deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

universidade
de aveiro

Secure Messaging Repository System

Relatório

Pedro Silva - 72645 - pedro.mfsilva@ua.pt;
Francisco Teixeira - 67438 - franciscoteixeira@ua.pt
Turma P2

Introdução

O objectivo deste projecto é a criação de um sistema/repositório de troca de mensagens entre clientes de forma segura. Os clientes estarão assim todos ligados a um servidor e através deste os clientes serão conectados a outros clientes ligados a este servidor para efetuar a troca de mensagens.
Nesta primeira fase deste trabalho foram tratados os aspectos ligados à comunicação entre os clientes e o servidor, tendo em conta questões de integridade e o uso de cifras(confidencialidade).
O trabalho foi implementado tendo como base o código JAVA fornecido.

Escolhas de implementação

- **Confidencialidade.**
- **Integridade.**
- **Troca de segredos.**
- **Futuros problemas.**

Confidencialidade

Em termos de confidencialidade, a forma que escolhemos para estabelecer a confidencialidade das mensagens trocadas entre os clientes e o servidor foi usando cifras assimétricas RSA para estabelecer a comunicação inicial até ao estabelecimento da chave simétrica de sessão DES, e a partir daí usamos esta chave para efeitos de troca de mensagens e assim impedimos que a chave secreta da sessão utilizada seja vista quando é trocada entre cliente e o servidor.

Integridade

Em termos de manter o controlo de integridade nas mensagens utilizamos o autenticador de mensagens HMAC usando SHA1 e assim quando são recebidas mensagens do tipo “secure” pelo servidor, é então feita uma verificação do MAC da mensagem para saber se o conteúdo da mensagem foi adulterado durante a transmissão desta.

Troca de segredos

Em termos de troca de segredos entre os clientes e o servidor, isto foi feito usando o método de “forward-backward secrecy” que é assegurado através do uso da chave assimétrica RSA para a troca de chave secreta da sessão DES durante o estabelecimento da ligação cliente-servidor e a ligação cliente-cliente. Caso esta mensagem que contém a chave da sessão(tipo “connect”/”client-connect”) tenha sido comprometida, esta estará cifrada com RSA e por isso o conteúdo da mensagem não será exposto.

Futuros problemas

Com esta implementação não temos maneira de impedir ataques como o “Man-in-the-Middle”, pois não temos maneira de saber se estamos de facto a trocar mensagens com o servidor ou com outra entidade personificada. Para resolvermos isto é preciso implementar autenticação dos utilizadores via login e através de challenges e também temos de renovar a chave simétrica de sessão após X mensagens trocadas ou ao fim de X tempo de forma a garantir a alteração da chave da sessão.