Segurança de Redes e Sistemas de Computadores 2017/2018

Ficha de Reporte do Trabalho Prático nº 1 (TP1)

Grupo

Nº de Aluno	Nome (elementos do grupo)
43149	**Gil Alves**
43858	**Miguel Pereira**

1. Introdução e contexto do trabalho

Indique X conforme o seu caso

Implementação e completude do trabalho	SIM	NÃO	PARC. (Parcialmente)
Foram implementados totalmente todos os requisitos da FASE 1 (ou protocolo STGC/TLP)	X		
Foram implementados totalmente todos os requisitos da FASE 2 (ou protocolo STGC-SAP)			X
A minha implementação da FASE 1 (ou implementação do STGC/STGC-TLP) concretiza completamente e exatamente as especificações desse protocolo que constam do enunciado	X		
A minha implementação da FASE 2 (ou implementação do STGC/STGC-SAP) concretiza completamente e exatamente as especificações desse protocolo que constam do enunciado			X

Se colocou X anteriormente em alguma posição PARC /Parcialmente do quadro, indique porque o fez e porque considera que a implementação é parcial. Se não deixe em branco ou indique N/A

A segunda fase está parcialmente implementada por falta de tempo. A implementação é parcial porque falta a parte do cliente processar a mensagem do servidor (2ª ronda). O envio do pacote por parte do servidor está a ser feito, assim como a recepção por parte do cliente, só faltou mesmo o processamento da mensagem.

2. Generalidade do desenvolvimento do protocolo STGC (Subprotocolo STGC-TLP) e sua evidência

Para suportar a aplicação de teste fornecida (testeMulticast) e para que esta seja protegida pela implementação do protocolo STGC-TLP, dado o código inicial (sem proteção da comunicação) dessa aplicação:

2.1 Apenas foi necessário modificar __2____ linhas de código, em relação ao número de linhas de código da aplicação inicial

2.2 É preciso modificar ___2___ linhas de código em relação ao número de linhas de código inicial, tendo ainda que se acrescentar mais __8___ linhas de código em relação ao código inicial

Diga em que consiste no essencial a modificação do código da aplicação para ser protegida pela sua implementação com o STGC/TLP:

A modificação do código testMulticast centra-se na troca da inicialização da socket Multicast (1 linha de código no receiver e 1 linha de código no sender) para a socket por nós implementada

STGCMulticastSocket.

As 8 linhas de código adicionadas são referentes à introdução da password da keystore por parte do utilizador (através de Scanner in) e inicialização do protocolo STGC.

3. Caracterização da implementação do protocolo STCG / subprotocolo STGC-TLP

A minha implementação do subprotocolo STGC foi feita do seguinte modo (caracterize com uma boa síntese, como construiu e desenvolveu o suporte do protocolo STGC/STGC-TLP.

O nosso subprotocolo STGC-TLP é constituído por 2 entidades (classes) essenciais: a primeira representa o subprotocolo TLP, que contém todas as operações referentes a segurança e interage com o ficheiro de configuração. A segunda representa uma socket Multicast protegida (recebe as mensagens da aplicação e processa-as de forma a ficarem seguras, antes de serem enviadas). Utiliza um objecto do subprotocolo TLP para adicionar as restrições de segurança necessárias.

4. Comprovação da correção da implementação do protocolo STGC-TLP

4.1 Utilizei como aplicação de comprovação e prova do funcionamento da minha implementação STGC/STGC-TLP	**SIM**	**NÃO**
a) a aplicação MCHAT	X	
b) a aplicação STREAMING		X

4.2 Nas minhas observações experimentais, a aplicação protegida pela minha implementação do protocolo STGC/STGC-TLP:	**SIM**	**NÃO**
a) Funciona corretamente	X	
b) Funciona bem mas apenas parcialmente		X

Justifique, apenas no caso de ter respondido SIM a 4.2 b). Se não deixe em branco ou coloque N/A

5. Flexibilidade e configuração de parametrizações de segurança para a execução do protocolo STGC/STGC-TLP

A minha implementação STCG/STGC-TLP segue as especificações do enunciado do trabalho, sendo *os endpoints de comunicação* parametrizáveis pelos seguintes ficheiros (configuração):

	SIM	**NÃO**
5.1 Ficheiro de configuração ciphersuite.conf	**X**	

5.2 keystore.jceks	**X**	

5.3 Uma configuração tipo no ficheiro ciphersuite,conf pode ser estabelecida do seguinte modo (exemplifique):

```
<224.0.0.1>
CIPHERSUITE:    AES/ECB/PKCS5Padding
KEYSIZE:        128
MACKM:          HMacSHA1
MACKMEYSIZE:    128
MACKA:          HMacSHA1
MACKAKEYSIZE:   128
</224.0.0.1>
<224.0.0.0>
CIPHERSUITE:    AES/CTR/NoPadding
KEYSIZE:        128
MACKM:          HMacSHA256
MACKMEYSIZE:    128
MACKA:          HMacSHA256
MACKAKEYSIZE:   128
</224.0.0.0>
<224.0.0.2>
CIPHERSUITE:    AES/CBC/PKCS5Padding
KEYSIZE:        128
MACKM:          HMacSHA384
MACKMEYSIZE:    128
MACKA:          HMacSHA384
MACKAKEYSIZE:   128
</224.0.0.2>
```

5.4 Com o suporte de configuração **ciphersuite.conf** e com a geração / utilização adequadas (correspondentes) do **keystore.jceks**, verifiquei que se suportarão de forma flexível quaisquer combinações criptográficas. No meu caso testei e comprovei experimentalmente as seguintes:

```
LISTA DE CIPHERSUITES testadas com sucesso: (ALG/MODO/PADDING):

AES/ECB/PKCS5Padding

AES/CTR/NoPadding

AES/CBC/PKCS5Padding
```

```
LISTA DE MACs (HMACs ou CMACs) testadas com sucesso:
HMacSHA1
HMacSHA384
HMacSHA256
```

6. RESPONDA A ESTA SECÇÃO APENAS SE IMPLEMENTOU O SUB-PROTOCOLO STGC-SAP, de acordo com os requisitos do enunciado. Se não, passe ao ponto 7 (Conclusões)

6.1 Apresente (usando notação apropriada) a especificação (o mais completa possível) das mensagens trocadas no contexto do processamento do subprotocolo STGC/SAP:

Ronda 1: Client > AS: Formato da mensagem com os componentes criptográficos e sua descrição: **Username || NonceC || MulticastAddress || AuthenticatorC** **tal que** **AuthenticatorC = E[K, (X)|| MACk(X)]** **X = NonceC || MulticastAddress || SHA512(password)** **K = PBE(SHA512(password))** **k = PBE(MD5(NonceC || SHA512(password)))**
Ronda 12 AS > Client: Formato da mensagem com os componentes criptográficos e sua descrição: **E[K, (X)|| MACk(X)]** **tal que** **X = NonceC+1 || NonceS || TicketAS** **K = PBE(SHA512(password) || NonceC+1)** **k = PBE(MD5(NonceC || SHA512(password)))** **TicketAS = ciphersuite || macKmAlg || macKaAlg || ks || km || ka**

6.2 O servidor AS possui configurações com os seguintes ficheiros, conforme a especificação do enunciado:

Ficheiro de configuração	SIM	NÃO
ciphersuite.conf **//gestão de ciphersuites utilizáveis para as sessões**		**X**
keystore.jceks **//chaves (criptográficas simétricas ou para MACs – HMACs ou CMACs)**		**X**
users.conf **//Utilizadores registados que podem participar em grupos multicast seguros STGC**	**X**	
dacl.conf **//configuração de listas de controlo de acesso (DAC) de utilizadores que podem participar em cada grupo multicast definido como grupo seguro**	**X**	

STGC		
stgcsap.conf **//configuração criptográfica para possíveis construções PBEncryption e MACs para o protocolo STGC-SAP**	**X**	

6.3 A minha implementação do protocolo STGC-SAP pode ser configurável no ficheiro stgcsap.conf, tendo sido verificado experimentalmente com configurações envolvendo:

PBE (Password-Based Encryption)	**SIM**	**NÃO**
PBEWithSHAAnd3KeyTripleDES	**X**	
BEWITHSHA256AND256BITAES-CBC-BC		**X**
PBEWITHSHA-1AND256BITAES-CBC-BC		**X**
PBEWithHmacSHA224AndAES_256		**X**
OUTRA(S) QUAIS:		**X**
MACS (HMACS)	**SIM**	**NÃO**
HMacSHA1		**X**
HMAC/SHA384		**X**
HMAC-SHA3-224		**X**
HMAC-SHA3-256		**X**
HMAC-SHA512	**X**	
OUTROS (QUAIS ?):		
MACS (CMACS)	**SIM**	**NÃO**
SKIPJACKMAC		**X**
AESGMAC		**X**
RC6GMAC		**X**
RC5MA		**X**
DES		**X**
OUTROS (QUAIS ?)		

6.4 Indique em que consiste o formato de um TocketAS (devolvido na ronda 2 do subprotocolo STGC-SAP). Pode copiar a estrutura de dados que o descreve:

O TicketAS tem o formato de um byte array concatenando
TicketAS = ciphersuite || macKmAlg || macKaAlg || ks || km || ka.

7. Conclusões e aspectos complementares

Inclua as conclusões sobre o seu desenvolvimento do TP1, podendo realçar aspectos complementares ou diferenciados da sua implementação. Se achar relevante pode argumentar sobre aspectos qualitativos que considera valorizáveis

7.1 Conclusões resumidas:

Numa perspetiva mais geral sobre o projecto, achamos que esteve dentro das expectativas. Um projecto demasiado grande para o tempo e carga de todas as cadeiras do semestre. Apesar disso fez com que o grupo assumisse responsabilidades ao nível das decisões de planeamento, bem como experiência em todas as fases de desenvolvimento de código, trazendo maior relevância a esta cadeira.

7.2 Aspectos complementares a salientar:

Nada a salientar.

7.3 Argumentação sobre fatores diferenciados e qualitativos implementados no TP1

Nada a salientar.