RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Mitigating Web Vulnerabilities to Strengthen Data Security Against Cybercrime

DR.K.NAGESWARARAO, PROFESSOR
DEPARTMENT OF CSE
Sai Tirumala NVR Engineering College, Narasaraopet
Mail Id: nageswararaokapu@yahoo.com

ABSTRACT

Speeches and videos are among the primary online distribution channels for terrorists. Terrorist organisations use the internet, especially social networks, to brainwash individuals and promote their ideology through inflammatory websites that entice defenceless people to join terrorist groups. Here, we offer an efficient web data mining technique for detecting such online items and automatically flagging them for human review. Web pages are built on top of HTML (Hypertext Markup Language), which may be used in a variety of ways to combine text, images, and other elements into a single webpage. We used both web mining and data mining to extract textual content and identify trends from websites. By using the email system in this instance, we are able to detect unsolicited messages that are more likely to be terroristic and will send the spam straight to the system user.

I. INTRODUCTION

After that the typical behavior of terrorists by applying a data mining algorithm to the textual content of terror-related Web sites. The resulting profile was used by the system to perform detection of users suspected of being engaged in terrorist activities. And this algorithm should be based on the content of existing terrorist sites and known terrorist traffic on the Web. Data mining is a technique used to mine out patterns of useful data from large data sets. Web mining also consists of text mining methodologies that allow us to scan and extract useful content from unstructured data. This system will check the sender messages and whether the message is promoting terrorism. Data mining as well as web mining are used together at times for efficient system development. System will find the unwanted messages that are more susceptible to terrorism and will send directly to the receiver's spam account. It will give more awareness to the users.

The rapid development of Internet technologies has immensely changed on-line users' experience, while security issues are also getting more overwhelming. The current situation is that new threats may not solely cause severe injury to customers' computers however conjointly aim to steal their cash and identity. Among these threats, phishing may be a noteworthy one and may be a criminal activity that uses social engineering and technology to steal a victim's identity knowledge and account info. Most social engineering attacks area unit initiated and administrated by the attackers in person. By means that of in person handled social engineering attacks area unit particularly those that use the manner of impersonation principally deception to be in distress, a troublesome state of affairs, or urgency. Social engineering attacks area unit initiated usually in 2 ways: By the attackers one by one and by creating use of computers. the opposite ways that of handling social engineering attacks area unit by exploitation computers or automatic means that. a way of assaultive is thru faux websites, that area unit simply created. Websites that appear as if the legitimate sites can also be created therefore simply. One very talked-about style of social engineering attack is finished by giving free downloads or terribly high discounts and inspiring them to use their

official ids. The persons could also be attracted and supply substantial details within the method. In the scope of social engineering, attackers use some necessary approaches that may be place into physical, social, and technical class. in an exceedingly physical approach, because the name implies, the offender performs some physical actions so as to urge data regarding the victim like looking through Associate in Nursing organization's trash, that is termed Dumpster diving. A Dumpster is a valuable supply {of data |of data |of knowledge} like personal information regarding staff, manuals, memos of sensitive data. in a very social approach, attackers deem socio psychological techniques like Cialdini's principles of persuasion to govern their victims. samples of persuasion strategies embody the employment of authority. Attackers typically use search engines to assemble personal data regarding future victims. There are tools that may gather and mixture data from completely different internet resources.

Server by clicking the creating account on the login page. The user can send or receive the email once he created the account. The system will check the mail data and will make the large data into smaller parts, classify the data and will crosscheck the server for the keywords which are spam. Then, it will classify whether the mail is spam or ham. The overview of the cybercrime data mining is to mine out the patterns in the email to prevent the crime anticipate criminal activity. The Naïve Bayes and the K-means algorithm are used to classify the datasets and to mine the patterns. So, that it can record and form the prediction or the output about the spamming mails. Data mining is a technique that are capable to scan the accuracy and performance in cybercrime. Web mining is also a technique of text mining technique which can mine out the patterns in the large datasets. The both are techniques to mine out the data present in the mail. After, finding the data in the dataset it is going to classify it and verify it with the keywords which are already in the given dataset. Web mining improves the functionality of an online software by classifying content and identifying web sites. It's utilized for internet searching (e.g., Google, Yahoo), as well as vertical searching (e.g., Fat Lens, Become, and so on). To forecast user behavior, web mining is used. Web mining is particularly beneficial to a certain website and e-service, such as landing page optimization. Website mining is separated into three categories of mining techniques: website mining, internet structure mining, and internet usage mining and data mining using methods.

Cybercrime has undergone a revolutionary modification, going from being productoriented to service-oriented as a result of the fact it operates within the virtual world, with totally different abstraction and temporal constraints, differentiates it from different crime taking place within the physical world [11]. As a part of this alteration, the crime underground has emerged as a secret crime marketplace as a result of rising technological changes have provided organized cybercriminal teams with unexampled opportunities for exploitation [12]. The crime underground includes a extremely skilled business model that supports its own underground economy [5]. This business model, referred to as CaaS, is ‘‘a business model employed in the underground market wherever illegal services are provided to assist underground consumers conduct cybercrimes, like attacks, infections, and concealing in an automatic manner,’’ [3]. Thus, CaaS is referred to as a do-it-for-me service, not like crimeware that may be a do-it-yourself product.

II. LITERATURE SURVEY

Remote Denial of Service Attacks and Countermeasures

As evinced by a series of high profile attacks, denial of service (dos), or prevention of legitimate access to resources, is a threat that demands attention. Of particular concern are distributed attacks, in which an adversary recruits several computers to aid in the attack. The first major distributed denial of service (ddos) attack brought down the University of Minnesota's network for three days in August 1999. About six months later, the attack by a Canadian teenager on several major sights including Yahoo, Amazon, ebay, CNN, and Buy.com made headlines. In accord with the underlying principle that destruction is simpler than construction, denial of service attacks come in many forms and are easy to carry out, but preventing them can sometimes be tricky. Although there is no panacea for all flavors of denial of service, there are several countermeasures that focus on either making the attacks more difficult or on making the attacker accountable via logging and tracing.

Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures

Distributed Denial of Service (DDoS) attacks have become a large problem for users of computer systems connected to the Internet. DDoS attackers hijack secondary victim systems using them to wage a coordinated large-scale attack against primary victim systems. As new countermeasures are developed to prevent or mitigate DDoS attacks, attackers are constantly developing new methods to circumvent these new countermeasures. In this paper, we describe DDoS attack models and propose taxonomies to characterize the scope of DDoS attacks, the characteristics of the software attack tools used, and the countermeasures available. These taxonomies illustrate similarities and patterns in different DDoS attacks and tools, to assist in the development of more generalized solutions to countering DDoS attacks, including new derivative attacks

Depth-in-defense approach against DDoS

Distributed denial-of-service attacks (DDoS) impose a great threat to the availability of resources. Not only is the attack difficult to carryout but also the methods and techniques used to prevent these attacks are so complex that it makes the job to protect the resources even harder. An analysis is carried out for various approaches of detection and prevention systems that can be deployed to reduce the effect of the attacks on the victim. In this paper a comparative analysis has been carried out amongst different techniques for prevention against DDoS attacks and at the end a novel solution is proposed.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

In an Existing system, detection of terrorism was presented by using Web traffic content as the audit information. After that the typical behavior of terrorists by applying a data mining algorithm to the textual content of terror-related Web sites. The resulting profile was used by the system to perform detection of users suspected of being engaged in terrorist activities. And this algorithm should be based on the content of existing terrorist sites and known terrorist traffic on the Web.

PROPOSED SYSTEM

There are two features used in this system that is data mining and web mining. Data mining is a technique used to mine out patterns of useful data from large data sets. Web mining also consists of text mining methodologies that allow us to scan and

extract useful content from unstructured data. This system will check the sender messages and whether the message is promoting terrorism. Data mining as well as web mining are used together at times for efficient system development. System will find the unwanted messages that are more susceptible to terrorism and will send directly to the receiver's spam account. It will give more awareness to the users.

IV. SYSTEM IMPLEMENTATION

Module Description :

This system comprises of 5 modules as follows,

Module 1: Mailing

First, User should Register with their basic details through create an account link. By using that details they need to Login for enter into the system. Then they will receive the message of "success". Here, we are using the system like E-mail. Hence, it contain the features of inbox, sent mail, spam, recent histories, etc., The user can compose the mail with whom to sent. It may be related to terrorism or may something related to common things. Here, the recent history denotes the person who is doing mail recently.

Module 2: Filtering

In this Module, I have a few data's in my Dataset. With that, I will check whether the sent message have contain the filteration words about terrorism or not? I have using Data mining technique to mine out text data from large data sets and make the most use of obtained results. Web mining consists of text mining methodologies. Through that text mining, we can extract the text or content what are all related to terrorism. If the filteration words are match with the sent message means, the receiver receives the mail in his/her spam box or else inbox.

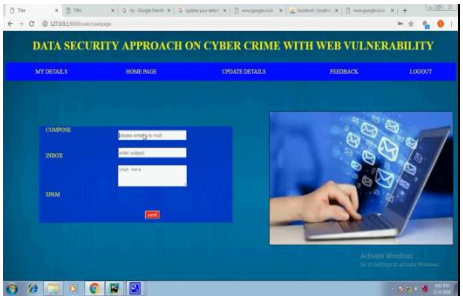
Module 3: Spam Detection

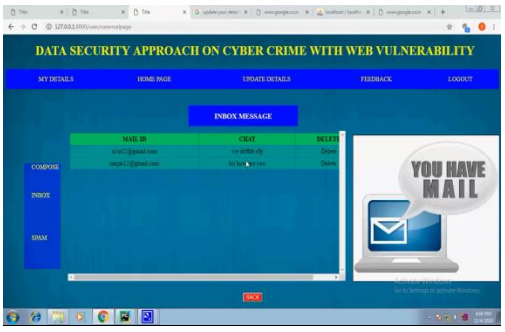
In this Module, Admin should login first. It will contain the predefined user name and password. Admin side, it will have the features of keywords, spam, analysis, chart. By using Mining concepts Administrator can add few terrorism related words manually in few parameters/ categories. That keywords will also going to add with the existing dataset . In spam, we can see what are all spam messages from starting. In analysis, It contains a mail having how many words in those keyword categories and their total count per each mail.

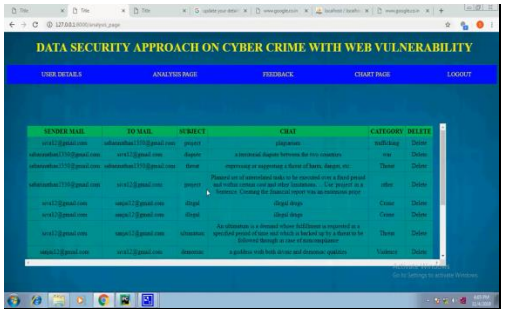
Module 4: Preprocessing

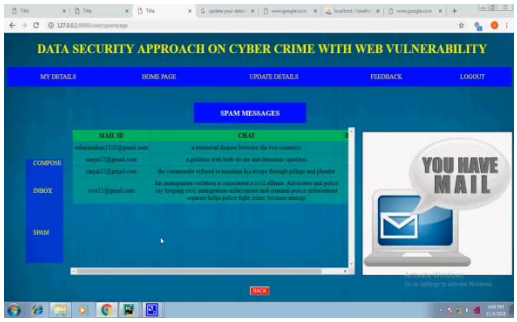
In this Module, Admin can see all the spam mail sent and receive in this system, whereas, Spam Detection will contain preprocessing which means it will remove all the common words/stop words such as the, and, or, here, there, etc., Here. I have used the Naïve Bayes algorithm. After preprocessing I have highlight the filteration words in mails. Then it contains every categories count as total spam Detection count. Finally by make use of the total spam Detection count, did the chart.

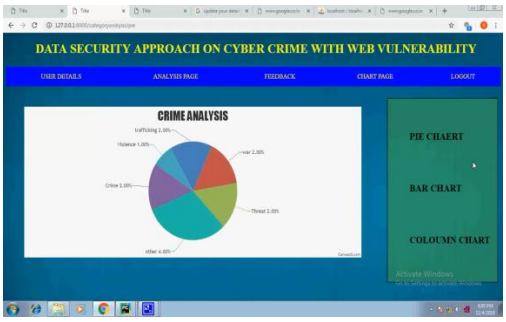
V. SCREEN SHOTS

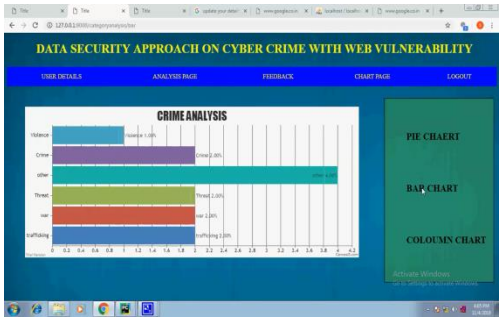












VI. CONCLUSION

To prevent and remove terrorism and the spread of its activities through social media on the internet by delivering unsolicited messages and images to the defenceless, we must use a powerful method or system. That approach ought to be useful to the police in promptly increasing public awareness and identifying those who are

disseminating hate speech and carrying out terrorist acts.

REFERENCES

1. David Karig and Ruby Lee, "Remote Denial of Service Attacks and Countermeasures," Princeton University Department of Electrical Engineering Technical Report CE-L2001-002, October 2001.

2. Lincoln Stein and John N. Stuart. "The World Wide Web Security FAQ", Version 3.1.2, February 4, 2002. http://www.w3.org/security/faq/ (8 April 2003).

3. Paul J. Criscuolo. "Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht CIAC-2319". Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

4. "Yahoo on Trail of Site Hackers", Wired.com, February 8, 2000. http://www.wired.com/news/business/0,1367,3422 1,00.html (15 May 2003).

5. "Powerful Attack Cripples Internet". Associated Press for Fox News 23 October 2002. http://www.foxnews.com/story/0,2933,66438,00.h tml. (9 April 2003)

6. Joseph Lo and Others. "An IRC Tutorial", irchelp.com. 1997. http://www.irchelp.org/irchelp/irctutorial.html#par t1. (8 April 2003).

7. Nicolas Pioch. "A Short IRC Primer". Edition 1.2, January 1997. http://www.irchelp.org/irchelp/ircprimer.html#DD C. (21 April 2003).

8. Kleinpaste, Karl, Mauri Haikola, and Carlo Kid. "The Original IRC Manual". March 18, 1997. http://www.user-com.undernet.org/documents/ircmanual.html#seen (21 April 2003).

9. Kevin J. Houle. "Trends in Denial of Service Attack Technology". CERT Coordination Center, Carnegie Mellon Software Engineering Institute. October 2001. www.nanog.org/mtg0110/ppt/houle.ppt. (14 March 2003).

10. Federal Computer Incident Response Center (FedCIRC), "Defense Tactics for Distributed Denial of Service Attacks". Federal Computer Incident Response Center. Washington, DC, 2000.