Acesso Gratuito A Internet - Uma proposta de cadastro e autenticação para acesso à Internet em locais públicos

Marcelo de Borba
UNISINOS
celoborba@gmail.com

Rafael Bohrer Ávila
UNISINOS
rbavila@unisinos.br

***Resumo*—Iniciativas de prover uma estrutura de cidade digital e consequentemente, fornecer Internet gratuita à população vem se tornando uma característica comum de muitos gestores públicos no Brasil. Porém, em muitos projetos que foram ou estão sendo postos em operação, pode-se encontrar diversas falhas e vulnerabilidades, como por exemplo, falta de autenticação e criptografia. Estas características propiciam a ocorrência de graves problemas de segurança além de prover um cenário ideal para a prática de crimes na Internet. Diante deste cenário o presente artigo propõe uma solução segura para o fornecimento de Internet em locais públicos.**

I. Introdução

Atualmente as tecnologias de informação e comunicação estão convergindo para uma solução única, cujo objetivo principal é prover uma infraestrutura dotada dos mais diversos serviços à população. É cada vez mais comum o desenvolvimento de soluções públicas para acesso à Internet e demais serviços eletrônicos, entretanto, os modelos de concessão de acesso a Internet que estão sendo implantados em diversos municípios demonstram um elevado grau de despreparo das empresas, gestores e técnicos em relação à segurança da informação [1], [2].

A utilização de ferramentas e processos devidamente estruturados para estabelecer segurança às soluções de acesso gratuito muitas vezes são deixados de lado em virtude dos custos elevados e a complexidade para implantação e gerenciamento da solução. A falta de mão-de-obra qualificada em conjunto com a ausência de legislação específica para a área de tecnologia e Internet também contribuem para a ausência de segurança.

Em um cenário onde estão envolvidas pessoas das mais diversas classes econômicas, faixas etárias, serviços, além das etapas envolvidas no processo de acesso e utilização da Internet, é importante que a solução desenvolvida possa prover um cenário que abranja os requisitos básicos de segurança como autenticação e criptografia, e ao mesmo tempo, ofereça facilidade e transparência na sua utilização em virtude das características referentes ao conhecimento técnico da maioria dos usuários.

Considerando este contexto, o objetivo principal deste trabalho é propor uma solução segura, além de permitir um processo automatizado para entrada de novos usuários na rede, utilizando bancos de dados comuns a todas as prefeituras brasileiras como por exemplo, o banco de dados dos usuários do SUS - CADSUS e o banco de dados referentes ao cadastro de imóveis e proprietários - IPTU [3], [4].

Tabela I
Consolidado Geral - soluções de acesso público à Internet

SOLUÇÕES DE ACESSO				
Cidade	**Cripto.**	**Autent.**	**Cad.**	**T. Uso**
Garibaldi-RS	NÃO	NÃO	NÃO	SIM
S. J. da Varginha-MG	NÃO	NÃO	NÃO	NÃO
Manoel Vitorino-BA	SIM	NÃO	NÃO	NÃO
Ribeirão Preto-SP	NÃO	SIM	PRÉVIO	NÃO
Alvorada-RS	NÃO	SIM	SIM	SIM
Santa Isabel-SP	NÃO	NÃO	NÃO	NÃO
Porto Alegre-RS	NÃO	NÃO	NÃO	NÃO
Seattle-EUA	NÃO	NÃO	NÃO	SIM
Atenas-Grécia	NÃO	NÃO	NÃO	NÃO

O artigo inicia por uma análise das soluções atualmente empregadas conforme apresentada na seção a seguir.

II. Soluções Atuais

Para o levantamento de soluções atualmente implantadas foi efetuado uma pesquisa por cenários semelhantes ao proposto neste artigo levando-se em consideração a utilização de criptografia, cadastramento, autenticação e termo de uso, conforme especificado na Tabela I . Os projetos apresentados a seguir foram selecionados em virtude da quantidade de informações disponíveis, visto que diversas prefeituras não possuem informações técnicas a respeito de seus projetos implementados.

As cidades de Garibaldi [5], São José da Varginha [6], Manoel Vitorino [7], Ribeirão Preto [8], Alvorada [9], Santa Isabel [10], Porto Alegre [11], *Seattle* [12] e Atenas [1] são utilizadas para comparação com a solução proposta por este artigo. Através dessa pesquisa e possível identificar particularidades que as diferem no quesito de segurança da rede.

A utilização de criptografia presente na solução do município de Manoel Vitorino possibilita uma camada adicional de proteção aos dados trafegados dificultando, por exemplo, a captura de dados através de ataques como o *parking lot* [13], porém, a ausência de cadastro e autenticação individual impossibilita a identificação dos usuários e consequentemente, a responsabilização em caso de incidentes de segurança.

É importante ressaltar que nesse contexto a utilização de criptografia se torna ineficaz à medida que a chave de acesso se torna pública. A utilização de um protocolo criptográfico como WEP e WPA na versão pessoal, implica em compartilhamento das informações de autenticação

para todos os usuários de um determinado ponto de acesso fazendo com que os mesmos sejam divulgados ou compartilhados em diversos meios, como por exemplo, em redes sociais.

A utilização de certificados digitais para prover confidencialidade pode ser implantada de forma satisfatória, porém, como solução de autenticação se torna inviável pois cada cidadão necessita possuir seu próprio certificado digital. A adoção desse modelo torna-se inviável a medida que o custo de implantação e manutenção tornam-se elevados, além de que é inapropriado impor a aquisição de um certificado digital à cada cidadão, ou até mesmo, a Prefeitura Municipal tornar-se uma autoridade certificadora provendo de forma gratuita certificados à toda população. Também se faz necessário ressaltar a dificuldade de utilização desse modelo para cidadãos sem conhecimentos técnicos ou especializados.

Nas soluções analisadas também se pode verificar que a ausência de autenticação é acompanhada da falta de cadastro dos usuários, conforme demonstrado na Tabela I.

Dos nove municípios analisados, somente dois apresentaram mecanismos de autenticação, o que demonstra a necessidade de um modelo adequado para acesso gratuito à Internet. Sem a presença de autenticação e um processo de cadastro confiável, é praticamente inviável efetuar a correta identificação dos usuários da rede e prover a auditoria dos acessos.

Os diferentes processos de cadastro de usuários nas soluções avaliadas possuem algumas características que comprometem a sua eficácia e a autenticidade dos dados informados, entre as quais se pode citar:

1) Falta de mecanismos para confirmação e validação dos dados enviados no cadastro;
2) Processos estatizados demandando alocação de recursos humanos para validação e análise de documentação;
3) Ausência ou geração inadequada de senhas para o primeiro acesso, comprometendo a confidencialidade das mesmas;
4) Utilização de email pessoal como meio para confirmação da autenticidade dos dados informados no cadastro.

De maneira geral, é possível destacar mecanismos para formulação de uma solução adequada, mecanismos de cadastro, autenticação e criptografia, quando utilizados em conjunto são capazes de propiciar um nível de segurança adequado para acesso público a Internet.

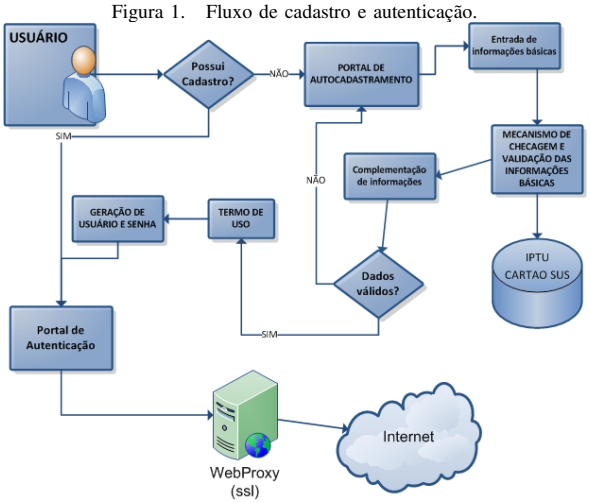
Por fim observa-se que tanto o processo de cadastro e autenticação dos usuários quanto a navegação na rede devem ser protegidos, ou seja, as informações devem ser trafegadas sob canais seguros dotados de criptografia.

Com base no conteúdo exposto, a abordagem proposta apresenta uma solução que atende as demandas elencadas.

III. Proposta para implementação de concessao de acesso à Internet gratuita para a população

A partir do conjunto de fatores até então apresentados, este trabalho propõe uma solução que visa fornecer um modelo técnico para implementação de acesso gratuito à Internet de forma segura.

Figura 1. Fluxo de cadastro e autenticação.



Utilizando recursos adicionais que fazem parte da realidade de órgãos públicos municipais, como por exemplo, banco de dados existentes, é possível prover a sua aplicabilidade na maioria dos municípios brasileiros sem alterações significativas na solução a ser proposta.

Atualmente o governo federal mantém vários serviços que utilizam banco de dados nacionais como fonte de alimentação, porém, o acesso aos dados nem sempre é facilitado ou não possui acesso universalizado às prefeituras.

Assim, as bases de dados escolhidas para a solução são o cadastro de imóveis do município e o cadastro nacional de usuários do Sistema Único de Saúde - SUS, presentes na quase totalidade de municípios do território brasileiro. Tais fontes de dados possuem atualização constante, abrangência em todas as faixas etárias e geralmente possuem um processo de contato direto com o cidadão.

O escopo deste trabalho está delimitado ao processo de concessão de Internet gratuita em locais públicos como praças e escolas, envolvendo apenas as etapas do acesso do usuário à rede pública.

A. Fluxo de Cadastro e Autenticação

As bases de dados mencionadas podem ser utilizadas na construção de um mecanismo seguro e automatizado para cadastramento de usuários. Através de conexão segura utilizando o protocolo HTTPS, os usuários efetuam seu cadastramento ou autenticação, conforme fluxo demonstrado na Figura 1.

Ao efetuar a conexão de seu dispositivo ao PAP (Ponto de Acesso Público), o usuário é direcionado ao portal de Acesso Gratuito, este portal possui as opções de autenticação e cadastramento, cabendo ao usuário a escolha apropriada.

Ao se tratar de um novo usuário, o mesmo deve selecionar a opção de autocadastramento, conforme demonstrado na Figura 1, o usuário será então redirecionado para uma

nova página de cadastro onde deverá preencher as informações básicas para início do processo de cadastramento.

As informações básicas solicitadas podem ser personalizadas de acordo com cada projeto ou ponto de acesso, sendo obrigatório o fornecimento de no mínimo, o nome completo e um documento de identificação como RG ou CPF.

A partir do momento do envio destas informações à aplicação, entra em funcionamento o mecanismo de busca e validação dos dados, este mecanismo efetua buscas nas bases de dados cadastrados na solução e seleciona os registros cujos dados informados pelo usuário sejam idênticos aos encontrados pelo mecanismo de busca.

Após efetuar a busca e encontrar ao menos um cadastro válido, a aplicação apresenta ao usuário um questionamento referente aos dados relativos ao cadastro encontrado cabendo ao usuário respondê-las e enviá-las novamente para a aplicação.

Os dados selecionados podem variar conforme a base de dados selecionado, quando utilizado a base da dados do CADSUS pode-se utilizar os campos relativos ao nome da mãe, número do cartão do sus e parte do endereço. Quando utilizada a base de dados referente aos imóveis (IPTU) é possivel utilizar dados como o numero de cadastro do imóvel, endereço ou o próprio código de ativação enviado anteriromente na emissao do tributo ao cidadão.

Ao receber as informações complementares informadas pelo usuário o mecanismo efetua a validação das mesmas mediante comparação com os dados armazenados na aplicação. Se o processo de validação ocorrer com êxito é então apresentado os termos de uso da rede, mediante a aceitação do usuários a aplicação gera as credenciais de acesso apresentando-as na tela do usuário.Após confirmar o recebimento das informações o usuário é redirecionado para o portal de autenticação da solução.

Nos casos onde o mecanismo de validação não consegue encontrar dados suficientes, ou quando as perguntas não são respondidas adequadamente o sistema deve abortar as operações seguintes orientando o usuário a reiniciar o processo de cadastramento, ou então, efetuar o cadastro de forma presencial junto ao órgão responsável pela rede de acesso no município.

Após a complementação de informações e a validação dos dados informados, o usuário é redirecionado ao portal de autenticação onde poderá efetuar o seu login para acesso à Internet.

Para a proteção do tráfego dos dados, a solução utiliza uma aplicação de *webproxy* disponível sobre o protocolo SSL. Através de configurações específicas no *firewall* somente o tráfego através deste serviço é permitido, fornecendo assim, uma camada de proteção contra *sniffing* de pacotes ou ataques do tipo *parking lot* [13], [14].

A solução de auto-cadastro e validação deve ser desenvolvida de acordo com cada solução utilizada para o gerenciamento das bases de dados especificadas anteriormente, em virtude das diversas aplicações utilizadas para gerenciamento desse tipo de dados é preciso adaptar os mecanismos de consulta nas bases de dados.

Figura 2. Portal de Autenticação.

IV. Protótipo da Solução

Para implementação da solução descrita na seção anterior são utilizadas soluções existentes no mercado: a distribuição Pfsense [15], baseada no sistema operacional FreeBSD [16] e o aplicativo Glype [17], responsável pelo serviço de webproxy. A escolha das ferramentas para apresentação do protótipo levam em consideração a facilidade de implementação, bem como, o alto grau de documentação de suporte disponíveis nos sites respectivos de cada solução.

A. Portal de Acesso

Desenvolvido utilizando-se a solução Pfsense o portal tem por objetivo prover a autenticação dos usuários, a Figura 2 demonstra o portal de autenticação que será utilizado na implementação da solução. Através da utilização da própria ferramenta Pfsense foi desenvolvido um portal para interface do usuário com o mecanismo de autenticação da rede suportanto autenticação em base local, *Radius* ou até mesmo, integração com o serviço *Active Directory da Microsoft* [18].

Após a autenticação ser efetuada com sucesso o portal de autenticação redireciona o tráfego do cliente autenticado para o proxy seguro da rede, o qual será o ponto de navegação para a Internet.

B. Webproxy

A solução utilizada para prover um sistema de *webproxy* operando exclusivamente pela porta 443 utilizando protocolo SSL [19] foi desenvolvida utilizando um servidor Apache em conjunto com a ferramenta *Glype*. Toda navegação via protocolo HTTP ou HTTPS é redirecionada para o webproxy em questão. Os esforços na construção do solução levaram em conta a transparência e a facilidade de utilização, visto que o usuário não precisa efetuar quaisquer alterações em seu navegador bastanto apenas, digitar os endereços desejados no formulário disponível no próprio *webproxy*, conforme demonstrado na Figura 3.

Durante a navegação o usuário pode visualizar, na parte superior do navegador, uma barra de ferramentas disponibilizada para permitir a mudança de site sem ter que retornar à página principal do webproxy, conforme demonstrado na Figura 4.

Figura 3. Página de acesso - Webproxy.

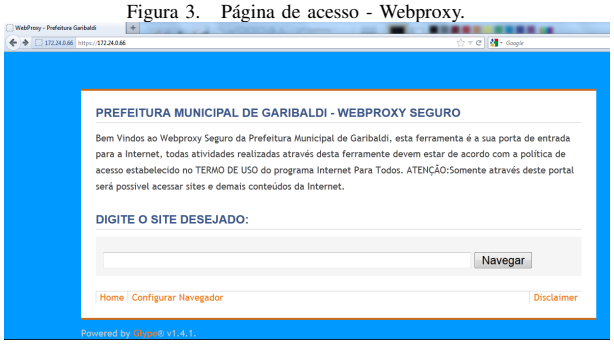


Figura 4. Navegando com WebProxy.

A aplicação pode ser configurada para efetuar o log de todas as conexões efetuadas, fornecendo uma alternativa para efetuar a auditoria dos acessos. Em conjunto com os dados da autenticação é possível identificar todo o tráfego oriundo de um mesmo usuário, os *logs* armazenados apresentam as informações referentes ao IP de origem, data e hora do acesso e o endereço acessado na Internet.

V. Conclusões Finais

Prover um meio alternativo, dotado de requisitos de segurança com baixo custo e com elevado nível de compatibilidade com a infraestutura de redes públicas existentes é uma das principais premissas da solução apresentada, a próxima etapa deste trabalho consiste na aplicação do mecanismo de auto-cadastramento, os detalhes de funcionamento estão sendo ajustados e a integração com base de dados semelhantes as do Cartão do SUS e IPTU do município de Garibaldi já estão em fase de testes.

A união das ferramentas propostas num único ambiente em conjunto com os requisitos de cadastramento seguro, autenticação e e auditoria serão implementadas ao longo do segundo semestre de 2012 como projeto piloto no município de Garibaldi em duas das principais praças da cidade.

Referências

[1] D. Ztoupis, K. Zarifis, I. Stavrakakis, and C. Xenakis, "Towards a security framework for an established autonomous network," in *Wireless Pervasive Computing, 2008. ISWPC 2008. 3rd International Symposium on*, may 2008, pp. 749 –754.

[2] G. Camponovo and A. Picco-Schwendener, "Motivations of hybrid wireless community participants: A qualitative analysis of swiss fon members," in *Mobile Business (ICMB), 2011 Tenth International Conference on*, june 2011, pp. 253 –262.

[3] CARTAONET. (2012) Portal de cadastros nacionais. Disponível em: http://cartaonet.datasus.gov.br. Acesso em 15 de abril de 2012.

[4] Brasil, "Lei 10.257 de 10 de julho de 2001. regulamenta os artigos 182 e 183 da constituição federal, estabelece diretrizes gerais da política urbana e dá outras providencias." Brasília, DF., 2001.

[5] P. M. de Garibaldi. (2011) Internet para todos. Garibaldi - RS. Disponível em: http://internetparatodos.garibaldi.rs.gov.br. Acesso em 23 dezembro 2012.

[6] P. M. de São José da Varginha. (2012) Internet grátis na praça são josé. São José da Varginha - MG. Disponível em: http://www.saojosedavarginha.mg.gov.br/destaques/internet-gratis-na-praca-sao-jose. Acesso em 22 de Abril de 2012.

[7] P. M. de Manoel Vitorino, "Site institucional," Manoel Vitorino - BA., 2012, disponível em: http://manoelvitorino.com. Acesso em 22 de Abril de 2012.

[8] P. M. de Ribeirão Preto. (2012) RibeirÃo digital. Ribeirão Preto - SP. Disponível em: http://www.ribeiraopreto.sp.gov.br/cidadao/i99rdigital.php. Acesso em 20 de abril de 2012. Acesso em 22 de Abril de 2012.

[9] P. M. de Alvorada, "Atendenet," 2012, disponível em: http://177.43.243.105/atendenet/>. Acesso em 05 de maio de 2012.

[10] P. M. de Santa Isabel. (2012) Site institucional. Santa Isabel - SP. Disponível em: http://www.santaisabel.sp.gov.br/internet. Acesso em 22 de Abril de 2012.

[11] PROCEMPA., "Procempa livre e gratuita," 2012, disponível em: http://www.procempa.com.br/default.php?p_secao=76. Acesso em 19 de maio de 2012.

[12] G. Seattle, "Wifi in seattle," Seattle - EUA., 2012, disponível em: http://www.seattle.gov/html/citizen/wifi.htm. Acesso em 22 de Abril de 2012.

[13] H. K. INFOSEC., "Wireless network security," 2010, disponível em: http://www.infosec.gov.hk/english/technical/files/wireless.pdf. Acesso em: 1 abril 2012.

[14] M. Mallick, *Mobile and Wireless Design Essentials*. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[15] B. P. LLC, "pfsense open source firewall," 2012, disponível em:http://www.pfsense.org/. Acesso em: 12 julho 2012.

[16] FreeBSD, "The power to server," 2012, disponível em:http://www.freebsd.org/. Acesso em: 12 junho 2012.

[17] Glype, "Glype proxy script," 2012, disponível em:http://www.glype.com/. Acesso em: 12 junho 2012.

[18] Microsoft, "Active directory overview," 2012, disponível em: http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx. Acesso em: 20 julho 2012.

[19] C. Peikari and A. Chuvakin, *Security warrior - know your enemy*. O'Reilly, 2004.