Criptografia Aplicada 2005/2006
Enunciado do Trabalho Prático

Manuel Bernardo Barbosa – mbb@di.uminho.pt
Alcino Cunha – alcino@di.uminho.pt

October 23, 2005

1 Introdução

As aulas práticas de Criptografia Aplicada serão preenchidas com a elaboração de pequenos projectos de programação, por grupos de dois alunos.

O objectivo final das aulas práticas é a integração dos componentes desenvolvidos ao longo do semestre numa aplicação demonstrativa das tecnologias abordadas no âmbito da disciplina.

Os projectos serão implementados na linguagem JAVA, utilizando as seguintes APIs especializadas em funcionalidades de segurança:

- Java Cryptography Architecture (JCA) – API básica para integração de funcionalidade de segurança em aplicações JAVA.
- Java Cryptography Extension (JCE) – extensão à JCA que inclui técnicas criptográficas mais poderosas.
- APIs utilitárias para manipulação de estruturas de dados ASN.1.

A JCA é um componente básico da infra-estrutura JAVA distribuída pela SUN (JDK). Esta infra-estrutura inclui também a implementação da JCE da própria SUN. Conjuntamente, estas duas APIs fornecem implementações dos algoritmos criptográficos mais comuns. No entanto, recomenda-se a utilização da implementação JCE da IAIK que, para além de mais completa, está integrada de forma elegante com a API para manipulação de estruturas de dados ASN.1, do mesmo fabricante. A instalação básica do JDK apresenta uma limitação das políticas de utilização de algoritmos criptográficos que tem de ser desbloqueada substituindo os ficheiros correspondentes por versões mais liberais. Estes ficheiros podem ser descarregados do site da SUN.

2 Instalação das APIs

A instalação deve ser feita do seguinte modo:

1. Instalar o Java SDK.
2. Alterar a politica de segurança, expandindo o ficheiro `jce_policy` fornecido pela SUN na directoria `$JAVA_PATH/jre/lib/security`.
3. Instalar a biblioteca IAIK, que pode ser obtida em `http://jce.iaik.tugraz.at/`.
4. Copiar o ficheiro `iaik_full.jar` para a directoria `$JAVA_PATH/jre/lib/ext`.
5. Instalar o provider IAIK inserindo no ficheiro `$JAVA_PATH/jre/lib/security/java.security`. a seguinte linha

```
. . .
security.provider.7=iaik.security.provider.IAIK
. . .
```

3 Objectivos do Trabalho Prático

Os componentes de software desenvolvidos durante as aulas serão utilizados para implementar um sistema Peer-To-Peer para comunidades fechadas, em que as seguintes funcionalidades serão protegidas com técnicas criptográficas adequadas:

- Registo de máquinas para partilha de ficheiros e respectivos administradores num servidor central que concentra a informação relativa aos ficheiros partilhados.
- Identificação de administradores para acesso à funcionalidade de pesquisa no servidor central.
- Ligações entre máquinas de partilha de ficheiros e o servidor central para actualização dos índices relativos aos ficheiros a serem descarregados / partilhados.
- Ligações Peer-To-Peer, incluindo confidencialidade e autenticação da informação.
- A partilha de ficheiros poderá ser restrita a grupos, e deverá ser possível detectar e identificar os responsáveis pela introdução de alterações em ficheiros partilhados.
- Outras ...

Durante as aulas teórico-práticas será discutida uma arquitectura para este sistema. Esta arquitectura estará inicialmente reduzida uma infra-estrutura básica de comunicação, e evoluirá através da incorporação gradual de técnicas e protocolos criptográficos apresentados nas aulas teóricas.

Algumas das técnicas que deverão ser utilizadas na elaboração dos trabalhos práticos são as seguintes:

- Servidor HTTPS com configuração avançada do modo SSL, incluindo especificação de algoritmos e configuração de certificados X.509 de servidor e de cliente.
- Cifras simétricas e MACs.
- Cifras assimétricas e assinaturas digitais.
- Protocolos de acordo de chaves.
- Pedidos de certificado PKCS#11 e armazenamento de credenciais PKCS#12.

A identificação dos requisitos de segurança inerentes a cada tipo de interacção, e a sua correcta implementação, serão também discutidas nas aulas da disciplina, e serão o factor central na avaliação dos trabalhos práticos.

4 Avaliação

A avaliação do trabalho prático basear-se-á num relatório do trabalho efectuado, a entregar no final do semestre. Na altura da entrega do relatório terá lugar uma apresentação/demonstração da aplicação desenvolvida, sujeita também a avaliação.