Segurança de Redes e Sistemas de Computadores
2016/2017, 2º Semestre

Trabalho Prático nº 1 (vA-1.0)

Resumo

Neste trabalho pretende-se iterar o sistema de CHAT/MESSAGING com comunicação multicast segura, a partir dos objetivos antes realizados no Trabalho Prático Nº 1, de modo a endereçar três novos objetivos que podem ser desenvolvidos em partes distintas. O primeiro objetivo visa fazer evoluir o protocolo de autenticação e controlo de acesso às conversas MCHAT (protocolo antes associado aos requisitos da FASE 2 do trabalho prático nº 1) de modo a ser agira suportado num canal de comunicação seguro baseado em TLS, com suporte para configuração flexível de ciphersuites e modos de autenticação, o que permitirá usar o protocolo TLS em suas diferentes opções de configuração. O segundo objetivo visa dotar o sistema de um processo de estabelecimento de chaves de sessão (para as sessões multicast) com base num acordo DH autenticado e com propriedades de segurança passada e futura perfeitas, com refrescamento de chaves cada vez que um utilizador entra ou sai da sessão de CHAT.

1. Introdução

Pretende-se iterar o sistema de CHAT/MESSAGING seguro (anteriormente desenvolvido no trabalho prático nº1) sendo esta iteração baseada na realização dos seguintes dois objetivos (sendo o primeiro de implementação obrigatória e o segundo de implementação opcional) e que podem ser realizados em três partes distintas do desenvolvimento.

- Protocolo de autenticação e controlo de acessos (na funcionalidade associada à FASE 2 do TP1) com base num canal TLS com suporte de configuração da versão do protocolo utilizado, modos de autenticação, e parametrização de *ciphersuites* estabelecidas no canal TLS;
- Estabelecimento de chaves de sessão (para a comunicação *multicast*) com base na implementação de um acordo com o método Diffie-Hellman, estendido ao grupo e implementação de garantias de segurança futura e passada perfeitas, com refrescamento da chave das sessões *multicast*, cada vez que um novo utilizador entra em sessão e cada vez que um utilizador sai da sessão.

Para a realização dos três anteriores objetivos devem atender-se os requisitos e as pré-especificações a seguir indicados.

2. Requisitos e pré-especificações

2.1 Protocolo de autenticação e controlo de acesso baseado em TLS (obrigatório: 14 valores)

Todos os clientes bem como o servidor de autenticação e controlo de acesso, deverão usar agora certificados de chave pública (formato X509) que serão geridos em *keystores* e *public-key truststores* por parte de cada principal, devendo cada um usar em segurança as respetivas chaves privadas mantidas em *keystores* protegidas por passwords.

O protocolo a implementar deve permitir obter a chave de sessão nos moldes inicialmente especificados na FASE 2 do TP1, devendo providenciar as garantias de segurança equivalentes às anteriormente associadas. No entanto, essas garantias serão agora estabelecidas a partir de um canal TLS entre os clientes e o servidor que implementa a autenticação e o controlo de acesso às sessões.

Para tal implementação, os alunos devem garantir as propriedades de segurança antes associadas à especificação da FASE 2 (trabalho TP1), tirando partido das propriedades de segurança já suportadas pela normalização TLS, tendo no entanto em atenção que:

a) O servidor não deve ter acesso às passwords dos utilizadores (podendo apenas ter acesso às transformações dessas passwords, com base em funções seguras de HASH ou HMAC, de acordo com solução a propor e implementar);
b) Não deve haver sobreposição de proteções desnecessárias entre o que já é garantido pelo suporte TLS e o que seja garantido pelo protocolo (nível aplicação) que implementa o serviço de autenticação e controlo de acesso de utilizadores às salas CHAT-Multicast.

Adicionalmente, será implementado suporte de configuração flexível das condições de segurança do canal TLS, nomeadamente:

- Possibilidade de se adoptar autenticação unilateral do servidor, autenticação unilateral do cliente e autenticação mútua cliente-sevidor;
- Apenas possibilidade de se usar TLS v1.2 como garantia base da configuraçãoo de segurança TLS;
- Possibilidade de se usar *ciphersuite*s para os seguintes modos de autenticação (de acordo com a especificação do protocolo TLS)
    - Autenticação em modo RSA (chaves de 2048 bits)
    - Autenticação em modo DSA (chaves de 2048 bits)
    - Autenticação em modo Diffie-Hellman Ephemeral (ou EDH), autenticado com RSA ou DSA – com números de 2048 bits
- Possibilidades de se usar parametrização de *ciphersuites* na conexão TLS (conforme suporte JAVA-JSSE) mas condicionando a utilização das seguintes:

```
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_DH_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA256
TLS_DH_RSA_WITH_AES_256_GCM_SHA256
```

Para o efeito, a implementação terá que permitir as necessárias configurações (para além das associadas à gestão das necessárias keystores usadas na conexão TLS, de acordo com a respetiva configuração.

Para o efeito, em cada principal (utilizador ou servidor de autenticação), deve existir um ficheiro de configuração **(tls.config)** que permitirá descrever todas as necessárias configurações no canal TLS, do seguinte modo:

TLS: version // só deve permitir versão tls 1.2

AUT: valor // valor: CLIENTE, SERVIDOR ou CLIENTE-SERVDIOR

CIPHERSUITES: CIPHERSUITE

PRIVKEYSTORE: // ficheiro keytore da chave privada

TRUSTSTORE: // ficheiro keystore com as chaves públicas confiáveis

Nota: a implementação do trabalho deverás ser testada de modo a avaliar que permite utilizar qualquer uma das combinações de configuração TLS acima indicadas. Nesta

avaliação deverá instrumentar-se o código de modo a obter a latência de entrada de um utilizador na sessão, medido o tempo desde o início do estabelecimento da sessão TLS e o momento em que um participante está apto a entrar na sessão.

2.2 Estabelecimento de chave de sessão com base num acordo de DH com garantia de segurança futura e passada perfeitas: 6 valores

Neste objetivo pretende-se que o estabelecimento de chaves de sessão (para a comunicação *multicast*) seja evoluído para uma implementação de um acordo em grupo, com base no método Diffie-Hellman, com garantias de segurança futura e passada perfeitas. Para tal será necessário que, a partir da primeira chave de sessão obtida do protocolo de autenticação e controlo de acesso, se proceda ao refrescamento da *ciphersuite* e da chave usada de facto nas sessões *multicast*, cada vez que um novo utilizador entra em sessão e cada vez que um utilizador sai da sessão. Este refrescamento será feito de acordo com a parametrização de *ciphersuites* da sessão que resultou do protocolo de autenticação e controlo de acesso (nos moldes similares ao especificado para a FASE 2 do TP1).

Para a realização deste objetivo (que para efeitos de entrega deve ser implementado como um projeto à parte a partir da implementação do objetivo anterior), deve atender-se à seguinte pré-especificação.

- Cada participante que entra na sessão (Multicast-CHAT), envia em *multicast* e cifrado com a chave de sessão obtida do serviço de controlo de acesso, um número público DH gerado dinamicamente para o efeito, juntamente com uma assinatura digital dessa mensagem, provando que o envio é realizado por um participante autorizado e autenticado na sessão, sendo apenas assim aceite pelos outros participantes;
- Como resposta à mensagem anterior cada participante envia em *multicast* um número público de D-H, que por sua vez foi gerado numa mensagem que é por si assinada.
- Após receberem todos os números públicos, os participantes calculam por um acordo de DH em grupo uma nova chave de sessão, para o algoritmo criptográfico simétrico que vai ser usado para o protocolo de comunicação segura em *multicast*. Neste contexto devem ser geradas: a chave criptográfica de sessão (para o algoritmo simétrico a usar na sessão) e os demais parâmetros necessários de acordo com a suite criptográfica a utilizar para o canal seguro de comunicação *multicast*.
- O restabelecimento desta chave de sessão será feito cada evz que houver uma mudança de vista no grupo de participantes, isto é: quando um novo utilizador entra ou quando um utilizador sai.

Data de entrega: 5/Junho/2017 (em moldes similares à entrega do TP1)

Relatório: deve ser entregue impresso por cada grupo (ficando um dos elementos do grupo com essa incumbência) na secretaria, até 2ª feira, 12/Junho/2017 (17h00)
