Available online at www.sciencedirect.com

ScienceDirect

Journal of Network and
Computer Applications 30 (2007) 445–465

Journal of NETWORK and COMPUTER APPLICATIONS

www.elsevier.com/locate/jnca

The design and implementation of an agent-based framework for acceptable usage policy monitoring and enforcement

B. Stephen*, L. Petropoulakis

Department of Electrical and Electronic Engineering, University of Strathclyde, Royal College,
204 West George Street, Glasgow G1 1XW, USA

Received 11 November 2005; accepted 7 June 2006

Abstract

Reliance on the Internet in the workplace means that manually monitoring compliance with an Acceptable Usage Policy (AUP) is impractical given the volumes of data generated. Therefore, for such a system to function effectively, the processing of vast audit trails obtained must be processed by automated means. This paper introduces the incorporation of a novel user-monitoring framework into the domain of software agents for large-scale auditing of Internet use with possible extensions to general network use. It is intended that such an approach would replace current ad-hoc methods such as those based on perusing server logs with a more accurate representation of user activity. The system described herein is an experimental multi-agent one provisionally known as WebEngzilla, which actively monitors and reports on the Web browsing behaviour habits of network users unifying an ambient client monitoring system with a distributed data mining back end.

Keywords: Data mining; Collaborative filtering; Software agents; User profiling

1. Introduction

Abuse of network resources is becoming an increasingly serious threat to business. With rising numbers of employers having to discipline staff due to violations of their corporate

*Corresponding author. Tel.: +44 141 548 4840; fax: +44 141 552 2487.
E-mail address: bstephen@eee.strath.ac.uk (B. Stephen).

1084-8045/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2006.06.004

Acceptable Usage Policy (AUP), the costs of abuse emanate from more than just time wasting. Into every contract of employment there is an unwritten, mutual degree of trust between both parties. Implicitly this would amount to 'Do your work and I won't ask you if you're doing your work'. More formally however, most companies opt for an AUP signed by employees before they are permitted to use network resources. After all, the directors of a company are responsible for misuse of their company's resources. A recent survey by Hoffman et al. (2003) showed that in email usage alone, more than half of employees asked admitted to behaving 'immorally' in using the medium with almost a third having sent offensive material.

The majority of companies questioned in the (Hoffman et al., 2003) study monitored their employees Internet usage either constantly or constantly 'only with good reason' i.e. a particular offender. This 'good reason' was based upon allegation of misconduct derived from routine manual checks on URL requests. This fairly laborious process entailed taking the top 10 requested URLs and looking for those that served no apparent business purpose. Whether this entails manually checking the content of the offending URL or merely its presence on a blocking list, this is an operation that would have to be performed regularly by IT personnel in order to be effective. Manual monitoring in this way also incurs additional precautions to be taken, particularly with regard to privacy and data protection. Many laws on corporate monitoring both in the UK and the US advocate an automated approach to monitoring of employees behaviour and use of corporate communications devices (100 STAT, 1848; Statutory Instrument, 2000).

This more recent development calls for far greater accuracy in categorising the nature of access. If a decision to confront an employee on this issue is made on the basis of a false alarm, management may face harassment claims from the employee who triggered it. Inevitably, sites will be visited out with the control of the user, either through:

- mistyping the URL,
- 'hi-jacking' a domain name,
- pop-up advertisements,
- automated browser redirection.

To counter the shortcomings in existing approaches to network usage monitoring, this paper proposes a system that automates this task using an expandable community of software agents performing common information retrieval tasks. The approach proposed for gathering usage data is capable of providing far more detail than existing 'network edge' approaches. While this paper focuses entirely on monitoring Web browsing use of the Internet, the principles can be applied to any data source such as email or even general computer use. Commercial software exists that monitors computer use, but not in a collaborative and distributed approach like the one proposed here, one that would permit an in context representation of behaviour and content. The major problem with monitoring usage in this way is the vast quantities of data obtained and lack of a centralised data source for viewing information in context.

1.1. Existing approaches to monitoring

Many tools opt for a 'network edge' approach to monitoring users. While this is good for monitoring traffic it does not give an accurate picture of user activity in terms of content or behaviour. The so-called network edge approach is usually in the form of a proxy server (Fig. 1), for HTTP specific monitoring or a packet sniffer for more general