Chapter 2.3
A Multistage Framework to Defend Against Phishing Attacks

Madhusudhanan Chandrasekaran
SUNY at Buffalo, USA

Shambhu Upadhyaya
State University of New York, USA

ABSTRACT

Phishing scams pose a serious threat to end-users and commercial institutions alike. E-mail continues to be the favorite vehicle to perpetrate such scams, mainly due to its widespread use combined with the ability to easily spoof them. Several approaches, both generic and specialized, have been proposed to address this growing problem. However, phishing techniques, growing in ingenuity as well as sophistication, render these solutions weak. To overcome these limitations, we propose a multistage framework – the first stage aims at detecting phishing based on their semantic and structural properties, whereas in the second stage we propose a proactive technique based on a challenge-response technique to establish the authenticity of a Web site. Using live e-mail data, we demonstrate that our approach with these two stages is able to detect a wider range of phishing attacks than existing schemes. Also, our performance analysis study shows that the implementation overhead introduced by our tool is negligibly small.

INTRODUCTION

Phishing is a form of Web based attack where attackers employ deceit and social engineering to defraud users of their private and confidential information such as password, credit card number, social security number (SSN), and bank account number. As the Internet is becoming the *de facto* medium for online banking and trade, phishing attacks are gaining notoriety, especially amongst hacker communities. Anonymity over the Internet, coupled with the potential for large

DOI: 10.4018/978-1-61350-323-2.ch2.3

financial gains serves as strong motivation for attackers to perpetrate such seemingly low risk, yet high return scams. The first recorded mention of phishing attacks was in AOL forums ("Phishing - Wikipedia,") wherein attackers posing as system administrators tricked the registered users into disclosing their account information. Since then, phishing attacks growing in sophistication and ingenuity have affected millions of users causing heavy monetary damage. For example, in the year 2006 alone, phishing attacks cost $2.8 billion in losses to consumers and commercial organizations worldwide (Gartner Press Release, 2006).

Due to its widespread adoption and ability to be easily spoofed, email continues to be the favorite vehicle to perpetrate such scams. Email based phishing attacks are usually carried out as a three step process: (i) In the first step, phishers harvest email addresses of their potential victims from Web pages, online forums and by other social engineering mechanisms; (ii) For the second step, a large volume of specially crafted emails appearing to originate from legitimate domains is dispatched to the assimilated list using open SMTP servers and compromised machines. These emails contain hyperlinks which redirect the users to a fake Web site similar in appearance to the legitimate domain; (iii) Finally, account details and other personal information are collected from the users who unsuspectingly provide them into the fake Web site thinking it to be a legitimate one. Phishing attacks, like other social engineering attacks, for their success depend upon users' lack of system knowledge. Phishers adopt a variety of visual deception agents to imitate the legitimate Web site's look-and-feel (Drake, Oliver, & Koontz, 2004). The mimicry of a legitimate Web site is usually achieved through spoofing the URLs with non-ASCII Unicode characters using customized images to mask fake URLs and embedding the fake Web sites within images that resemble a browser window. Recent studies (Dhamija, Tygar, & Hearst, 2006) show that naïve users are inept in identifying common browser based cues such as address bar, status bar, SSL certificates, and toolbar indicators and often fall prey to such imitation sites.

Until recently, anti-spam techniques were employed to detect phishing emails. However as phishing emails closely resemble their legitimate counterpart, they do not share similar features as that of spam emails. Also, there exist a vast number of readily available tools that can bypass both the statistical and rule based spam filters. Several browser extensions and plug-ins have been proposed to detect phishing attacks. Although these techniques act as a first line of defense, they suffer from many limitations. First, as these approaches operate on the fake Web site, they take the users a step closer to the attack giving little leeway for suspicion. Second, most of the existing defense mechanisms are not automated and delegate the onus of decision making onto the users. Third, as these tools embrace the authenticity of the IP address as an important classification criterion, they fail to protect from attacks that are launched within the realm of legitimate domain. For example, an attacker could compromise a Web server and launch phishing pages from the domain itself[1].

To overcome these limitations, we leverage on our prior works (Chandrasekaran, Chinchani, & Upadhyaya, 2006; Chandrasekaran, Narayanan, & Upadhyaya, 2006) and present a two-stage solution to protect users against email based phishing attacks. The first stage aims at detecting phishing emails based on their semantic and structural properties, whereas in the second stage a proactive approach using the *challenge-response* technique is presented to test the authenticity of links present in the email. The essential driving force for this two-stage approach is that cleverly fabricated emails can evade even the most smart spam filters which are put in place for phishing detection. In the first stage, the existing phishing email corpus are analyzed and *context models* are constructed which encapsulate the underlying meaning of the emails using their syntactic and semantic properties. These context models then