IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. V (Nov – Dec. 2015), PP 76-78
www.iosrjournals.org

Automatic Detection of Social Engineering Attacks Using Dialog

Pooja kale, Shital Kashiwant, Nisha Kamble, Subodh Awate
Prof. Sonali Tidke

Department of Computer Engineering Pimpri Chinchwad College of Engineering, Nigdi, pune.

Abstract: *Cyber attacker target the weakest part of security system which is increasingly the people who use and interact with a computer-based system is the easiest way for cyber attacker to attack the user. A separate research area is provided in order to protect computer assets. But by exploiting human vulnerabilities, an attacker can find a way for many computer-based defences. Phishing is the most common attack of social engineering attacks where someone pretend to be an authority figure or someone your trust to gain access to your login information. A robust and novel approach is needed to detect social engineering attacks and to send alert to the user while sharing confidential information to the unauthorized target. We proposed an approach which uses a dynamic Topic Blacklist (TBL) to verify the discussion topics of each line of text generated by the potential attacker. Using Natural language processing and machine learning, system can automatically detect social engineering attacks. Our approach is applicable to any attack vector since it depends only on the dialog text. System can recognize shortcut as well as incorrect grammar.*

Keywords: *Social Engineering, Security,Data Security.*

I. Introduction

Social engineering is a art of manipulating people so, they give up confidential information. Social engineering (SE) has been largely misunderstood, leading to many differing opinions on what social engineering is and how it works [1]. The Psychosomatic manipulation of people in order to get access to a system for which the attacker is not authorized. Cyber attacker attack the weakest part of security system. Social engineering is a modern form of the confidence scam which is grifter has always performed. Phishing emails are common version of attack, which is request for private information, but social engineering come in many form design to exploiting psychosomatic weakness of the target.

Social Engineering remains a popular method of compromising the security of computing systems. According to Thornburgh (2004) social engineering has gained profound acceptance in the information technology community as an effective social and psychological tool for exploiting the IT security mechanism of a target organization. The primary aim of the research was to assess the threat that social engineering vulnerabilities pose to IT systems and to raise staff awareness of the threat.[2]

Numerous experimental studies over the years have demon strated the susceptibility of people to social engineering attacks [3], [4]. The effectiveness of social engineering has encouraged attackers to use it more frequently, relying on social engineering as a component of larger attacks. A study by Verizon of security breaches in 2013 has shown that 29% of all security breaches involve social engineering to extract information for use primarily for phishing, bribery, and extortion [5].

Social engineering attacks is a communication between attacker and victim in order to obtain the some confidential information. Information gathered might include secure information such as mobile number, password, credit number which can support for larger attack. An attacker also convinces the victim to perform task which would support an attack, Such as going to a websites.

This attack firstly executed via email but also in person via phone, SMS and other documents. The efficiency of social engineering makes it a serious safety issue which must be addressed. Phishing emails are a class of social engineering attack which are simple, attempting to establish trust in a single communication to a victim. Phishing email attack is a simple but not effective as dialog based attack because gaining trust often required a two-way communication with a victim. Previous work in the automatic detection of social engineering attacks is limited to emails and websites, and do not attempt to detect the more subtle class of social engineering attacks which are purely dialog-based. Other previous work has focused on the training of individuals about social engineering attacks in order to make them more aware and resistant in the future.

II. Topic Blacklist

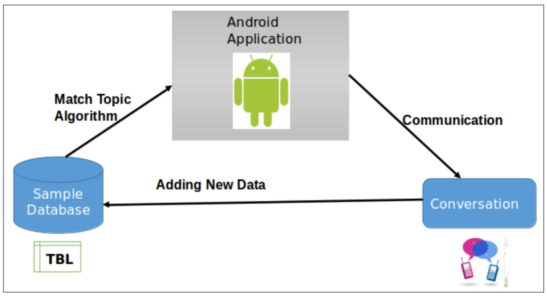

Fig 1: Topic BlackList

TBL is one of the most important part in this topic. Initially Topic Blacklist (TBL) which describes all forbidden topics of conversation with the victim having all possible topics which are entered manually as an input. Further a new topics get added automatically into TBL and then it will be derived as a dynamic which based on a basic understanding common security requirements, or an existing security policy document associated with a system. All US federal agencies are required to provide information security by the "Federal Information Security Act of 2002" [7], and policy documentation is part of that requirement [8]. Although private industry is not required to provide such documentation, the significant cost associated with cyber attacks has led many companies to document their security policies as well.

III. Proposed System

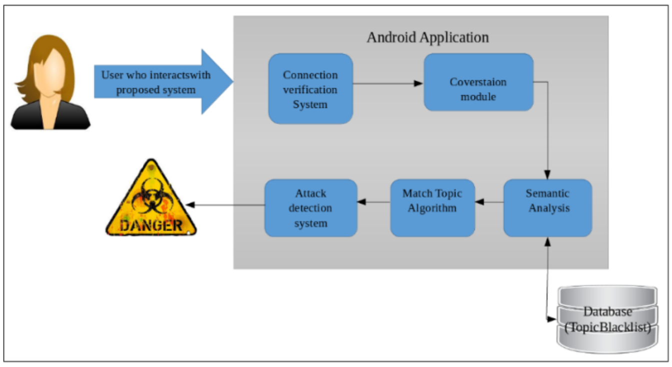

Fig2. Proposed System

We present an approach to the detection of social engineering attacks by performing semantic analysis of all text transmitted to the victim to guess at the topics being discussed on each line. Each topic is then checked for its appropriateness. A statement is considered to be inappropriate if it either requests secure information or requests the performance of a secure operation. An ability to evaluate the appropriateness of a question or command depends on the existence of a Topic Blacklist (TBL).[1] If there is an attack is detected, then warning message will be generated as a alert to the victim.

IV. Algorithm

In this paper we are using two algorithm for detecting the attack as following:
1.Social Engineering Detection Algorithm.
2.Match Topic Algorithm.

I) Detection Algorithm:

The top-level algorithm for scanning the dialog to identify attacks is shown in Figure. The outer loop scans through each line I in the text spoken by the attacker, TEXT. The inner loop iterates through each entry n in the TBL. Line 3 invokes the Match Topic function to determine if the topic of entry n is contained in line I.If the topic is found then the attack is detected and a warning message is display.

```
1. For each l € TEXT.
2.     For each n € TBL.
3.         If Match Topic (l,n).
4.             ATTACK_DETECTED.
```

II) Match Topic Algorithm:

The algorithm for the Match Topic function is shown in Figure. The purpose of the outer loop (line 1) is to scan through each token in the line and compare it to n.action ,the action associated with TBL entry n. The comparison to n.action is performed on line 2. If the action is found then the inner loop is entered (line 3) to scan through the remaining tokens on the line and compare them to n.resource, the resource associated with t. If both the action and resource are found then the function returns TRUE on line 5. The Compare function called on lines 2 and 4 performs a string comparison, but it also compares the first argument to any synonyms of the second argument.[1]

```
1. For i = 0 to | token in l |
2.   If Compare (l[i], n.action).
3.     For j = I + 1 to |token in l|.
4.       If Compare (l[j], n.resource).
5.         Return TRUE.
6. Return FALSE.
```

Table 1 shows the TBL which we use. The TBL was dynamically generated based on our understanding of common generic social engineering attack goals. Each root word in the TBL is associated with a set of synonyms which are considered to be equivalent. The synonyms for each root word which are considered by our tool are not shown.

ACTION	RESOURCE
Send	Money
Send	Sensitive Data
Call	Number
Visit	Website

Table1. Topic Blacklist (TBL)

V. Future Scope

In the future we plan to identify more social engineering attack transcripts which we can use to identify weaknesses in our detection approach. The examples which we use here are all examples of relatively generic attacks which could be broadly applied to most people. We will identify targeted social engineering attacks which are designed for specific people or institutions. Detection of targeted attacks will present challenges in defining the topic blacklist to protect institution-specific assets.

VI. Conclusion

We present an approach to detect social engineering attacks by verifying conversation, topics against a topic blacklist. The approach is robust enough to effectively analyze the language of real attacks, including the incorrect English which is often used in casual conversation.

The performance of our tool is good enough to provide attack warnings in real time during a conversation to prevent the victim from violating security protocol.

References

[1]. Ram Bhakta and Ian G. Harris “Semantic Analysis of Dialogs to Detect Social Engineering Attacks” University of California Irvine, USA 2015

[2]. C. Hadnagy and P. Wilson, “Social Engineering: The Art of Human Hacking”. Wiley, 2010.

[3]. T. Bakhshi, M. Papadaki, and S. Furnell, "A practical assessment of social engineering vulnerabilities." in Human Aspects of Information Security and Assurance (HAISA), 200S.

[4]. A. Karakasilitiosis, S. M. Furnell, and M. Papadaki, "Assessing end-user awareness of social engineering and phishing." in Australian information WGI!are and Security Conference, 2006.

[5]. 2013 Data Breach Investigations Report. Verizon, 2013.[Online].Available:http://books.google.com/booksd=YXiOnQEACAAJ

[6]. "Federal information security management act of 2002," 2002, title III of the E-Government Act of 2002 (Public Law 107-347).

[7]. "Minimum security requirements for federal information and information systems." National Institute of Standards, Tech. Rep., March 2006,j]PS Pub 200.