World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 7, 307-310, 2011

Implementing a Web Browser with Web Defacement Detection Techniques

Tushar Kanti
Department of Computer Science And Engineering
Lakshmi Naraian College of Technology,
Bhopal(M.P.), India

Prof. Vineet Richariya
Department of Computer Science And Engineering
Lakshmi Naraian College of Technology,
Bhopal(M.P.), India

Prof. Vivek Richariya
Department of Computer Science And Engineering
Lakshmi Naraian College of Technology,
Bhopal(M.P.), India

Abstract—Website Defacement is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. The most common method of defacement is using SQL Injections to log on to administrator accounts. Defacements usually consist of an entire page. This page usually includes the defacer's pseudonym or "Hacking Codename." Sometimes, the Website Defacer makes fun of the system administrator for failing to maintain server security. Most times, the defacement is harmless, however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware or deleting essential files from the server. Web defacement results in extreme embarrassment to the web site owner, regardless of the commercial interest in the web site. However, persons and companies who are targets of web defacement, often have substantial interest in maintaining the professional image and integrity of the web site. This paper proposes a checksum based web defacement detection mechanism. We developed a prototype web browser which can be used to check the defacement on a particular website. We also propose a recovery mechanism for the defaced pages using the same checksum based approach.

Keywords- Web defacement; web security; threat detection; prevention.

I. INTRODUCTION

The problem of protecting web servers from crackers and vandals has received substantial attention as the commercial interests in the web have grown. This problem is the general and familiar security problem of protecting confidentiality, integrity and availability. All three aspects need to be maintained and improved in order to build the multi-billion dollar facet of trade known as e-commerce. Despite the broad understanding of the problem and numerous guidelines, there are few ways to enforce, or guarantee these security aspects. Prevention of web defacement is a practical facet of the problem of maintaining web server software and content integrity. This paper forms part of the internationally ongoing research to address this situation. Web defacement differs from other forms of system breaches in two ways. Firstly, such defacements are typically very visible to the outside world. Secondly, such defacements are often used to use an organization's server to distribute a hate speech message, or some other message that the organization does not want to be associated with. Hence, such defacement could cause considerable embarrassment to an organization and be the cause of a significant loss of credibility.

Web defacement occurs when an intruder maliciously alters a Web page by inserting or substituting provocative and frequently offending data. The defacement of an organization's Web site exposes visitors to misleading information until the unauthorized change is discovered and corrected. Web defacement is a significant and major threat to businesses developing an online presence. Defacement of a Web site can detrimentally affect the credibility and reputation of the organization as a whole. Unlike other attack cases where the hacker hides his activities, in defacement incidents, the major goal of the hacker is to gain publicity by demonstrating the weakness of the existing security measures. The damage from a Web defacement incident can be disproportionate. Damage can

range from loss of customer trust to loss of revenue. An e-retailer can lose considerable patronage if its customers feel its e-business is insecure. Financial institutions, which emphasize security and credibility, may experience significant loss of business and integrity, due to security breaches in their Web site. Along the spectrum, consumer confidence and loyalty in these organizations can have serious negative implications.

There's an overwhelming need for a solution that eliminates compromises to the Web server, especially Web page defacement. Ideally, it would prevent the hacker from making any modifications, thereby precluding any possibility of attracting attention. The Web server would never present a defaced page to a user. Equally important, a proactive solution would eliminate any after-the-fact need for recovery and fixes, and be transparent to standard operations.

II. BACKGROUND

The modern day internet as we know it, is no longer a text based system used for sharing files among universities as it used to be many years ago. In today's internet there are all types of multimedia, graphics, animation and so forth. People are now able to hold databases online, conduct blogs, forums, chat, and use many other forms of communication. As technology advances in favor of more potent and efficient means of transferring data and as the internet becomes more elaborate, so do the hackers. Common day non-technical people now have to deal with constantly upgrading, patching, and employing anti-virus software in order to protect themselves from attacks and vulnerabilities. An important and often overlooked aspect of web design is web security, securing your website is an extremely important step in maintaining data integrity and availability of resources.

Web defacement once considered a joke or a prank pulled off by kids is now considered a major threat to websites. It used to only embarrass the company who had gotten defaced. However we are now seeing it evolve into more sinister and dangerous intentions. Personal information such as credit card numbers or other forms of identity can be picked off by savvy hackers who manage to break into a website. For these reasons, web defacements warrants serious considerations from security experts and should be a top priority for any website owner.

The following graph will show the web defacement statistics[10] of Indian websites for a period of three months:

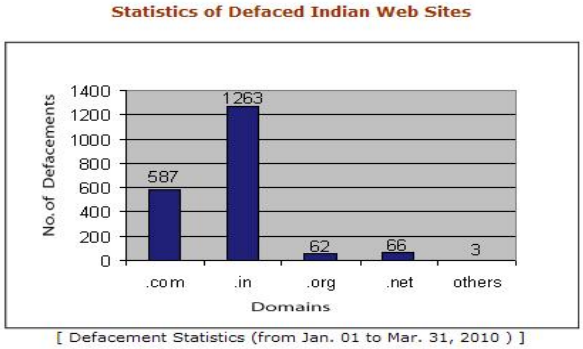

Figure 1: Defacement statistics of indian websites

Webpage defacement occurs when an attacker completely changes the appearance of a site. Today, most web page defacements take place when attackers manage to find any vulnerability in the Web application and then inject a remote scripting file. Basically, all attackers need to deface a site is a certain vulnerability in the way the website is put up. Once they discover this shortcoming, they can make their way in and severely alter the appearance of a page.

Website defacement is an extremely important topic that should warrant as much focus on security as any other area of information Technology. If a hacker is able to deface a website, this essentially means that a serious breach has occurred. Many defacers do it as a form of internet graffiti, but once inside your website a lot of information can get stolen, such as credit card numbers and other personal information.

III. METHOD

In this paper we have proposed an algorithm for defacement detection. We have also implemented a Web browser with inbuilt defacement detection techniques. We periodically calculate the checksum for Defacement detection frequency is based on the saved hash code or checksum for each web page.

Web page links	Checksum
p1	c1
p2	c2
p3	c3
p4	c4
p5	c5
p6	c6
p7	c7

Here, ci represents the checksum code of the web page pi. First the web page will be input the checksum for the web page will be calculated. This page if new will be saved in the database of checksum as ci.

For any web page if it is changed the checksum will be calculated as nci and it will be compared with the saved checksum, if the checksum is found to be same then it is not defaced otherwise it is will be marked as defaced. The

proposed method can be summarized in the following flowchart:

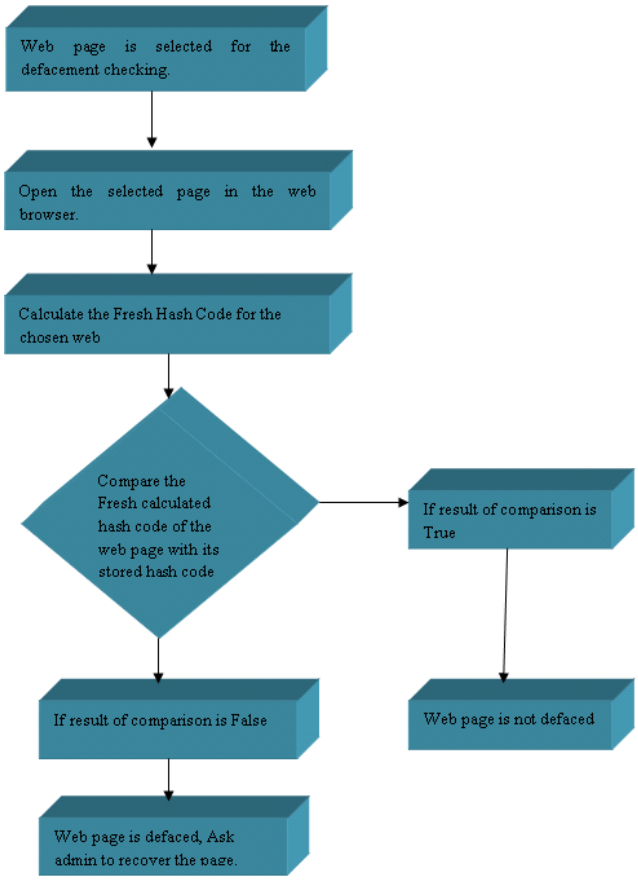

Figure 2: Proposed method of defacement detection

IV. IMPLEMENTATION

Our prototype currently includes a C#.Net implementation of a web browser. Installation of the system is simple. The server admin will have to use this web browser for opening the web pages. He will not see a difference for regular pages as the core of the browser is wrapped around Internet explorer's engine. In case defacement is detected the admin is notified and is advised to recover the page. Proposed algorithm for Web defacement detection and recovery is as follows:

1) On the basis of web page relevance and its defacement checking a web page (pi) is selected for the defacement checking.
2) Calculate the Fresh Hash Code (ci) for the chosen web page pi in step 1, using MD5 or SHA1 algorithms.
3) Compare the Fresh calculated hash code (nci) of the web page pi with its stored hash code ci in the database.
   a) if result of comparison (nci == ci) is True, then the web page is not defaced and process will stop.
   b) if result of comparison (nci == ci) is False, then the web page is defaced or the contents of the page is changed, so go to step 4.

Reload the web page pi, and stop the process.

The screenshots for the prototype web browser are as follows:

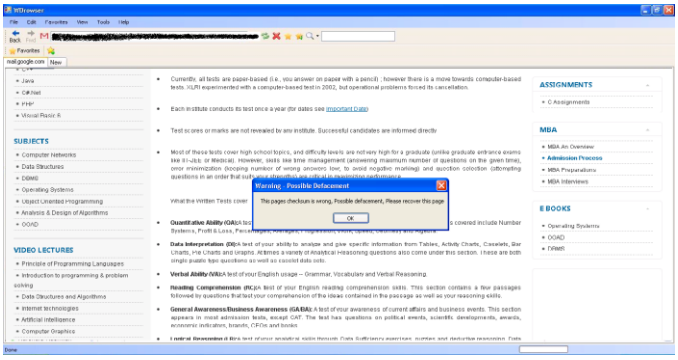

Figure 3: Screenshot of proposed implementation

V. RESULT

The proposed algorithm web compared with the existing integrity based web defacement detection methods, Our proposed method found to be detecting approximately 45% more defacements. The details of the tests can be illustrated in a graphical form as:

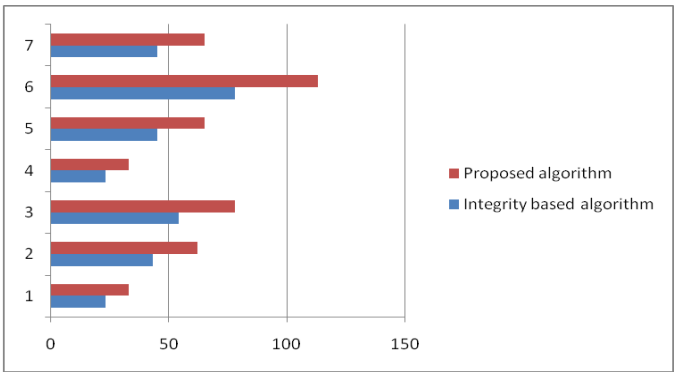

Figure 4: Defacement detection using integrity based approach and proposed algorithm

VI. CONCLUSION

In this paper, a technique is presented for website defacement detection and recovery using checksum. Web defacement checking will reduce the processing overhead of calculating the checksum of whole website frequently. Since the proposed framework will provide more frequent defacement checking of the selected pages so it reduces the risk from defacement. Since integrity based web defacement methods are not feasible for dynamic web pages and the proposed framework is also based on integrity, so the framework is applicable to static web pages only. The proposed algorithm used in conjunction with the proposed prototype of web browser will help the server admin to get notified of possible defacements and will help them to recover such pages.

REFERENCES

[1] M Bishop. Computer Security, Art and Science. Addison Wesley, Boston, MA, USA, 2003.

[2] C Liu, J Marchewka, J Lu, and C-S Yu. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. Information and Management, January 2004. doi:10.1016/j.im.2004.01.003.

[3] H Nam, J Kim, S J Honga, and S Lee. Secure checkpointing. Journal of Systems Architecture, 48:237–254, March 2003. doi:10.1016/S1383-7621 (02) 00137-6.

[4] David Buttler, Daniel Rocco and Ling Liu, "Efficient Web Change Monitoring with Page Digest", May 17–22, 2004, New York, USA. ACM 1581139128/ 04/0005.

[5] Guohun Zhu and YuQing Miao, "Co-operative Monitor Web Page Based on MD5", LNCS 3033, pp. 179–182, Springer- Verlag Berlin Heidelberg 2004.

[6] Project Gamma. Defaced web site archive. http://defaced.projectgamma.com/.

[7] Anonymous. Approximately 35 South African Web sites cracked simultaneously. SA Computer Magazine, 12(5):12, May/June 2004.

[8] B B Madan, K Goeva-Popstojanova, K Vaidyanathan, and K Trivedi. A method for modeling and quantifying the security attributes of intrusion tolerant systems. Performance Evaluation, 56:167–186, March 2004. doi:10.1016/j.peva.2003.07.008.

[9] J Jacob. The basic integrity theorem. In Computer Security Foundations Workshop IV, June 1991.

[10] http://100miles.yolasite.com/blog/1981-indian-websites-defaced-in-just-three-months

AUTHORS PROFILE

Tushar Kanti

Final Year Student Master of technology in Software Engineering (Dec'11) from Lakshmi Naraian college of Technology, Rajiv Gandhi University, Bhopal(M.P.), India

Vineet Richariya

Vineet Richariya is Head Of Department of Computer Science And Engineering, Lakhmi Narain College Of Technology, Bhopal, India. He did his MTech(Computer Science & Engineering) from BITS Pillali in year 2001.He did his B.E (Computer Science & Engineering) from Jiwaji University, Gwalior, India in year 1990.

Vivek Richariya

Vivek Richariya is Professor in department of Computer Science And Engineering, Lakhmi Narain College Of Technology, Bhopal, India.