View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by International Institute for Science, Technology and Education (IISTE): E-Journals

Computing, Information Systems, Development Informatics & Allied Research Journal
ISBN 978-2257-44-7(Print) ISSN 2167-1710 (online)
Vol. 4. No. 2, 2013 – www.cisdijournal.net

www.iiste.org

AN INTEGRATED SYSTEM FOR DETECTION AND IDENTIFICATION OF SPAMBOT WITH ACTION SESSION AND LENGTH FREQUENCY

*** I. Adegbola,**
Department of Computer Science
Emannuel Alayande College of Education
Lanlate Campus
Oyo State, Nigeria

R. Jimoh
Department of Computer Science
University of Ilorin
Ilorin, Nigeria
jimoh_rasheed@yahoo.com

O.B. Longe
Department of Computer & Information Systems
Adeleke University
Ede, Nigeria
longeolumide@fulbrightmail.org

[1]Corresponding Author

ABSTRACT
We propose an integrated system for detection and identification of spambot with action session and length frequency based on the notion of *control-flow graph*, which models interactions of the end-user's machine and browser with the Web site, and assists a lot in detecting possible anomalies. User's interaction with the web is premised on Document Object Model (DOM) Events since the DOM forms a representation of the Web page which shows acceptance of asynchronous input from the user. The DOM is a platform-independent, event-driven interface which accepts input from the user and allows programs and scripts to access and update the content of the page. Proof of concept will be established by deploying the DOM antiSpambot as an add-on for Mozilla Firefox using JavaScript.

Keywords: Antispam, DOM, detection, frequency, Action Session, Browsers and Web.

1. INTRODUCTION

A **spambot** is an automated computer program designed to mimic human behaviour in the sending and spreading of spam. Spambots usually create fake accounts and send spam using them. This has been made possible with the advent of **web 2.0** which is a terminology used to describes websites that use technology beyond the static pages of earlier websites. A Web 2.0 site may allow users to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community, in contrast to websites where people are limited to the passive viewing of content. Examples of Web 2.0 include social networking sites, blogs, wikis, video sharing sites, hosted services, web applications, mashups and folksonomies.[4] This has given rise to a new trend of spam called spam 2.0 i.e a fake profile in an online community, an unsolicited comment in blog, a commercial unwelcome thread in an online discussion boards etc [1, 2].

To stop spambots activities, generally most websites adopt *Completely Automated Public Turing test to tell Computers and Human Apart* (CAPTCHA) which is a popular challenge-response technique to differentiate web robots from humans [8]. However, CAPTCHA is not a suitable solution for stopping spambots and it inconveniences human users. Existing research shows that by making use of machine learning algorithm even CAPTCHA based techniques can be deciphered by programming code [9-11]. Other filtering techniques are content based i.e. focusing on spam content classification rather than spambot detection [1, 3]

2. REVIEW OF LITERATURE

Currently, it is relatively easy to manage and filter ordinary spam content. However detection and management of spambot on web 2.0 generally refer to as spam 2.0 has not received a comprehensive attention.

To the best of our knowledge spam 2.0 is a contemporary issue and its actively being investigated by researchers in a field considered to be quiet young. The table below listed relevant papers and technique applied in them on spambot detection and management. This review is generally based on recency of publication.
.

S/N	Spambot Detection Technique	References
1	*Completely Automated Public Turing test to tell Computers and Human Apart* (CAPTCHA)	[7] [8-10]
2	Detection of unseen and camouflaged web robots	[3]
3	Malicious web robot detection method based on HTTP headers and mouse movement	[6] [16]
4	User web access logs techniques	[14], [15]
5	Web tracking system to track spambot data HoneySpam2.0	[5]
6	Interaction with spam botnet controllers	[17]
7	Study of opinion spam in review-gathering websites	[11] [25] [26]
8	Identification of video spammers in online social network by means a Support Vector Machine classifier	[13]
9	Survey spam filtering techniques	[12]

Traditionally websites adopt (CAPTCHA) *Completely Automated Public Turing test to tell Computers and Human Apart* which is a popular challenge-response technique to differentiate web robots from humans [8]. However, CAPTCHA is not a suitable solution for stopping spambots and it inconveniences human users. Existing research shows that by making use of machine learning algorithm even CAPTCHA based techniques can be deciphered by programming code [9-11]. In the web robot detection, Tan et al. [3] propose a framework to detect unseen and camouflaged web robots. They use navigation pattern, session length and width as well as the depth of webpage coverage to detect web robots. This research has not been study in detection of spam 2.0. where a spam can mimic human user.

Park et al. [7] present a malicious web robot detection method based on HTTP headers and mouse movement. However this work has also not study spambots in Web 2.0 applications.

Yiquen et al.[18] and Yu et al. [19] utilise user web access logs to classify web spam from legitimate webpages. However the focus of their work relies on user web access log as a trusted source for web spam classification.

HoneySpam 2.0 [4] proposed a web tracking framework to track spambot data. This is a framework for accumulating spambot web usage data rather than for detecting spambots.

Another spam filtering approach proved to be yielding was that proposed by Göbel et al. [2] [21] [19]. Their proposed framework includes interaction with spam botnet controllers which can provide the latest spam messages. Later, it can present a template for current spam runs to improve spam filtering techniques.

Jindal and Liu [12] study opinion spam in review-gathering websites. They propose a machine learning approach based on 36 content-based features to differentiate opinion spam from legitimate opinion.

Zinman and Donath [13] attempted to create a model to distinguish spam profiles from legitimate ones in Social Networking Services. Their machine learning based method uses content-based features to do the classification.

Benevenuto et al. [16] provide a mechanism to identify video spammers in online social network by means of a Support Vector Machine classifier against content-based features. Heymann et al. [15] survey spam filtering techniques on the social web and evaluate a spam filtering technique on a social tagging system.

Pedram et al [20] experimented with Behaviour-Based web spambot detection by utilising action time and action frequency. In [21] an approach was presented for detecting e-mail spam originating hosts, spam bots and their respective controllers based on network flow data and DNS metadata

Most of the above reviews focus on one particular type of spam and are limited to the content attributes of that particular domain. Moreover, they do not study the source of the spam problem, i. e. the spambot. Others are for accumulation of spambot web usage data rather than for detection of spambots.

3. RESEARCH APPROACH

.

DOM Detection for Web Spambot Attack

We want to design the web Spambot detection based on the notion of *control-flow graph*, which models interactions of the end-user's machine and browser with the Web site, and assist a lot in detecting possible anomalies. [20][21]. To capture the users' interactions with the browser we rely on DOM (Document Object Model) Events , since the DOM forms a representation of the Web page as shown to the user and accepts asynchronous input from the user.

The DOM is a platform-independent, event-driven interface which accepts input from the user and allows programs and scripts to access and update the content of the page. As a proof-of-concept, we are going to deploy the DOM antiSpambot as an add-on for Mozilla Firefox, using JavaScript.

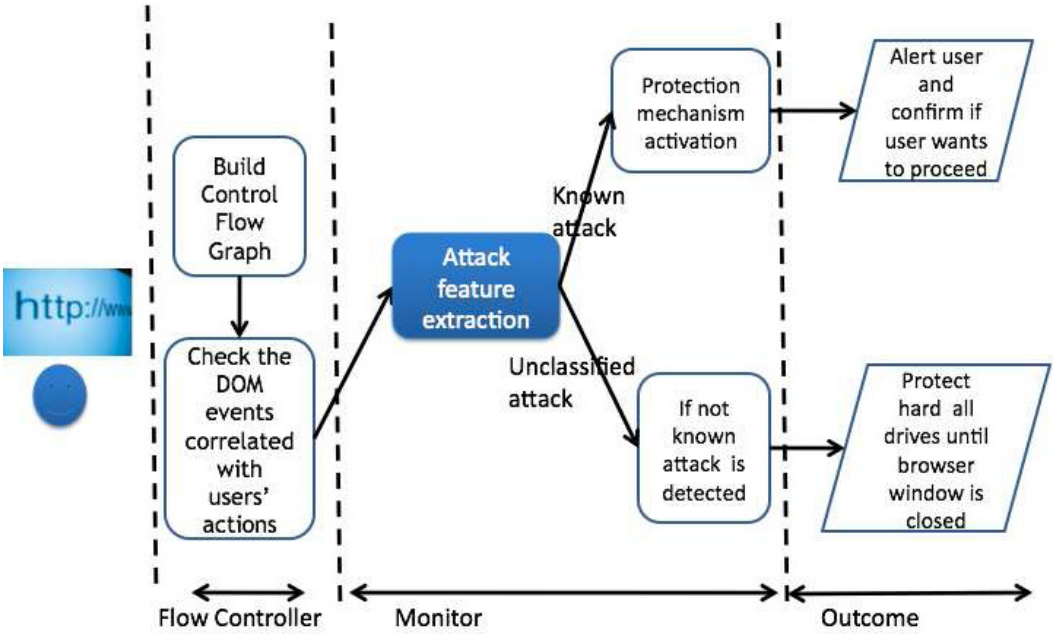

Fig. 1: Proposed Framework for the Integrated Spam Detection System

4. CONCLUDING REMARKS

We have presented a development paradigm for an integrated spam detection system to tackle the problem of spambots and botnets. We intend to establish a Proof of concept of the workability of the system by experimenting it as an add-on an open source software browser – the Mozilla Firefox.

REFERENCES

[1] P. Hayati and V. Potdar, "Toward Spam 2.0: An Evaluation of Web 2.0 Anti-Spam Methods " in *7th IEEE International Conference on Industrial Informatics* Cardiff, Wales, 2009.
[2] P. Hayati, K. Chai, V. Potdar, and A. Talevski, "HoneySpam 2.0: Profiling Web Spambot Behaviour," in *12th International Conference on Principles of Practise in Multi-Agent Systems*, Nagoya, Japan, 2009, pp. 335-344.
[3] A. Luis von, B. Manuel, and L. John, "Telling humans and computers apart automatically," *Commun. ACM,* vol. 47, pp. 56-60, 2004.
[4] 031072208 (2005-10-01)."Web 2.0: Compact Definition".Scholar.googleusercontent.com. Retrieved 2013-06-15.
[5] P. Hayati, K. Chai, V. Potdar, and A. Talevski, "HoneySpam 2.0: Profiling Web Spambot Behaviour," in *12th International Conference on Principles of Practise in Multi-Agent Systems*, Nagoya, Japan, 2009, pp. 335-344.
[6] R. M. Donald, "PATRICIA\—Practical Algorithm To Retrieve Information Coded in Alphanumeric," *J.ACM,* vol. 15, pp. 514-534, 1968.
[7] M. Kurt, "Compressed tries," *Commun. ACM,* vol. 19, pp. 409-415, 1976.
[8] R. Cooley, B. Mobasher, and J. Srivastava, "Web mining: information and pattern discovery on the World Wide Web," in *Tools with Artificial Intelligence, 1997. Proceedings. Ninth IEEE International Conference on*, 1997, pp. 558-567.
[9] C. Aggarwal, J. L. Wolf, and P. S. Yu, "Caching on the World Wide Web," *Knowledge and Data Engineering, IEEE Transactions on,* vol. 11, pp. 94-107, 1999.
[10] J. Dean and M. R. Henzinger, "Finding related pages in the World Wide Web," *Computer Networks,* vol. 31, pp. 1467-1479, 1999.
[11] J. Nitin and L. Bing, "Opinion spam and analysis," in *Proceedings of the international conference on Web search and web data mining* Palo Alto, California, USA: ACM, 2008.
[12] H. Paul, K. Georgia, and G.-M. Hector, "Fighting Spam on Social Web Sites: A Survey of Approaches and Future Challenges," *IEEE Internet Computing,* vol. 11, pp. 36-45, 2007.
[13] F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, C. Zhang, and K. Ross, "Identifying Video Spammers in Online Social Networks," in *AIRWeb '08* Beijing, China, 2008.
[14] L. Yiqun, C. Rongwei, Z. Min, M. Shaoping, and R. Liyun, "Identifying web spam with user behavior analysis," in *Proceedings of the 4th international workshop on Adversarial information retrieval on the web* Beijing, China: ACM, 2008.
[15] H. Yu, Y. Liu, M. Zhang, L. Ru, and S. Ma, "Web Spam Identification with UserBrowsing Graph," in *Information Retrieval Technology*, 2009, pp. 38-49.
[16] Cooley, R., Mobasher, B., Srivastava, and J.: Web mining: information and pattern discovery on the World Wide Web. Tools with Artificial Intelligence, 1997. Proceedings., Ninth IEEE International Conference on (1997) 558-567
[17] G. Jan, Bel, H. Thorsten, and T. Philipp, "Towards Proactive Spam Filtering (Extended Abstract)," in *Proceedings of the 6th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* Como, Italy: Springer- Verlag, 2009.
[18] H. Yu, Y. Liu, M. Zhang, L. Ru, and S. Ma, "Web Spam Identification with User Browsing Graph," in *Information Retrieval Technology*, 2009, pp. 38-49.
[19] L. Yiqun, C. Rongwei, Z. Min, M. Shaoping, and R. Liyun, "Identifying web spam with user behavior analysis," in *Proceedings of the 4th international workshop on Adversarial information retrieval on the web* Beijing, China: ACM, 2008
[20] Pedram Hayati , Kevin Chai Vidyasagar Potdar , Alex Talevski (2010)
Proceeding ICCSA'10 Proceedings of the 2010 international conference on Computational Science and Its Applications - Volume Part II Pages 351-360 Springer-Verlag Berlin, Heidelberg ©2010
[21] Willa K. Ehrlich, Anestis Karasaridis, Danielle Liu, and David Hoeflin (2011). Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling www.usenix.org/event/leet10/tech/full_papers/Ehrlich.pdf