IRM PRESS
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com

ITB9165

Chapter VII

User Types and Filter Effectiveness: A University Case Study

Geoffrey Sandy
Victoria University, Australia

Paul Darbyshire
Victoria University, Australia

ABSTRACT

As the amount of content on the Web grows almost exponentially, one of the new growth industries is that of filtering products. The effectiveness of Web-filtering software depends on a number of factors including the architecture of the software itself, and the sophistication of the users operating within its application domain. The main use of filtering software is to "block" access to controversial content such as pornography. This paper reports an investigation of the effectiveness of a filter called squidGuard in the real-world environment of an Australian University. The product is used to "block" pornographic material. This investigation simulates three classes of web users in trying to access pornography. While squidGuard did have limited success in blocking such material from novice users, the blocking rate dropped dramatically for the more experienced users using access lists. In all cases, however, access to *supposedly filtered material was gained in seconds. Under such testing, the effectiveness of squidGuard as a specific-content filter for "pornographic" material can only be seen as superficial approach at best. The use of anonymous proxy servers was found to be an easy means to by-pass the filter.*

INTRODUCTION

Filter software is increasingly used by a wide variety of groups in society and in many societies, its use is mandated by law. Filter software is used in the home and school markets. Parents and teachers use a filter to prevent children from accessing content deemed not suitable for them. Sexually explicit and violent material is of most concern to parents and teachers. The regulation of controversial material in respect to children is also an issue for organizations like libraries and universities. Recently the corporate world has embraced filter technology because of concerns expressed about loss of productivity and risks of litigation.

Fundamental to the acceptance and use of a filter are two questions. First, how effective is it in blocking content that is intended to be blocked? Second, how effective is it in not blocking content that is intended not to be blocked? Vendors claim their product is highly effective. Many vendors also claim that the product is highly effective because, before content is blocked, it is evaluated by a person using a rating or classification system. Another question that concerns effectiveness is the ease with which the software can be disabled or by-passed.

This paper reports on testing the effectiveness of a filter product, called *squidGuard*, that is used in a number of Australian universities. The test is conducted in a real-world environment at one of these universities (Victoria University), and simulates different types of consumers of Internet pornography that may be found in this environment. Victoria University mainly uses the filter to block what the vendor's blacklist describes as pornography. The university does add its own sites to the blacklist, and the product offers a number of blacklists additional to pornography.

In the following sections some background material is provided on the main approaches to filtering and the effectiveness of a range of filtering products. A description of the *squidGuard* filter is then provided. A classification scheme — that classifies users that browse the Web for Internet pornography in terms of their sophistication in browsing for specific-content — is described. A first set of trials to test the effectiveness of *squidGuard* in blocking material intended to be blocked for two levels of users is discussed. A second set of trials to test the effectiveness of *squidGuard* in blocking material that is not intended to be blocked is also discussed. The results of both sets of trials are presented. A third set of trials to test the ease with which *squidGuard* may be by-passed is discussed and the results presented.