DEPARTAMENTO DE MATEMÁTICA

Licenciatura: Informática - Redes e Multimédia

Segurança e Gestão em Redes
Ano Lectivo 2012/2013

Projecto D – *Java Security*

Objectivos:

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

É pretendido que os alunos apliquem os conhecimentos científicos adquiridos na referida cadeira, de forma a conseguirem um objecto final funcional, com implementação de segurança, e qualidade.

Proposta de Trabalho:

Em linguagem de programação por objectos Java, construir uma aplicação em Swat/Swing que implemente o cenário criptográfico abaixo apresentado, de comunicação segura, entre pessoas, para que as mesmas possam trocar mensagens seguras por chat e enviar ficheiros garantidos por propriedades de segurança. Para tal, existirá uma aplicação servidora e uma aplicação cliente.

Pretende-se que uma dada pessoa, através da aplicação cliente, possa:

- requerer à aplicação servidora o seu par de chaves RSA/DSA, com um determinado número de bits;
- requerer o certificado digital da sua chave pública, assinado pela Autoridade de Certificação gerida pela aplicação servidora;
- aceder à "pool" das chaves públicas RSA/DSA e respectivos certificados, para poder transferir as chaves públicas e certificados das pessoas que pretende comunicar. A "pool" será uma pasta criada na máquina da aplicação servidora e será acedida pela aplicação servidora e cliente;
- construir um canal de comunicação seguro, através de autenticação mútua Two-way, por certificados digitais. Após o canal de comunicação ser estabelecido, os intervenientes partilham uma chave simétrica, gerada pelo algoritmo *Diffie Hellman*, e escolhem um algoritmo de cifra simétrica para poderem cifrar toda a comunicação entre os intervenientes;
- trocar mensagens no chat (embutido na aplicação cliente) pelo canal seguro.

– poder efectuar sínteses seguras, por HMAC, de um documento e enviá-lo ao destinatário. O destinatário, por seu turno, poder confirmar o *checksum*. A chave simétrica para o HMAC será gerada por *Diffie-Helman*.

A aplicação servidora tem como funções:

– gerar o par de chaves RSA/DSA requeridas por determinada pessoa, através da aplicação cliente. Envia o par de chaves à pessoa e pública na "pool" a chave pública. A "pool" é uma pasta criada na máquina da aplicação servidora;
– emitir certificado digital para certificar a chave pública de determinada pessoa. Envia o certificado digital à pessoa e pública-o na "pool".

Java Security:

Links da API do Java que contêm os packages de java security
http://docs.oracle.com/javase/7/docs/api/index.html
e o guia de referência JCA (Java Cryptography Architecture), que contem pequenos exemplos ilustrativos de programação sobre a temática.
http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html

Entrega e Regras:

- No *site* da cadeira, na plataforma *Moodle*, encontra-se as regras de constituição e inscrição do grupo de trabalho e escolha do projecto, bem como as datas de entrega e discussão do mesmo.
- O grupo de trabalho, até à data limite de entrega do trabalho, terá de entregar, em formato digital (pdf), na plataforma *Moodle,* o relatório do trabalho de projecto, contendo:
    - toda a fundamentação teórica pertinente e de sustentação do trabalho, que justifiquem as tomadas de decisão efectuadas pelo grupo de trabalho;
    - os ficheiros de construção da aplicação, com os comentários necessários para o bom entendimento da aplicação, ou programação por contratos.
    - exemplos ilustrativos, com recurso a *screenshots,* que demonstrem o funcionamento do "objecto" final;
    - outra informação que considerem relevante e necessária para o projecto.
- Entrega dos ficheiros da aplicação, via plataforma Moodle.
- A data e hora da discussão do trabalho será agendada pela docente e disponibilizadas no site da cadeira.
- No dia da discussão do trabalho, o grupo de trabalho entregará à docente o relatório do trabalho do projecto, em formato de papel.
- O plágio implica exclusão do trabalho.