UNIVERSIDADE FEDERAL DO AMAZONAS

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

DEPARTAMENTO DE APOIO À PESQUISA

PROGRAMA INSTITUCIONAL DE BOLSAS DE INICIAÇÃO CIENTÍFICA

PARENTAL CONTROL EM NAVEGADORES WEB

Bolsista: Diego Santos Azulay, CNPq

MANAUS

2012

UNIVERSIDADE FEDERAL DO AMAZONAS
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

DEPARTAMENTO DE APOIO À PESQUISA

PROGRAMA INSTITUCIONAL DE BOLSAS DE INICIAÇÃO CIENTÍFICA

RELATÓRIO FINAL

PIB-E/0132/2011

PARENTAL CONTROL EM NAVEGADORES WEB

Bolsista: Diego Santos Azulay, CNPq

Orientador: Prof. Dr. Eduardo Luzeiro Feitosa

MANAUS

2012

RESUMO

Este trabalho de pesquisa visa desenvolver uma solução de *Parental Control* para navegadores Web. Soluções de *Parental Control* (traduzindo do inglês, controle dos pais) tem como objetivo filtrar conteúdo, moderar o uso e controlar as atividades em qualquer ambiente que possa oferecer algum tipo de risco a algum usuário, como aparelhos de telefone, programas de computador e jogos eletrônicos. Focando na segurança na Internet, as soluções de *Parental Control* são de suma importância para os pais poderem controlar e monitorar o acesso de seus filhos e também filtrar as informações que chegam aos mesmos. Utilizando o método de *blacklists*, a solução proposta cria uma lista de sítios Web, palavras e conteúdos que não devem ser utilizados ou vistos, monitorando e controlando o acesso com base nessa lista, definida pelos pais. Desta forma, crianças ou adolescentes não são expostos a conteúdos considerados impróprios.

SUMÁRIO

1 INTRODUÇÃO

A Internet vem se consolidando cada vez mais como uma grande ferramenta de diversão, estudo e pesquisa para crianças e adolescentes. Porém, sem o uso adequado, esta ferramenta acaba se tornando prejudicial e perigosa. O grande aumento de sítios Web ofensivos e inapropriados vem preocupando pais do mundo todo e fazendo-os rever seus conceitos em relação ao conteúdo que seus filhos estão expostos ao navegarem na Internet.

Muitas vezes a criança acaba sendo levada a um conteúdo ofensivo por um clique errado ou propaganda enganosa. Redes sociais e salas de bate papo podem levar a criança ou adolescente até pessoas mal intencionadas, pondo em risco sua integridade física e mental, saindo do escopo virtual e se tornando um problema real. Além disso, o rendimento escolar também pode ser prejudicado devido ao grande número de “atrações” que se tem acesso ao navegar na Internet.

Especialistas na área afirmam que a melhor prevenção contra os perigos da Internet é o dialogo entre pais e filhos (Freeh 2001). Porém, quando esta alternativa falha, a solução mais eficaz é a de *parental control*. Soluções de *parental control* (traduzindo do inglês, controle dos pais) são aquelas que fazem monitoramento, filtragem de conteúdo e controle de acesso a qualquer ambiente em que o filho, ou usuário, corra algum risco ou perigo.

Focando na segurança na Internet, ferramentas ou soluções de *parental control* permitem o monitoramento de acesso a sítios Web, controle de horário de navegação e controle de conteúdo, podendo bloquear acesso a sítios impróprios e o acesso a conteúdos ofensivos. Tais soluções podem ser encontradas em alguns navegadores por padrão, porém tais ferramentas não suprem as necessidades básicas de controle com eficiência.

Assim, o principal objetivo deste trabalho foi desenvolver uma ferramenta de *parental control* completa e eficiente para o navegador Web Google Chrome.

2 REVISÃO BIBLIOGRÁFICA

2.1 Conceito de ferramentas de parental control na Internet

Segundo a Common Sense Media (2010), ferramentas de *parental control* podem ser softwares, hardwares ou plug-in que filtram ou bloqueiam qualquer acesso ou conteúdo que pode ser considerado como ofensivo ou inapropriado para crianças ou adolescentes na Internet.

É importante ressaltar que ferramentas de parental control são de suma importância quando a opção de diálogo entre pais e filhos não funciona, protegendo crianças e adolescentes de aliciadores.

2.2 Os perigos da navegação sem controle por parte de crianças e adolescentes

De acordo com a ChildNet International (2009), os perigos da navegação na Internet podem ser divididos em quatro categorias: (i) Contato indesejado (aliciadores, intimidadores), (ii) Conteúdo impróprio (pornografia, fotos extremas, etc.), (iii) Propagandas agressivas e (iv) Ameaças Web veladas (softwares maliciosos).

Dentre todas as categorias, a de maior perigo é a primeira, pois são as pessoas mal intencionadas na rede que entram em salas de bate papo e mensageiros instantâneos fingindo ser pessoas que não são e acabam pondo em risco a integridade física e moral dos jovens (FREEH,2001). Outro risco é a exposição a conteúdos impróprios e ofensivos a certas idades, o que acaba comprometendo o desenvolvimento sócio-cultural da criança e do adolescente.

A Figura 1 ilustra uma estatística feita pela empresa Safeline contendo a classificação de conteúdos ofensivos a crianças e adolescentes.

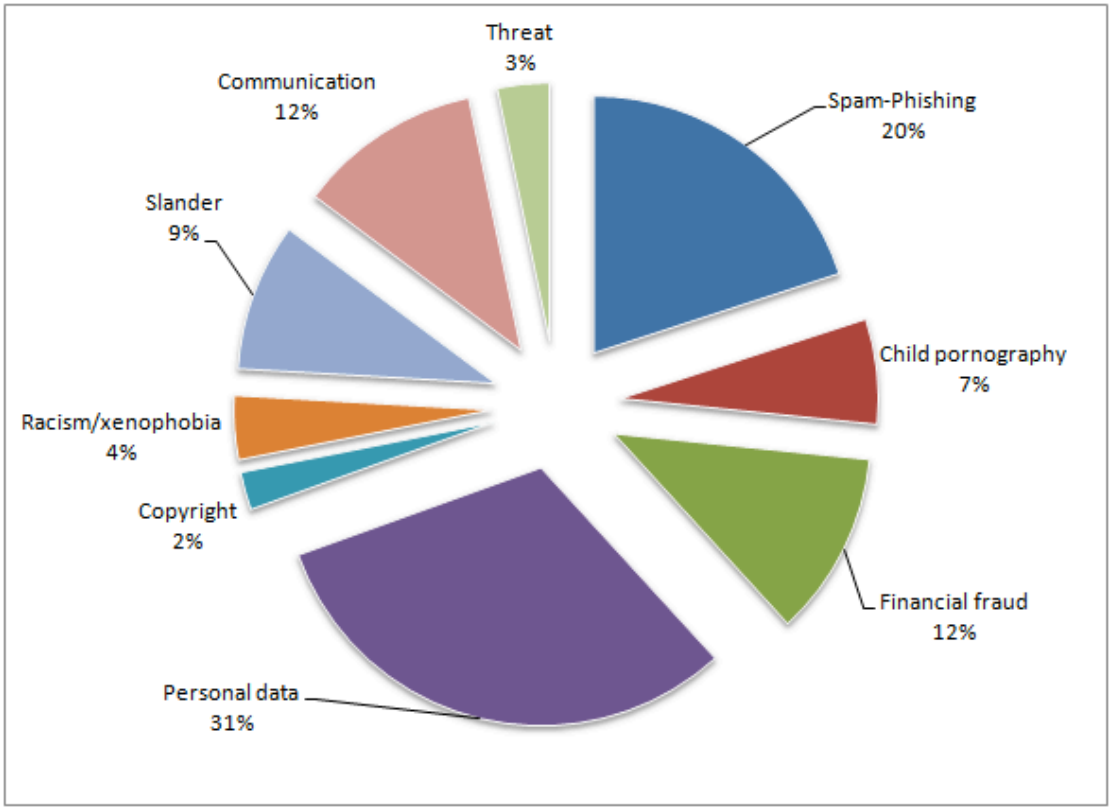

Figura 1 – Contéudo ilegal reportado ao Safeline

3.2 Ferramentas existentes

Em uma pesquisa feita pela Safeline (2011) avaliando as ferramentas existentes, percebeu-se que nenhuma cobre todas as funcionalidades de *parental control*. A mais abrangente obteve uma avaliação de 3.4 numa escala de 0 a 4. Alguns pontos são destacados:

- A maioria das ferramentas são no idioma inglês;
- As ferramentas possuem baixa efetividade em conteúdos Web 2.0 (como blogs e redes sociais);
- Algumas ferramentas possuem falhas de seguranças, possibilitando desinstalar a ferramenta ou burlar seus mecanismos de bloqueio. A falha mais comum é permitir o acesso de páginas proibidas através de sites de tradução ou do Google cache.

3 METODOLOGIA

O projeto elaborado e descrito neste documento foi desenvolvido durante certas etapas, descritas abaixo.

1. *Levantamento e estudo das ferramentas e soluções existentes de parental control*. Nesta etapa, as ferramentas existentes foram avaliadas para o entendimento de suas funcionalidades e identificação de características positivas, que pudessem ser empregadas na realização do projeto, e negativas, que pudessem ser resolvidas com o projeto.

2. *Levantamento e estudo de técnicas, mecanismos e metodologias para controle de conteúdo*. No decorrer desta etapa foram realizados levantamentos bibliográficos, pesquisas e estudos referentes ao uso de controle de conteúdo na Internet e nas soluções de *parental control* já existentes, levantando dados de cada método e comparando-os.

3. *Desenvolvimento da solução de parental control para navegadores Web*. Com base nos estudos definidos nas etapas anteriores foi desenvolvido a solução de *parental control* para o navegador Google Chrome, utilizando as técnicas com melhores performances nas avaliações, resultando em um protótipo funcional.

4. *Avaliação da solução proposta*. Nesta etapa foi feita uma avaliação do protótipo, rendendo várias sugestões de melhorias na interface e também nas suas funcionalidades, tornando a ferramenta mais eficiente e se adequando a sua proposto inicial.

5. *Ajuste da solução.* Partindo dos resultados de avaliação da etapa anterior, foi desenvolvido a versão final da ferramenta, com novas funcionalidades e uma nova interface.

4 RESULTADOS OBTIDOS

Este projeto desenvolveu a solução CURUPIRA, capaz de identificar e bloquear conteúdo Web considerado inapropriado para crianças e adolescentes. Mais especificamente, CURUPIRA utiliza duas estratégias principais de filtragem: listas negras (*blacklist*) de URL e listas de conteúdo. Na primeira, pais ou responsáveis classificam as URLs com conteúdo inapropriado, inserindo-as em uma *blacklist*. Na segunda, pais ou responsáveis inserem palavras-chaves que remetem ou representam conteúdo inapropriado em uma *blacklist*.

O fluxo de funcionamento do CURUPIRA é apresentado na Figura 1 e pode ser descrito como se segue. Quando uma URL é digitada pelo usuário, seu endereço é analisado pelo filtro de URL para verificação. Se o endereço da URL estiver na *blacklist* de páginas consideradas inapropriadas, seu acesso é automaticamente bloqueado e um alerta (e-mail e/ou SMS) é enviado para o pai ou responsável. Caso contrário, a URL segue para avaliação de conteúdo. Nesta etapa, cada página em questão tem seu conteúdo avaliado pelo filtro de conteúdo. O objetivo é verificar se alguma palavra ou texto classificado como inapto está presente no conteúdo da página. Para tanto, o filtro de conteúdo utiliza expressões regulares. É importante ressaltar que todas as classificações (URL e conteúdo) são configuradas por pais ou responsáveis.

4.1 Implementação e instalação

Antes de iniciar a descrição da implementação, é necessário esclarecer os motivos da escolha do navegador Web *Chrome* como objeto de estudo e implementação da solução CURUPIRA.

Primeiro, após meses de exaustiva busca na Internet iniciada em Abril de 2011, percebeu-se que não existiam soluções de *parental control* para o Chrome. Somente em Maio deste ano (2012) que a InspiredEffect.com anunciou uma versão do FoxFilter para Chrome. Em segundo lugar, o Chrome possui uma API simples e prática, o que facilita o desenvolvimento da solução. Além disso, nenhum deles possui versões para a língua portuguesa.

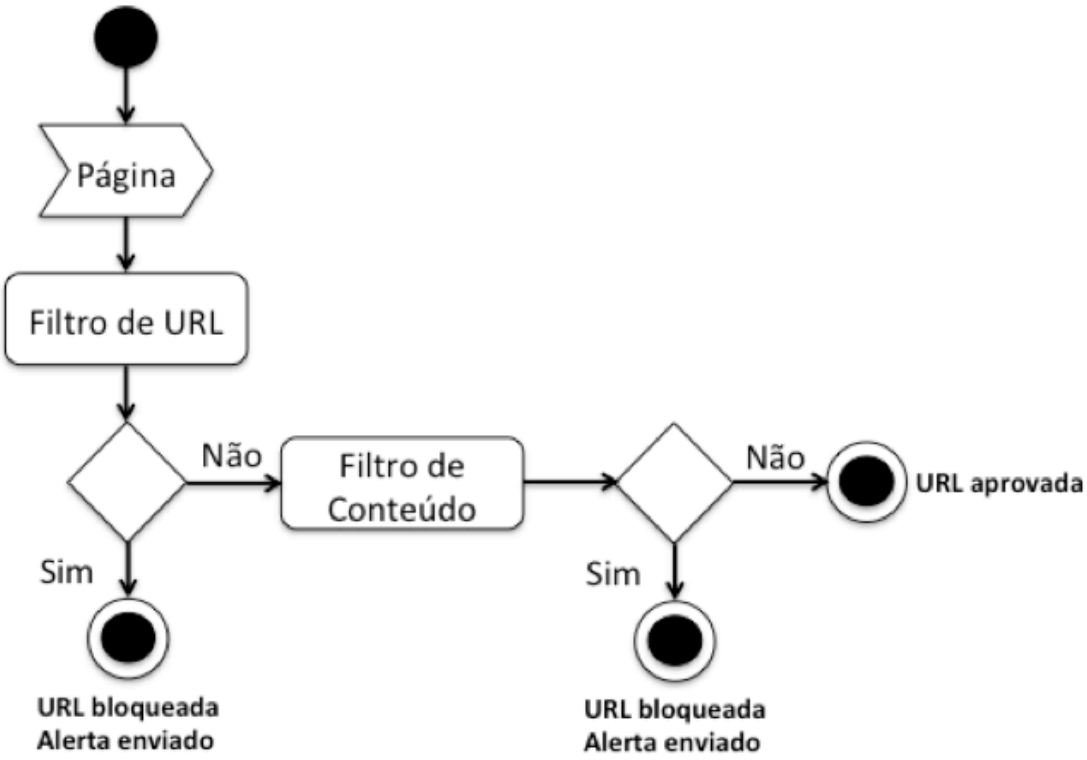

Figura 1. Fluxo de funcionamento do Curupira.

Implementação

A solução CURUPIRA foi desenvolvida na forma de uma extensão (plug-in) para o navegador Google Chrome. A extensão funciona como uma página Web. Sua interface foi feita através de HTML e CSS e a programação em si é feita com JavaScript. Para interação com o navegador, foram utilizadas funções da API do Chrome.

A Figura 2 ilustra os componentes internos da solução. O API do plug-in fornece a interface para o navegador Chrome. Ela também implementa os módulos que executam as opções de filtragem (URL e Conteúdo) para o usuário (pais ou responsáveis), adicionando ou removendo filtros do processo de validação. O plug-in faz uso do módulo chrome.tabs para obter informações sobre cada atualização das abas do navegador, permitindo assim fazer a validação dos sítios Web através dos filtros. O plug-in também possui um arquivo JSON de manifesto que inclui informações como nome, versão e permissões das ações executadas pela extensão.

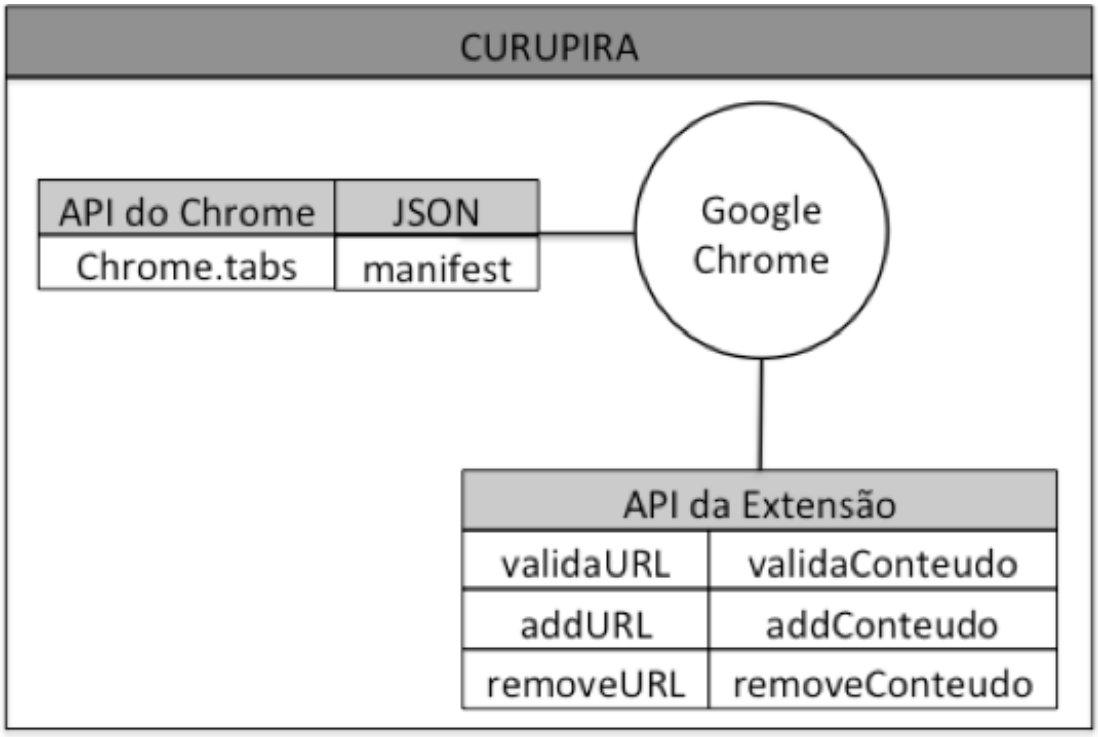

Figura 2. Visão interna do plug-in CURUPIRA.

Interface

A interface do CURUPIRA é responsável por efetivar as configurações desejadas e consideradas necessárias por pais ou responsáveis, a fim de evitar que crianças e adolescente tenham acesso a conteúdo Web inapropriado. Para isso, ela fornece diferentes tipos de entradas para configuração dos filtros. São elas:

- *Sugestão de filtros*: potenciais tópicos de conteúdo inapropriado são apresentados durante o processo de configuração dos filtros, tornando o uso da ferramenta mais simples e intuitiva (Figura 3). Na atual versão da ferramenta, tais tópicos são previamente estabelecidos.

- *Filtragem de URLs:* para bloquear ou filtrar o acesso à páginas da Internet, são utilizadas blacklist. A ideia é gravar URLs de sítios Web considerados ofensivos e/ou perigosos na blacklist e caso o usuário (criança e/ou adolescente) tente acessar algum dos sítios listado, ele é automaticamente bloqueado. A Figura 4 apresenta um exemplo da interface para essa função.

- *Filtragem por Palavras-Chave*: além da blacklist de URLs, também foram usadas expressões regulares para filtragem. As expressões regulares possuem o mesmo método de funcionamento da blacklist, porém não

bloqueiam diretamente uma URL, mas sim palavras (expressões) encontrados na página propriamente dito, podendo ser aplicada em todo o conteúdo da pagina e também no título.

Figura 3. Sugestão de filtros na forma de tópicos.

Figura 4. Lista de URLs definidas pelo usuário.

É importante ressaltar que durante o desenvolvimento da interface do CURUPIRA levou-se em consideração, como principal premissa, a facilidade de uso. A ideia sempre foi possibilitar que usuários sem qualquer experiência em segurança de computadores e/ou na configuração de aplicativos pudessem utilizar a solução de forma simples e prática, evitando um longo tempo de aprendizagem para uso e a necessidade de tutoriais extensos.

Segurança

No aspecto segurança, o CURUPIRA utiliza um mecanismo inicial básico (login e senha) para impedir que a ferramenta seja desativada ou tenha suas configurações alteradas por usuários indevidos.

4.2 Teste de funcionalidade dos recursos

Antes dos resultados, é importante enfatizar que os testes de recursos visam averiguar a correta filtragem dos sites considerados indevidos.

A solução CURUPIRA teve seu recurso de filtragem testado de duas maneiras diferentes. Na primeira, a ferramenta SIKULI (SIKULI 2009) configurou o plug-in, fazendo uso da opção de tópicos e palavras-chave. Dessa forma, para cada um dos oito tópicos, em conjunto com um grupo de palavras-chave (associado ao

tópico da vez), a ferramenta de automação de testes acessou um grupo de 28 páginas Web, registrando devidamente quantos bloqueios corretos e incorretos acometeram os testes. Por exemplo, na verificação sobre PORNOGRAFIA, das 28 páginas inseridas, 5 foram bloqueadas corretamente (http:// www.redtube.com, http://www.brazzers.com/, http://www.pornfail.com/, http://xvideos.com e http://xtube.com) e 5 não foram bloqueadas corretamente (http://www.bestgore.com, http://www.ladonegro.net, http://suzi9mm.com/, http://www.adultfriendfinder.com e http://www.fuckbook.com/). A principal razão para o não bloqueio reside no fato das páginas em questão não estarem listadas na *blacklist* e não possuírem em sua página principal palavras-chave relacionadas a pornografia. Por exemplo, o sítio bestgore.com possui fotos pornográficas, algo que a solução não está apta a detectar.

No segundo tipo de teste de funcionalidade de recurso, foi testado filtro de URLs. Para isso, um conjunto de 23.400 URLs (adquiridas do firewall do Centro de Processamento de Dados da Universidade Federal do Amazonas), dividido em 3 categorias, foi inserida na solução CURUPIRA. A Tabela 1 apresenta os resultados da avaliação.

Categoria	**URLs**		
	Disponíveis	**Bloqueadas**	**Não Bloqueadas**
Pornografia	22.333	21.710	623
Violência	1.040	840	200
Proxy	27	23	4

Assim como no teste anterior, a principal razão para o não bloqueio das URLs reside no fato das páginas em questão não estarem listadas na *blacklist*.

5 CONCLUSÃO

Através da pesquisa desenvolvida nesse projeto, pode-se inferir que soluções de *parental control* são importantes para segurança de crianças e adolescentes, mas elas não substituem o diálogo entre pais e filhos, sendo uma solução alternativa ou complementar.

As pesquisas ainda mostram que apesar de existir uma ampla variedades de ferramentas de *parental control*, nenhuma possui todas as funcionalidades, fazendo com que o usuário utilize mais de uma para obter o resultado esperado.

Partindo desses cenários foi proposta a ferramenta CURUPIRA, para exercer uma solução de *parental control* eficiente e tentando suprir a necessidade de se usar mais de uma ferramenta de *parental control*.

Durante o desenvolvimento do projeto, um grande tempo foi gasto na curva de aprendizagem das tecnologias usadas (linguagem JavaScript e a API do Google Chrome). Outra dificuldade encontrada foi o tratamento das exceções no uso de expressões regulares, afim de evitar que termos ou expressões não fossem bloqueados indevidamente.

Atualmente, a ferramenta está sendo testada por um grupo de voluntários com e sem experiência na área de segurança, tendo o intuito de avaliar a satisfação com o uso da ferramenta e verificar se a experiência em segurança e/ou o uso de outras ferramentas de *parental control* influenciam na avaliação.

Apesar de possuir as principais funcionalidades usadas em *parental control*, a ferramenta ainda pode ser melhorada com a adição de mais recursos a mesma, como controle de horário e configurações pré-estabelecidas, baseadas em perfis de idades e melhorando sua segurança, para evitar que seus mecanismos de bloqueio sejam burlados. Além disso ainda é possível portar o CURUPIRA para outras plataformas como celulares e tablets.

6 REFERÊNCIA BIBLIOGRÁFICA

BAIO, Cintia; FERREIRA, Lilian. Controle de pais é ferramenta útil para proteger filhos na Internet. UOL Tecnologia. Disponível em <http://tecnologia.uol.com.br/dicas/ultnot/2008/05/15/ult2665u333.jhtm>. Acessado em junho de 2012.

CIOFFI, C.; PAGLIARECCI, F.; SPALAZZI, L. An Anomaly-Based System for Parental Control. International Conference on High Performance Computing & Simulation (HPCS '09). Pp. 193-199. June, 2009.

SHIRALI-SHAHREZA, Sajad; SAMETI, Hossein; SHIRALI-SHAHREZA, Mohammad. Parental Control Based on Speaker Class Verification. IEEE Transactions on Consumer Electronics, Vol. 54, No. 3, August 2008.

SafeLine.gr. Disponível em: <http://www.safeline.gr/en>. Acessado em junho de 2012.

InspiredEffect.com. FoxFilter. Disponível em <http://www.inspiredeffect.com/FoxFilter>. Acessado em junho de 2012.

ANDERSON, James N. LeechBlock. Disponível em <http://www.proginosko.com/leechblock.html>. Acessado em junho de 2012.

ProCon. ProCon - Parental Filter Add-on for Firefox. Disponível em <http://procon.mozdev.org/>. Acessado em junho de 2012.

Projeto SIKULI. (2009) “SIKULI”, http://sikuli.org.