Analysis Detection and Prevention of Users from Click Jacking Attack Using DDoS

[1]Jeena James, [2]Agnes.A, [3]Hajera.S.H
Academician,
Computer Science and Engineering,
DMI College of Engineering, Chennai.

***Abstract* - Click jacking is an act of hijacking users clicks inorder to perform undesired actions which are beneficial for the attackers. This paper presents a new distributed approach to detecting DDoS (Distributed Denial of Services) flooding attacks at the traffic flow level. The new defense system is suitable for efficient implementation over the core networks operated by Internet service providers (ISP). At the early stage of a DDoS attack, some traffic fluctuations are detectable at Internet routers or at gateways of edge networks. Recently many prominent web sites face so called Distributed Denial of Service (DDoS) Attacks. While former security threats could be faced by tight security policy and active measures like using firewalls, Vendor pathes etc. We proposed a click jacking attack to prevent DDoS. Click jacking vulnerability can use the browser to exploit weaknesses in cross domain isolation and the same origin policy. Although there are protections available for click jacking, the web applications implementing these mitigations are far and in between. Additionally, although the possibility for an attacker to frame a page is easy to detect, it is much more difficult to demonstrate or assess the impact of a click jacking vulnerability than more traditional client-side vectors.**

Keywords - Click jacking, DDoS, Internet Service Providers, firewalls, traffic fluctuations.

1. INTRODUCTION

Click jacking [1] is a very common attack through frames, in which, the user unknowingly clicks on a malicious page that sits on top a benign page. This is usually done by loading the malicious page as a transparent page over a benign page that genuinely requires a click or some input (Like user login, send email, etc). When the user gives the input that was asked, an event is sent to the malicious page (usually a click event) that causes dome undesirable action to be taken on the user's behalf.

Click jacking is also referred to as UI redressing [3, 4]. The most famous example of overlaying an invisible frame was the Click jacking Tweet bomb [2] – in which a malicious page embedded Twitter.com on a transparent IFRAME. The victim page enticed the user by placing a 'Don't click' button directly above the invisible 'Tweet' button. If the user clicked on the button, a status message, which contained a link to the malicious website is posted on behalf of the user. Click jacking can also be implemented by simply hiding single UI elements, rather than the whole page in an IFRAME. Likejacking attacks [5] and Tapjacking attacks [6] are examples of such link of attacks. In all such attempts of attack, browser is the main source of attack.

Therefore, our focus remains in the context of web browsers. Many defences have been suggested for click jacking for web browsers but they have all been circumvented by malicious users. Mostly, the defense consists of frame busting [7][8], which simply limits browser functionality by disallowing the IFRAME feature, but it does work as the webpage cannot get framed over another webpage. But the biggest problem with this technique is that it doesn't work with third-party widgets, such as Facebook 'Like' button. There are other defences that have been suggested (Discussed in Section II), but most have been circumvented, or more importantly can be circumvented later, and suffer from poor usability and incompatibility with webpages and widgets.

According to Huang et al., click jacking has not properly addressed and prevented [9]. It was found out that some test attacks still had an effectiveness of 98%. Duri ng our literature review, we realized that Balduzzi [10] gave out the best mitigation results and was also the most cited and authoritative result. A major limitation of almost all of the existing techniques is that they try to work before the user has clicked the clickjacked link and offer no support for the false negatives that they can't detect.

Consequently, if a prevention method is circumvented then it becomes essentially useless. Considering the current defence techniques and some of their shortcomings, we kept the following objectives when developing our own defence to click jacking:

- The solution should be compatible with old websites.
- The solution should grow with time rather than remain stagnant.
- The solution shouldn't degrade the surfing speed.
- Even the most naive users should be able to make use of the solution.

• The solution should have the potential to be applied to other browser vulnerabilities as well.

T Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE Abstract— A low-rate distributed denial of service (DDoS) attack has significant ability of concealing its traffic because it is very much like normal traffic. It has the capacity to elude the cur- rent anomaly-based detection schemes. An information metric can quantify the differences of network traffic with various probability distributions.

In this paper, we innovatively propose using two new information metrics such as the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. The proposed generalized entropy metric can detect attacks several hops earlier (three hops earlier while the order) than the traditional Shannon metric. The proposed information distance metric outperforms(six hops earlier while the order) the popular Kullback–Leibler divergence approach as it can clearly enlarge the adjudication distance and then obtain the optimal detection sensitivity. The experimental results show that the proposed information metrics can effectively detect low-rate DDoS attacks and clearly reduce the false positive rate. Furthermore, the proposed IP traceback algorithm can find all attacks as well as attackers from their own local area networks (LANs) and discard attack traffic. Index Terms—Attack detection, information metrics, IP trace- back, low-rate distributed denial of service (DDoS) attack.

The distributed denial of service (DDoS) attack is a serious threat to the security of cyberspace. It typically exhausts bandwidth, processing capacity, or memory of a targeted ma- chine or network. A DDoS attack is a distributed, cooperative and large-scale attack. It has been widely spread on wired [11] or wireless networks [12]. A low-rate DDoS attack is an intelli- gent attack as the attacker can send attack packets to the victim at a sufficiently low rate to elude detection. Today, a large-scale DDoS attack is usually combined with multiple low-rate attacks, which are distributed on the Internet to avoid being detected by current detection schemes. An attacker can use botnetsto launch a low-rate DDoS attack, producing network behavior that ap- pears normal. Therefore, it is difficult to detect and mitigate such attacks [13].

2. BACKGROUND AND RELATED WORK

A. Motivation

Currently, research on Web service vulnerability testing remains limited, with studies focusing mainly on functionality testing[2, 5, 6], reliability analysis[3], data perturbation[7-9], and Web service rule mutation[10-12]. Existing techniques can be classified into 3 categories based on how the mitigation is being done:

• *Browser Add-on/Browser based:* It refers to mitigation techniques that are solely based upon the browser or an add-on. In such a case, the browser itself is responsible for the mitigation of click jacking. Examples of such add-ons are NoScript [11] and FlashBlock [12].

• *Website code/script:* These mitigation techniques are those that are implemented on the website where the website is solely responsible for mitigation. Examples of such techniques include frame busting scripts [7], [8] which disable iframes from employing click jacking.

• *Website + Browser Code:* This category represents a new, yet more difficult to implement techniques which require coordination from the browser and the website. The first of these techniques was the X-Frame options [13] presented by IE8 and soon adopted by other browsers as well. This category of techniques requires that the browser is capable of utilizing the technique and that the website also employs the relevant code.

Therefore, many information-theory-based metrics have been proposed to overcome the above limitations. In information theory, information entropy is a measure of the uncertainty associated with a random variable. Information distance (or divergence) is a measure of the difference between different probability distributions. Shannon's entropy and Kull- back–Leibler's divergence methods have both been regarded as effective methods for detecting abnormal traffic based on IP address-distribution statistics or packet size-distribution statistics [10]–[12]. Early detection and detection accuracy (such as a low false positive rate) of DDoS attacks are the two most important criteria for the success of a defense system. In this paper, we innovatively propose two new and effective anomaly-based detection metrics which not only identify attacks earlier, but also produce lower false positive rates when compared with the traditional Shannon's entropy method and the Kullback–Leibler divergence method.

B. Contributions

In this section we will present our approach to mitigate click jacking via user community feedback; we will also illustrate the consequences of the user chancing upon a previously flagged click jacking website (by user community). Once the DOM has finished loading, we parse the page for malicious redirect intent and possible clickable elements (that is, elements which the user can interact with). After attaching scripts to the loaded page and modifying its code, our add-on will intercept user clicks by displaying a popup and stopping event execution whenever the user clicks on a clickable element.

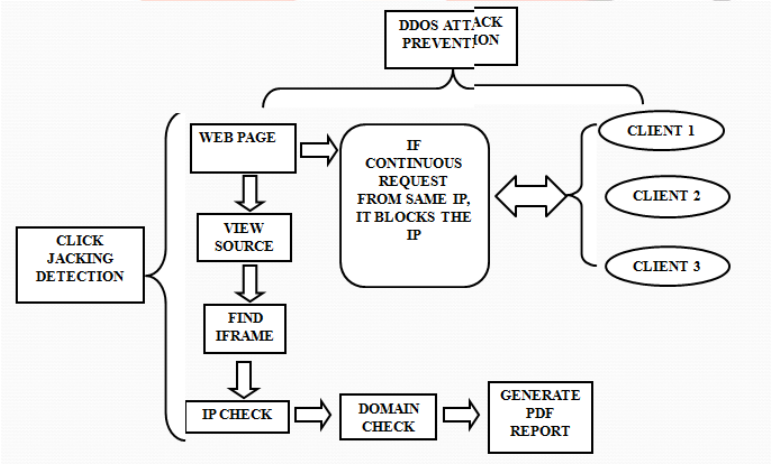
In summary, our contributions are highlighted below in four technical aspects. The details and proofs are given in subsequent sections:
(a). Traffic anomaly detection at superflow level: Monitoring Internet traffic at routers on individual flows is identified by a 5-tuple: {source IP, destination IP, source port, destination port, protocol applied}. The superflow consists of those traffic flows destined for the same network domain and applied the same protocol. This level of traffic monitoring and anomaly detection is more cost-effective for DDoS defense in real-life Internet environments.

(b). Distributed change-point detection : Considering the directionality and homing effects of a DDoS flooding attack, we propose to use collaborative routers for distributed change-point detection and use the domain servers for alert correlation and aggregation.

(c). Hierarchical alerts and detection decision making: Our system adopts a hierarchical architecture at the router and domain levels. This simplifies the alert correlation and global detection procedures and enables the DCD system implementation in ISP networks.

(d). Novelty of SIP (secure infrastructure protocol): We propose a new trust-negotiating SIP protocol to secure inter-server communications. The SIP has removed some of the shortcomings of the existing IPSec and application-layer multicasting protocols [14, 15]. SIP appeals for implementation on VPN tunnels or over an overlay network built on top of all domain servers.

Here we add some new attack detection with addition of existing system. It is performed as close to attack sources as possible providing a protection to subscribed customers and saving valuable network resources. We used to distinguish packets that contain genuine sources IP address from those that contain spoofed addresses.First, we prepared a web page that accepts a single parameter denoting a URL that should be embedded in an IFRAME. Once the page and all contents (i.e., the IFRAME) finished loading and rendering,
we verified that the IFRAME was still present.



Pages that perform frame busting would substitute the whole content in the browser window, thus removing the IFRAME. To automate this experiment, we implemented a Firefox extension that takes a list of URLs to be visited. Once a page is loaded, the extension waits for a few seconds and then verifies the presence of the IFRAME. If the IFRAME is not part of the document's DOM-tree anymore, we conclude that the embedded page performed frame-busting. This may lead to a message DENY. We surveyed the frame busting practices of the top 500 websites. Using both known and novel attack techniques, we found that all of the click jacking defenses we encountered could be circumvented in one way or another.

3. RESULTS

Part of the reason for this is that our current implementation iterates through each element checking it is clickable and then modifies the page's code accordingly. If this preprocessing could be incorporated while the page is being loaded or while the user is busy with other actions, it may reduce the load time.
Our add-on was unable to detect all clickable elements on websites because of the following factors:

• JavaScript Obfuscation
• Dynamic processing and rewriting of JavaScript code
• Event Listeners
• URL redirection

The metrics of anomaly-based detection have been the focus of intense study for years in an attempt to detect intrusions and attacks on the Internet. Recently, information theory as one of the statistical metrics is being increasingly used for anomaly detection.

The DDoS attacks show anomalies in the characteristics of the selected packet attributes, and the detection accuracy and performance are analyzed using live traffic traces from a variety of network environments. However, because the proposed detector and responder lack coordination with each other, the possible impact of responses on legitimate traffic and expenses for computational analysis are increased.

It is very important and significant that we can obtain the optimal value of divergence between the attack traffic and the legitimate traffic in a DDoS detection system by adjusting the value of order of information divergence. In addition to this, we also study the properties of Kullback–Leibler divergence and information divergence in theory and overcome their asymmetric property when used in real measurement. We successfully convert the information di- vergence into an effective metric in DDoS attack (including both low-rate and high-rate) detection.

4. CONCLUSION AND FUTURE WORK

It is crucial to detect the DDoS flooding attacks at their early launching stage before widespread damages done to legitimate applications on the victim system. This paper presents a novel approach to counter click jacking. The solution utilizes user feedback to create dynamic black and white lists and overcome limitations posed by previous solutions. Despite a few limitations, Clicksafe is effective in providing security against click jacking attacks.Here we have discussed about how we can block an IP but if the user changes then the attack must not happen, so we must make use of cookies or the session id along with the IP to block a node.

5. REFERENCES

1. A. Chonka *et al.*, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *J. Netw. Comput. Applicat.* Jun. 23, 2010 [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2010.06.004
2. X. Jin *et al.*, "ZSBT: A novel algorithm for tracing DoS attackers in MANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 2006, no. 2, pp. 1–9, 2006.
3. A. Shevtekar, K. Anantharam, and N. Ansari, "Low rate TCP Denial-of-Service attack detection at edge routers," *IEEE Commun. Lett.*, vol. 9, no. 4, pp. 363–365, Apr. 2005
4. G. Carl *et al.*, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan./Feb. 2006.
5. P. Du and S. Abe, "IP packet size entropy-based scheme for detection of DoS/DDoS attacks," *IEICE Trans. Inf. Syst.*, vol. E91-D, no. 5, pp. 1274–1281, 2008.
6. S. Ledesma and D. Liu, "Synthesis of fractional Gaussian noise using linear approximation for generating self-similar network traffic," *Comput. Commun. Rev.*, vol. 30, no. 2, pp. 4–17, 2000.
7. E. Perrin *et al.*, " th-order fractional Brownian motion and fractional Gaussian noises," *IEEE Trans. Signal Process.*, vol. 49, no. 5, pp. 1049–1059,May 2001.
8. E. Perrin *et al.*, "Fast and exact synthesis for 1-D fractional Brownian motion and fractional Gaussian noises," *IEEE Signal Process. Lett.*, vol. 9, no. 11, pp. 382–384, Nov. 2002.
9. Y. Bao and H. Krim, "Renyi entropy based divergence measures for ICA," in *Proc. IEEE Workshop on Statistical Signal Processing*, 2003, pp. 565–568
10. Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in *Proc. ACM SIGCOMM Conf. Internet Measurement (IMC 2005)*, 2005, pp. 32–32.
11. H. Aljifri, "IP Traceback: A New Denial-of- Service Deterrent," *IEEE Security and Privacy* , May/June 2003, pp. 24-31.
12. T. Anderson, et al, "Rocketfuel: An ISP Topology Mapping Engine", http://www.cs.washington.edu/research/networking/rocketfuel/, 2006.
13. S. Bellovin, J. Schiller, and C. Kaufman, "Security Mechanism for the Internet", *RFC 3631*, Internet Eng. Task Force, 2011.

14. Jawwad A. Shamsi, Sufian Hameed, Waleed Rahman, Farooq Zuberi, Kaiser Altaf, Ammar Amjad, "Clicksafe: providing security against clickjacking attacks attacks", 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering.
15. Yang Xiang, *Member, IEEE*, Ke Li, and Wanlei Zhou, *Senior Member, IEEE,"* Low-Rate DDoS Attacks Detection and Traceback by using new information metrics" IEEE Transaction Formation Forecies and security VOL. 6, NO. 2, JUNE 2014, Digital Object Identifier 10.1109/TIFS.2014.2107320.
16. Jinfu Chen_, Huanhuan Wang, Dave Towey, Chengying Mao, Rubing Huang, and Yongzhao Zhan, "Worst-Input Mutation Approach toWeb Services Vulnerability Testing Based on SOAP Messages" TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 02/13 pp429-441 Volume 19, Number 5, October 2014.
17. Yu Chen, *Member IEEE*, Kai Hwang, *Fellow IEEE*, and Wei-Shinn Ku, *Member, IEEE, "*Collaborative Detection of DDoS Attacks
over Multiple Network Domains" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, TPDS-0228-0806 *Manuscript received August 14, 2006; revised Dec. 23, 2006; accepted April 10, 2007; published online June 2007***.** *Recommended for acceptance by S. Olariu.*