Laboratórios de Comunicações 6
MECom (3° ano)

Projecto

Ano Lectivo 2006/07

1 Objectivos

Com este projecto integrado pretende sedimentar-se os conhecimentos relativos a:

- Criptografia
- Redes de Computadores 2
- Bases de Dados B

2 Organização e Funcionamento

O projecto será desenvolvido em grupos de 2 alunos dentro e fora das aulas da disciplina (2 sessões semanais de 2 horas cada).

Nos pontos de controlo a definir e no fim do semestre, cada grupo apresentará à equipa docente e à turma o trabalho realizado e os resultados obtidos, devendo entregar um relatório técnico de desenvolvimento devidamente estruturado e fundamentado.

Em cada aula estarão presentes dois docentes que irão esclarecendo questões específicas dentro da sua área de trabalho.

2.1 Avaliação

A nota final será calculada aproximadamente de acordo com a seguinte expressão:

$$\texttt{Nota Final} = 0.3 \cdot \mathbf{Q} + 0.20 \cdot \mathbf{RI} + 0.30 \cdot \mathbf{RF} + 0.20 \cdot \mathbf{AF}$$

Em que a descrição de cada parâmetro é a seguinte:

- **Q** – Testes de avaliação contínua efectuados em algumas aulas laboratoriais.
- **RI** – Relatório intermédio - Pequeno relatório que apresentará já a estrutura do relatório final a apresentar a meio do semestre.
- **RF** – Relatório final - Este relatório reflectirá todo o trabalho desenvolvido durante o semestre nesta disciplina.
- **AF** – Apresentação final do Projecto.

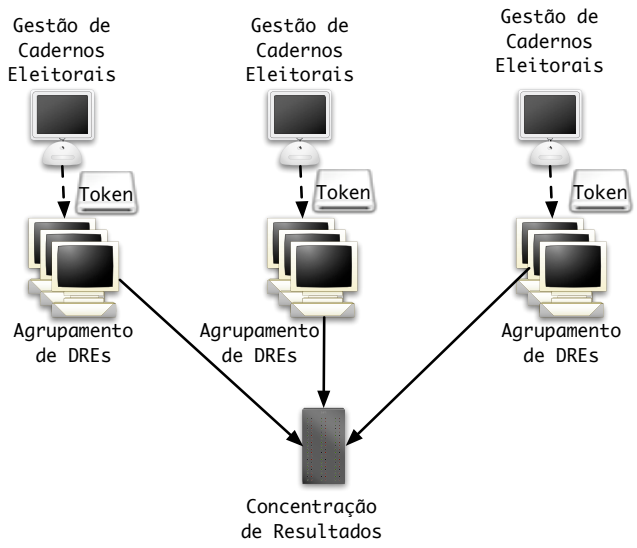

Figure 1: Arquitectura global do sistema de votação.

3 Enunciado

O projecto proposto insere-se na área da votação electrónica. Pretende-se desenvolver um sistema de recolha e contagem automática de votos baseado no paradigma das *Direct-recording electronic (DRE) voting machines*.

Uma DRE é uma máquina de recolha de votos que durante um processo de votação desempenha as seguintes tarefas:

- Verifica que o eleitor foi autorizado a votar.
- Visualiza o boletim de voto e recolhe a intenção de voto do eleitor.
- Armazena a intenção de voto de forma segura.

No final do processo de votação, os votos são recolhidos de todas as DREs para que possam ser contados, utilizando meios de armazenamento físico, ou uma ligação remota a um servidor central.

A autorização para aceder a uma DRE e depositar um voto é geralmente controlada por uma autoridade (geralmente um conjunto de pessoas que representam a comunidade) presente no local. Essa autorização deve ser conferida apenas a um votante legítimo, e deve ser válida para apenas um voto.

Geralmente as DREs permanecem completamente isoladas durante o processo de votação por motivos de segurança. O facto de armazenarem informação crítica durante este período faz com que geralmente estejam dotadas de mecanismos de tolerância a faltas e blindagem que as tornam equipamentos caros.

Neste projecto pretende-se explorar a potencialidade de interligar um subconjunto de DREs durante o processo de votação para obter os mesmos resultados em termos de segurança e fiabilidade, mas reduzindo as restrições inerentes a cada uma delas.

3.1 Arquitectura do Sistema

O sistema de votação a desenvolver será constituído pelos seguintes componentes:

- Software para uma DRE que poderá ser instanciado em diversas máquinas.
- Um sistema central de gestão de listas de eleitores e controlo da votação utilizando um conjunto de DREs

- Um sistema central de contagem dos votos que poderá receber informação de um número arbitrário de DREs.

Vejamos cada um destes componentes mais em detalhe:

- **Listas de eleitores e controlo de votação** Este componente deverá permitir armazenar os cadernos eleitorais, e gerir todo o processo de acesso às DREs:
  - Abrir e encerrar a votação.
  - Identificar eleitores.
  - Emitir uma autorização de voto que permita a um eleitor votar uma vez numa DRE.
  - Assinalar aqueles eleitores que já votaram.
  - Produzir um relatório final com as estatísticas da votação.
- **DRE** A funcionalidade pretendida para a DRE será a seguinte:
  - Estabelecer uma associação com outras DREs para estabelecer redundância no armazenamento e eliminar a possibilidade de associação eleitor/voto depositado.
  - Recolher correctamente um voto de um eleitor autorizado pela mesa.
  - Armazenar localmente esse voto de forma a que não seja possível recuperar a ordem de inserção.
  - Propagar o armazenamento de votos a outras DREs associadas e aceitar o mesmo tipo de solicitação das DREs vizinhas.
  - Enviar os votos armazenados para o sistema de contagem.
- **Contagem** Este componente deverá ser um serviço acessível via rede, que permitirá a uma DRE submeter todos os votos que recolheu. O sistema deverá ser capaz de:
  - Reconhecer DREs associadas dentro de um determinado grupo.
  - Validar a consistência entre os votos submetidos por cada uma delas e eliminar a redundância.
  - Fazer uma contagem final.
  - Gerar resultados parciais e totais.

3.2 Componente de Redes de Computadores

Para a elaboração deste projecto será necessário implementar e configurar toda a infra-estrutura de comunicação em rede, bem como desenvolver um conjunto de protocolos de comunicação que permitam a coordenação e a transferência de informação entre todos os componentes do sistema.

3.3 Componente de Criptografia

Será necessário identificar os requisitos de segurança inerentes a cada funcionalidade presente no sistema, bem como desenvolver e implementar mecanismos que permitam satisfazer esses mesmos requisitos. Aspectos importantes a considerar são:

- Identificação dos votantes e autorizações de voto. Uma forma de resolver este problema será através da utilização de *tokens* portáteis, como *smartcards* ou canetas USB.
- Comunicação segura entre DREs dentro de um determinado grupo e armazenamento seguro da informação.
- Comunicação segura entre uma DRE e o sistema central de contagem de votos.
- Possibilidade de auditoria ao sistema.

3.4 Componente de Bases de Dados

Todos os componentes do sistema deverão utilizar internamente uma base de dados para armazenar a informação necessária ao seu funcionamento. Essas bases de dados deverão ser desenhadas e implementadas no SGBD postgres ou mysql. Haverá lugar também à implementação de uma componente importante de sincronização entre bases de dados em diferentes DREs dentro de um determinado agrupamento.

4 Bibliografia

Toda a bibliografia apresentada nas Disciplinas mencionadas na Secção 1 deste documento.