Content Filtering Methods for Internet Pornography

Jengchung V. Chen
National Cheng Kung University, Taiwan

ShaoYu F. Huang
National Cheng Kung University, Taiwan

INTRODUCTION

The Internet is widely recognized as an important information and communication medium. It has also become a useful tool for children's education, but since the Internet is an open environment, it contains much information unsuitable for the under aged. This article introduces several content-filtering methods that can assist parents and educators in protecting children from harmful material. However, it must be noted that these are of limited value unless they are supported by sex education and parental monitoring of children's Internet use.

BACKGROUND

As a number of researchers have noted, the Internet is becoming inundated with pornographic materials (Avgoulea, Bouras, Paraskevas, & Stathakopoulos, 2003; Panko & Beh, 2002; Wishart, 2004). A simple Net search using common Internet search engines such as Google with keywords "XXX and porn" is likely to provide more than 10 million Web documents. Furthermore, these pornographic sites usually group together to form huge adult networks, thus increasing their strength and visibility (Lim, Teo, & Loo, 2002). They are also one of the first few groups to employ the latest Internet technologies in their business and Web site implementation.

THE FOUR MAJOR CONTENT-FILTERING TECHNIQUES AND WEB RATING

This section first introduces four content-filtering approaches, followed by the Web rating system. The four content-filtering techniques are Platform for Internet Content Selection (PICS), URL blocking, keyword filtering, and intelligent content analysis (Lee, Hui, & Fon, 2002).

Platform for Internet Content Selection (PICS)

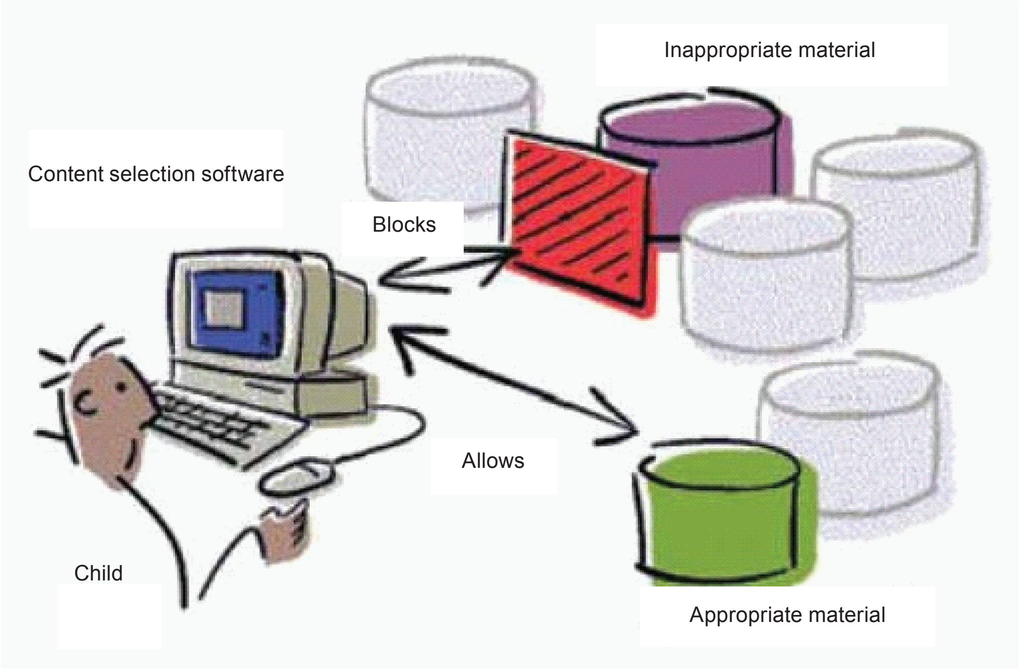
Not everyone needs to block reception of the same materials (Paul & James, 1996). The content-filtering software should consider at least three factors as follows:

1. **Supervisor:** Parenting styles differ, as do philosophies of management and government
2. **Recipient:** What's appropriate for one 15-year-old may not be for an 8-year-old, or even all 15-year-olds
3. **Context:** A game or chat room that is appropriate to access at home may be inappropriate at work or school

But in the traditional content-filtering software illustrated in Figure 1 (Paul & James, 1996), customers have limited abilities to set the software until Platform for Internet Content Selection appears. PICS is a set of specifications for content-rating systems. It lets Web publishers associate labels or metadata with Web pages to limit certain Web content to target audiences. Figure 2 shows the basic idea of flexible blocking. Parents can set the rating systems themselves.

The two most popular PICS content-rating systems are RSACi and SafeSurf. Created by the Recreational Software Advisory Council, RSACi (http://www.rsac.org/) uses four categories: harsh language, nudity, sex, and violence. For each category, it assigns a number indicating the degree of potentially offensive content, ranging from 0 (none) to 4. SafeSurf is a much more de-

Figure 1. Using a filter technique after selection software automatically blocks access to some documents, but not others (Source: Paul & James, 1996)



tailed content-rating system. Besides identifying a Web site's appropriateness for specific age groups, it uses 11 categories to describe Web content's potential offensiveness. Each category has nine levels, from 1 (none) to 9. Currently, Microsoft Internet Explorer, Netscape Navigator, and several content-filtering systems offer PICS support and can filter Web pages according to the embedded PICS rating labels. However, PICS is a voluntary self-labeling system, and each Web content publisher is totally responsible for rating the content. Consequently, content-filtering systems should use PICS only as a supplementary filtering approach.

URL Blocking

This technique restricts or allows access by comparing the requested Web page's URL (and equivalent IP address) with URLs in a stored list. Two types of lists can be maintained: a black list contains URLs of objectionable Web sites to block; a white list contains URLs of permissible Web sites. Most content-filtering systems that employ URL blocking use black lists. The chief advantages of this approach are speed and efficiency. A system can make a filtering decision by matching the requested Web page's URL with one in the list even before a network connection to the remote Web server is made. However, this approach requires implementing a URL list, and it can identify only the sites on the list. Also, unless the list is updated constantly, the system's accuracy will decrease over time, owing to the explosive growth of new Web sites. Most content-filtering systems that use URL blocking employ a large team of human reviewers to actively search for objectionable Web sites to add to the black list. They then make this list available for downloading as an update to the list's local copy. This is both time consuming and resource intensive. Despite this drawback, the fast and efficient operation of this approach is desirable in a content-filtering system. Using sophisticated content analysis techniques during classification, the system can first identify the nature of a Web page's content. If the system determines that the content is objectionable, it can add the page's URL to the black list. Later, if a user tries to access the Web page, the system can immediately make a filtering decision by matching the URL. Dynamically updat-