Segurança de Redes e Sistemas de Computadores 2017/2018
Ficha de Reporte do Trabalho Prático nº 2 (TP2) – VARIANTE 1

Nº de Aluno	Nome (até quatro elementos)
45020	**Simão Dolores**
45617	**André Lopes**
45694	**Nelson Coquenim**

PREENCHA OS QUADROS A, B, C, D e E de acordo com a sua implementação

QUADRO A

Introdução e contexto geral do desenvolvimento e validação experimental do trabalho que foi desenvolvido e entregue

Indique X nas colunas indicadas conforme o seu caso

A sua indicação X deve indicar SIM, NÃO OU PARCIALMENTE de acordo com as respetivas colunas		**SIM**	**NÃO**	**PAR C.**
1)	O desenvolvimento foi feito com base na variante 1 – **Aplicação cliente/serviço REDIS**, atendendo a todas as especificações requeridas no enunciado.	x		
2)	Foram implementados e testados com sucesso todos os requisitos gerais expressos **no ponto 1.1.1** do enunciado.	x		
3)	Concluí e testei todos os desenvolvimentos que permitem a um cliente (JEDIS) operar sobre o servidor (REDIS) com as operações SET, GET e ERASE, conforme foi requerido, de modo que no servidor REDIS os dados são mantidos sempre cifrados e assim com garantias de confidencialidade permanente durante essa operação, estando as chaves usadas para cifrar os dados mantidas apenas no lado do cliente JEDIS	x		
4)	Concebi um repositório que armazena os dados do lado do servidor REDIS seguindo as instruções indicadas, de modo a poder suportar uma tabela com vários atributos (colunas) que são mantidos sempre cifrados mesmo quando o cliente precisa de realizar operações sobre esses dados	x		
5)	Na minha implementação cada linha (tabela) permite armazenar pelo menos 6 atributos, de forma que pelo menos três deles podem ser usados para pesquisas do lado do cliente, já que existe um índice no cliente que permite obter a chave de indexação no REDIS Server, dado qualquer dos atributos pesquisáveis.	x		

6)	Em cada linha da tabela, tal como está armazenada no REDIS Server, existe uma assinatura digital com garantia de autenticidade e integridade dos dados sendo essa assinatura feita no momento em que cada entrada da tabela é armazenada.	x		
7)	O cliente JEDIS desenvolvido e que faz o *benchmark* requerido realiza ou valida as assinaturas digitais indicadas em 5., quando efetua operações de GET, SET ou ERASE			x
8)	A operação de ERASE envolve a reescrita da linha a apagar com base num conteúdo aleatório gerado, cifra com criptografia simétrica do conteúdo aleatório gerado, descarte da chave usada para esta cifra e escrita no repositório desse valor cifrado obtido.	x		
9)	Para além da assinatura digital indicada em 6., cada entrada (linha) da tabela, contem ainda adicionalmente uma prova do tipo HMAC, o que permite que o cliente possa obter uma prova de autenticidade e integridade do conteúdo das entradas da tabela de forma mais rápida (sem necessidade de realizar computações mais exigentes de validação das assinaturas digitais) quando houve quebra de integridade dos dados cifrados que estão contidos no repositório suportado pelo REDIS Server.	x		
10)	Foram desenvolvidos e testados os dois módulos TPM que permitem atestar a integridade do Software na pilha de componentes de software que suportam a execução do servidor REDIS	x		
11)	Em relação com a 9) foi implementado o TPM VMS que permite atestar provas do contexto de execução de processos que executam ao nível da máquina virtual bem como de integridade dos binários relativos aos processos em execução que são atestados, incluindo o próprio servidor REDIS e outros processos considerados como prova de conceito	x		
12)	Em relação a 10), também é incluída no TPM VMS a prova de integridade da execução do ambiente Java (JVM) que suporta a execução do próprio módulo TPM VMS	x		
13)	Em relação com a 9) foi implementado o TPM GOS que permite atestar provas do contexto de execução de processos que executam ao nível do sistema operativo nativo (HOST OS) bem como de integridade dos binários relativos aos processos em execução que são atestados, incluindo o próprio lançamento do ambiente de virtualização (VBOX ou VMWARE) que lança e executa a VM que é suposta executar	x		
14)	Em relação a 12), também é incluída pelo TPM GOS na prova de execução o ambiente Java (JVM) que suporta	x		

	a execução do próprio módulo TPM GOS			

15)	No protocolo de atestação implementado para que o cliente obtenha as provas de atestação do SW por parte dos módulos VMS e GOS, foram implementados todos os requisitos do enunciado, nomeadamente: - Suporte TLS nos canais de comunicação subjacentes aos protocolos de atestação (Cliente / Módulos TPM) - Envio pelo cliente d pedido de atestação <u>com base nas especificações do enunciado</u> com envio de: o ATTESTATION REQUEST CODE || PUB-DH (1024 bits) || Secure RANDOM NONCE PUB-DH: o que envolve a geração e envio pelo cliente de um núm número público Diffie-Hellman gerado pelo cliente para cada pedido de atestação o NONCE: número aleatório gerado pelo cliente para o pedido de atestação. • - Envio pelo servidor da resposta de atestação <u>com base nas especificações do enunciado</u> envolvendo: - ATTESTATION SIGNATURE: assinatura digital cobrindo: o Um número público Diffie-Hellman gerado pelo módulo em causa para a resposta o A resposta ao NONCE enviado pelo cliente no pedido de atestação o ATTETSTATION STATUS: lista com um conjunto (lista) das provas de síntese correspondentes ao estado auditado. A lista é enviado cifrada com AES, usando como chave K a chave derivada do acordo Diffie Hellman resultante da troca de números públicos DH.	x		
16)	O protocolo de atestação realizado pelo cliente e os módulos TPM é suportado em paralelo por duas threads do cliente, cada uma procedendo à atestação num dos módulos.			x

JUSTIFICAÇÕES SOBRE OS ASPECTOS DO QUADRO A

Se algum dos aspectos indicados nas alíneas 1) a 14) do **QUADRO A** foram indicados com a opção **PARC (PARCIALMENTE),** deve indicar a justificação ou a explicação para ter indicado essa opção. Se achar necessário pode complementar as **respostas SIM** com o que considere necessário que permita clarificar a sua resposta.

Para todos os efeitos a explicação deve ser feita de acordo com o que foi EFETIVAENTE IKPLEMETADO E SUBMETIDO e não sobre opções d eo fazer mas que não foram efetivamente realizadas

JUSTIFICAÇÃO ADICIONAL SOBRE 1)
JUSTIFICAÇÃO ADICIONAL SOBRE 2)
JUSTIFICAÇÃO ADICIONAL SOBRE 3)
JUSTIFICAÇÃO ADICIONAL SOBRE 4)
JUSTIFICAÇÃO ADICIONAL SOBRE 5)
JUSTIFICAÇÃO ADICIONAL SOBRE 6)
JUSTIFICAÇÃO ADICIONAL SOBRE 7)
Parcialmente devido a não ser preciso verificar a signature quando se remove da tabela.
JUSTIFICAÇÃO ADICIONAL SOBRE 8)
JUSTIFICAÇÃO ADICIONAL SOBRE 9)
JUSTIFICAÇÃO ADICIONAL SOBRE 10)
JUSTIFICAÇÃO ADICIONAL SOBRE 11)
Testou-se, mas no ficheiro de configuração em que estão presentes os comandos para o atestamento apenas foi deixado um comando mais geral de forma a ser mais portável, isto é, não gerar problemas com paths noutros computadores. Mas é facilmente parametrizável.

JUSTIFICAÇÃO ADICIONAL SOBRE 12)
Ver justificação do 11)
JUSTIFICAÇÃO ADICIONAL SOBRE 13)
Ver justificação do 11)
JUSTIFICAÇÃO ADICIONAL SOBRE 14)
Ver justificação do 11)
JUSTIFICAÇÃO ADICIONAL SOBRE 15)
TPM também manda para o cliente informação como configuração da encriptação simétrica que será utilizada posteriormente (igualmente para a assinatura).
JUSTIFICAÇÃO ADICIONAL SOBRE 16)
Código para multithreading está comentado pois não se conseguiu corrigir um bug.

QUADRO B

Indicadores concretos relativos à implementação e ao seu teste experimental

<table>
<tr><td>1)</td><td>Quantas colunas (número de atributos) considerou para concretizar a “tabela” que está armazenada do lado do servidor ? (INDIQUE UM NÚMERO INTEIRO)</td><td>6</td></tr>
<tr><td>2)</td><td>Nas suas observações experimentais, indique o desempenho (operações/segundo) que o seu cliente JEDIS é capaz de executar no Benchmark observado. Para ter um resultado mais interessante deve ser o valor médio observado em várias execuções (exemplo ~10)</td><td>105</td></tr>
<tr><td>3)</td><td>Quantas operações (TOTAL) são realizadas no benchmark relativo a 2), realizado nas suas observações experimentais ? Indique um número, exemplo: 100, 1000</td><td>300</td></tr>
<tr><td>4)</td><td>No número de operações sindicado em 3), quantas são GET?</td><td>100</td></tr>
<tr><td>5)</td><td>No número de operações sindicado em 3), quantas são SET ?</td><td>100</td></tr>
<tr><td>6)</td><td>No número de operações sindicado em 3), quantas são ERASE ?</td><td>100</td></tr>
<tr><td>7)</td><td colspan="2">Existem outras operações no seu benchmark ? Quais e quantas (indique se for o caso)
<table>
<tr><td>Operação</td><td>Nº de vezes realizadas no benchmark</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table></td></tr>
<tr><td>8)</td><td>O benchmark, realizado com o número de operações/segundo indicado em 1 e 2) inclui o “overhead” imposto pelo protocolo de atestação feito pelas threads de atestação, feito uma única vez em cada benchmark ? (Indicar SIM ou NÃO)</td><td>NÃO</td></tr>
<tr><td>9)</td><td>No seu teste (benchmark) relativo aos resultados indicados, o cliente executou na máquina virtual onde se encontrava o servidor REDIS ? Indicar SIM ou NÃO</td><td>SIM</td></tr>
<tr><td>10)</td><td>No seu teste (benchmark) relativo aos resultados indicados, o cliente executou na máquina nativa onde se encontrava o ambiente de virtualização (VBOX ou VWARE) onde estava a máquina virtual onde executou o servidor REDIS ? Indicar SIM ou NÃO</td><td>NÃO</td></tr>
<tr><td>11)</td><td>No seu teste (benchmark) relativo aos resultados indicados, o cliente executou num computador diferente do computador onde se encontrava o ambiente de virtualização (VBOX ou VWARE) onde estava a máquina virtual onde executou o servidor REDIS ? Indicar SIM ou NÃO</td><td>NÃO</td></tr>
</table>

Indique qualquer aspecto que entenda clarificar as respostas que deu no quadro C. Para o efeito indique a alínea a que a clarificação diz respeito (1), 2), etc ... 11)

QUADRO C

Aspetos de valorização que foram introduzidos na implementação do TP2

(QUADRO A PREENCHER SÓ PARA IMPLEMENTAÇÕES QUE INCLUEM VALORIZAÇÕES)

A sua indicação X deve indicar SIM, NÃO OU PARCIALMENTE de acordo com as valorizações que tenha incluído no seu trabalho		**SIM**	**NÃO**	**PAR C.**
1)	Na implementação do suporte TLS para o protocolo de atestação entre o cliente e os módulos TPM desenvolvidos, o suporte TLS é parametrizável sem necessidade de recompilação de modo a permitir: TLS com AUTENTICAÇÃO MÚTUA ou TLS com AUTENTICAÇÃO UNILATERAL (ONE WAY) DO SERVIDOR (o que pode fazer-se em ficheiros de configuração)	x		
2)	Na implementação do suporte TLS para o protocolo de atestação entre o cliente e os módulos TPM desenvolvidos, o suporte TLS é parametrizável no lado do cliente (sem necessidade de recompilação do cliente) de modo a permitir que o cliente possa propor um conjunto de CIPHERSUITES por si determinadas como ENABLED na oferta que fará ao servidor para o HANDSHAKE TLS (o que pode fazer-se em ficheiros de configuração)	x		
3)	Na implementação do suporte TLS para o protocolo de atestação entre o cliente e os módulos TPM desenvolvidos, o suporte TLS é parametrizável no lado do servidor (sem necessidade da recompilação do servidor) de modo a permitir que o servidor parametrize as CIPHERSUITES (ou ua CIPHERSUITE) determinadas pelo servidor como aceitáveis no Handshake TLS que fará com o cliente (o que pode fazer-se em ficheiros de configuração)	x		

4)	Os módulos TPM foram implementados e estão disponíveis como arquivos executáveis JAR	x		
5)	Os módulos TPM foram implementados e estão disponíveis como imagens DOCKER		x	
6)	No caso de 4), a execução dos arquivos JAR e a sua integridade são objeto da própria atestação que os módulos TPM incluem no protocolo de atestação	X		
7)	No caso de 5), a execução das imagens docker e a sua integridade são objeto da própria atestação que os módulos TPM incluem no protocolo de atestação		x	
8)	Na implementação podem configurar-se as CIPHERSUITES usadas pelo cliente (JEDIS) para cifrar os conteúdos escritos no repositório (REDIS-SEFVER), nomeadamente métodos de síntese usados para construção de chaves de acesso bem como de cifras simétricas, modo e *padding* usados para cifrar os atributos (colunas da tabela) bem como da assinatura digital ou HMACs que usa como provas de autenticidade e integridade	x		
9)	Na solução foi implementado suporte TLS para suportar as interações entre o cliente (JEDIS) e o servidor (REDIS), sendo essa solução baseada num proxy TLS entre o cliente e o servidor.		x	
10)	Na solução foi implementado suporte TLS para suportar as interações entre o cliente (JEDIS) e o servidor (REDIS), sendo essa solução baseada no suporte e configuração de um túnel TLS com port-forwarding do lado do cliente e do lado do servidor.		x	
11)	Se indicou SIM em 9), assinale com X a seguinte informação da sua implementação e observação experimental			
	O modo de autenticação no handshake TLS si permite usar modo de autenticaçãoo unilateral (one way) do lado do servidor			
	O modo de autenticação no handshake TLS é parametrizável (podendo parametrizar para autenticação mútua entre os lados cliente e servidor			
	É possível parametrizar CIPHERSUITES propostas pelo lado do cliente ou selecionadas pelo lado do servidor			
12)	Se indicou SIM em 10), assinale com X a seguinte informação da sua implementação e observação experimental			
	O modo de autenticação no handshake TLS si permite usar modo de autenticaçãoo unilateral (one way) do lado do servidor			
	O modo de autenticação no handshake TLS é parametrizável (podendo parametrizar para autenticação mútua entre os lados cliente e servidor			
	É possível parametrizar CIPHERSUITES propostas pelo lado do cliente ou selecionadas pelo lado do servidor			

De acordo com as valorizações anteriores, no caso de ter indicado PARCIALMENTE ou SIM, utilize o seguinte quadro para justificar a sua resposta ou para clarificar em que consiste o suporte que desenvolver para as valorizações que indicou.

6) (Ver justificação do 11) Quadro A**)**

No caso de querer destacar alguma outra valorização da sua implementação para efeitos de avaliação, utilize o seguinte quadro para a explicar.

-TPM totalmente configurável; -Implementação extensível do TPM pois no caso de adicionar mais TPMs apenas se tem que criar um novo ficheiro de configuração e estender a classe.