Phishing Aware: A Neuro-fuzzy Approach for Anti-Phishing on fog Networks

B. ARUNMOZHI, Assistant Professor of Computer science Department,
Department of Computer Science and Engineering
P. BHAVANI, Student of Computer Science Engineering
D. DEVADHARSHINI, Student of Computer science and Engineering
St.Joseph College of Engineering, Sriperumbudur, Chennai.

Abstract

Today search engines are tightly coupled with social networks, and present users with a double-edged sword. They are able to acquire information interesting to users but are also capable of spreading viruses introduced by hackers. People share their personal information on the web .It is challenging to define how a search engine spread viruses, since the search engine serves as a virus pool and creates propagation paths over the underlying network structure.

In this paper, we quantitatively analyze virus propagation effects and the stability of the virus propagation process in the presence of a search engine in social networks. Digital world is rapidly expanding and evolving ,likewise cybercriminals who rely on the illegal use of digital assets especially the personal information for inflicting damage to individuals. Although social networks have a community structure that impedes virus propagation, we find that a search engine generates a propagation wormhole. Third, we verify our analyses on four real-world data sets and two stimulated data sets.

Phishing is an example of a highly effective form of cybercrime that enables criminals to deceive users and steal important data. Moreover, we prove that the proposed model has the property of partial stability. Evaluation results show that, comp black with to a case without a search engine present; virus propagation with the search engine has a higher infection density, shorter network diameter, greater propagation velocity, lower epidemic threshold, and larger basic reproduction number.

Key Terms: HTML-Hyper Text Markup Language, JDBC- Java Database Connectivity, J2EE-Java 2 Platform, Enterprise Edition, SQL- Structured Query Language, SEP-Search Engine Poisoning

Introduction

Search engines supply a highly effective means of information retrieving way. But the search engine also a platform for spreading information. Because of these features, the propagators of malicious code have kept in step with search engines, building a hidden relationship within them. Moreover, the search engine poisoning(SEP) was applied by malicious software that published some vicious and fake pages to push the page ranking higher and attract more accesses. Phishing is similar to the ancient phishing strategy where the fishermen uses fish food as bait and wait for the fishes to eat so that they can easily catch them. The cyber attackers spread malicious links on the web and wait for the users to click and enter the link so that they can steal their personal information.

Literature Survey

The paper "Systematization of Knowledge (SoK): A Systematic Review of Software Based Web Phishing Detection." By Zuochao Dou, Isla Khalil, Abdallah Khreishah, Ala Al-Fuqaha in 2017, provide a systematic study of existing phishing detection works from different perspectives. We first describe the background knowledge about the phishing ecosystem and the state-of-the-art phishing statistics. Then we present a systematic review of the automatic phishing detection schemes. Specifically, we provide taxonomy of the phishing detection schemes, discuss the datasets used in training and evaluating various detection approaches, discuss the features used by various detection schemes, and discuss the underlying detection algorithms and the commonly used evaluation metrics.

The paper "A Page Rank Based Detection Technique for Phishing Web Sites." By A.Naga Venkata Sunil, Anjali Sardana in 2012, have considered GTR value as an additional heuristic, because Google's Page Rank is more reliable, and for legitimate sites GTR value will be high. So this technique will easily classify the phished URL's. Phishing sites will have very less GTR value so they can be easily identified as phished sites by using the values of this heuristic and other five heuristics.

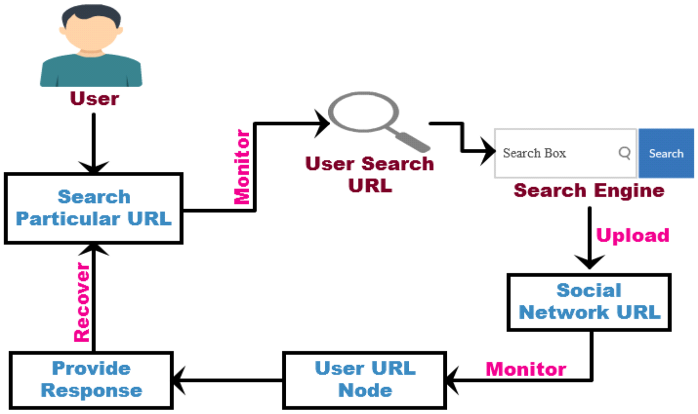
The paper" Software-defined Network Function Virtualization: A Survey" by YONG LI1, (Member, IEEE), AND MIN CHEN2 in 2015, investigate a comprehensive overview of NFV within the software-defined NFV architecture.

They introduced NFV its relationship with SDN. They also look at the history of NFV, presenting how middle boxes evolve to virtual network functions. They choose service chaining as a typical application of NFV.

The paper" Phishing-alarm: Robust and Efficient Phishing Detection via Page Component Similarity" by JIAN MAO1, WENQIAN TIAN1, PEI LI1, TAO WEI2, AND ZHENKAI LIANG3 in 2017 propose a robust phishing detection approach, Phishing-Alarm, based on CSS features of web pages. They develop techniques to identify effective CSS features, as well as algorithms to efficiently evaluate page similarity. They prototyped Phishing-Alarm as an extension to the Google Chrome browser and demonstrated its effectiveness in evaluation using real-world phishing samples.

System Design

Our goal is to address these challenges by analyzing the virus propagation effects of the search engine, which appears to be a hidden power for virus propagation and main source for spreading malware attacks. To achieve our research goal, we first need to analyze how a search engine increases propagation sources and routes in social networks and on the web. As a virtual virus pool, a search engine may contain a lot of viruses to increase propagation sources any user accessing web pages may be infected, and thus those activities increase the propagation routes for viruses. We need to quantitatively analyze the propagation effect of the search engines. In building the specific propagation model that combines the social network and the search engine, some key metrics of virus propagation need to be analyzed. We design experiments to verify this analysis. Data sets of current real social networks should be tested and discussed.



The major part of the databases is categorized as administrative components and the user components. The administrative components are useful is managing the actual master data that may be necessary to maintain the consistency of the system. The administrative databases are purely used for the internal organizational needs and necessities. The user components are designed to handle the transactional state that arise upon the system whenever the general client makes a visit onto the system for the sake of the report based information. The user components are scheduled to accept parametrical information for the user as per the systems necessities.

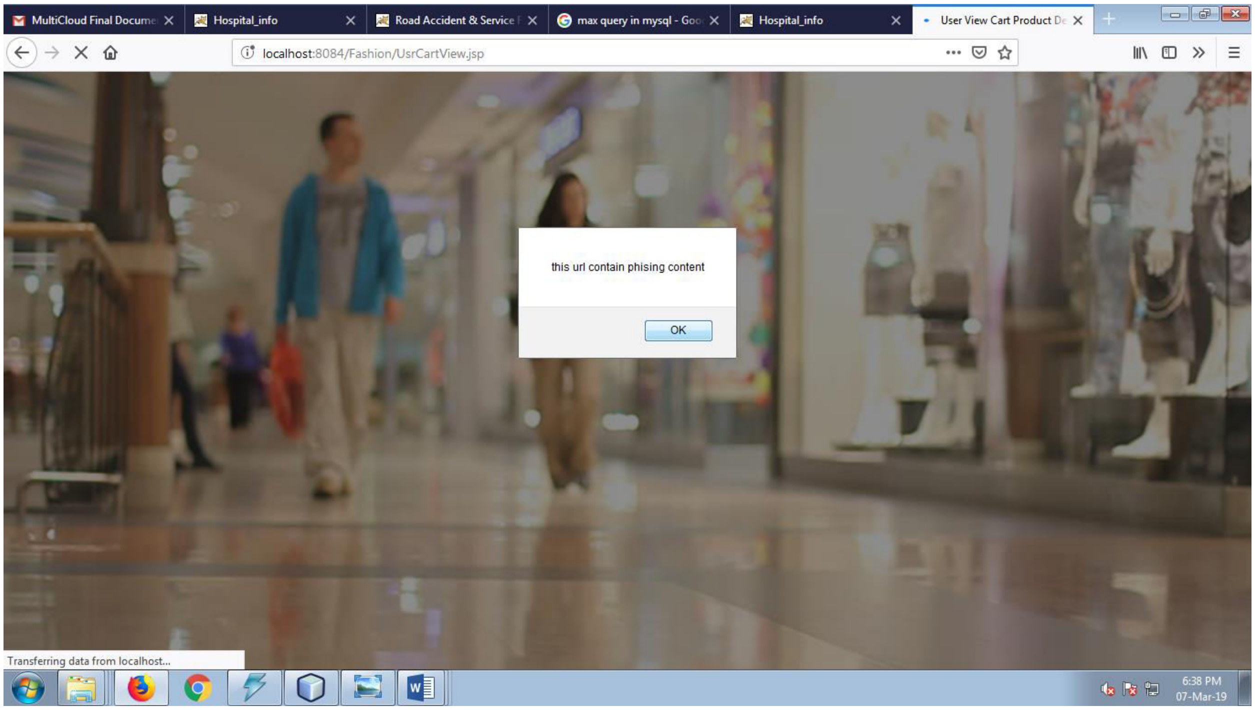
The administrative user interface concentrates on the consistent information that is practically, pact of the organizational activities and which needs proper authentication for the data collection. The interfaces help the visitors with all the transactional states like Data insertion, Data deletion and Data updating with the data search capabilities.

In this world of busy schedule with which the industrial professionals are getting through this kind of system is a boon for the kind of information they can readily access at the tip of their fingers. This involves misuse of information by cybercriminals and the that they gain by stealing the data and misusing it.

IMPLEMENTTION

```
{

    static int ran[]=new int[100];

    static int nsp;

    public static void find_tf()

        {

        int i,j=0,n,k=0,p,t,u,m=-1;

        double c=0.0,f=0.0;

        String s1="",s21="",s3="";

        String s[]=new String[100];

        String str[]=new String[100];

        String str1[]=new String[100];

        String str2[]=new String[100];

         String str3[]=new String[100];

          String str4[]=new String[100];

        double c1[]=new double[100];

         double c3[]=new double[100];

        double c2[]=new double[100];

         double c4[]=new double[100];

         String s2[][]=new String[100][100];

        String a[][]=new String[100][100];

        String a1[][]=new String[100][100];


       Scanner ip=new Scanner(System.in);
       DataInputStream din=new DataInputStream(System.in);

       n=onlineconnect.sniplength;


       int ranin=0;

       System.out.println("Enter the no of Snippet");

       nsp=ip.nextInt();

       System.out.println("-------------------SELECT  SNIPPETS(Max"  +nsp+")----------------------
");

       for( i=0;i<nsp;i++)

       {

         ran[i]=ip.nextInt();

       }


       for(int i1=0;i1<nsp;i1++){

      s2[i1]=HTML2Text.tks[ran[ranin++]];}

      n=nsp;

      j=nsp;


System.out.println("----------------SELECTED SNIPPETS-----------------------------");

       for(i=0;i<j;i++)

    {

for(p=0;s2[i][p]!=null;p++)
```

SNAPSHOT



this url contain phising content

CONCLUSION

With the proliferation of social networks and their ever-increasing use, viruses have become much more powerful. We investigate the propagation effect of search engines and characterize the positive feedback effect and the propagation wormhole effect. The virtual virus pool and virtual infection paths that are formed by a search engine make propagation take place much more quickly. We show that propagation velocity is quicker, infection density is larger, the epidemic threshold is lower, and the basic reproduction number is greater in the presence of a search engine. Finally, we conduct experiments that verify the propagation effect in terms of both infection density and virus propagation velocity. Results show the significant influence of a search engine particularly its ability to accelerate virus propagation in social networks.

REFERENCES:

[1] O. Ajao, J. Hong, and W. Liu. A survey of location inference techniques on twitter. Journal of Information Science, 1:1–10, 2015.

[2] E. Amig´ o, J. C. De Albornoz, I. Chugur, A. Corujo, J. Gonzalo, T. Mart´ın, E. Meij, M. De Rijke, and D. Spina. Overview of replab 2013: Evaluating online reputation monitoring systems. In Proceedings of CLEF, pages 333–352. Springer, 2013.

[3] F. Atefeh and W. Khreich. A survey of techniques for event detection in twitter. Computational Intelligence, 31(1):132–164, 2015.

[4] H. Bo, P. Cook, and T. Baldwin. Geolocation prediction in social media data by finding location indicative words. In Proceedings of COLING, pages 1045–1062, 2012.

[5] J. Bollen, H. Mao, and A. Pepe. Modeling public mood and emotion: Twitter sentiment and socio-economic phenomena. In Proceedings of ICWSM, pages 450–453, 2011.

[6] J. D. Burger, J. Henderson, G. Kim, and G. Zarrella. Discriminating gender on twitter. In Proceedings of EMNLP, pages 1301–1309, 2011.

[7] H.-w. Chang, D. Lee, M. Eltaher, and J. Lee. @ phillies tweeting from philly? predicting twitter user locations with spatial word usage. In Proceedings of ASONAM, pages 111–118, 2012.

[8] Y. Chen, J. Zhao, X. Hu, X. Zhang, Z. Li, and T.-S. Chua. From interest to function: Location estimation in social media. In Proceedings of AAAI, pages 180–186, 2013.

[9] Z. Cheng, J. Caverlee, and K. Lee. You are where you tweet: a content-based approach to geo-locating twitter users. In Proceedings of CIKM, pages 759–768, 2010.

[10] R. Compton, D. Jurgens, and D. Allen. Geotagging one hundred million twitter accounts with total variation minimization. In IEEE Big Data, pages 393–401, 2014.

FUTURE ENHANCEMENTS

The concept of the collaborative learning, the grouping and pairing of students for the purpose of achieving an academic goal, has been widely researched and advocated throughout the professional literature.

Mr.B.Arunmozhi M.E., is an Assistant Professor in the Department of Computer Science and Engineering at St.Joseph College of Engineering, Sriperumbudur, Chennai, Tamil Nadu. He has completed his M.E, CSE under Anna University Affiliation College in the year 2011. He has done his B.E, CSE under Anna University Affiliation College in the year 2007. Mr.B.Arunmozhi has 11 years of teaching experience and has 12 publications in International Journals and Conferences. His area of interests includes Network Security, Computer Networks, Data Science and Machine Learning. He is an active member of CSI and IEANG. He has organized various International Conferences, workshops and Seminars in the area of Computer Networks, Cloud Computing &Machine Learning respectively.

M. P. Bhavani, Student of Computer Science and Engineering at St.Joseph College of Engineering Sriperumbudur, Chennai, Tamilnadu. I had attended many Workshops and Seminars in Network Security and Machine Learning.

MS.D.Devadharshini B.E,. Student of Computer Science and Engineering at St.Joseph College of Engineering Sriperumbudur, Chennai, Tamilnadu. I had attended many Workshops and Seminars in Network Security and Machine Learning. I got placed in companies like Sutherland and GenXLead.