Segurança de Sistemas Computacionais
2013/2014, 1º Semestre

Trabalho Prático nº 3

FICHA/RELATÓRIO DE REFERÊNCIA DA IMPLEMENTAÇÃO
(Esta ficha impressa deve ser entregue por Email juntamente com a implementação do trabalho)

Prazo limite; 19/12/2013, 24h00

Identificador do Grupo*	
Nome do arquivo de SW (sources e binários) com a implementação bem como a presente ficha de avaliação, submetido por Email para henrique.domingos@gmail.com	**G17_TP3.zip**
Hash (SHA1) do arquivo com a implementação entregue	**Copiar o HASH (SHA-1) do ficheiro anexo ao Email contendo entregue com o arquivo acima: 7934d082408b407e3c122d50239ec6610a56761a**

Membros do Grupo que participaram na implementação do Trabalho (de acordo com o registo do grupo)

Nº	**41810**	**Nome**	**Ricardo Monteiro**
Nº	**41895**	**Nome**	**Rafael Bizarra**
Nº		**Nome**	

Resumo

Foi alterado o protocolo de autenticação do trabalho 2. Para além disso, foi melhorado alguns problemas que havia nos ficheiros de configuração das cifras para as emissões stream.
O protocolo de autenticação adoptado neste projecto foi SSL. Temos duas variantes deste protocolo, uma em que apenas o servidor autentica a sua autencidade através do seu certificado. E outra, em que os clientes também são autenticados por certificados. Também é feita a verificação da validade destes certificados.

1. Introdução

Tendo por base o resumo anterior, apresenta-se nesta introdução uma tabela de referencia normalizada que sintetiza e caracteriza a implementação. Nesta tabela, a referida caracterização está assinalada em cada linha com X (SIM ou NÃO) . Nas linhas marcadas com X apresenta-se ainda um indicador de autoavaliação relativa à observação experimental e testes da implementação do trabalho, correspondendo esta escala à seguinte grelha de critérios

5 – Excelente: se a implementação e o seu teste forem considerados perfeitos e completos de acordo com todos os requisitos obrigatórios e valorativos adicionais a destacar face ao enunciado, tendo todas as configurações apresentadas sido testadas e avaliadas bem como analisadas com base na observação de funcionamento do protocolo (*wireshark* ou outra ferramenta das que foram apresentadas na aula);
4 - Muito Bom: se a implementação for considerada completa nos requisitos obrigatórios e valorativos, mas com configurações dos aspectos valorativos ou adicionais não integralmente verificados e testadas nas condições enunciadas para valorização 5 ou não completamente verificadas na análise da operação do protocolo (*wireshark* ou outra ferramenta das que foram apresentadas na aula);
3 - Bom: se a implementação for considerada completa nos requisitos obrigatórios e com configurações integralmente verificadas e testadas embora a análise e verificação do protocolo (com a ferramenta *wireshark* ou outra ferramenta das que foram apresentadas na aula);
não tenha sido completa ou não tenha coberto todas as configurações.
2 – Suficiente: se a implementação for considerada não completa em todos os requisitos obrigatórios ou algumas das configurações não tenham sido testadas e verificadas.
1 – Insuficiente: se o trabalho for considerado muito incompleto face às especificações obrigatórias do enunciado, ou se apresentar deficiências

Requisito e objectivo (Caracterização da implementação)	**SIM**	**NÃO**	**Completude, Teste de Robustez e Correção para efeitos de demonstração. Utilize a escala 1, 2, 3, 4, 5, conforme se indica**
A – Configuração		**x**	

Só certificados (X509) com chaves RSA com chaves de tamanho fixo e apenas autenticação unilateral do servidor. Os certificados são usados numa base de confiança peer-peer sem noção de emissão por uma CA			
B - Configuração Só certificados (X509) com chaves RSA com tamanhos variáveis e autenticação unilateral do servidor. Os certificados são usados numa base de confiança peer-peer sem noção de emissão por uma CA		**X**	
C - Configuração Certificados (X509) com chaves RSA ou DSA, com tamanhos variáveis e autenticação unilateral do servidor. Os certificados são usados numa base de confiança peer-peer sem noção de emissão por uma CA		**X**	
D - Configuração Certificados (X509) com chaves RSA, com tamanhos variáveis e autenticação unilateral do servidor. Os certificados são emitidos por uma CA e geridos com base na confiança do certificado dessa CA e cadeia de certificação no protocolo SSL	**x**		**3**
E - Configuração Certificados (X509) com chaves RSA ou DSA, com tamanhos variáveis e autenticação unilateral do servidor. Os certificados são emitidos por uma CA e geridos com base na confiança do certificado dessa CA e cadeia de certificação no protocolo SSL		**x**	
F – Igual a A mas testado e verificado suportando autenticação mútua			
G – Igual a B mas testado e verificado suportando autenticação mútua			
H – Igual a C mas testado e verificado suportando autenticação mútua			
I – Igual a D mas testado e verificado suportando autenticação mútua			
J - Igual a E mas testado e verificado suportando autenticação mútua			
K – Igual a A mas testado e verificado suportando autenticação unilateral do cliente			
L – Igual a B mas testado e verificado suportando autenticação unilateral do cliente			
M – Igual a C mas testado e verificado suportando autenticação unilateral do cliente			
N – Igual a D mas testado e verificado suportando autenticação unilateral do cliente	**x**		**2**
O - Igual a E mas testado e verificado suportando autenticação unilateral do cliente			
P – A configuração (modo de autenticação SSL, configuração de ciphersuites SSL, gestão de			

certificados de chaves públivas) bem como gestão de autenticação e controlo de acessos de utilizadores estão completamente separadas da implementação (código)			
Q – Verificação do certificados do cliente em modo de autenticação mútua ou unilateral do cliente na sessão SSL envolvem identificador que deverá corresponder ao identificador de autenticação (userID/pwd) e controlo de acesso do utilizador, para acesso à sessão de *streaming*.		**x**	
R – Verificação dos certificados do servidor na sessão SSL em modo de autenticação unilateral do servidor ou autenticação mútua, envolvem *DNS name* ou endereço IP que deve corresponder ao endereço do socket do servidor observado pelo cliente na conexão.		**x**	

2. Aspectos complementares relativos ás implementações bem como testes realizados sobre as configurações

2.1 *Ciphersuites* testadas:

De entre as seguintes ciphersuites, foram testadas e verificadas no suporte da implementação realizada as indicadas na seguinte tabela

```
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5
TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA
TLS_KRB5_EXPORT_WITH_RC4_40_MD5
TLS_KRB5_EXPORT_WITH_RC4_40_SHA
TLS_KRB5_WITH_3DES_EDE_CBC_MD5
TLS_KRB5_WITH_3DES_EDE_CBC_SHA
TLS_KRB5_WITH_DES_CBC_MD5
TLS_KRB5_WITH_DES_CBC_SHA
TLS_KRB5_WITH_RC4_128_MD5
```

TLS_KRB5_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
Outra (indicar qual na seguinte tabela)

***Ciphersuites* suportadas e verificadas** (Nota: de acordo com a análise de resultados pretendida devem ter sido cobertas pelo menos as ciphersuites envolvendo autenticação RSA, DHE (em TLS ou em SSL) e variantes das mesmas com opções de métodos criptográficos diferenciados (ex., RC4_128, 3DES_EDE, AES_128, AES_256), tendo em vista os objectivos reportados no ponto 3 seguinte.
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_AES_128_CBC_SHA

2.2 Modos de autenticação implementados e testados

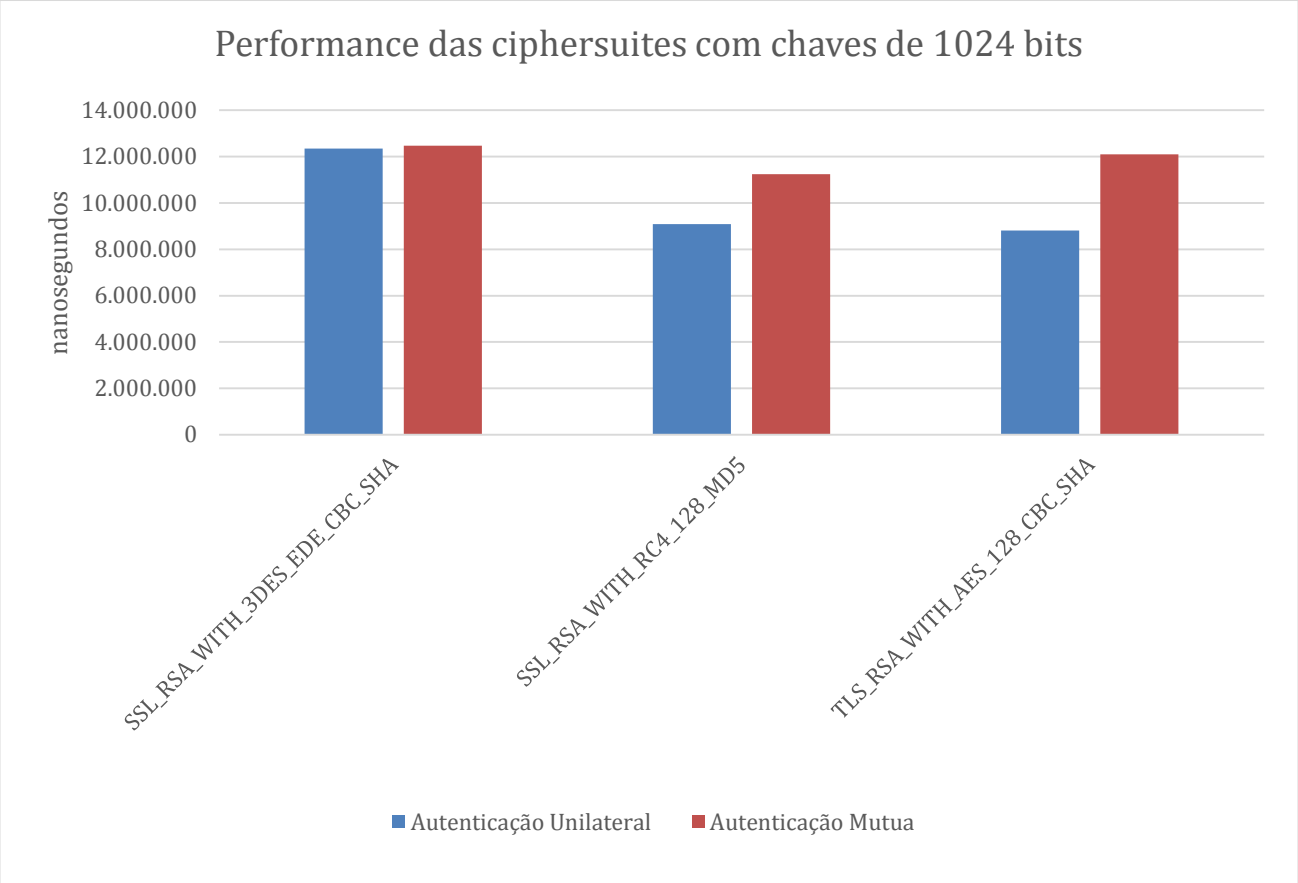
Assinalam-se na seguinte tabela com X os modos de autenticação que foram implementados e testados

Modo de autenticação	
Unilateral do servidor (server-only)	**X**
Unilateral do cliente (client-only)	
Mútua (cliente e servidor)	**X**

3. Análises de resultados de desempenho do protocolo

Apresentam-se nesta secção resultados experimentais obtidos relativos a diferentes *ciphersuites* e modos de autenticação (para suporte das conexões SSL ou TLS) e seu impacto na latência da operação do protocolo de autenticação implementado.

3.1 Análise comparativa de impacto entre modos de autenticação mútua e unilateral na sessão SSL subjacente ao protocolo de autenticação com diferentes ciphersuites



Para os testes de performance, realizámos 7 observações, excluímos a melhor e a pior e fizemos a média das 5 restantes.

4. Aspectos complementares considerados como destacáveis para efeitos da apreciação e avaliação do trabalho

Melhorámos a parametrização configurável do trabalho 2 em ralação às ciphersuites do streamcast.