BABEŞ-BOLYAI UNIVERSITY
CLUJ-NAPOCA

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
SPECIALIZATION DISTRIBUTED SYSTEMS IN INTERNET

DISSERTATION THESIS

Thesis Title

Author:
BREBAN Sergiu

Supervisor:
Dr. COJOCAR Dan,
Lector Universitar

June 12, 2018

UNIVERSITATEA BABEŞ-BOLYAI
CLUJ-NAPOCA

FACULTATEA DE MATEMATICĂ ŞI INFORMATICĂ
SPECIALIZAREA SISTEME DISTRIBUITE ÎN INTERNET

LUCRARE DE DISERTAŢIE

Thesis Title

Absolvent:
BREBAN Sergiu

Conducător ştiinţific:
Dr. COJOCAR Dan,
Lector Universitar

June 12, 2018

BABEŞ-BOLYAI UNIVERSITY CLUJ-NAPOCA

Abstract

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
SPECIALIZATION DISTRIBUTED SYSTEMS IN INTERNET

Master's degree

Thesis Title

by BREBAN Sergiu

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Parental controls

1.1.1 Overview

Parental controls developed in the digital era as a means to allow parents to restrict the access of content to their children and may be included in digital television services, computer and video games and mobile devices. The content may not be appropriate for their age and is aimed more at adult audiences. The characteristics of inappropriate content depends for each parent, and is also correlated with the child's age and maturity level and includes information and images that can upset the child, inaccurate information or information that can cause dangerous behavior. Some of this content could be:

- pornographic material
- content containing swearing
- sites that encourage vandalism
- pictures, videos or games which shows images of violence
- gambling sites
- unmoderated chatrooms

It is very easy for the child to stumble upon unsuitable sites by accident on any internet enabled device, like mobile phone or tablet and it can be difficult to monitor and filter the content. (*Inappropriate Content*)

Parental control solutions fall into four categories:

- content filters, which limit access to different types of inappropriate content
- usage control, which works by constraining the usage of certain devices by placing time-limits on usage or forbid some types of usage
- computer usage management tools, which enforces the use of certain software

- monitoring, which can track the activity when using the devices

The rising availability of the Internet increased the demand for methods of parental control that restrict content. Mobile phones offer the most convenient and constant method for content access, and teens ages 13 to 17 are going online frequently. A study by Pew Research Center found that 92% of teens report going online daily, 24% of which are using the internet almost constantly, 56% going online several times a day and 12% reporting once a day use. Only 6% go online weekly and 2% less often. (Lenhart et al., 2015)

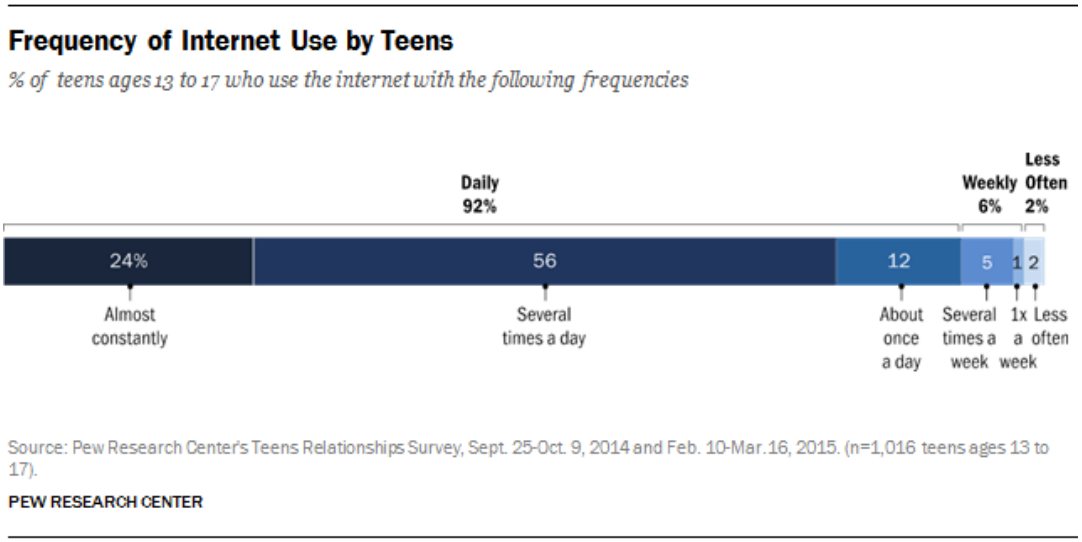

FIGURE 1.1: Frequency of Internet Use by Teens

The same study finds that nearly three-quarters have or have access to a smartphone and only 30% have a basic phone and 12% of teens 13 to 17 have no cell phone of any type.

1.1.2 Techniques

There are two types of control techniques, behavioral control, which consists of controlling the amount of time and how much the child can view, and psychological control, which involves parents tying to influence children by affecting their emotional side by manipulating or insensitivity. Adult control can be divided into three prototypes, each of which has influenced greatly the child-rearing practices (Baumrind, 1966):

- permissive: the parent attempts to behave in a nonpunitive, acceptant and affirmative manner and consult with the child about policy decisions and gives explanations for rules
- authoritarian: the parent attempts to shape, control and evaluate the behavior of the child in accordance with a set standard of conduct, by valuing obedience as a virtue and favoring punitive, forceful measures to curb self-will

- authoritative: the parent attempts to direct the child's activities in a rational manner, by sharing the reasoning behind the policy and soliciting the child's objections when he refuses to conform; disciplined conformity and autonomous self-will are valued by the authoritative parent

Several techniques exists for creating parental controls to block certain websites. Parental control software can monitor API to observe applications such as web browsers or chat applications and to intervene based on certain criteria, such as time based criteria or as a match in a database of banned words. Other techniques that involve a proxy server are also used, in which the proxy server serve as an intermediary which can intervene in the delivery of some content based on various criteria based on the content, but this method has a major disadvantage because it requires client configuration to use the service, which can be easily bypassed.

The difference between content filters and computer usage management methods is that the later is focused on empowering the parents to balance the computing environment for children, by allowing parents to enforce the learning component into the computing time of children, where children can earn play time by working through educational content. This method is very powerful because it stimulates self-regulation in children, instead on relying solely on parental control, and we will use some ideas from this method to develop our control and regulation system.

Recently, some devices which are used for network based parental control have emerged. These devices use different methods to block inappropriate content, such as packet filtering, DNS Response Policy Zone (RPZ) and Deep packet inspection (DPI), and work as a firewall router. Some commercial and governmental communication networks use these methods also, but these type of devices were developed for home also, and are used to create a new home wireless network specifically designed for kids to connect to. We developed our system using the same approach, by creating a custom wireless network for different type of users, different age level children and parents, and by using the packet filtering and DNS techniques to manage content filters.

1.1.3 Content filters

The increased use of mobile devices has created a demand for parental controls for these devices. The first carrier which offered age-appropriate content filters was Verizon, in 2007. With the release of iPhone OS 3.0 in 2009, Apple introduced a mechanism to create age brackets for users, to block unwanted applications from being downloaded. Filtering options are also offered by most internet providers, to limit internet browsing options and block unsuitable content. The software used to restrict or control the content a user is capable to access is commonly referred to as internet filter or content filter.

The content access restrictions can be applied at different levels, from governments applying them nationwide, to ISP blocking it's clients and by a parent to a child's computer. The implementation of this content filtering mechanism can be done at different levels also, by software on the client computer,

by using the network infrastructure such as proxy servers, DNS servers or firewall, but none of these solutions alone provides complete coverage, so a mix of technologies have to be used to achieve proper content control.

- Browser based filters are the most lightweight solution, and the filtering is done by using a third-party browser extension
- E-mail filters are commonly implemented using a statistical method, Bayesian filters, by acting on information contained in the mail body, headers or attachments
- Client side filters work by installing it as software on each target device
- Content-limited (or filtered) ISPs are service providers that offer access to only a set of Internet content, to implement government, regulatory or parental control over its subscribers
- Network-based filtering is done at the transport layer, by implementing a transparent proxy, redirecting user requests to it by a switch or a router, or at the application layer, by configuring the client to send requests directly to the proxy server. (*Content Gateway explicit and transparent proxy deployments*)
- DNS-based filtering is implemented at the DNS layer and works by preventing lookups for domains that do not fit within a set of rules, parental control or company rules
- Search-engine filters work by filtering out inappropriate search results, but if the client knows the URL for a specific content, he can access it without using a search engine; search providers offers child friendly versions of their engines, which filter content inappropriate for children from the search results

We implement a DNS-based filtering mechanism, to be able to easily filter out the content that is definitely harmful for a child and does not bring any value, while not being too restrictive and giving the children room to explore and find by themselves what values means and how the time is best spent on the device. The main reason for filtering is to protect the user from harmful content, but it is used also to block malware and other intrusive material, as adware, spam, computer viruses, spyware, which can be even more harmful to children. The first level of filtering that we try to do is to block ads by integrating with the open-source ad-blocking solution Pi-hole, which works as a DNS sinkhole to block advertisement and internet trackers.

Filtering mechanisms are not always efficient, and are also subject to some criticism. The filtering errors are of two kinds, overblocking, when the filter is too zealous and mislabels content that should be acceptable, such as labeling health related information as being porn-related, and under-blocking, when the filter is unable to update quickly to new information available on the Internet. Content filtering can be a powerful censorship tool and there is a lot of discussion around the morality and legality of this kind of methods

at a certain level, mostly state and country level. But it can be harmful if used incorrectly even at the family level, because using too strict policies can influence children behavior, and not always for good.

1.2 A self regulation approach

An in-depth study conducted on 75 Android apps that have the main purpose of promoting teens and children mobile online safety found that the majority of them (89%) are supported by features of parental control, and only 11% favour self-regulation. The study presented a framework for Teen Online Safety Strategies which describes the difference between parental control and teen-self regulation. The three main parental control strategies identified are:

- monitoring is the surveillance of online activities, such as text messages, call logs or web browser history; Some studies found that monitoring was associated with higher online risks for some, suggesting to use monitoring only after some kind of online problem occurred.(Duerager and Livingstone, 2012)
- restriction occurs by placing rules on online activities, as setting limits on screen time and content acceptable for viewing. This kind of methods have some positive impact, such as reducing cyberbullying, but can also have negative effects, by causing children to take more risk-seeking behaviors. (Shin and Ismail, 2014)
- active mediation involves discussions regarding online activities between parents and children, and it reduces online risks without reducing the benefits of online engagement. (Duerager and Livingstone, 2012)

Self-regulation is the ability to control the emotions and behaviors by monitoring and evaluating oneself against given social standards. The analogous teen self-regulation strategies are:

- self-monitoring is a key component of self-regulation, and children must be aware of their own motivations and actions through self-observation. (Bandura, 1991)
- impulse control is the ability to inhibit short term desires in favor of the long term consequences caused by ones' actions, and losing control of this is the main reasons why self-regulation fails (Baumeister and Heatherton, 1996)
- risk-coping is a self-regulatory process that occurs after a stressful situation, by attempting to address the problem and the negative emotions caused. Actively coping with risky online situations help teens to feel less bothered about a risky event that occurred. (d'Haenens, Vandoninck, and Donoso, 2013)

Usability was another issue in finding a good and efficient parental control mobile application. From the 89 application tested, 14 had configuration issues, some required users to have a Gmail account, other needed a VPN connection configured, some where showing annoying ads. Other apps were not meeting the goal of protecting the children from online risks, most of them were focusing on regulating web browsing and social media was one of the least prevalent activity monitored, but research suggest that most online risks, at least for adolescents, are encountered through the use of social media platforms. The features offered did not promote any values like trust, accountability, respect and transparency.

Most of the apps related to parental controls support mostly monitoring and restriction of mobile activities. Only some of the them support features like parental active mediation (<1%), teen risk-coping (4%), self monitoring (2%), or impulse control (<1%), but some of them added education as another safety strategy. We will try to have a different approach, by focusing more on the self-regulation approach while keeping the monitoring and restriction features to the minimum necessary, and try to add the education component also, to drive children to some learning resources and interactive quizes before rewarding them with some device time.

We try to design out solution by following the practices suggested in the study from (Wisniewski et al., 2017) and to focus on usability, social media control and to implement features that match the self regulation techniques. Firstly, we create 4 age brackets, 0-5, 6-10, 11-13, 14+, to be able to have more granular control and to implement specific features for each age, and we try to design the application experience by taking into account the view of the clients, the children, not just the parent's perspective. The process of establishing the rules and starting the parental control system should be done also as a collaboration between parents and children. The current solutions are fairly simplistic: as new functionality becomes available, new apps are created to regulate and monitor the children activities. While these approach prevent the risks, it also has the potential of limiting some positive engagement. As we can see in the figure below, the new framework proposed for developing mobile online safety application is founded on core family values and emphasizes parental active mediation and self-regulation. The benefit of this framework is that it is not technically tied directly to children mobile activities and can focus on supporting more important needs of parents and children. We propose prototypes to promote collaborative practices between parents and children that support risk-coping and active parental mediation, by implementing a system for the children to learn about online risks and encouraging collaborative efforts when establishing policies. Another unique opportunity for design is in the are of supporting self-regulatory processes in the absence of parents. Instead of simply giving an SOS feature to get help from adults, some other ways to support the children can be found, so that they can come up with their solutions to online problems or to come to the aid of others who could benefit from their help.

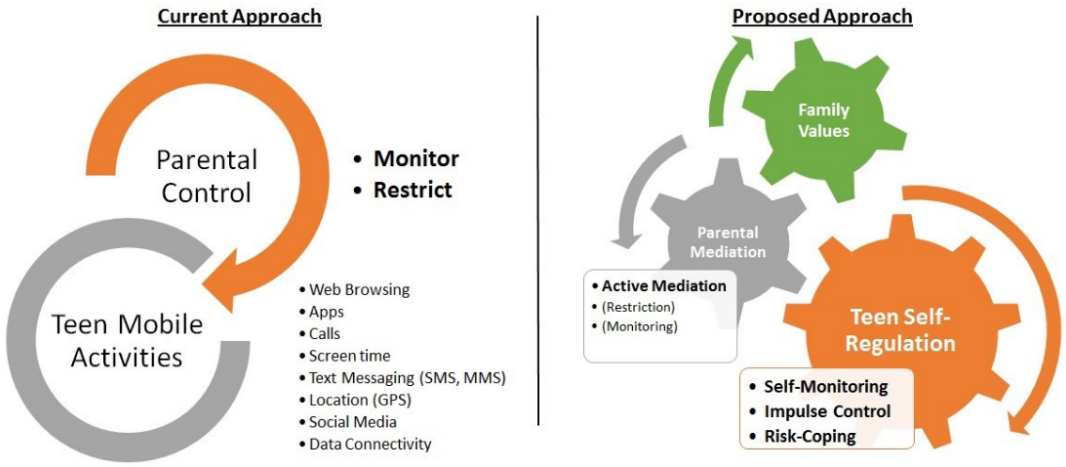

FIGURE 1.2: Current versus Proposed Approach for Online Safety Apps

Chapter 2

Content-control software and providers

Content control policies can be implemented at different levels. Some ISPs offer parental control options and even parental control software, other content control systems are integrated with the operating system, such as MacOS, which offers parental controls for some applications (Mail, Finder, iChat, Safari). The two major forms of content filtering technology are application gateway and packet inspection. The application gateway is called web-proxy for HTTP access and works by inspecting the request and the returned page using some rules and deciding if it should return the response. The packet inspection technique does not interfere with the connection, but inspect the data as it goes past and may decide at a later point to disconnect the client, by inject a TCP-Reset or similar faked packet. A combination of these two techniques is very popular because it allows more detailed filtering and can significantly reduce the cost of the system.

We will present next some parental control application and their features, on which we will try to build our system by taking a more self-regulatory approach.

2.1 Net Nanny

Net Nanny provides a content-control software as a way to monitor and control children's computer activity. The main features include blocking and filtering Internet content, place time limits on use and block PC games. Websites are blocked by content rather than URL, preventing children from accessing blocked websites through proxy websites. It is available on desktop platforms, Windows and Mac, and also on mobile platforms, Android and iOS, but the features and usability is not consistent on all platform, with some key features lacking on the mobile. It uses a dynamic filter that scans and analyses each web site to determine if it is appropriate for a child, based on a unique customization done by the parent. All the initial configuration is done online and it enforces the rules via a local client on each device it is installed. For each client, you can select from 4 profiles: Child, Pre-Teen, Teen and Adult, which can be further customized. (*Net Nanny Features*)

2.1.1 Content Filtering

Content filtering is the most used feature in all parental control systems and Net Nanny filters by analyzing the content for each web page in real time. Each site is matched against 17 objectionable categories, and each child profile have different level of blocking. Some categories are not completely blocked for some profiles, but the parents get a notification when the child visit sites in these categories. Parents can also create custom rules, to temporary allow access for some devices, and whitelists and blacklists for each child, to always allow or block certain websites. We follow the same approach by creating two classes of users for domain filtering and use a custom blocking mechanism to block certain domains for children, while allowing them for parent users.

2.1.2 Internet Time Scheduling

Children's internet use can be controlled in two ways using Net Nanny, by creating weekly schedules in half-hour increments, and you can also create weekly allowance duration in one-hour increments. This system does not depend on the system clock, so it cannot be bypassed. But it would be more useful to have more granularity when setting time limits, that's why we support 15-minute increments allowance periods for each day.

2.1.3 Email notifications

Net Nanny have two types of email notifications enabled. The first type of notification is sent when a child request a blocking exception for a specific domain, and the other one is in the form of a weekly summary. You can configure to get notification for multiple types of events, when a child hits a blocked site, continues after a warning or request a change in the blocking status. It would be more useful to have multiple options of getting notified about certain events occurring in the system, that's why we introduced mobile notifications into our system.

2.1.4 Detailed Reporting

Net Nanny offers an online console where you can view all the activity reports. You can view the activity by day, week and month, but not older than 30 days. It shows the blocked content in a pie chart, with some more information on mouse over. The report goes as deep as to show the page title, the time stamp and the user for each URL visited on a specific device. we do not include any type of reporting, because we thing that it would be a privacy issue for the child, since we try to implement a self-regulation system. All the discussion should be done in the family and the child should be warned about visiting certain domains, but not by checking every move he makes online. That's why we don't include any location related features, and Net Nanny does not support location either, but some other parental control systems do.

2.1.5 Mobile Support

The mobile support for Net Nanny is similar to the desktop experience, with some limitations. For the system to work, all the browsing should be done through the proprietary browser offered. On the iPhone the features are even more limited, because it does not interact with other apps and services at all. Since we started developing for mobile first and we try to keep the application features decoupled from the client device and system, we should not suffer of these limitations and we provide a seamless experience on both mobile platform, Android and iOS. (*Net Nanny*)

Chapter 3

A self regulation approach

Bibliography

Bandura, Albert (1991). "Social cognitive theory of self-regulation". In: *Organizational behavior and human decision processes* 50.2, pp. 248–287.

Baumeister, Roy F and Todd F Heatherton (1996). "Self-regulation failure: An overview". In: *Psychological inquiry* 7.1, pp. 1–15.

Baumrind, Diana (1966). "Effects of authoritative parental control on child behavior". In: *Child development*, pp. 887–907.

Content Gateway explicit and transparent proxy deployments. https://www.websense.com/content/support/library/deployctr/v78/dic_wcg_deploy_expl_trans.aspx. Accessed: 2018-05-30.

d'Haenens, Leen, Sofie Vandoninck, and Veronica Donoso (2013). "How to cope and build online resilience?" In:

Duerager, Andrea and Sonia Livingstone (2012). "How can parents support children's internet safety?" In:

Inappropriate Content. https://www.internetmatters.org/issues/inappropriate-content/. Accessed: 2018-05-30.

Lenhart, Amanda et al. (2015). *Teens, social media & technology overview 2015*. Pew Research Center [Internet & American Life Project].

Moore, Ben and Neil J. Rubenking. *Net Nanny*. https://www.pcmag.com/article2/0,2817,2467479,00.asp. Accessed: 2018-02-28.

Net Nanny Features. https://www.netnanny.com/features/. Accessed: 2018-05-31.

Shin, Wonsun and Nurzali Ismail (2014). "Exploring the role of parents and peers in young adolescents' risk taking on social networking sites". In: *Cyberpsychology, Behavior, and Social Networking* 17.9, pp. 578–583.

Wisniewski, Pamela et al. (2017). "Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?" In: *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. ACM, pp. 51–69.