UNIVERSIDADE DOS AÇORES
DEPARTAMENTO DE MATEMÁTICA

Informática – Redes e Multimédia
Disciplina: Segurança e Gestão de Redes

Trabalho Individual 2

Objectivos:

Este trabalho de projecto individual tem por objectivo a aplicação e praticabilidade dos conteúdos ministrados nas aulas teóricas e práticas da cadeira de Segurança e Gestão de Redes.

É pretendido que os alunos apliquem os conhecimentos científicos adquiridos e possam construir pequenos shell scripts, em bash.

Proposta de Trabalho:

No âmbito de segurança – Infra-estrutura de Chave Pública (PKI) e correio electrónico seguro -, por enumeras vezes necessitamos de comunicar de forma segura, garantido confidencialidade, autenticidade e integridade.

Neste sentido, pretende-se que o aluno construa uma pequena aplicação em shell script que permita ao utilizador enviar/receber mail seguro, recorrendo a chaves públicas contidas em certificados digitais e realizando operações de segurança sobre documentos a enviar ou verificar a autenticidade e integridade de documentos recebidos de terceiros.

Descrição do Trabalho:

Pretende-se que o aluno concretize uma aplicação de shell script (em bash), de nome **secmailSGR** de funcionalidades descritas de seguida.

O aluno terá de utilizar os comandos necessários do openssl para realizar as funcionalidades pretendidas, onde os mesmos serão embebidos em shell script. Para um melhor grafismo da aplicação a realizar, o aluno poderá utilizar o comando dialog e/ou Xdialog, onde beneficiará de uma majoração.

secmailSGR

FUNÇÂO

Executa a aplicação de envio/recepção de mail e implementação de segurança de documentos.

PREAMBULO

A aplicação **secmailSGR** para funcionar correctamente é necessário uma estrutura de pastas que armazene: o par de chaves pública-privada do utilizador da aplicação (o qual pode estar em um ou dois ficheiros); os certificados do utilizador da aplicação (um para garantir autenticidade e integridade e outro somente para cifra); o repositório de certificados digitais; os mails enviados; e os mais recebidos.

Os certificados contidos no repositório pertencem a duas CA's raizes (PKI's baseadas em RSA), cada qual com três certificados e onde o utilizador da aplicação pertence a uma das CA's.

Toda a estrutura (pastas, chaves e certificados) necessária terá de ser criada pelo aluno, para o bom funcionamento da aplicação.

Na pasta dos mais recebidos, terá de ser simulado a recepção de mail, colocando na referida pasta mail previamente enviado.

SINTAXE

./secmailSGR

DESCRIÇÃO

A aplicação **secmailSGR** ao ser executada apresentará o seguinte **Menu Principal**:

- Nova Mensagem de SMIME
- Abrir Mail Assinado / Abrir Envelope de Dados
- Abrir Envelope de Dados Assinado

Após a execução de qualquer opção do Menu Principal a aplicação terá de retornar ao mesmo.

Seguidamente é apresentado a(s) funcionalidade(s) a implementar por cada opção:

- Nova Mensagem SMIME

Ao seleccionar esta opção, o utilizador terá de seleccionar que tipo de mensagem quer criar (Enveloped Data, Signed Data, Clear-Signed Data ou Signed Enveloped Data). Também terá de especificar/introduzir o(s) certificados e a(s) chaves necessárias à realização da operação. A mensagem criada será armazenada na pasta de mails enviados.

No caso de o utilizador optar pelas opções Signed Data ou Clear-Signed Data, o mesmo terá de especificar se a mensagem será assinada por um ou mais remetentes, ou, ainda, se a mensagem será re-assinada por algum destinatário. Após selecção da forma de assinar, especificar/introduzir o(s) certificados e a(s) chaves necessárias à realização da operação.

No caso de o utilizador optar pela opção Signed Enveloped Data, o envelope será assinado por Signed Data.

- Abrir Mail Assinado/ Abrir Envelope de Dados

Ao seleccionar esta opção o utilizador terá de escolher a acção pretendida e fornecer os dados necessários à acção. No caso da verificação da assinatura, o utilizador tem de ter em conta o tipo de assinatura e o número de remetentes que assinaram ou re-assinaram a mensagem.

Falta isto

- Abrir Envelope de Dados Assinado

Esta opção servirá para abrir um envelope digital assinado, contido pasta dos mails recebidos. Para tal o utilizador terá de fornecer os dados necessários para realizar a acção.

Bónus:

O aluno pode optar por realizar todo ou parte do *frontend* da aplicação com recurso a janelas de shell script, utilizando o comando dialog e/ou Xdialog. A implementação deste bónus terá um valor máximo de 3 valores, o qual dependerá da sua implementação e funcionalidade.

– Instalação do dialog e Xdialog (em root):

fedora: yum install dialog Xdialog

ubuntu: apt-get install dialog Xdialog

- Referências Bibliográficas:

http://linuxgazette.net/101/sunil.html

http://www.linuxjournal.com/article/2807?page=0,0

http://www.linuxjournal.com/article/2460

http://linux.die.net/man/1/dialog

Entrega e Avaliação:

- A data limite de entrega do trabalho é dia 19 de Dezembro de 2011, às 23:55 H.
- O aluno, até à data limite de entrega do trabalho, terá de entregar, na plataforma Moodle, na actividade "Envio do Trabalho Individual Nº 2", um ficheiro de formato zip ou rar, contendo o(s) ficheiro(s) de shell script e um ficheiro de texto com a sua auto-avaliação.
- Serão aceites trabalhos fora do prazo, via mail, num máximo de 48 horas, mas o aluno terá uma penalização de 2 valores por cada 24 horas passadas a data e hora estipuladas.
- O plágio implica exclusão do trabalho.
- Alguns dos parâmetros de avaliação são: funcionalidade, estrutura, desempenho, algoritmia, comentários, clareza do código.