Security Study: Phishing URLs Using Mobile Eye Tracking and Anomaly Based Detection

LUDDY
SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING

By: Sydney Kaniuk & Dhruv Patel Mentor: Xinyao Ma

Abstract

There are numerous phishing websites and password hackers on the internet that are highly driven to steal sensitive data. It is difficult to recognize phishing websites and determine when a password is being stolen on the user's end. Given this fact, this research describes some of the aspects of phishing URLs and mobile authentication that a normal person can use and recognize.

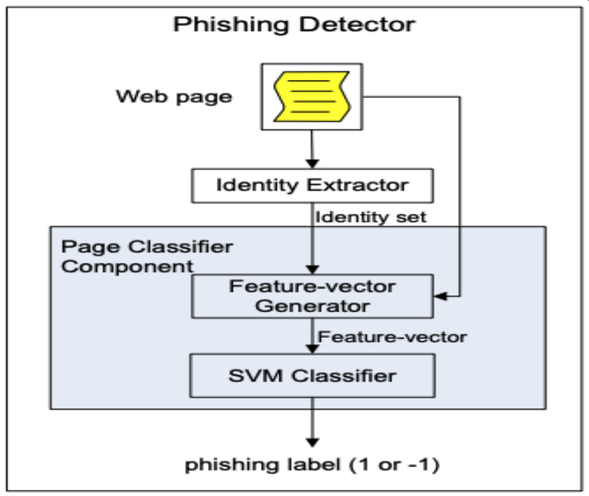
Introduction

•Phishing URLs and original URLs look similar to each other, but there are some minor details that make them differ.
•By using different methods, we have extracted some major points that prove phishing URLs can be different compared to the original.
•The methods mentioned have 97% accuracy, and most of them have used databases - offline database or Google crawl database

Methodology

•To extract the difference between the URLs, we have used different paper and all the papers have different methods
•First method: Utilizing mobile eye tracking to analyze user authentication and eye movement while browsing on the mobile web to see where the core of security issues are arising.
•Second method: Using Google crawl database since every URL obtains a given specific ranking number that determines if the URL is legit or if it is a phishing URL. The lower the ranking the higher the possibility that that URL is a phishing URL.
•Third method: Getting the short URL from social media
•Fourth method: Forming an offline database of a particular organization and comparing the URLS. This method uses Identity Extractor and Page Classifier.

Figure 1:



Results

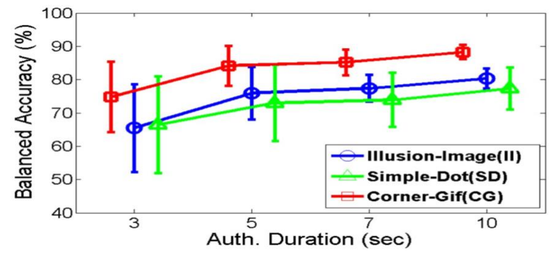


Figure 2: Above

Method 1: In this method, eye tracking technology – EyeVeri - is used for mobile devices that can track where users are looking on websites, and it can be used as a replacement for touch screen passwords. Regarding social media, short URLs are being used to target users. PhishTank, which is a verification system, can track this early on to prevent further phishing.

Method 2 and 3:

Different types of URLs:
1.Obfuscating the Host with an IP address
2.Obfuscating the Host with another Domain name
3.Obfuscating with large host name
4.Domain unknown or misspelled

Abnormal Server Handler: The server path is either left empty or it is replaced by "about: blank". And even the server path to different domain is suspicious because it rare that data goes to different domain.

Abnormal cookie: Cookies of the phishing sites usually be in the domain, which is inconsistent of the claimed identity

Abnormal Certificate in SSL: In. many phishing attacks, the Distinguished Names(DN) in their certificates are inconsistent with the claimed identities.

Conclusion

In this paper, we looked at EyeVeri, an authentication solution for mobile security based on eye movement since mobile devices are increasing in password hacks. We also described short URLs in regard to social media attacks and using Google crawl databases to determine if a URL is a phishing or original one.

Below is table that captures the research:

Figure 3:

Criteria	N	Component	Layer No.
URL & Domain Identity (Weight = 0.3)	1	Using the IP Address	Layer One
	2	Abnormal Request URL	
	3	Abnormal URL of Anchor	Sub weight = 0.3
	4	Abnormal DNS record	
	5	Abnormal URL	
Security & Encryption (Weight = 0.2)	1	Using SSL certificate	Layer Two
	2	Certification authority	
	3	Abnormal Cookie	
	4	Distinguished Names Certificate(DN)	
Source Code & Java script (Weight = 0.2)	1	Redirect pages	Sub weight = 0.4
	2	Straddling attack	
	3	Pharming Attack	
	4	Using onMouseOver to hide the Link	
	5	Server Form Handler (SFH)	
Page Style & Contents (Weight =0.1)	1	Spelling errors	Layer Three
	2	Copying website	
	3	Using forms with "*Submit*" button	
	4	Using Pop-Ups windows	
	5	Disabling Right-Click	
Web Address Bar (Weight = 0.1)	1	Long URL address	Sub weight = 0.3
	2	Replacing similar characters for URL	
	3	Adding a prefix or suffix	
	4	Using the @ Symbol to Confuse	
	5	Using Hexadecimal Character Codes	
Social Human Factor (Weight = 0.1)	1	Much emphasis on security and response	
	2	Public generic salutation	
	3	Buying Time to Access Accounts	