Mestrado de Eng.ª Informática e Sistemas de Informação

Cadeira de Gestão de Identidade e Aplicações Federativas

Enunciados de Avaliação

1. Avaliação

Este enunciado apresenta os temas de avaliação da Cadeira de **Sistemas de Gestão de Identidade** do 2º Semestre do Mestrado de Engenharia Informática e Sistemas de Informação.

A avaliação é composta por três componentes, a realizar individualmente pelos alunos:

1. A apresentação de um tema escolhido de entre os temas abordados na cadeira e acordada com o professor, que deverá ser apresentado no decorrer de uma aula (ver lista de temas propostos no ponto 6).

2. Dois trabalhos de implementação prática realizando provas de conceito de tecnologias de Gestão de Identidade abordadas na cadeira.

São apresentados de seguida vários temas dos quais dois (à escolha) deverão ser realizados pelos alunos. Os trabalhos deverão ser acompanhados de um relatório de execução devidamente identificado, devendo na sua discussão o aluno responder a questões sobre a realização do mesmo.

2. Implementação de um Algoritmo de Autenticação

Pretende-se com este trabalho implementar uma versão simplificada do ***Challenge Handshake Authentication Protocol***, protocolo de autenticação baseado em chave secreta, que permite a um programa cliente autenticar um utilizador junto de um programa servidor, sem nunca enviar a password pela rede.

O protocolo deverá constar pelo menos dos seguintes passos:

1. A aplicação servidor conhece um conjunto de credenciais de utilizadores (*usernames* e *passwords*) que deverão ser armazenados num ficheiro, sendo as passwords obrigatoriamente guardadas sob forma de *digest* (p.ex. MD5).
2. A aplicação cliente começa por pedir ao utilizador o seu *username*.
3. O cliente abre uma conexão para o servidor (utilizando p.ex. a socket API), envia o nome do utilizador em claro e fica à espera de receber uma resposta.
4. O servidor verifica que conhece o nome do utilizador e o *digest* da respectiva *password* armazenado.

5. Se for o caso, envia de volta uma mensagem de *challenge* ao cliente contendo um *nonce* N de 64 bits (8 bytes), obtido p.ex. pela concatenação do valor do tempo sistema (32 bits - 4 bytes) com um número inteiro aleatório (32 bits - 4 bytes), e fica à espera da resposta do cliente.
6. O cliente pede ao utilizador a sua password P e calcula o seu *digest* (p.ex.MD5), obtendo assim Dp = MD5(P), com 128 bits (16 bytes).
7. O Cliente efectua a concatenação do *nonce* N com o *digest* Dp da password, obtendo N || Dp e calcula a resposta R = MD5 (N || Dp) que envia de volta ao servidor (16 bytes).
8. O servidor realiza a mesma concatenação que o cliente a partir do valor do *digest* Dp da *password* do utilizador que tem armazenada e do *nonce* N que enviou, obtendo R' = MD5 (N || Dp).
9. Se R == R', então o cliente está de posse da password certa e está a responder directamente ao servidor, pois o nonce é válido, provando portanto a sua identidade: o servidor envia uma mensagem de sucesso ao cliente
10. Se R != R´ não há prova de autenticação e o servidor envia uma mensagem de erro ao cliente.

A implementação pode ser realizada em Unix, Windows ou ambiente Web.

Referências para implementação:

Protocolo CHAP (Challenge Handshake Authentication Protocol)
www.ietf.org/rfc/rfc1994.txt e netlab.ulusofona.pt/im/teoricas/IM-02-IdMgmt.pdf

Exemplo de geração de um *nonce*:
http://netlab.ulusofona.pt/cr/praticas/nonce.c

Exemplo de cálculo do digest MD5 de uma string
http://netlab.ulusofona.pt/cr/praticas/md5.c

3. Operacionalização de um Identity Provider

Pretende-se com este trabalho aplicar as técnicas de Gestão de Identidade apresentadas nas aulas teóricas através da implementação de um exemplo prático.

Assim, o trabalho deverá consistir na escolha de uma plataforma existente, no seu estudo e na construção de um use case capaz de demonstrar as suas características principais.

3.1 Indicações para a realização do trabalho

O trabalho deverá constar das fases seguintes:

1. Escolha de uma tecnologia específica e estudo das suas características

2. Determinação dos componentes necessários à sua operacionalização
3. Criação de um repositório de identidade na tecnologia mais adequada à plataforma e seu aprovisionamento (ou cadastro) com um conjunto de perfis de demonstração
4. Instalação do ambiente numa máquina do laboratório ou num outro ambiente à escolha que possa ser utilizado para a demonstração
5. Validação da funcionalidade implementada através da utilização dos seus serviços para autenticar acessos a um site protegido por um Service Provider utilizando a mesma tecnologia
6. Avaliação das possíveis falhas de segurança

4. Operacionalização de um Service Provider

Pretende-se com este trabalho aplicar as técnicas de Gestão de Identidade apresentadas nas aulas teóricas através da implementação de um exemplo prático.

Assim, o trabalho deverá consistir na escolha de uma plataforma existente, no seu estudo e na construção de um use case capaz de demonstrar as suas características principais.

4.1 Indicações para a realização do trabalho

O trabalho deverá constar das fases seguintes:

1. Escolha de uma tecnologia específica e estudo das suas características
2. Determinação dos componentes necessários à sua operacionalização
3. Criação de um conjunto de recursos protegidos pelo Service Provider, para o acesso dos quais sejam necessários acessos autorizados
4. Instalação do ambiente numa máquina do laboratório ou num outro ambiente à escolha que possa ser utilizado para a demonstração
5. Validação da funcionalidade implementada através da realização de acessos autenticados por um Identity Provider utilizando a mesma tecnologia
6. Avaliação das possíveis falhas de segurança.

Nota: Dada a complementaridade dos trabalhos 3 e 4, seria aconselhável serem realizados em colaboração por dois alunos.

5. Prazo de Entrega

A entrega dos trabalhos deverá ser realizada até **30 de Junho de 2015**, devendo a defesa do trabalho decorrer até **15 de Julho**. A demonstração das funcionalidades implementadas deverá ser realizada nas instalações da Universidade Lusófona.

6. Lista de Temas de Apresentação

1. OpenID (versão 1): http://netlab.ulusofona.pt/im/Book.pdf
2. OAuth (versão 1): http://oauth.net
3. OPenID Connect (OpenID 2 ou OAuth2) : http://openid.net; https://developers.google.com/accounts/docs/OAuth2Login
4. SAML e Google Apps: https://developers.google.com/google-apps/sso/saml_reference_implementation
5. Shibboleth: http://www.internet2.edu/products-services/trust-identity-middleware/shibboleth
6. Comparação de SAML e OPenID: http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html

Podem ser sugeridos outros temas desde que estejam inseridos no programa da cadeira e sejam aprovados pelo docente da cadeira.