Licenciatura engenharia informática

New trends in Access Control Modes applied to Social Networks

Autores:

Adérito Brás Carreira Pereira **20080119**

Amílcar da Silva Morais **20081801**

Orientador:

Mestre **Sérgio Guerreiro**

Abstract

This work studies, evaluates and tests a mechanism of ACM (Association for Computing Machinery) in a social network.

Social networks are web-based communities where participants establish relationships and share resources with other users. Despite the advantages in terms of propagation of the contents there is a growing need for content owners to have control over their resources since they can be accessed by a huge number of other users. To control access to contents in a social network we see today essentially authentication via user / password. In this complex context it is insufficient and subject of all kinds of attacks.

So we intend to use RBAC (Role Based Access Control) as a mechanism to control access to contents along with the implementation of an auxiliary mechanism for user authentication in open source Elgg social network to demonstrate our proposed implementation.

With the solution developed, we implemented a system of registration, authentication and validation activity controlled by the data from the citizen card. The aim of this solution is to obtain more security in social networks.

Keywords: social networking, citizen card, authentication, validation, elgg

Resumo

Este trabalho estuda, avalia e testa um mecanismo de ACM (Association for Computing Machinery) numa rede social.
As redes sociais baseadas na Web são comunidades onde os participantes estabelecem relações e partilham recursos com outros utilizadores.
Apesar das vantagens em termos de divulgação há uma necessidade crescente dos proprietários dos conteúdos terem controlo sobre os seus recursos uma vez que estes podem ser acedidos por um número indeterminado de outros utilizadores.
Para controlar os acessos aos artefactos numa rede social assistimos hoje essencialmente à autenticação por via exclusiva de user/password.
Num contexto complexo isto é insuficiente e utilizador está sujeito a ataques de todo o tipo.
Assim utilizamos o RBAC (Role Based Access Control) como mecanismo de controlo de acesso aos artefactos juntamente com a implementação de um mecanismo auxiliar de autenticação do utilizador numa rede social open source ELGG para demonstrar a nossa proposta de implementação.
Com a solução desenvolvida, implementámos um sistema de registo, autenticação e validação de atividade controlado pelos dados do cartão do cidadão.
Pretende-se assim com esta solução obter mais segurança nas redes sociais.

Palavras-chave: rede social, cartão cidadão, autenticação, validação, elgg

Índice

Lista das Figuras

Lista de Abreviaturas

ACM	Association for Computing Machinery
RBAC	Role-Based Access Control
MAC	Mandatory Access Control
DAC	Discretionary Access Control
ELGG	Open Source Social Networking Engine
XAMPP	Free and open source cross-platform web server Apache/MySQL/PHP and Perl.
SAPO	Servidor de Apontadores Portugueses Online

1. Introdução

Inicialmente os utilizadores da internet eram simples consumidores de informação que era disponibilizada e basicamente a comunicação era unidirecional.
Hoje os utilizadores passaram a produzir os seus próprios conteúdos e a disponibiliza-los. São criadas comunidades virtuais onde os utilizadores partilham preferências, fazem amigos, disponibilizam fotos, comentários, musicas, filmes de uma forma cada vez mais facilitada.
Nascem comunidades e serviços de partilha, as redes sociais.
Não são apenas os utilizadores domésticos que utilizam as redes sociais, as empresas descobriram que as poderiam utilizar para fazer chegar a sua imagem a todo o público de uma forma simples e barata.
Uma das maiores ameaças à segurança e privacidade dos utilizadores advém do tipo de conteúdo que partilham. Ao colocar ao alcance de outros utilizadores tanta informação, por vezes pessoal, o proprietário da informação corre o sério risco de ver adulterado ou ver divulgado onde não quereria o seu conteúdo, pois apesar das redes sociais disponibilizarem alguns mecanismos que permitem agrupar a informação para que só alguns visitantes da rede tenham acesso não nos podemos esquecer que os conteúdos estão apenas à distância de uma simples validação de user / palavra-chave.
Igualmente as empresas ao recorrerem às redes sociais como complemento de avaliação de candidatos a postos de trabalho podem constituir uma ameaça ao possível candidato ao aceder ao seu perfil.
Existem alguns modelos para implementar controlo de acesso nas redes sociais.
Utiliza-mos o RBAC (Role Based Access Control) que vai mais além do simples controlar que utilizador pode aceder onde. O RBAC introduz o conceito de role (perfil) que pode ser definido com um conjunto de ações e responsabilidades associadas.
Apesar de constituir um modelo de controlo excelente implementa-mos neste trabalho controlos adicionais como por exemplo para que um utilizador consiga interagir com as atividades da rede social como por exemplo colocar um comentário no blog ,fazer upload de fotografias, ou escolha de grupo, este terá de ter colocado o cartão do cidadão no leitor para confirmar a sua autenticação.
Para a implementação deste trabalho elege a rede social open source ELGG.
Em primeiro lugar contextualizamos de uma forma geral alguns dos controlos de acesso existentes, o que são, a sua importância e conceitos.
Em seguida apresentaremos especificamente os conceitos e o modelo que implementamos.

2. Enquadramento Teórico

Diferentes Modelos de Controlos de Acesso

Existem vários modelos de controlo de acesso, sendo os mais conhecidos os MAC (Mandatory Access Control) e o DAC (Discretionary Access Control). O primeiro surgiu para proteger sistemas militares, enquanto o segundo sempre foi indicado como a solução para sistemas civis e comerciais.

Um modelo em particular que vem ganhando cada vez mais aceitação científica e prática é o RBAC (Role-Based Access Control), principalmente em substituição ao DAC, que oferece significativas vantagens na definição e administração do controle de acesso a recursos informáticos.

Enquanto tanto o MAC quanto DAC controlam apenas o acesso a informações, RBAC trata o acesso tanto de funções quanto de informações. Além disso, introduz o conceito de *role* (perfil, ou cargo), que pode ser definido como um conjunto de ações e responsabilidades associados com um cargo em particular. Utilizadores e operações são associados aos *roles*, tornando a manutenção de um sistema RBAC mais consistente e organizada, já que as relações entre permissões e cargos costumam ser mais persistentes que entre permissões e utilizadores específicos.

A especificação RBAC introduz também o conceito de hierarquia de cargos, com herança de permissões. Traz o importante conceito de *constraints* (restrições), predicados que podem operar sobre a autorização de um acesso, negando-o ou permitindo-o com base em critérios mais complexos do que o envolvido em operações simples.

DAC: Discretionary Access Control

Controle de acesso discricionário tem sua origem no contexto de pesquisa académica em sistemas de tempo compartilhado que surgiram no início dos anos setenta.

DAC é baseado na noção de que utilizadores individuais são “proprietários” de conteúdos e portanto tem controlo total em quem deve ter permissões para aceder ao conteúdo. Um utilizador transforma-se em proprietário do conteúdo ao criá-lo.

É um modelo muito popular de controlo de acesso, pela sua utilização em grande escala em sistemas comerciais. Todas as variantes do UNIX, o Netware e a série Windows NT, 2000 e XP utilizam o modelo DAC como modelo básico de controlo de acesso. Estes sistemas operativos utilizam a técnica de listas de controlo de acesso para conceber a implementar as suas permissões.

Ao contrário de MAC, não existem políticas de controlo de acesso em DAC popularmente difundidas e em utilização, já que o modo de operação “padrão” do modelo é suficiente para as necessidades de uma boa parte do mundo comercial.

O modelo DAC possui uma fraqueza inerente: o facto de que informação pode ser copiada de um conteúdo para outro, de modo que acesso a uma cópia é possível mesmo que o proprietário do conteúdo original não tenha origem no acesso ao original.

Utilizadores que possuem acesso ao conteúdo original podem inadvertidamente permitir a realização de cópias não-autorizadas, ao executar um programa "cavalo de tróia" que faça a cópia dos dados do conteúdo sem a explícita autorização ou cooperação do utilizador.
Essa fraqueza do modelo DAC tornou-o insuficiente para sistemas militares, em que a informação precisava ter um alto nível de controlo e ser resistente a ataque por cavalos de tróia, fomentando a criação do modelo MAC.

MAC: Mandatory Access Control

Enquanto o ponto-chave do DAC é o facto de que os utilizadores são considerados proprietários dos conteúdos e portanto responsáveis pelas suas permissões de acesso, este modelo prevê que utilizadores individuais não tem escolha em relação a que permissões de acesso que eles possuem ou a que conteúdos podem aceder.
Neste modelo, os utilizadores individuais não são considerados proprietários dos conteúdos, e não podem definir suas permissões – isso é realizado pelos administradores do sistema.
O modelo MAC é conhecido – a tal ponto de ser as vezes confundido – pela sua utilização em políticas de acesso multinível, em que se deseja controlar o fluxo de informações num sistema. Em geral, quer-se garantir que a informação só transite num determinado sentido: por exemplo, de níveis mais baixos de confidencialidade para níveis maiores de confidencialidade – nunca de níveis mais altos para níveis mais baixos.
Esta área de pesquisa desenvolveu-se fortemente nos anos setenta, com base nas necessidades de confidencialidade dos sistemas militares norte-americanos.
O fluxo de informações dentro destes sistemas deve seguir regras claras para garantir a sua confidencialidade.

RBAC: Role-Based Access Control

O controlo de acesso baseado em perfis (RBAC) é um mecanismo de segurança que pode reduzir extremamente o custo e a complexidade da administração de segurança para grandes aplicações de rede.
RBAC simplifica a administração de segurança usando os perfis, as hierarquias e as restrições para organizar os privilégios.
As principais características do RBAC são a capacidade de articular e executar políticas específicas de segurança e para agilizar os processos normalmente complexos de gestão de segurança.
A noção central é que as permissões são associadas a perfis, e utilizadores são associados aos seus perfis corretos na organização. As permissões para executar determinadas operações são atribuídas a funções específicas. Como aos utilizadores não são atribuídas permissões diretamente, mas apenas adquiri-los através do seu perfil, a gestão de direitos de utilizador torna-se uma questão simples. Este conceito básico tem a vantagem de simplificar a compreensão e gestão dos privilégios: os perfiles podem ser atualizados sem ter que actualizar os privilégios para cada utilizador individualmente.

Três regras básicas são definidas para RBAC:

1. Atribuição de função: Um utilizador pode executar uma operação apenas se o utilizador tem selecionado ou foi atribuído um perfil.
2. Perfil de autorização: perfil ativo do utilizador deve ser autorizado para o assunto. Com a regra 1 acima, esta regra garante que os utilizadores podem assumir perfis apenas para a qual estão autorizados.
3. Autorização da transação: Um utilizador pode executar uma operação apenas se a transação esta autorizada para o perfil ativo do utilizador. Com regras 1 e 2, esta regra garante que os utilizadores podem executar operações somente para a qual estão autorizados.

Restrições adicionais podem ser aplicadas, e as funções podem ser combinadas numa hierarquia onde as funções de nível superior assumem permissões de propriedade de subfunções.

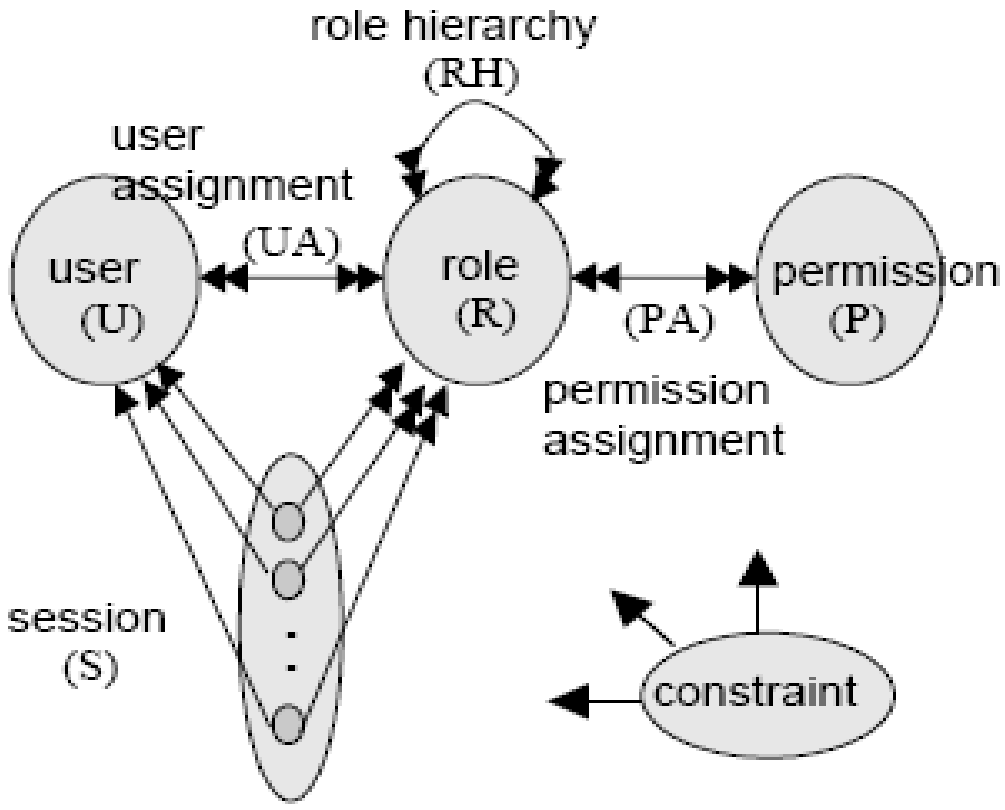

Figura 1: Modelo RBAC

Autores: Adérito Pereira, Amílcar Morais
Orientador: Mestre Sérgio Guerreiro

RBAC tem duas fases: atribuição do utilizador-conteudo e atribuição da conteudo-permissão. A vantagem a mais significativa de RBAC é que simplifica a gestão de autorizações.

- **Utilizador**: "pessoas que se ligam através de um sistema informático. Em muitos projetos, é possível um utilizador ter no início de uma sessão, múltiplos IDs, e estes IDs estarem simultaneamente ativos. Os mecanismos de Autenticação tornam possível atribuir os IDs múltiplos a um único utilizador."
- **Sessão:** "Um exemplo de sessão é o diálogo de um utilizador com um sistema."
- **Assunto:** "processos ativos no computador são considerados como um assunto. Todas as ações de um utilizador num sistema informatizado estão a ser executadas com algum programa que funciona no computador. Um utilizador pode ter assuntos múltiplos na operação, mesmo se o utilizador tiver somente um início de uma sessão e uma sessão. Por exemplo, um sistema do E-mail pode estar a carregar o correio de um utilizador periodicamente, enquanto o utilizador utiliza um web browser. Cada um dos programas de utilizador é um assunto, e os acessos de cada programa serão verificados para assegurar-se de que estejam permitidos para o utilizador que invocou o programa."
- **Objeto**: "algum recurso acessível num sistema informático, incluindo ficheiros, periféricos tais como impressoras, em bases de dados, e em entidades fine-grained tais como campos individuais em registos da base de dados. Os objetos são vistos tradicional como as entidades passivas que contêm ou recebem a informação, embora os modelos adiantados uniformes do controle de acesso incluam a possibilidade de tratar programas, impressoras, ou outras entidades ativas dos objetos"
- **Operações**: "é um processo ativo invocado por um assunto. Os modelos adiantados do controle de acesso que foram concebidos estritamente com o fluxo de informação aplicam o assunto do termo a todos os processos ativos, mas os modelos de RBAC requerem uma distinção entre o assunto e a operação. Para o exemplo, quando um utilizador do ATM entra com um cartão e com um PIN correto, o programa de controlo que opera no interesse do utilizador é um assunto, mas o assunto pode iniciar mais de uma operação: depósito, levantamento, transferências, ou outro."
- **Permissão**: "são as autorizações para executar alguma ação no sistema. Na maioria da literatura de segurança do computador, a permissão do termo consulta alguma combinação do objeto e da operação. Uma operação particular usada em dois objetos diferentes representa duas permissões distintas, e similarmente, duas operações diferentes aplicadas a um único objeto representam duas permissões distintas."
- **Identidade**: A "identidade é o conceito fundamental excecionalmente de identificar um objeto (pessoa, computador, etc.) dentro de um contexto. O contexto pode ser local (dentro de um departamento), incorporado (dentro de uma empresa), nacional (dentro dos limites de um país), global, e possivelmente universal (extensível aos ambientes desconhecidos). Muitas identidades existem para domínios locais, incorporados, e nacionais."

Estado da Arte.

Com o crescente utilização do cartão do cidadão, e com a sua banalização este passou a ser aproveitado para garantir de forma segura o acesso a plataformas e serviços.
Existem aplicações desenvolvidas para acesso a aplicações bancarias, finanças, segurança social bem como recentemente para acesso a plataforma de pesquisa.
Referente às plataformas de pesquisa existe acesso ao SAPO (Servidor de Apontadores Portugueses online) através do cartão do cidadão, mas fazendo a sua validação de forma diferente, validado através dos certificados do cartão.
Este portal foi desenvolvido na universidade de Aveiro, por seis membros do centro de informática e é propriedade atualmente da Saber & Lazer - Informática e Comunicação S.A. Empresa esta que é detida a 100% do seu capital pela PT multimédia.

Figura 2: Portal SAPO

3. Solução

Atualmente as soluções de autenticação existentes são baseadas nas credenciais de utilizador e palavra passe. Esta autenticação torna vulnerável a garantia de autenticidade dos utilizadores. Em especial as soluções que utilizam a internet, por estarem expostas a qualquer utilizador de internet, são mais facilmente enganadas por tentativas de adivinhação, bem como aplicações existentes para decifrar dados utilizador.

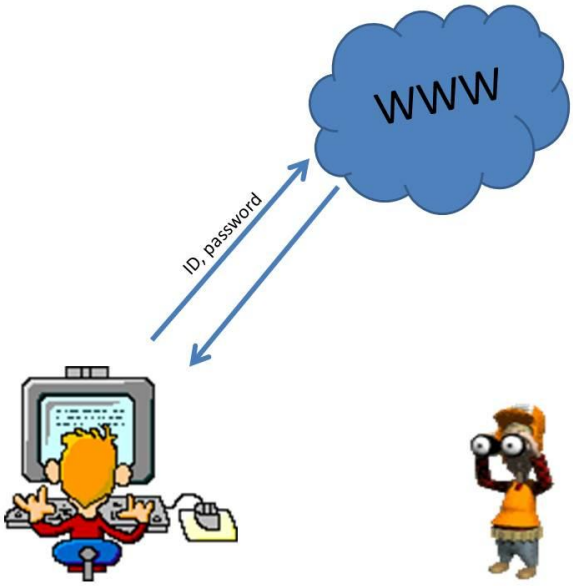

Figura 3: Solução existente atualmente.

Perante esta realidade apresentamos uma solução que não dependendo do nome de utilizador e palavra passe escritos diretamente no teclado do computador, consegue validar utilizador recorrendo a leitura de um dispositivo externo credível.

Utilizando o cartão de cidadão podemos garantir autenticidade da informação.

Assim para se registar na rede social basta inserir o cartão do cidadão e apenas escrever o email e nome a utilizar na rede. Os restantes dados que servirão para autenticação serão recolhidos do cartão do cidadão de forma automática. Após confirmado o registo por administrador da rede poderá autenticar-se, bastando para isso inserir o cartão para leitura e clicar no botão de login. Os dados para autenticação serão também recolhidos de forma automática. Utilizamos este processo para registo de utilizador e autenticação.

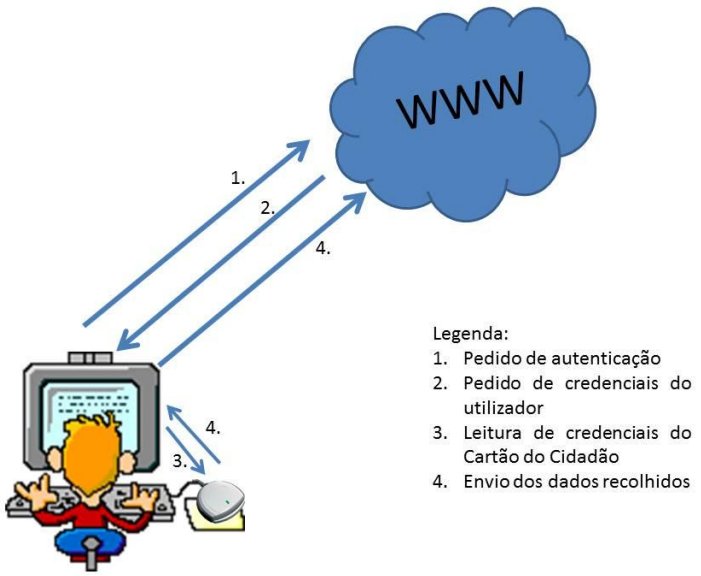

Figura 4: Solução Apresentada para autenticação e registo

Para o processo de validação de acesso a conteúdos pois será necessário garantir a autenticidade do utilizador. Neste processo cada vez que se pretender inserir conteúdo no blog,file,bookmarks, ou criar novo grupo será necessário manter o cartão inserido no leitor, pois será confirmada a sua autenticidade.

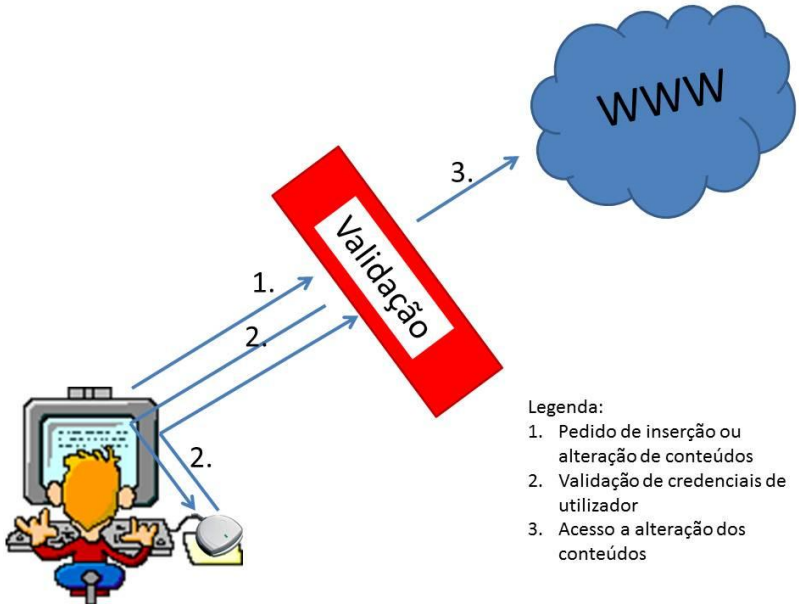

Figura 5: Solução apresentada para validação acesso a conteúdos.

4. Método

Escolha da Plataforma

Utilizamos para correr o Elgg, o XAMPP que é um servidor independente de plataforma, software livre, que consiste principalmente na base de dados MySQL, o servidor web Apache e os interpretadores para linguagem de script: PHP e Perl. O nome provém da abreviação de X (para qualquer dos sistemas operativos), Apache, MySQL, PHP, Perl. O programa está disponível sob licença GNU e atua como um servidor web livre, fácil de usar e capaz de interpretar páginas dinâmicas

Escolha da Rede social

Com variada e múltiplas opções de escolhas de ambiente onde poderíamos desenvolver e aprofundar o trabalho (Dolphin,mahara,VMuhti,Elgg,..entre outras),nem sempre é fácil a sua escolha. Essa escolha recaiu na rede Open Source Elgg.

E porquê uma rede social?

Apenas por ser uma solução onde nos é possível delimitar o ambiente onde é desenvolvido o trabalho, e ser também uma amostra para as múltiplas situações onde se pode implementar no meio empresarial.

Elgg é um software Open Source de rede social. Oferece a possibilidade de ter um blog, recolher informações de Rss feeds e partilhar ficheiros. Tudo pode ser partilhado com a comunidade havendo no entanto restrições de privacidade. Todo o conteúdo colocado no espaço pelos membros pode ser controlado por restrições de acesso. Cada item disponibilizado pode igualmente ser catalogado com palavras-chave de forma a facilitar a terceiros a sua pesquisa na plataforma. Pode ser modificada ou acrescentada com a adição de plugins. Alguns plugins que se encontram instalados por default:

- **Activity:** Exibe as últimas atividades do site, pode-se filtrar pelo plugin do qual deseja ver as últimas atividades (plugin File por exemplo) ou ainda separar pelas últimas atividades de todos, dos amigos, ou apenas minhas;
- **Blogs:** Sistema que funciona como um blog no qual pode-se colocar qualquer tipo de conteúdo e receber comentários. Também permite filtragem de visualização dos posts de todo o site, dos amigos ou apenas os nossos.
- **Bookmarks:** Sistema de marcadores para sites ou outros recursos (Favoritos). Permite comentários aos itens marcados.
- **Files:** Sistema para colocação de arquivos com possibilidade de comentar os arquivos.
- **Friends:** Possibilita adicionar e retirar amigos, organização deles em grupos e envio de mensagens.
- **Groups:** Possibilita a criação de grupos (comunidades) com fóruns de discussão, colocação de arquivos, criação de páginas e qualquer outro recurso oferecido por algum plugin externo.
- **Members:** Oferece a visão de todos os membros do site e opções de busca.
- **Page:** Plugin para criação de páginas de conteúdo, possibilita a criação de páginas e sub-páginas com possibilidade de edição colaborativa e colocação de comentários.

- **The Wire:** Sistema semelhante ao Twitter, já existem plugins externos que permitem adicionar seguidores.

Equipamento de validação e autenticação

A validação é feita através do cartão do cidadão. Para a sua utilização necessitamos também de um leitor de cartões. A escolha deste meio para autenticação advém do facto de este ser emitido e garantida a sua segurança por uma entidade idónea.
O Cartão de Cidadão segue as normas internacionalmente recomendadas para que este seja um documento de identificação e um documento de viagem reconhecido oficialmente. Assim, este encontra-se alinhado pelas orientações correntes da União Europeia, nomeadamente as do grupo de trabalho para o European Citizen Card (ECC), pelas normas definidas pela International Civil Aviation Organization (ICAO) para documentos de viagem internacionais (documento 9303) e os standards 7501 e 7810 definidos pela International Organization for Standardization (ISO).
Em função dos objetivos de utilização, das aplicações previstas e das soluções neste momento perspectivadas, o chip do Cartão de Cidadão tem as seguintes características:

- É um chip Java Card, multi-aplicação;
- Suporta a versão mais recente da plataforma Java Card e o uso de logical channels;
- Possui uma capacidade de memória EEPROM (ou equivalente) mínima de 64 KB;
- Possui capacidades de gestão de memória dinâmica, suportando garbage collection pela JVM e de proteção de memória;
- Possui capacidades de gestão de espaço de armazenamento, incluindo desfragmentação e reutilização de espaço libertado;
- Possui capacidades de true random number generation. Suporta múltiplos PIN. Os PIN estão em conformidade com a norma ISO/IEC 7816-4;
- Suporta mecanismos de bloqueio em caso de erro na introdução do PIN após N tentativas e respetivo desbloqueio por meio de introdução de PUK do cidadão e de chave administrativa de acesso ao cartão, para desbloqueio;
- Suporta mecanismos de geração de novo PIN do cidadão, em caso de esquecimento deste, mediante a introdução do PUK do cidadão e de PUK aplicacional de geração de PIN;

Possui um motor criptográfico interno que suporta:

- Assinatura e verificação RSA de 1024 bits;
- Assinatura eletrónica qualificada segundo a norma CEN CWA 14169 (Secure Signature-creation devices “EAL 4+”);
- DES e TDES (triple Data Encription Standard);
- MD5, SHA-1 e SHA-256, no mínimo;
- MAC (message authentication code);
- PKCS#1 (RSA Cryptography Standard) e PKCS#15 (Cryptographic Token Information Format Standard);
- É compatível com leitores de cartões da norma EMV-CAP, para funcionamento de autenticação multicanal baseada em one-time password;

- Possui uma chave de proteção da personalização inicial e está preparado para resistir aos ataques conhecidos do tipo “hardware attack”,“timing attack”, “simple power analysis” e “differential power analysis” entre outros.

Para leitura do cartão é necessário estar munido de um leitor de cartão do cidadão, por exemplo o modelo Desktop, um modelo de leitor externo sem PIN-pad nem lógica aplicacional, para ligação a um computador pessoal e comunicação com aplicações existentes no Cartão de Cidadão.

A interface com o cartão é de contacto e os leitores deverão ainda estar de acordo com as normas em vigor da Comunidade Europeia relativas à segurança de produtos (selo CE), e redução de substâncias perigosas (RoHS).

Implementação e controlo de autenticação

Instalar máquina virtual.

Para a realização do trabalho a que nos propusemos, começámos por criar uma máquina virtual e instala-la, para assim termos mais mobilidade na realização do mesmo.

Instalar XAMPP e configurar

Sendo necessário um servidor para alojar a rede social instala-mos o XAMPP, conforme documento em anexo “Using XAMPP (Apache-MySQL-PHP-Perl) for Windows”.

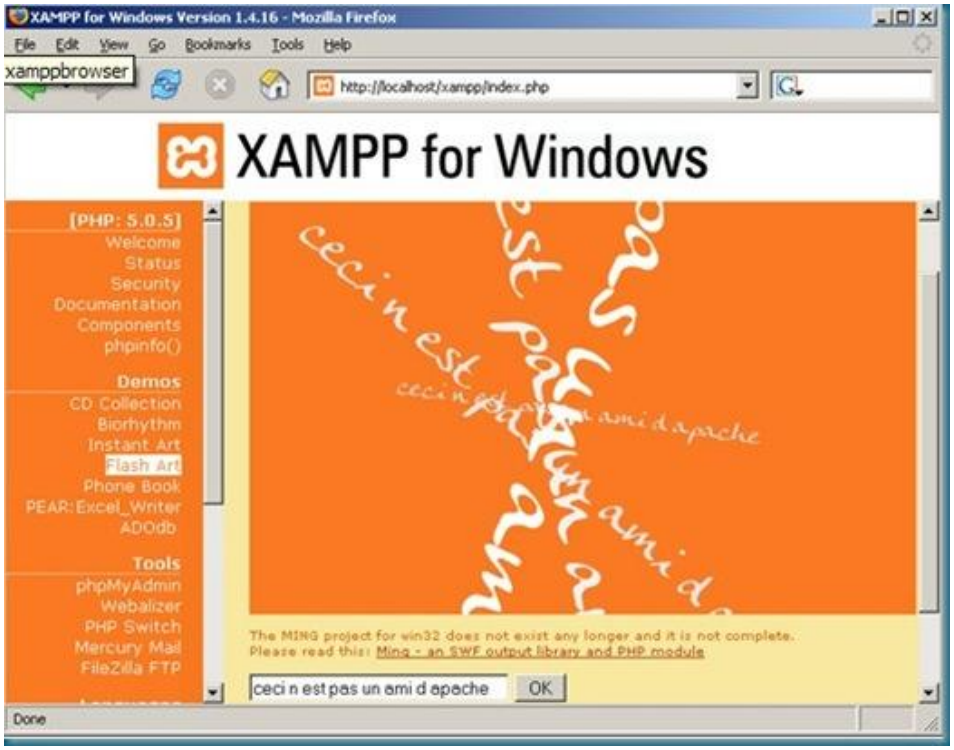

Figura 6: Xampp instalado

Instalar Elgg e configurar

Para desenvolvimento do trabalho, escolhemos a rede social open source Elgg.

Para baixar a última versão do script fomos a **http://www.elgg.org/download.php**,que descompactamos o ficheiro e coloca-mos no servidor, na pasta htdocs.

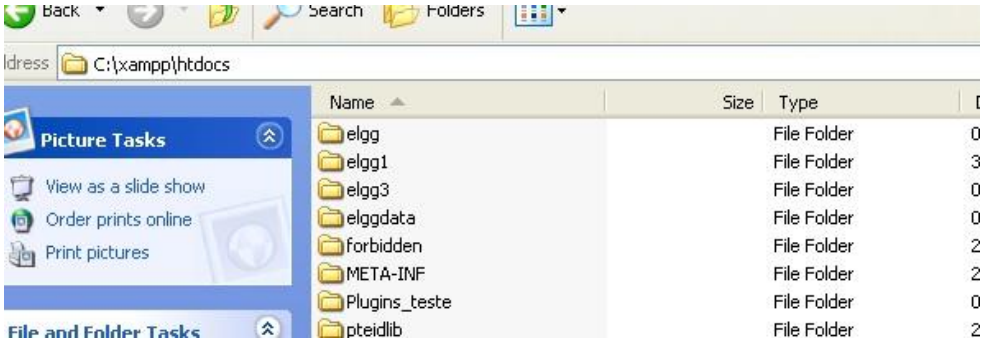

Figura 7: Elgg instalada

Acedendo de seguida para que se desse inicio á configuração.

Após a configuração do mesmo foi necessário criar base dados para o mesmo.

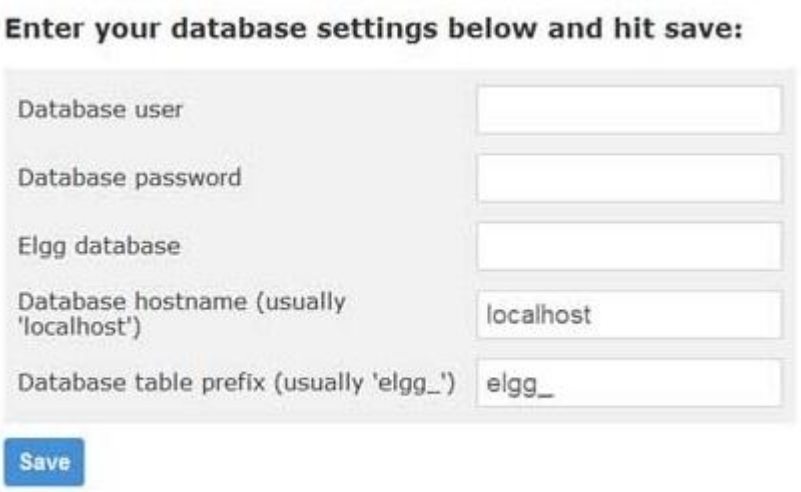

Figura 8: Criar Base dados para Elgg

Estas configurações podem ser consultadas detalhadamente no anexo “instalando o Elgg”

Instalar aplicação leitor cartão

Para a utilização do cartão de cidadão é necessário instalar a aplicação para a leitura do cartão de acordo com o sistema operativo utilizado, mais detalhes no anexo“Manual_Cartao_de_Cidadao_v1.24.pdf”

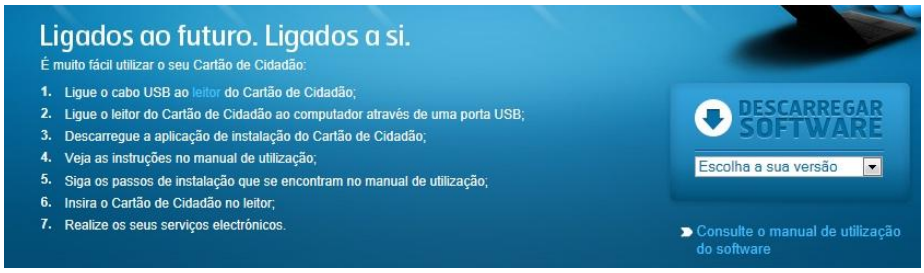

Figura 9: instalar aplicação leitor cartão ,sitio senha 01

Aceder elgg a partir do exterior

Para aceder à elgg a partir do exterior via ip tentamos a solução de fazer a seguinte configuração:

Na pasta C:\xampp\apache\conf procuramos pela linha:
ServerName localhost:80
No bloco-notas alteramos o valor de 80 para 8080

```
175  #
176   ServerName localhost:8080
177
```

Figura 10: ServerName localhost:8080

Alteramos também a linha Listen 80 para 8080. Guarda-mos o ficheiro e reinicia-mos o servidor. Tentamos aceder via IP, mas sem sucesso.

```
46  #Listen [::]:80
47  Listen 8080
```

Figura 11: Listen 8080

Após muita pesquisa e tentativas conseguimos, não por esta opção mas configurando a base dados da Elgg. Alterando na tabela elgg_sites_entity onde aparece localhost colocando o ip onde esta a funcionar a rede social.

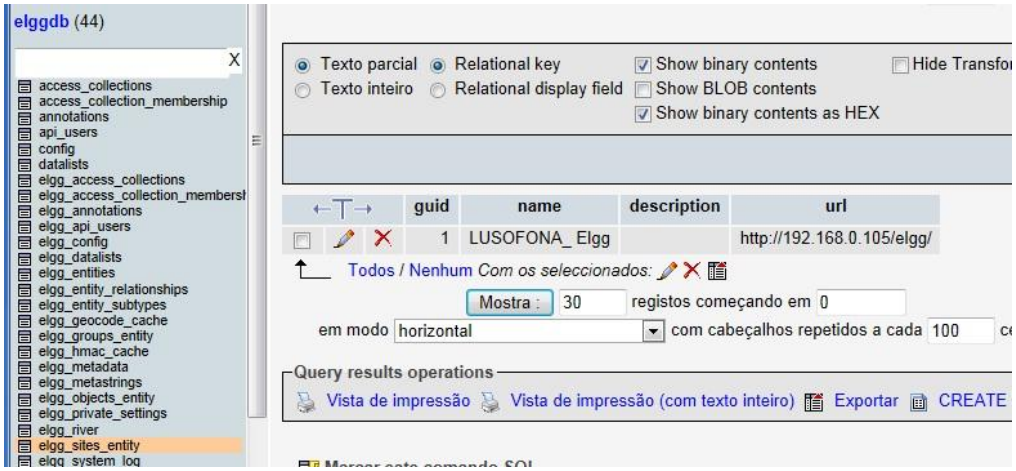

Figura 12: base dados elgg alteração para aceder exterior

Desenvolvimento da applet

Requisitos para a applet funcionar no computador cliente:

- ter ligação à Internet;
- ter leitor de Cartão de Cidadão instalado e ligado ao computador;
- ter o Java RE instalado e activado no computador;
- ter o javascript activado no browser;
- ter o software do Cartão de Cidadão instalado no computador;
- ter o software CCTools instalado no computador (Windows | Mac | Linux rpm/deb).
- Nota: O sistema deverá reconhecer automaticamente estes componentes, mas se não o fizer será necessário que cumpra estes requisitos manualmente.

Arquitectura de Autenticação:

Visão geral do Cartão de Cidadão:
O Cartão de Cidadão tem, no seu chip, informações sobre o seu titular.
Descrição das interfaces disponibilizadas pelo "middleware"do Cartão de Cidadão:

As seguintes interfaces podem ser encontradas no middleware do Cartão de Cidadão:
- CryptoAPI/CSP
- PKCS#11
- eID lib (= a 'SDK' ou 'Software Development Kit')

A CSP está apenas disponível em ambiente Windows; as outras 2 bibliotecas estão disponíveis em Windows, Linux e Mac OS X.
As primeiras 2 interfaces são APIs standard para operações criptográficas; a eID lib tem uma API nonstandard
que é direcionada à funcionalidade não-criptográfica do Cartão de Cidadão.

No Windows, estas bibliotecas podem ser encontradas na pasta System32; no Mac OS X no diretório /usr/local/lib e em Linux depende do diretório de instalação.
Tray applet

A aplicação "Tray applet" é instalada como uma funcionalidade da área de notificação.
No Windows, aparece normalmente no canto inferior direito do ecrã, no Mac no canto superior direito do ecrã. Quando ativada (o utilizador pode
descativá-la), verifica se um cartão eID está inserido. Após inserir o cartão será mostrada a fotografia do cidadão durante uns segundos.
Irá também registar automaticamente (se esta opção estiver ativada) os certificados do cartão na Microsoft certificate store, caso ainda não estejam registados. Quando o cartão é removido os certificados registados são automaticamente removidos da certificate store (se esta opção estiver ativada).
Este modo é também conhecido como modo “Kiosk”. Esta funcionalidade a nível de certificados é apenas implementada na plataforma Windows devido às outras plataformas (Mac e Linux) não suportarem o conceito de “certificate stores”.

A interface PKCS#11
A interface PKCS#11 (v2.20) é utilizada por aplicações não Microsoft como por exemplo o Netscape.
A interface PKCS#11 é por vezes chamada de Cryptoki.
Biblioteca/interface utilizada neste trabalho;
eID Lib API
- Uma interface C/C++, como biblioteca dinâmica
- Uma biblioteca Java wrapper (JNI) sobre uma interface C/C++
- Uma biblioteca C# wrapper para .NET sobre uma interface C/C++

Organização API

As funções estão divididas em 4 categorias:
 Funções Initialisation e termination, mandatórias para iniciar e terminar a utilização.
 Funções de Identity, usadas para obter dados identificativos (nome, morada, etc.) do cartão
 Funções General purpose de alto nível, usadas para aceder a dados de uma forma genérica (ficheiros, PIN), principalmente em outras aplicações que não as de Identity.
Para assegurar que os dados no cartão são genuínos, um ficheiro SOD é colocado no cartão contendo as hashes criptográficas assinadas sobre os dados identificativos, a morada, a

fotografia e a chave de autenticação pública do cartão (pelo menos um é usado para autenticação CVC).

A função PTEID_GetID() de identificação por nós utilizada, usa este SOD para verificação.
Verificação "SOD" significa que a validade dos dados de identificação, morada, fotografia e chave pública de autenticação do cartão, é verificada de modo a assegurar que não é falsificada. Este processo é efetuado através da leitura do ficheiro SOD que contém hashes sobre os dados mencionados acima e está assinada por um certificado DocumentSigner.
Applet "ValidaCC.java"
Devido à especificidade dos requisitos incluírem uma aplicação a ser executada em PHP num servidor APACHE e o acesso ser feito desde o browser de um qualquer cliente foi necessário recorrer à criação de uma applet.
Esta applet está "instalada" junto com a aplicação PHP e é chamada por esta mas no browser cliente pois é aí que terá de estar ligado o leitor e o respetivo cartão do cidadão.
Não acedemos diretamente da applet ao cartão mas sim ao middleware do cartão de cidadão que por sua vez acede ao hardware do cartão.
Nesta applet implementámos o acesso à API disponibilizada pela instalação do software do Cartão de Cidadão.
Utilizámos a "eID Lib API" de modo a que fosse possível ler o "Nome" do proprietário do cartão de cidadão e o PAN (número único).
Funções na applet:
getFirstName()
Devolve o nome que está guardado no cartão como titular (função de identidade)
getPan()
Devolve o Numero único que está guardado no cartão (função de identidade)
Conforme se pode visualizar no anexo Applety ValidaCC.
Procedimentos necessários à criação da applet:

No Eclipse por exemplo criar um novo projeto como java applet.
Incluir todos os ficheiros extraídos (.class) do pteidlibj.jar
Incluir o source da applet ValidaCC.java
Fazer o run as java applet para que seja criada o ValidaCC.class

Os comandos necessários à geração da applet que vai ler o cartão são:
set JAVA_HOME=c:\jdk1.6.0_21;
set PATH=c:\jdk1.6.0_21\bin;
set CLASSPATH=pteidlibj.jar;

Para compilar a applet:
javac ValidaCC.java
appletviewer -J-Djava.security.policy=polfile ValidaCC.html
Criamos também polfile (ficheiro sem extensão) com o seguinte conteúdo para dar permissões

```
grant {
  permission java.security.AllPermission;
};
```

Criamos o ficheiro JAR com a classe envolvida, pois a assinatura é feita em cima do jar.
Na linha de comando, fomos até a pasta em que o.class e escrevemos: JAR com a seguinte instrução:
jar cvf ValidaCC.jar ValidaCC.class
Neste momento foi criado um jar chamado ValidaCC.jar.

Para criarmos o par de chaves (chave pública e privada)

Na linha de comandos escrevemos:
keytool -genkey -dname “cn=ValidaCC, ou=TFC, o=TFC, c=PT” –alias
ValidaCC -storepass 123456 -validity 3655

Detalhes do comando

-dname = dados da organização/empresa/site
-alias = nome da chave criada, no caso “ValidaCC”
-storepass = pass da chave, para assinar um jar com esta chave será necessário escrever este pass
- validity = quantos de dias de validade tem a assinatura digital
Esta chave fica guardada na pasta home do utilizador.
Assinar o JAR do applet, pois existem várias questões de segurança envolvendo a chamada de arquivos e aplicações externas de dentro do navegador, e para executar alguma função mais específica, ou até mesmo correr o executáveis do sistema operativo a partir do applet, é preciso criar uma assinatura digital.
Até mesmo para identificar que este applet é assinado pela empresa ou site onde está a ser executado.
jarsigner -storepass 123456 ValidaCC.jar validacc
De seguida coloca-mos o ficheiro Jar na aplicação.

Criação de ficheiro em HTML "ValidaCC.html" para podermos testar a applet.

Começamos por desenvolver um ficheiro simples que preencheria dois forms e enviaria para um url definido.

Figura 13: Form inicial da applet

Tentativas de acesso

Com a appplet a funcionar, no exterior seria necessário integra-la na rede social para procedermos à validação dos dados. Foi um processo de muita pesquisa, muita tentativa e erro.

A dificuldade consistia onde colocar a applet , e onde colocar os ficheiros Jar e bibliotecas.

Na tentativa de login, coloca-mos a applet na C:\xampp\htdocs\elgg\views\default\forms\ login.php mas sem sucesso, ficando nós na duvida o que estaria errado…a localização da applet ou bibliotecas.

Criamos uma pagina php onde inicialmente colocámos um ficheiro txt com username e password e colocando um include dessa página em C:\xampp\htdocs\elgg\actions\login.php e funcionava na perfeição. Opta-mos então por colocar a applet nessa página, mas continuávamos a não obter os resultados pretendidos. A applet não era carregada. Muita pesquisa de como era carregada a página de login da elgg, mas sem sucesso. Após muitas tentativas e um contínuo conhecimento da rede social conseguimos encontrar uma página onde a applet funcionou: C:\xampp\htdocs\elgg\views\default\core\account\login_box.php

Alterar paginas login

Com a applet a funcionar na página de login_box.php, seria necessário alterar o form existente e colocar o nosso form em funcionamento. Para isso foi comentado código das forms existentes que não seriam utilizadas, na página C:\xampp\htdocs\elgg\views\default\forms\ login.php como se pode verificar no anexo " Página de login form". Alteramos a página onde correm as forms existentes com as forms da nossa apple tem:

C:\xampp\htdocs\elgg\views\default\core\account\login_box.php, anexo "Página login_box" e aí conseguimos redirecionar para a página pretendida:

C:\xampp\htdocs\elgg\actions\login.php, anexo “Página login action”.

```
$username1 = get_input('username');
$password = get_input("password");
$persistent = get_input("persistent", FALSE);
$result = FALSE;

$username = str_replace(" ","",$username1);
```

Figura14: Solução encontrada para retirar espaços entre nomes

Deparamo-nos ainda com uma situação posterior em existem cartões cidadão com dois nomes e por consequente com espaço entre nomes. Situação esta que não é aceite pelo MYSQL e resolvemos com o retirar do espaço entre palavras. Repetida também na opção de registo.

Alterar pagina registo e criação de nova

Para criar a página de registo surgiram-nos outras situações. Conseguimos identificar o layout da página onde corre, mas contudo esse layout está a ser utilizado para outras páginas. Tivemos que criar um novo, chamando-o depois na página de registo. Esse layout encontra-se em: C:\xampp\htdocs\elgg\views\default\page\layouts\one_column_a.php em anexo com nome”layout one_column_a”.Alterámos tambem a página das forms, ignorando as que não precisaríamos: C:\xampp\htdocs\elgg\views\default\forms\register.php em anexo com nome “Página registo form”.Nesta situação foi difícil o reencaminhamento para a nova página pois era solicitado os elgg_ token bem como elgg_ts da página estava difícil de conseguir, mas resolvemos com a integração do script da applet no php.Para a situação de carregar username com duas palavras resolvemo-la como descrito anteriormente no login.

```
9
10  <?php
11  $__elgg_ts = time();
12  $__elgg_token = generate_action_token($__elgg_ts);
13
14  elgg_make_sticky_form('one_column_a');
15  elgg_make_sticky_form('register');
16
17  // Get variables
18  $username1 = get_input('username');
19  $password = get_input('password');
20  $password2 = get_input('password2');
21  $email = get_input('email');
22  $name = get_input('name');
23  $friend_guid = (int) get_input('friend_guid', 0);
24  $invitecode = get_input('invitecode');
25
26  $username = str_replace(" ","",$username1);
```

Figura 15: Register action onde página form é chamada

Alterar pagina acesso blog/files

Para fazermos a validação de interação, surgiram-nos a situação de identificar o layout onde estava inserido o botão da ação bem como descobrir como estava o botão a ser carregado. Identificamos a página de layout como sendo:
C:\xampp\htdocs\elgg\views\default\page\layouts\content\header.php. Este form carrega o título e botão de forma dinâmica, assim a solução mais fácil, de colocarmos aí um novo botão foi invalidada, pelo motivo de haver vistas em que o botão não faria sentido e estava sempre presente. Optamos por pesquisar de onde estava a ser chamado o botão existente e orientá-lo para uma página que iria-mos criar com a validação. Essa função está em:
C:\xampp\htdocs\elgg\engine\lib\navigation.php.

```
function elgg_register_title_button($handler = null, $name = 'add') {
        if (elgg_is_logged_in()) {

                if (!$handler) {
                        $handler = elgg_get_context();
                        $_SESSION["zim"] =$handler;
                }

                $owner = elgg_get_page_owner_entity();
                if (!$owner) {
                        // no owns the page so this is probably an all site list page
                        $owner = elgg_get_logged_in_user_entity();
                }
                if ($owner && $owner->canWriteToContainer()) {
                        $guid = $owner->getGUID();
                        elgg_register_menu_item('title', array(
                                'name' => $name,
                                'href' => "mod/validate/validate.php",
                                'text' => elgg_echo("$handler:$name"),
                                'link_class' => 'elgg-button elgg-button-action',
                        ));
                }
```

Figura 16: função que carrega botão orientado para página criada.

Criar nova página para validação

Para criar página de validação descobrimos após várias tentativas que apenas se consegue a inserção de uma nova página através da criação de um plugin.. Esse plugin tem de correr na action ou então no mod.Foi o que fizemos, cria-mos um plugin para podermos correr a página de validação. Os forms necessários são diferentes dos anteriormente utilizados para o register e criamos um layout com forms diferentes para correr a applet na validação. Esse Layout demos-lhe o nome em anexo de"layout validação". Nessa nova pagina através do botão existente nesse form carrega os dados do cartão e envia para a página anteriormente solicitada. Para esse fim, foi necessário criar uma função para apanhar o destino anteriormente solicitado, pois trata-se de um menu dinâmico.

```
function elgg_GET_url(){

     $destino =$_SESSION["am"];
    $url = "/elgg/$destino/add/66";

    return "$url";
    }
```

Figura 17: função para apanhar url seguinte.

Após ser direcionado para a página de destino é feita aí a validação ondes se compara os dados colhidos do cartão com os existentes com os dados do utilizador logado.

```
10
11
12  //input from one_column_b
13  $username_cc = get_input('username_cc');
14
15  //compared  whith username session
16  if($_SESSION["username"]!=$username_cc){
17     //trigger_elgg_event('logout'user,$_SESSION['user'])
18
19     register_error(elgg_echo('logout_cc'));
20         logout();
21         forward();
22  }
23  // end validation
24
25
```

Figura 18: Validação dos dados do cartão com utilizador logado.

Se os dados forem coincidentes segue a via solicitada, se não coincidirem é feito o logout e reencaminhamento para página inicial.

5. Resultados

Os resultados obtidos podem ser apresentados em três vertentes: registo, autenticação e validação.

Registo

Ao aceder à rede social, o utilizador, se não estiver registo efetuado pode através de um link existente na página inicial aceder à página de registo.

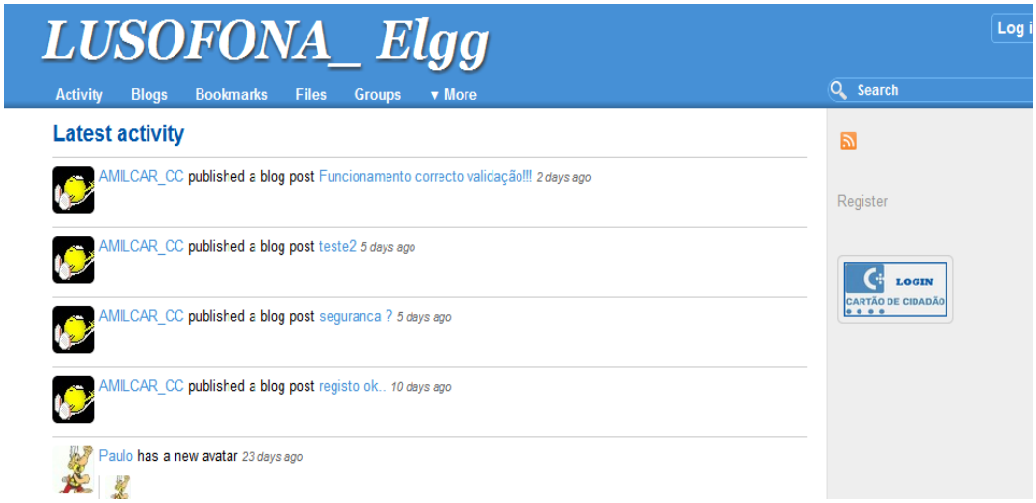

Figura 19: Página inicial da Rede Social

Tendo o cartão cidadão inserido no leitor, é solicitado que introduza apenas o email e nome a utilizar na rede. Os restantes dados de validação serão recolhidos através do cartão do cidadão. Esse dados são o username e password que ficam guardados nas tabelas já existentes para registo.

Figura 20: Página de Registo da elgg

O registo fica efetuado aguardando apenas validação de um membro com poderes de administrador.

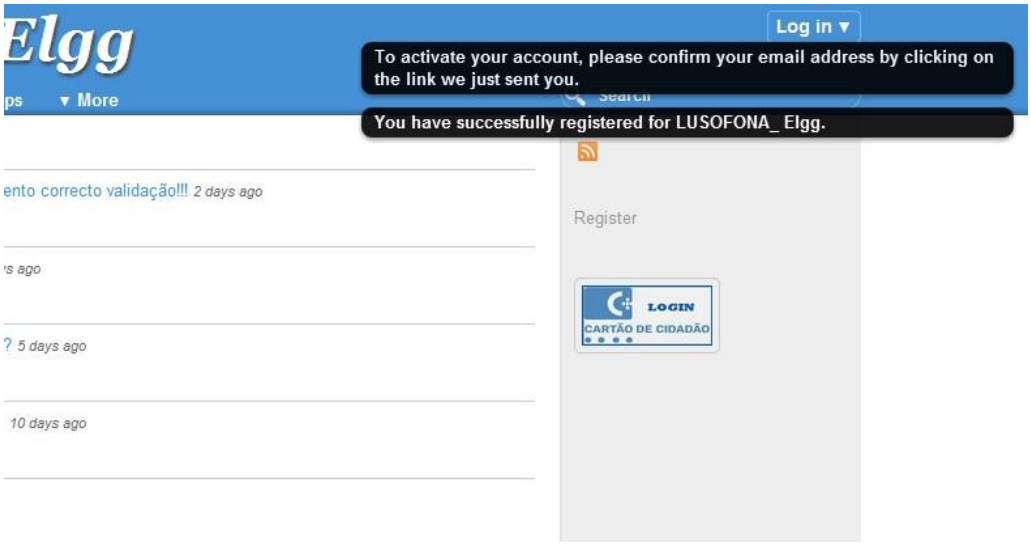

Figura 21: Registo efetuado com sucesso na com cartão.

Autenticação

Ao iniciar acesso á rede social, a autenticação é efetuada através dos dados do cartão do cidadão, bastando apenas clicar no botão referente ao login, se os dados estiverem corretos é confirmado o login.

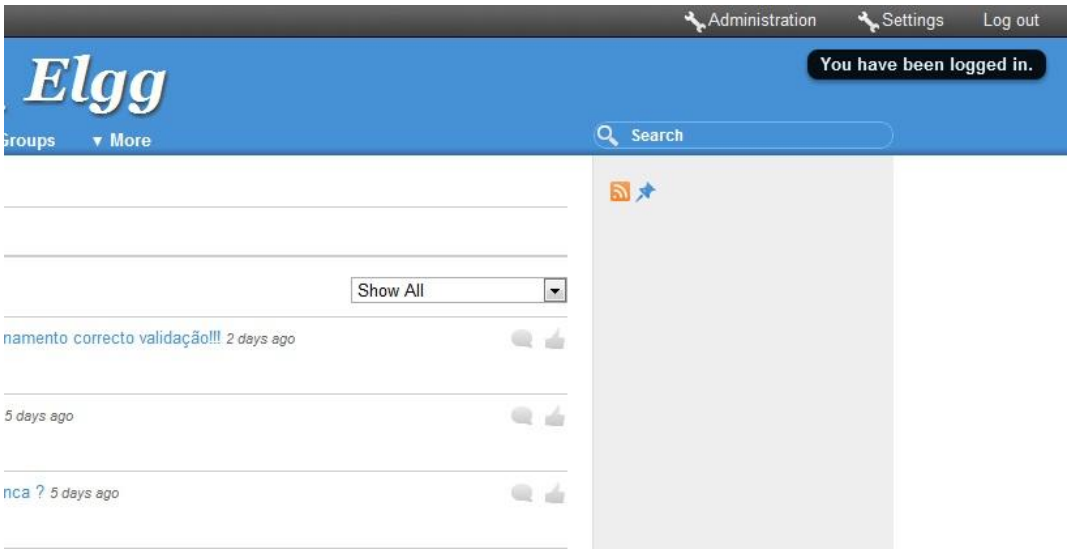

Figura 22: Login efetuado com sucesso com cartão.

Validação.

Estando logado, para aceder a adicionar conteúdos como: comentários, fotografias, grupos, é validado a autenticação através da leitura do username do cartão do cidadão.

Figura 23: Página de validação.

Se o username do cartão inserido não corresponder ao registado ou não se encontrar cartão inserido no leitor é negado o acesso e feito o reencaminhamento para logout indicando a mensagem relativa á ocorrência.

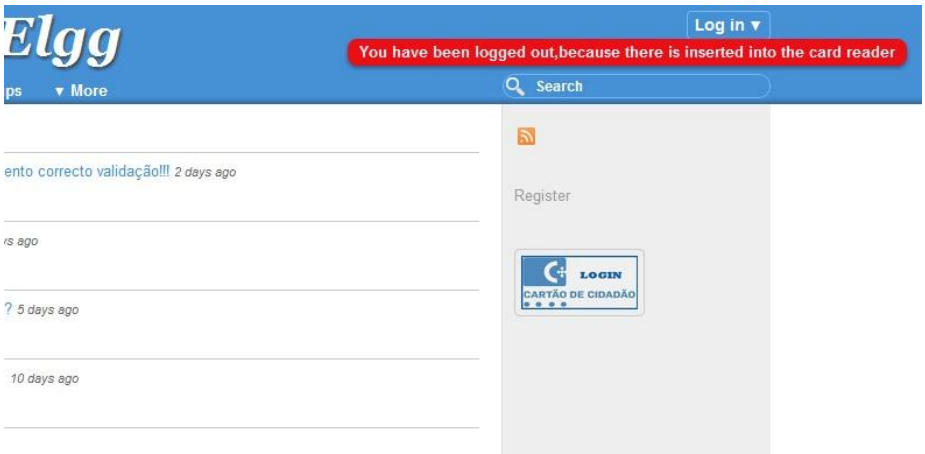

Figura 24: Página de logout após validação

6. Conclusão e Trabalho Futuros

A solução apresentada cumpre os objetivos a que se propôs, que foram o aumento de segurança numa rede social open source.

Essa segurança é aumentada através de:

- O registo feito através do cartão do cidadão
- A autenticação através do cartão do cidadão
- A validação para interagir com a rede feita com cartão cidadão

No entanto as desvantagens que possam surgir, prendem-se com a necessidade de ter cartão de cidadão bem como aquisição do leitor de cartões.

Contudo, o ponto crucial é a incremento de segurança numa rede social. Neste especto ainda se verifica que pode haver um grande trabalho a desenvolver, pois com a massificação da utilização das redes sociais, leva a que seja "esquecida" cada vez mais o aspeto da segurança.

Contudo existem pontos que podem ser melhorados:

- Implementação de Plugin
- Validação através de certificados

7. Bibliografia

- west_side.blogs.sapo.pt/356407.html
- xtechpt.com/index.php?topic=1785.0
- www.ionline.pt/conteudo/46019-uniao-europeia-apela-maior-seguranca-nas-redes-sociais
- blogs.globalcrossing.com/?q=pt-br/content/so-senha-nao-e-suficiente
- hissa.nist.gov/rbac/newpaper/rbac.html
- www.tech-faq.com/role-based-access-control-rbac.html - Estados Unidos

SANTOS, Vinicius Souza dos, BEZERRA, Ed Porto e ALTURAS, Bráulio. Análise de mecanismos de controle de acesso nas redes sociais. Rev. Portuguesa e Brasileira de Gestão. [online]. set. 2010, vol.9, no.3 [citado 01 Junho 2011], p.50-60.

- www.scielo.oces.mctes.pt/scielo.php?script=sci_arttext&pid=S1645-44642010000200006&lng=pt&nrm=iso>. ISSN 1645-4464.
- en.wikipedia.org/wiki/Role-based_access_control
- especificacoes - leitores base_v1.0
- Manual_Cartao_de_Cidadao_v1.24
- pt.wikipedia.org/wiki/Plugin
- textpattern.net/wiki/index.php?title=Using_XAMPP_(Apache-MySQL-PHP-Perl)_for_Windows
- *Criando uma Base de Dados no XAMPP! Palmierinet.com*
- www.senha001.gov.pt/instalacao.php
- http://www.digitalismo.com.pt/pt/pags/gloss
- http://pt.wikipedia.org

8. Anexos

Using XAMPP (Apache-MySQL-PHP-Perl) for Windows
Criar Base de Dados no XAMPP!
Instalando o Elgg
Manual_Cartao_de_Cidadao_v1.24.pdf
Página login _box
Página login action
Página login form
layout one_column_a
layout validação
Applet ValidaCC

9. Glossário

Administrador: Diz-se no contexto informático, da figura do responsável por garantir o bom funcionamento de um sistema, seja ele uma base de dados, uma rede de computadores ou sítio Internet.

ACM: Association for Computing Machinery (lit. Associação para Maquinaria da Computação) ou ACM, foi fundada em 1947 como a primeira sociedade científica e educacional dedicada a computação.

Applet : Um software aplicativo que é executado no contexto de outro programa (como por exemplo um web browser)

Autenticação: (login no Inglês)
Por norma, o utilizador introduz o seu nome de utilizador e a respetiva senha. Após este processo, acredita-se que o utilizador está identificado e portanto é seguro conceder-lhe acesso privilegiado.

Base de Dados: No contexto informático, refere um programa de computador que armazena toda e qualquer informação, e permite um acesso muito rápido. São exemplos o Microsoft Access, o MySQL e o Oracle.

Blog: É um site cuja estrutura permite a atualização rápida a partir de acréscimos dos chamados artigos, ou posts. Estes são, em geral, organizados de forma cronológica inversa, tendo como foco a temática proposta do blog, podendo ser escritos por um número variável de pessoas, de acordo com a política do blog.

Carregar: (upload no Inglês) Diz-se que um utilizador "carrega" ficheiros quando os envia do seu computador para um servidor.

Cliente: Diz-se do computador do utilizador quando acede a uma máquina remota (servidor), por intermédio de uma rede, como a Internet, por exemplo. Em rigor, também se pode considerar "cliente" a um qualquer programa que use os serviços disponibilizados por outro programa ou máquina — isto implica que um único computador pode albergar vários "clientes".

Conta de Utilizador: Um sistema informático gere os assuntos de quem o utiliza através de contas independentes entre si e fazendo corresponder cada uma a um utilizador. Para aceder à sua conta, cada utilizador tem de se autenticar. A forma mais comum é através de uma senha — o utilizador introduz o seu nome e senha e o sistema confere se correspondem.

EEPROM: É um chip de armazenamento não-volátil. Pode ser programada e apagada várias vezes, eletricamente.

Endereço IP: Número que identifica cada computador ligado à Internet, e que tradicionalmente tem o formato "nnn.nnn.nnn.nnn", sendo "nnn" um número entre 0 e 255 (embora alguns sejam reservados para usos específicos). Cada computador tem de ter um endereço IP que é único em toda a Internet.

HTML :(HyperText Markup Language) É um código simples que descreve as páginas Internet.

Internet: É a maior rede de computadores do mundo. Para potenciar toda essa conectividade, são oferecidos numerosos serviços, dos quais os mais conhecidos são: HTTP, correio eletrónico, FTP e Instant Messaging.

ISO: Organização Internacional de Normalização.

Login: Veja autenticação.

Motor de busca: Sítio Internet cuja função é encontrar outros sítios e páginas.

Navegador: (browser no Inglês) Programa de computador que permite "navegar" na Internet.

Open Source: O termo código aberto, ou open source em inglês, foi criado pela OSI (Open Source Initiative) e refere-se a software também conhecido por software livre.

Página Internet: Parte de um sítio na Internet, geralmente dedicado a um assunto específico. Um sítio é por norma constituído por várias páginas, mas por vezes usa-se "página Internet" como sinónimo de "sítio Internet".

Plugin: Programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica.

Post: Menor unidade de um Blog, também conhecido como artigo.

Rede de Computadores: Sistema constituído por vários computadores que comunicam entre si e que geralmente partilham recursos.

Rss Feeds: Oferecem conteúdo Web ou resumos de conteúdo juntamente com os links para as versões completas deste conteúdo e outros metadados.

Servidor: Máquina que "serve" outras. A sua função é desempenhar as tarefas que os clientes lhe solicitam. Por exemplo, quando se acede à Internet, o navegador solicita ao servidor que lhe forneça o conteúdo de uma página num determinado endereço ou seja, o nosso computador é o "cliente" nessa operação.

Sítio Internet: (site no Inglês) Conjunto de textos, imagens, sons e outros, alojado num servidor ligado à Internet. Cada sítio é referido pelo seu nome, ou mais concretamente, pelo seu domínio, que ao mesmo tempo o identifica e localiza.

Twitter : É uma rede social que permite aos utilizadores enviar e receber atualizações pessoais de outros contatos (em textos de até 140 caracteres, conhecidos como "tweets"), por meio do website do serviço, por SMS e por software específico.

URL : Endereço de uma página Internet. Basicamente, um URL refere um domínio e depois a localização da página dentro dele. O domínio permite encontrar o servidor que aloja o sítio, e a localização indica a página.

XAMPP: É um servidor independente da plataforma, software livre, que consiste principalmente na base de dados MySQL, o servidor web Apache e os interpretadores para linguagens de script PHP e Perl.