Protótipo SISBLOQUE:
Técnica de Filtragem e Bloqueio de Conteúdos Web

Filipe Pires [1], Alexandre Fonte [1], Vasco Soares [1].

1) Escola Superior de Tecnologia – Instituto Politécnico de Castelo Branco, Castelo Branco, Portugal.

{fpires, adf, vasco_g_soares}@est.ipcb.pt

Resumo

Os sistemas de bloqueio e filtragem de conteúdos Web encontram-se maioritariamente associados a regimes políticos opressivos, cujo principal objectivo na sua utilização é a censura. Infelizmente, este tipo de aplicação não só limita os direitos dos utilizadores como revoga o princípio daquilo que é uma rede global de partilha de informação pública, a Internet. Não obstante a filtragem e bloqueio de conteúdos Web é uma área franca em proliferação, cuja a sua correcta utilização tem vindo a demonstrar-se extremamente benéfica em determinadas áreas como a detecção e bloqueio de conteúdos pedófilos. Neste artigo apresentamos o protótipo Sisbloque, um sistema de filtragem e bloqueio de conteúdos Web projectado para ser implementado sobretudo em ISPs (Internet Service Providers), grandes instituições ou companhias, que propõe não só um mecanismo de filtragem de conteúdos com novas técnicas aperfeiçoadas e inovadoras como a intersecção de conteúdos relativos bem como a garantia de execução transparente suportada por um mecanismo de manipulação de erros.

Palavras chave: Filtragem de Conteúdos Web; Segurança de Redes Informáticas;

1. Introdução

Ao longo da evolução das tecnologias são introduzidos novos sistemas e serviços que organizações e instituições utilizam para seu benefício. Contudo, actualmente para além destas entidades que exploram tais meios tecnológicos, também a criminalidade começa a tirar partido de forma consistente das novas tecnologias; o que por conseguinte torna a Internet num ambiente inseguro quer para a partilha de informação, quer para qualquer outra actividade.

A correcta utilização de sistemas de filtragem e bloqueio de conteúdos Web apresenta-se como uma solução eficaz não só face a problemas como a publicação on-line de conteúdos pedófilos, como também na restrição de acesso a conteúdos improdutivos por parte de funcionários em organizações, instituições ou empresas. Presentemente a maioria dos sistemas de filtragem e bloqueio de conteúdo Web, ou são soluções proprietárias ou produtos comerciais, o que afasta o conhecimento da comunidade científica da maioria dos detalhes de implementação destes sistemas.

Esta lacuna motivou o desenvolvimento e concepção de um sistema aberto de filtragem e bloqueio de conteúdos Web, designado por Sisbloque. Este sistema encontra-se em fase de desenvolvimento e a sua concepção tem como principal objectivo o potencial uso em ISPs, grandes companhias ou instituições que necessitem deste tipo de serviço. O sistema Sisbloque propõe um mecanismo de filtragem de conteúdos mais conciso e fiável, proveniente do

melhoramento de métodos existentes como a filtragem baseada na origem e introdução de novos conceitos nos métodos de avaliação de conteúdos.

O restante conteúdo deste artigo encontra-se organizado da seguinte forma. A secção 2 descreve as tecnologias integradas no protótipo do sistema. A secção 3 apresenta os detalhes científicos da implementação do protótipo do sistema, as técnicas de filtragem de conteúdos utilizados e o conceito de transparência que este sistema disponibiliza. Por fim, a secção 4 conclui este artigo.

2. Software Integrado no Protótipo Sisbloque

O software integrado no protótipo do sistema Sisbloque é composto por um conjunto de extensões desenvolvidas de modo a aperfeiçoar, aumentar e introduzir novas técnicas nos componentes de código aberto, amplamente disponíveis e de uso livre.

2.1. Software de Código Aberto

O software de código aberto utilizado pelo sistema Sisbloque consiste num servidor HTTP de tecnologia Apache [Apache 2009] que faculta ao Sisbloque a capacidade de combinar determinados parâmetros do protocolo HTTP durante a sua actividade de bloqueio do tráfego HTTP. A gestão de acessos a endereços URL/IP é implementada com base na integração do Web proxy Squid [Squid 2009] e do respectivo plugin SquidGuard [SquidGuard 2009]. Todo este conjunto de componentes possui como ambiente base de execução o sistema operativo Linux, mais especificamente a distribuição Fedora Core 8 [Fedora 2009] de kernel 2.6.25.9 a qual confere suporte a uma framework de filtragem de pacotes designada de Netfilter [Netfilter, 2009].

2.2. Extensões Introduzidas

No que diz respeito a extensões embutidas, o protótipo do sistema Sisbloque integra um mecanismo que permite a auto-configuração de cada módulo, este mecanismo confere ainda a todo o sistema, tolerância e recuperação de possíveis falhas de energia. No módulo de manipulação de erros [Pires et al. 2008], foi do mesmo modo implementado uma extensão que permite efectuar a alternância de erros, pela gama 5xx do protocolo HTTP, no respectivo servidor deste serviço do protótipo. Quanto ao módulo de filtragem de conteúdos, também neste foram embutidas extensões de modo a optimizar e introduzir novas técnicas de avaliação de conteúdos que iremos descrever em detalhe na secção 3 deste artigo.

3. Protótipo

Ao longo do desenvolvimento do sistema Sisbloque, os conceitos utilizados têm vindo a sofrer permanentes alterações o que por conseguinte motiva também a constante alteração do próprio protótipo do sistema. Estas alterações ocorrem de forma gradual constituindo os diferentes passos de evolução do sistema. Nesta secção apresentamos o actual estado do protótipo Sisbloque.

3.1. Métodos de Filtragem de Conteúdos

O sistema Sisbloque possui dois mecanismos de filtragem, o filtro transparente e filtro de conteúdos, estes dois filtros são na realidade dois módulos físicos distintos que contêm técnicas de filtragem diferentes e adequadas à sua função e posição física na topologia de rede onde o sistema se encontra em actividade.

De modo a não induzir latência no acesso à informação residente nos servidores de conteúdos Web, o filtro transparente é composto por métodos de filtragem de conteúdos, que apesar de

serem extremamente concisos, não requerem tempo de processamento significativo. Estes métodos consistem na filtragem de endereços URL do protocolo HTTP e de endereços IP contidos nos pacotes de dados. Após esta filtragem, os endereços URL/IP são comparados com endereços URL/IP contidos nas listas de inclusão e exclusão, caso se confirme veracidade na comparação do endereço em causa com um dos endereços contidos na lista de exclusão, a respectiva ligação ao servidor de conteúdos é interrompida e redireccionada para o mecanismo de manipulação de erros.

O filtro de conteúdos é composto por duas técnicas que abordam uma perspectiva bastante diferente da que se encontra implementada no filtro previamente descrito, estas técnicas designam-se de filtragem por avaliação e intersecção de conteúdos relativos.

A filtragem por avaliação provém da melhoria da existente técnica de filtragem por palavras [Greenfield et al. 2001]. Deste modo o conteúdo de um endereço URL/IP não é avaliado pelas palavras que possui, mas sim pelo valor resultante da soma de todas as cotações atribuídas a cada palavra, podendo esta cotação ser positiva ou negativa caso a palavra seja ou não considerada ofensiva. Após a avaliação do conteúdo referente ao endereço URL/IP, é efectuada a comparação entre o resultado obtido e o valor predefinido pelo administrador do sistema, que constitui o limiar do que é ou não considerado conteúdo malicioso, o que por conseguinte leva a que o endereço URL/IP do conteúdo avaliado seja ou não adicionado às listas de exclusão do filtro transparente. Os endereços URL/IP que são avaliados por esta técnica provêm do filtro transparente, e consistem em todos os endereços desconhecidos ao sistema, ou seja, aqueles que não se encontram quer nas listas de exclusão quer na lista de inclusão, de notar ainda que esta técnica confere ao sistema Sisbloque o suporte de diferentes línguas.

A intersecção de conteúdos relativos é uma técnica inovadora, desenvolvida e integrada no protótipo do sistema Sisbloque, que garante a consistência e precisão das respectivas listas de exclusão. As listas de exclusão, da maioria dos sistemas de filtragem e bloqueio de conteúdos Web disponíveis, são actualizadas por entidades externas como a Internet Watch Foundation [IWF 2009], End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purpose [Ecpat 2009] ou Urlblacklist [Urlblacklist 2009]. Contudo, este procedimento pode causar o bloqueio de determinados servidores de conteúdos Web que tenham sido de forma maliciosa referenciados como ofensivos. A intersecção de conteúdos relativos utiliza a coerência e capacidade de processamento de vários motores de busca para efectuar uma pesquisa concreta de um determinado conteúdo, posteriormente os resultados obtidos pela pesquisa dos diferentes motores de busca são comparados e sempre que a ocorrência de um determinado endereço URL/IP seja relevante, este é adicionado às listas de exclusão (ver figura 1). Esta técnica permite ao sistema poupar o seu tempo de processamento, que é finito e precioso, obtendo ao mesmo tempo uma lista de exclusão completamente actualizada em menos de 60 segundos com mais de 60,000,000 endereços URL/IP relativos ao conteúdo pesquisado.

As listas de exclusão utilizadas no filtro transparente, do protótipo do sistema Sisbloque, são desta forma elaboradas e actualizadas pelo filtro de conteúdos o que por conseguinte significa que quanto maior for o seu tempo de execução, melhor será a sua precisão e rapidez no que consiste em filtrar e bloquear conteúdos Web.

3.2. Transparência

A transparência que um sistema de filtragem e bloqueio de conteúdos Web proporciona durante a sua execução é um factor de extrema importância. Quanto menos perceptível for para um utilizador Internet que algo se encontra entre o seu sistema informático e o servidor de conteúdos Web a que este está a aceder, menos vulnerável estará o sistema em causa.

De entre os sistemas de filtragem e bloqueio de conteúdos Web que preponderam nesta área, sempre que o acesso de um utilizador a determinado conteúdo Web é bloqueado, é apresentado

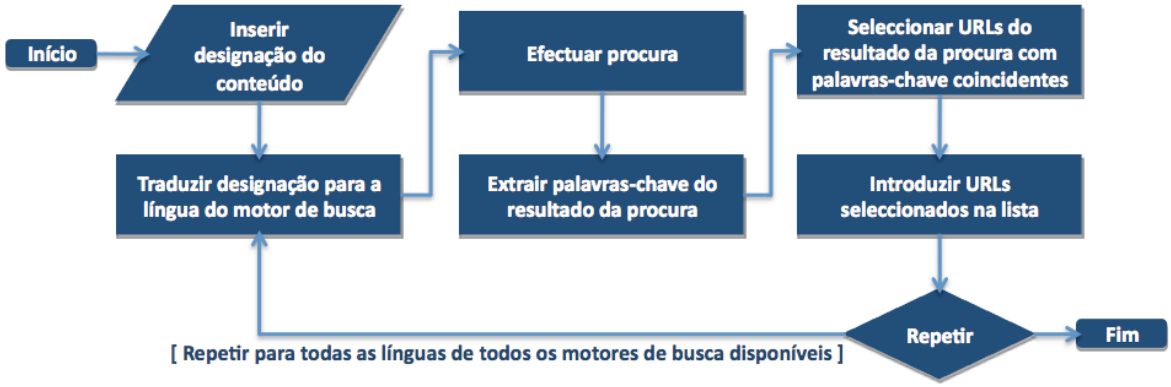

Figura 1 – Fluxograma do algoritmo de intersecção de conteúdos relativos

ao utilizador um aviso ou inclusivamente em alguns casos este é simplesmente deixado sem resposta. Este género de bloqueio evidência e estimula possíveis ataques ao sistema sendo um dos ataques mais comuns o denominado ataque Oracle [Lowe, 1995]. Segundo Lowe [Lowe, 1995], um ataque Oracle consiste em fazer com que um sistema responda rigorosamente a qualquer número de questões que lhe são efectuadas, sem este ter noção das possíveis consequências que as respostas proporcionam. Este tipo de ataque foi efectuado e documentado sobre o sistema Cleanfeed [Clayton, 2005], o resultado foi a percepção dos endereços URL/IP que se encontravam a ser filtrados o que posteriormente motivou a sua alteração para que o conteúdo Web bloqueado continua-se disponível.

O mecanismo de manipulação de erros do sistema Sisbloque gera aleatoriamente erros da gama 5xx do protocolo HTTP. Deste modo sempre que um utilizador tenta aceder a conteúdo malicioso, é apresentado um erro gerado por este mecanismo iludindo o utilizador perante uma falha referente ao servidor de conteúdos em causa, tornando-se imperceptível ao utilizador se o erro é proveniente do servidor de conteúdos Web ou do sistema Sisbloque. Este mecanismo de manipulação de erros coloca o sistema Sisbloque num patamar completamente distinto, dos sistemas de filtragem e bloqueio de conteúdos Web existentes, através da introdução deste conceito designado de transparência.

3.3. Implementação

O protótipo do sistema Sisbloque é constituído por três módulos físicos distintos sendo estes o módulo do filtro transparente, o módulo do filtro de conteúdos e o módulo do mecanismo de manipulação de erros (ver figura 2).

O módulo do filtro transparente é composto por uma bridge de rede controlada pela framework Netfilter, e encontra-se posicionado num ponto bastante especifico da topologia de rede onde filtra todo o fluxo de dados que nele passa. O controlo de acessos a conteúdos Web é efectuado exactamente neste módulo, através do Web proxy Squid e caso ocorra uma tentativa de acesso a um endereço URL/IP que se encontre nas listas de exclusão, este módulo interrompe e redirecciona de imediato o pedido para o módulo de manipulação de erros. Qualquer endereço URL/IP que não se encontre na lista de inclusão ou nas listas de exclusão deste módulo é enviado ao módulo de filtragem de conteúdos para posterior análise e avaliação.

O módulo do filtro de conteúdos recebe os endereços URL/IP provenientes do anterior módulo de filtragem de conteúdos e efectua a sua análise. Sempre que um conteúdo se revela ofensivo o seu endereço URL/IP é adicionado às listas de exclusão do sistema. Este módulo é ainda responsável pela actualização das listas de exclusão do sistema, efectuando no intervalo de tempo predefinido pelo administrador do sistema a intersecção de conteúdos relativos.

No que diz respeito ao módulo de manipulação de erros este, como já foi previamente descrito, efectua a geração de códigos de erro aleatórios da gama 5xx do protocolo HTTP. Para tal efeito é utilizado neste módulo o servidor HTTP Apache, o qual é periodicamente forçado a causar de forma aleatória os erros da respectiva gama do protocolo. Cada erro gerado encontra-se associado a um tempo de duração, o que faz com que vários utilizadores não se deparem com erros diferentes quando tentam aceder ao mesmo servidor de conteúdos Web no mesmo intervalo de tempo.

Por questões de segurança apenas o módulo de filtragem de conteúdos Web interage directamente com a rede, encontrando-se os restantes módulos isolados da rede principal e sendo apenas acessíveis pelo mesmo módulo do filtro transparente.

A arquitectura do sistema Sisbloque segue uma abordagem de implementação de um sistema distribuído. Esta característica confere a cada módulo do sistema a capacidade de dedicar o seu processamento bem como os seus recursos exclusivamente às tarefas que lhe são atribuídas, o que aumenta significativamente o desempenho e a capacidade de resposta global do sistema em si.

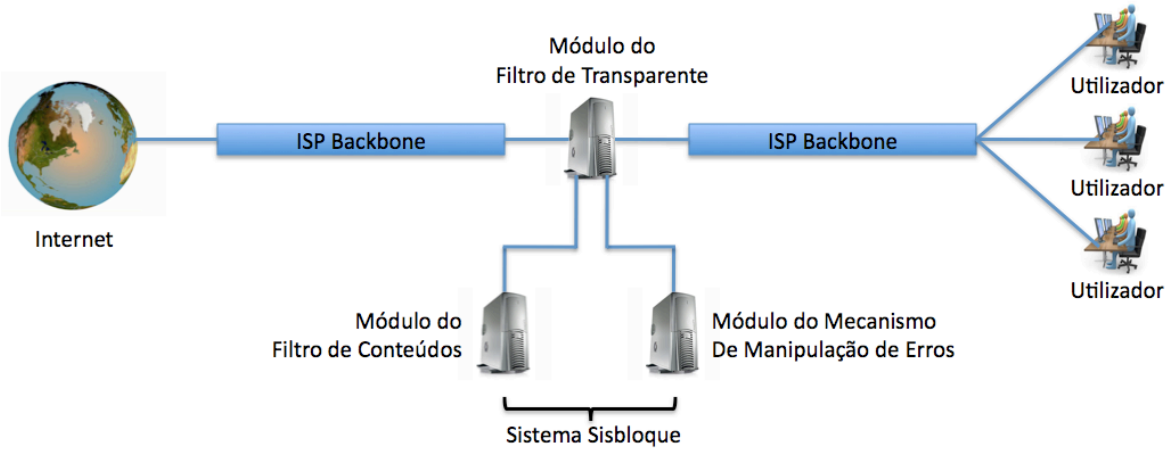

Figura 2 – Módulos físicos do Sistema Sisbloque

4. Conclusão

Apesar da actual controvérsia em torno de sistemas de filtragem e bloqueio de conteúdos Web, estes revelam-se úteis quando aplicados a determinados conteúdos como é o caso de conteúdos implícitos de abuso de menores, e necessários no bloqueio de qualquer conteúdo que reduza a produtividade de uma organização.

Neste artigo apresentámos as técnicas de filtragem e o modo de funcionamento de um sistema de filtragem e bloqueio de conteúdos Web desenvolvido para ser implementado sobretudo em ISPs. O Sisbloque tem como principais objectivos garantir um baixo custo de implementação e manutenção, associado a uma fiabilidade e a um sistema de filtragem e bloqueio de conteúdos Web extremamente preciso. A sua arquitectura, as técnicas de filtragem melhoradas, o seu inovador conceito de intersecção de conteúdos relativos juntamente com o seu mecanismo de manipulação de erros, introduzem um novo conceito de transparência e uma nova relação na capacidade de processamento necessários para identificação de conteúdos considerados ofensivos.

A capacidade de resposta que o protótipo do sistema demonstra nesta sua fase, embora o ambiente onde se encontra em execução seja relativamente reduzido, revela-se já de forma excepcional. O desenvolvimento deste projecto irá oferecer à comunidade científica informação única, e contribuições inovadoras naquilo que é a filtragem e bloqueio de conteúdos Web.

5. Referências

Apache 2009, The Apache Software Foundation, viewed 27 May 2009, <http://www.apache.org/>.

Squid 2009, Squid-cache.org - Optimizing Web Delivering, viewed 27 May 2009, <http://www.squid-cache.org/>.

SquidGuard 2009, Squidguard, viewed 27 May 2009, <http://www.squidguard.org/>.

Fedora 2009, Fedora Project, viewed 27 May 2009, <http://fedoraproject.org/>.

Netfilter 2009, Netfilter/Iptables Project Homepage, viewed 27 May 2009, <http://www.netfilter.org/>.

Pires, F., Fonte, A., Soares, V. 2008. "Democratizando" a Filtragem e Bloqueio de Conteúdos Web. 4ª Conferencia Nacional sobre Segurança Informática nas Organizações. pp. 2-4.

Greenfield, P., Rickwood, P., Cuong Tran, H. 2001. Effectiveness of Internet Filtering software products. CSIRO Mathematical and Information Sciences. pp. 6-12.

IWF 2009, "The Internet Watch Foundation", viewed 27 May 2009, <http://www.iwf.org.uk/>.

Ecpat 2009, Ecpat Sverige, viewed 27 May 2009, <http://www.ecpat.se/>.

Urlblacklist 2009, URLBlacklist.com, accessed at 27 May 2009, <http://urlblacklist.com/>.

Lowe, G. 1995. An Attack on the Needham-Schroeder Public-Key Authentication Protocol. Information Processing Letters. p. 131-133.

Clayton, R. 2005. Failures in a Hybrid Content Blocking System. Workshop on Privacy Enhancing Technologies. p. 12.