data and test the 30 percent of remaining data. Whittaker, et al. [6] developed a scalable machine learning classifier to detect phishing attacks by analysing millions of pages a day by examining the URLs and pages contents to determine whether a phishing or not. The drawback of current machine learning techniques including [5, 6] is no longer enough depending on training data set as a main part as phishing attacks have dynamic and changeable behaviours. These techniques stand short to detect or predict new attacks with high accuracy unless the system is trained on the new phishing. We have tackled this issue in our previous work[2] by proposing a CBR-PDS system that dynamically adapt and proactively scale to detect new phishing attacks regales the dataset.

Abutair and Belghith [2] proposed a Case-Based Reasoning (CBR) Phishing Detection Systems (CBR-PDSs) to detect phishing attacks based on CBR methodology. This system is using the human-like thinking to predict phishing attacks based on previous similar experiences or cases. CBR-PDS is connected with an Online Phishing Threats (OPT) component for updating the case database. The accuracy rate exceeds 95.62%. In spite of CBR-PDS is proactively adapt and dynamically react to detect phishing attacks intelligently, there is a need to extend its capabilities to react in a large scale distributed system to get more insights and intelligence to efficiently predict or detect phishing attacks.

In this study, we integrate Multi-Agent system with CBR-PDS system to detect phishing attacks in large scale distributed system. Mobile agents' role is to participate in predicting phishing attacks based on the knowledge they possess and intelligently cooperate or negotiate with other agents to decide on certain indecisive suspicious phishing attacks.