Autenticação Web na rede e-U

Luís Frazão Mário Antunes Vítor Távora

Instituto Politécnico de Leiria, ESTG
Morro do Lena, Alto Vieiro
2401-951 Leiria, Portugal

luis.frazao@ipleiria.pt mario.antunes@estg.ipleiria.pt vntavora@estg.ipleiria.pt

RESUMO

A rede e-U é uma infra-estrutura de rede sem fios (*wireless)* existente nas instituições de ensino superior, através da qual os membros de todas as comunidades académicas nacionais podem aceder a conteúdos e serviços disponibilizados pelas suas instituições, bem como aceder à internet. A rede e-U assegura aos seus utilizadores uma efectiva mobilidade ("*roaming*") entre as diferentes instituições de ensino superior. De forma a facilitar o acesso aos membros das comunidades académicas, e de alguns visitantes, à rede e-U é essencial a existência de um mecanismo de autenticação simples e de fácil configuração. Este artigo descreve um mecanismo de autenticação com essas características que foi desenvolvido e se encontra a funcionar em todas as unidades orgânicas do Instituto Politécnico de Leiria. Este mecanismo de autenticação em redes *wireless* é baseado no acesso através de uma página *web*. No artigo será descrita a arquitectura do serviço de autenticação e os seus principais componentes, onde se inclui um mecanismo que assegura a alta disponibilidade do serviço de autenticação e a sua tolerância a falhas.

Categories and Subject Descriptors

K.3.1 [**Computers and Education**] : Computer Uses in Education

H.5.2 [**Information Interfaces and Presentation**]

General Terms

Management, Reliability, Human Factors.

Keywords

Web based login, autenticação Web, rede e-U.

1. INTRODUÇÃO

As redes sem fios instaladas nas instituições de ensino superior portuguesas permitiram às respectivas comunidades passar a usufruir de uma nova forma de acesso aos conteúdos e serviços digitais disponibilizados e à internet. A rede e-U [1], gerida pela Fundação para a Ciência e Computação Nacional (FCCN) [2], assegura também a mobilidade dos seus utilizadores nas áreas cobertas, assegurando-lhes o *roaming* não só entre as várias unidades orgânicas pertencentes à mesma instituição de ensino superior (por exemplo Faculdades ou Escolas), como também o *roaming* entre instituições. Por exemplo, um docente que desenvolva a sua actividade em duas instituições de ensino superior pode ter um acesso transparente, independentemente da localização física, aos serviços de internet e intranet disponibilizados pelas instituições. O acesso do utilizador à rede é efectuado através de um processo de autenticação em que são validadas as suas credenciais (login e password). Estas encontram-se normalmente armazenadas no servidor da instituição de ensino superior onde o utilizador se encontra registado.

O método de autenticação aconselhado pela FCCN para a rede e-U assenta no uso da norma IEEE 802.1X [3][4], por se tratar de um protocolo seguro. Este método não é suportado por vários dispositivos de acesso a redes *wireless* (por exemplo PDAs, Playstation e algumas placas de rede), e torna-se um pouco complexo para utilizadores com pouca experiência na configuração de equipamentos. Esta complexidade torna-se num sério obstáculo para a massificação da utilização da rede e-U.

Foi também desenvolvido um método de autenticação alternativo que cria VPNs (*Virtual Private Network*) entre o dispositivo do utilizador e o servidor de autenticação. Para tal torna-se necessária a instalação e a configuração de um cliente de VPN no dispositivo do utilizador. Esta solução para além de não ser suportada por todos os dispositivos e/ou respectivos sistemas operativos revelou-se um pouco instável principalmente quando vários utilizadores acedem em simultâneo ao servidor.

Tendo como objectivo principal a eliminação das barreiras de acesso à rede e-U descritas, foi criado um mecanismo de autenticação dos utilizadores através de uma página *web* – o WebBasedLogin (WBL). Este mecanismo é suportado por todos os dispositivos que disponham de um navegador ("browser") na Internet, e os utilizadores apenas terão de inserir as suas credenciais na página de acesso à rede *wireless* que aparecerá de imediato. Este mecanismo não requer qualquer tipo de configuração por parte do utilizador, sendo bastante fácil de utilizar nos mais variados tipos de dispositivos e por todos membros da comunidade académica – em especial por aqueles com conhecimentos mais básicos de informática.

SIIE'2007, November 14–16, 2007, Porto, Portugal.

Este artigo inicia-se com uma descrição geral do projecto e-U e do sistema WBL desenvolvido para aceder à rede e-U. De seguida, é apresentada a aplicação de administração desenvolvida para monitorizar e gerir o sistema WBL. Encontra-se também descrita a solução desenvolvida para assegurar a alta disponibilidade e a tolerância a falhas do WBL, o que permite a sua utilização em ambientes críticos, dinâmicos e de grande utilização. Por fim, apresentam-se alguns dados referentes à utilização do WBL e as conclusões do trabalho desenvolvido.

2. PROJECTO E-U

O principal objectivo do projecto e-U, ao qual o Instituto Politécnico de Leiria (IPL) aderiu, é a constituição de um campus virtual com todos os estabelecimentos de ensino superior portugueses. Este projecto teve início em 2003 e faz parte do programa "Portugal Digital" [5], promovido pela Unidade de Missão, Inovação e Conhecimento (UMIC) [6] e financiado pelo Programa Operacional Sociedade da Informação (POSI).

Este projecto visa a criação de aplicações e redes de comunicações, a produção de conteúdos e a disponibilização de serviços junto das instituições de ensino superior. Tem igualmente promovido a massificação do uso de computadores portáteis dentro das instituições, bem como de tecnologias móveis para acesso a serviços de Internet, conteúdos e aplicações disponibilizados na Intranet de cada instituição. Por exemplo, através de um portátil com acesso *wireless* à rede sem fios instalada em cada *campus*, os alunos podem ter acesso à documentação das aulas, artigos científicos, trabalhos, notas e serviços académicos, entre outros. A possibilidade de *roaming* nacional dentro da rede e-U permite o acesso sem fios em qualquer instituição aderente.

O projecto e-U é uma experiência inovadora a nível mundial, tendo sido apresentada várias vezes como exemplo de boas práticas a seguir para a melhoria da mobilidade no ensino superior [7][8]. O IPL integra actualmente na rede e-U os *campus* de todas as escolas, os serviços centrais e a totalidade das residências de estudantes [9]. A conformidade da rede *wireless* do IPL com os requisitos definidos pela FCCN permite que um utilizador registado no domínio IPL ("ipleiria.pt") se possa movimentar fisicamente para outra instituição aderente, mantendo o acesso aos serviços e recursos de Internet e Intranet disponibilizados. As suas credenciais são sempre validadas no servidor de autenticação do domínio do IPL. A Figura 1 ilustra o cenário genérico de um campus com ligação à rede e-U. Cada *campus* possui uma rede *wireless* e servidores locais, entre os quais o servidor RADIUS que é o responsável pela autenticação dos utilizadores. A ligação à rede e-U é efectuada através da rede de investigação e ensino nacional (RCTS).

Os utilizadores poderão aceder a duas redes distintas, geridas pela FCCN e identificadas pelos SSID[1], a "e-U" e a "guest-e-U". A rede "e-U" é protegida e registada como escondida, não sendo possível a um utilizador visualizá-la sem ter previamente efectuado a sua respectiva configuração. Devido à segurança que oferece esta rede é a recomendada pela FCCN. Os utilizadores podem aceder automaticamente à rede e-U através do método de autenticação IEEE 802.1X. A rede "guest-e-U" é aberta e acessível por todos, tendo a desvantagem de ser pouco segura pois não utiliza qualquer tipo de codificação dos dados. Esta rede pretende ser o ponto de partida para qualquer utilizador na rede. Um utilizador após ligar-se à "guset-e-U", quando tentar aceder a algum conteúdo da Internet, será redireccionado para uma página informativa sobre os métodos de autenticação recomendados e respectivas configurações.

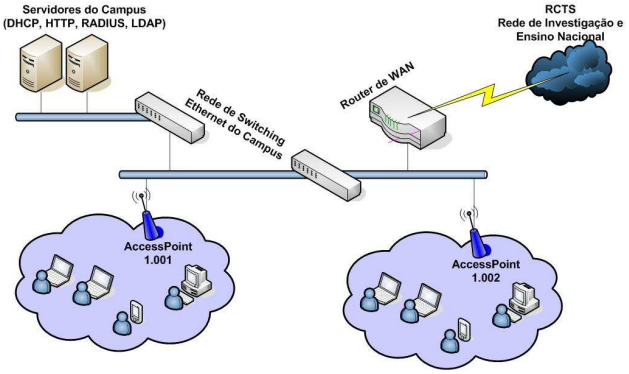

Figura 1. Infra-estrutura da rede wireless e-U no IPLeiria.

No IPL optou-se inicialmente por utilizar um método de acesso a cada uma das redes: o baseado no protocolo IEEE 802.1x para a rede e-U e um baseado na criação de VPNs para acesso à rede guest-e-U.

O protocolo IEEE 802.1x, necessário para o acesso à rede e-U, não é suportado por vários dispositivos de acesso a redes *wireless* (por exemplo PDAs, Playstation e algumas placas de rede), e torna-se um pouco complexo para utilizadores com pouca experiência na configuração de equipamentos. Esta complexidade torna-se num sério obstáculo para a massificação da utilização da rede e-U.

O método de autenticação através da criação de VPNs (*Virtual Private Network*) entre o dispositivo do utilizador e o servidor de autenticação implica a instalação e a configuração de um cliente de VPN no dispositivo do utilizador. Esta solução para além de não ser suportada por todos os dispositivos e/ou respectivos sistemas operativos revelou-se um pouco instável principalmente quando vários utilizadores acedem em simultâneo ao servidor.

3. SISTEMA DE AUTENTICAÇÃO WEB (WBL)

O mecanismo de autenticação o WebBasedLogin (WBL) tem como objectivo principal eliminar as barreiras e os problemas colocadas pelos mecanismos existentes (802.1x e acesso por VPNs). O WBL permite aos utilizadores acederem à rede wireless após efectuarem a sua autenticação numa página *web*, para que são redireccionados ao tentarem aceder à internet. Este mecanismo não requer qualquer tipo de configuração por parte do utilizador, sendo bastante fácil de utilizar nos mais variados tipos

[1] Um *service set identifier* (**SSID**) é um código presente em todos os pacotes de dados de uma determinada rede wireless. Esse código pode atingir um máximo de 32 caracteres alfanuméricos. Qualquer equipamento que queira comunicar com outro, necessitam de partilhar o mesmo SSID.

de dispositivos e por todos membros da comunidade académica – - em especial por aqueles com conhecimentos mais básicos de informática.

O WBL garante a segurança na autenticação, através da utilização do protocolo *https*, mas não assegura a segurança dos dados (garantida pelo protocolo 802.1x). Note-se que ao desenvolver o WBL foi dada a prioridade máxima à simplicidade do acesso, pretendendo-se apenas garantir a segurança durante o processo de autenticação.

Na Figura 2 encontram-se representados os principais componentes do sistema WBL, bem como as acções mais relevantes que são executadas: redireccionamento dos utilizadores para uma página de autenticação, comunicação entre o sistema de autenticação *web* (WBL Server) e o servidor de autenticação da instituição (RADIUS), e a segurança da autenticação (p.e. recorrendo a certificados digitais).

Na implementação do WBL foram apenas utilizados componentes *open-source* e o sistema operativo Linux Ubuntu Servidor 6.10.

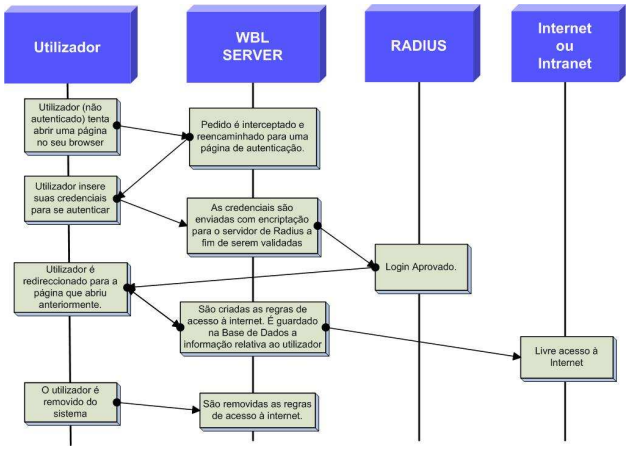

Figura 2. Diagrama de funcionamento do sistema WBL

Os serviços fundamentais que suportam o sistema de WBL desenvolvido são assegurados pelas seguintes soluções *open-source*:

- Servidor *web* – Apache
- Servidor de Proxy Cache e *Redirector* – Squid e Squirm
- Servidor RADIUS – FreeRadius
- Servidor de Base Dados – MySQL
- Servidor de DNS – Bind
- Serviço de *Firewall* – IPTables
- Linguagem de Programação – PHP e Perl

Para se poder efectuar a gestão do mecanismo de WBL, foi desenvolvido um módulo que permite a sua administração através de um interface *web*. O módulo encontra-se descrito na secção 4.

Foi projectado e implementado um mecanismo que assegura a disponibilidade e a tolerância a falhas para o WBL, pois para o sistema funcionar torna-se necessário assegurar o funcionamento de todos esses serviços, normalmente residentes na mesma máquina. Basta um serviço parar, ou a máquina que os suporta "crashar", para comprometer o funcionamento de todo o sistema.

O mecanismo de alta disponibilidade implementado no WBL recorre ao uso de *clusters* que, em caso de falha, asseguram a retoma dos serviços numa máquina de *backup*. Este mecanismo encontra-se descrito na secção 5.

4. INTERFACE DE ADMINISTRAÇÃO

A interface de administração *web* do sistema WBL proporciona ao administrador do sistema a monitorização e o controlo de todos os seus serviços. A interface *web* é vocacionada para facilitar a tarefa dos administradores do sistema, especialmente para os que tiverem pouca experiência na gestão de serviços no sistema operativo Linux.

Através da interface *web* o administrador pode aceder ao estado dos serviços do sistema, bem como alterar as suas configurações. São também disponibilizados um conjunto de dados estatísticos em tempo real, tais como, o número de utilizadores autenticados, a duração de cada sessão, o tráfego gerado e o historial de cada utilizador. Assim sendo, foi necessário assegurar que num único serviço o sistema de gestão do WBL integrasse todas estas funcionalidades.

Para auxiliar no desenvolvimento do módulo de administração do WBL foi utilizado o programa *open-source* Webmin [11]. Esta aplicação permite a configuração de vários serviços através de uma interface *web*, e possui alguns módulos configurados de serviços que são utilizados no WBL (Apache, Bind, IPTables, MySQL, Cron Jobs, entre outros). O Webmin permite a integração e criação de novos módulos (feitos à medida de cada administrador), exigindo apenas que o seu desenvolvimento seja realizado com base num template já definido. Esta característica da aplicação foi explorada, tendo sido desenvolvido o "meta-serviço" WBL que inclui a informação adicional necessária à gestão do sistema WBL.

A Figura 3 ilustra o módulo desenvolvido para o Webmin, para que esta aplicação passasse a suportar a gestão do "meta-serviço" WBL.

Figura 3. Interface de Administração Webmin com o WBL

Através do módulo desenvolvido no Webmin para suportar a administração do WBL, é possível aceder a dados estatísticos, apresentar informações em tempo real referentes aos utilizadores, monitorizar e configurar directamente todos os serviços envolvidos.

Foram analisadas as aplicações comerciais "*Zone CD Gateway*"[12], "*FirstSpot*"[13], e as utilizadas pelos principais

operadores de telecomunicações nacionais (Vodafone e PT Comunicações). Algumas destas aplicações são utilizadas em locais públicos nacionais (aeroportos, restaurantes, cafés, entre outros). Na análise realizada verificou-se que, para além do custo das soluções, não existe flexibilidade ao nível das opções de administração, nomeadamente a facilidade de integração na mesma interface da gestão e da configuração de todos os serviços envolvidos. A utilização do Webmin ultrapassa esses problemas pois utiliza uma licença GNU[2] e permite integrar na mesma interface gráfica, baseada na *web*, a configuração de todos os componentes do serviço de autenticação WBL.

5. ALTA DISPONIBILIDADE E TOLERÂNCIA A FALHAS

De forma a assegurar o funcionamento do WBL em caso de falha de um dos seus serviços, ou da máquina em que estão alojados, foi implementado um mecanismo de alta disponibilidade e tolerância a falhas (*High Availability* – HA [14]).

O mecanismo de tolerância a falhas desenvolvido monitoriza os vários serviços de suporte ao WBL que se encontram a correr na respectiva máquina. Ao detectar uma situação crítica (p.e. paragem do servidor *web* – Apache), é despoletada uma acção automática de reactivação desse serviço na máquina. Se a máquina parar (p.e. avaria num disco), a activação dos serviços do WBL será realizada numa outra máquina de *backup*.

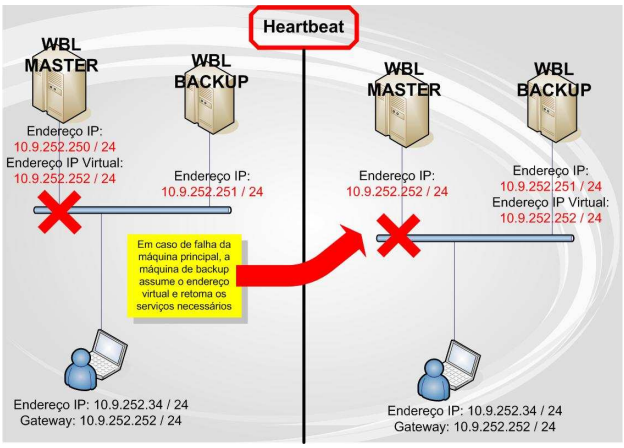

Figura 4. Funcionamento do Heartbeat em caso de falha do sistema primário.

Para detectar a falha da máquina que aloja os serviços de suporte ao WBL é utilizado o software *open-source Heartbeat* [14]. Esta aplicação implementa uma solução de alta disponibilidade recorrendo ao uso de um *cluster* - composto por pelo menos duas máquinas (uma principal e outra de *backup*). São enviadas regularmente mensagens de teste à conectividade (*keepalive*) das máquinas. Quando a máquina de *backup* deixa de receber mensagens de *keepalive* da máquina principal, esta inicia um processo de retoma automática dos serviços do WBL. Este processo é denominado "*takeover*"[16]. A transição transparente dos recursos de uma máquina para a outra é efectuada através do uso de IPs virtuais. O utilizador apenas utiliza o endereço virtual, que tanto poderá estar associado à máquina principal como à de *backup*, conforme se ilustra na Figura 4.

O uso do *Heartbeat*, juntamente com outras aplicações e serviços de monitorização (p.e. MON [15]), torna o serviço WBL robusto e tolerante a falhas que possam ocorrer nos serviços de suporte ou na máquina em que são executados. Esta solução assegura, de uma forma transparente para os utilizadores, a disponibilidade do mecanismo de WBL.

6. RESULTADOS E TESTES

Desde a entrada em funcionamento do WBL no IPL, em Outubro de 2006, foi possível recolher informação sobre a sua utilização. Os resultados apresentados na Tabela 1 demonstram que a utilização do sistema tem vindo a crescer gradualmente – - actualmente cerca de 27% dos utilizadores utiliza este mecanismo.

Também se verificou que o WBL teve um contributo fundamental para o aumento de utilizadores da rede *wireless*, cerca de 900, principalmente em escolas onde os membros da comunidade académica têm conhecimentos mais básicos de informática. Verificou-se também que existem Escolas em que o número de utilizadores do WBL representa mais de 50% do número de utilizadores.

Tabela 1. Utilização da autenticação *web* no IPL

IPLeiria							
Mês	**802.1x**		**WBL**		**VPN**		**Total**
Setembro 06	728	65%	0	0%	350	31%	1078
Outubro 06	1267	59%	285	13%	583	27%	2135
Novembro 06	1651	61%	480	18%	597	22%	2728
Janeiro 07	1647	61%	520	19%	535	20%	2702
Março 07	1697	57%	747	25%	551	18%	2995
Maio 07	1890	57%	890	27%	522	16%	3302

Foram também efectuados testes de alta disponibilidade e tolerância a falhas que permitiram aferir sobre a boa prestação da arquitectura baseada no *Heartbeat*. No caso de uma falha na máquina principal, o *HeartBeat* consegue efectuar o *takeover* de todos os componentes do sistema WBL em apenas 8 segundos. Atendendo a que esse é o tempo em que o serviço ficará indisponível, pode-se considerar que o impacto nos utilizadores é quase insignificante.

7. CONCLUSÕES E TRABALHO FUTURO

O mecanismo de autenticação WebBasedLogin (WBL) foi desenvolvido tendo como objectivo principal eliminar as barreiras e os problemas colocados pelos mecanismos existentes (802.1x e acesso por VPNs) de acesso à rede *wireless*. O WBL permite que os utilizadores possam aceder à rede *wireless* após efectuarem a sua autenticação numa página *web* para que são redireccionados ao tentarem aceder à internet. Este mecanismo não requer

[2] Projecto com o objectivo de criar um sistema operacional totalmente livre, que qualquer pessoa tem direito de usar e distribuir sem ter que pagar licenças de uso.

qualquer tipo de configuração por parte do utilizador, sendo bastante fácil de utilizar nos mais variados tipos de dispositivos e por todos os membros da comunidade académica – em especial por aqueles com conhecimentos mais básicos de informática.

O mecanismo de WBL desenvolvido possui um módulo que permite a sua administração através de um interface *web*. Foi também implementado um mecanismo que assegura a disponibilidade e a tolerância a falhas do WBL. Este mecanismo assegura o funcionamento do WBL, de uma forma transparente para os utilizadores, caso ocorra uma falha nos serviços que o suportam ou na máquina em que estes estão alojados.

O WBL encontra-se a funcionar, desde Outubro de 2006, em todas as unidades orgânicas do Instituto Politécnico de Leiria. A utilização desse meio de acesso tem vindo a aumentar gradualmente, e teve um contributo fundamental no aumento do número de utilizadores da rede *wireless*.

Prevê-se, no futuro, vir a testar o WBL noutros projectos que necessitem de um método de autenticação dos utilizadores simples e eficaz, nomeadamente no projecto Leiria Região Digital[17]. Neste projecto, estão a ser criados pontos públicos de acesso à internet em banda larga.

8. REFERÊNCIAS

[1] Página oficial do projecto e-U : www.e-u.pt

[2] Página da Fundação para a Ciencia e Computação Nacional: www.fccn.pt

[3] Publicação do 802.1x: www.ieee802.org/1/pages/802.1x.html

[4] Edwin Lyle Brown; "802.1x Port-Based Authentication"; ISBN: 1420044656; publicado em 2006.

[5] Página oficial sobre o programa "Portugal Digital": www.cidadesdigitais.pt

[6] Página da Unidade de Missão e Inovação e Conhecimento: www.umic.pt

[7] Anabela Pedroso; "Electronic University, Virtual Campus (Portugal) http://epractice.eu/index.php?menu=4&pn=11&page=gpcase&case=152

[8] Delia Meth-Cohn, Katherine Shields; "Accessing EU funds in the new member states: best practice from around Europe"; Editado por "Economist Corporate Network"; Publicado em Março de 2005

[9] Página oficial da rede e-U no Instituto Politécnico de Leiria: http://wireless.ipleiria.pt

[10] Página do Instituto Politécnico de Leiria com a descrição de equipamentos *wireless* que foram testados nos centros de informática e apoio ao utilizador: http://wireless.ipleiria.pt/configuracao/placaswifi

[11] Software de gestão de serviços em Linux: www.webmin.com

[12] Página oficial do software "*Zone CD Gateway*": www.publicip.net

[13] Página oficial do software "*FirstSpot*": www.**patronsoft**.com/firstspot/

[14] Página oficial do software *open-source Heartbeat*: www.linux-ha.org

[15] Página oficial do software *open-source* MON: www.kernel.org/software/mon/

[16] Filipa Ferreira, Nélia Santos, Mário Antunes; "Clusters de Alta Disponibilidade – uma abordagem Open Source"; in actas da conferência Engenharias 2005, Vol. 2 pp 179-183, Portugal

[17] Página oficial do projecto Leiria Região Digital: www.leiriaregiaodigital.pt