SRSC-T2-AB1920-C001507

DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
2º Semestre, 2018/2019
Teste de frequência nº 2 (15/Junho/2019)

Copie para a sua folha de resposta o código de referencia indicado: SRSC-T2-AB1920-C00157

Parte I - Resposta sem usar elementos de consulta

Questão 1. Para evitar o problema de possíveis ataques a passwords no protocolo Kerberos, pretende-se usar criptografia assimétrica e o método de acordo de Diffie Hellman (DH) na ronda de autenticação de utilizadores (apenas troca de mensagens de autenticação de utilizadores perante o *Authentication Server (AS)*. Para o efeito, o acordo DH será feito com base em parâmetros partilhados, com um número primo P de 2048 bits e um valor dado para uso como raiz primitiva. Quer os utilizadores (C), quer o Authentcation Server (AS) passam a dispor de certificados de chaves públicas X509v3, sendo esses certificados enviados em cadeias diretas de certificação para validação das respetivas chaves públicas `KpubC` e `KpubAS` no decurso da fase de autenticação do protocolo ($\text{CertificateChain}_A$ enviado pelo cliente C a AS e $\text{CertificateChain}_{AS}$ enviado pelo servidor AS a C). Ambas as cadeias estão em hierarquias com o certificado da mesma autoridade de certificação na raiz.

Versão original Kerberos V5:

Nota: recorde-se que $K_{c,tgs}$ é a chave derivada da password partilhada entre o cliente e o AS

(1) C → AS $Options \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $Realm_c \| ID_C \| Ticket_{tgs} \| \mathrm{E}(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$Ticket_{tgs} = \mathrm{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $Realm_c \| ID_C \| Ticket_v \| \mathrm{E}(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$Ticket_{tgs} = \mathrm{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

$Ticket_v = \mathrm{E}(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| \mathrm{AD}_C \| Times])$

$Authenticator_c = \mathrm{E}(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Options \| Ticket_v \| Authenticator_c$

(6) V → C $\mathrm{E}_{Kc,v}[\, TS_2 \| Subkey \| Seq\# \,]$

$\mathrm{Ticket}_v = \mathrm{E}(K_v, [\mathrm{Flags} \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = \mathrm{E}(K_{c,v}, [ID_C \| Realm_c \| TS_2 \| Subkey \| Seq\#])$

(c) Client/Server Authentication Exchange to obtain service

Variante proposta para robustecimento do protocolo na ronda de autenticação.

Nota) apenas abrange a fase de autenticação - ronda (a), mensagens (1), (2) e que pode comparar com a versão original. Todos os *Tickets* emitidos e todas as restantes mensagens das rondas (b) e (c) são iguais à versão original.

(1)Options||ID_c||$Realm_c$||ID_{tgs}||*Times*||Nonce_1 ||E_{KpubAS}(H(P),Yc)||$\text{CertificateChain}_A$
(2)$Realm_c$||ID_c||$Ticket_{tgs}$||E(K_s,[$K_{c,tgs}$||*Times*||$Realm_{tgs}$||ID_{tgs}]||E_{KpubC}(Nonce_1+1,Yas)||$\text{CertificateChain}_{AS}$

- H(P) é uma síntese da password partilhada entre o cliente e AS
- Yc é um número público de um par gerado por C para estabelecimento da chave Ks
- Yas é um número público de um par gerado por AS para estabelecimento da chave Ks

a) Concorda com a solução proposta para o fim em vista ? Sim ou Não ?

b) Se respondeu Sim argumente porquê. Se respondeu Não indique o que deve ser corrigido na variante proposta?

Questão 2. Bob pretende assinar uma mensagem cuja representação tem 2000 bits, usando uma assinatura digital RSA com construção padrão que usa uma função de síntese SHA-512 e *padding* normalizado. Bob pretende usar uma chave RSA de 2048 bits.

a) Apresente duas razões que justificam a importância de Bob usar *padding* e este ser gerado com valores aleatórios, para incremento da segurança da assinatura digital.

b) Se Bob decidisse usar assinaturas DSA as razões apontadas em a) seriam igualmente válidas? Justifique.

c) Qual o tamanho máximo que poderá ter a representação do valor de *padding* (independentemente de como será gerado) para que a assinatura RSA possa ser possível? Justifique.

d) Poderá a assinatura utilizar *padding* PKCS#1 (v1.5) sabendo que neste caso o valor de *padding* adiciona pelo menos 11 bytes, dos quais 8 bytes representam um valor gerado aleatoriamente entre 1 e 255? Justifique.

e) Se Bob quiser usar o seu par de chaves para distribuir um envelope com uma chave de sessão, que vantagem de segurança tem em usar padding OAEP em vez de padding PKCS#1 ? Justifique.

Questão 3. Indique **VERDADEIRO ou FALSO** nas seguintes alíneas devendo justificar se considerar **FALSO**

Um cliente e um servidor (JAVA) vão usar TLS 1.2 com autenticação mútua. Após concluírem com sucesso a fase de *handshake* estabelecera a *ciphersuite* **`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`**
e as respetivas associações de segurança. Nesse caso:

a) cliente e servidor, que trocaram uma cadeia de certificados, certamente todos os certificados da cadeia certificam chaves públicas DSA a partir de um certificado raiz de confiança de ambos.

b) a troca dos números públicos Diffie-Hellman que permitiram estabelecer a chave de sessão AES de 128 bits foi feita de modo que ambos (cliente e servidor) assinaram esses números com assinaturas DSA.

Questão 4

a) Porque é que um certificado X509v3 que é válido e foi emitido por uma CA para um principal, não pode ser usado como certificado numa cadeia de validação de outro certificado? Como é isso detectado?

b) No modelo de uma PKI, qual a diferença entre uma *Registration Authority* e uma *Certification Authority*?

c) Um certificado em formato CSR (*Certificate Signed Request*) é um certificado assinado por uma CA? Justifique.

d) Na validação de certificados X509v3, porque é que é possível saber-se qual o URL para suporte do protocolo OCSP (*On Line Status Revocation Protocol*) ?

e) Numa CRL (*Certification Revocation List*), cada certificado revogado é assinado pela CA que o revoga? Justifique.

Questão 5

a) Qual o papel do subprotocolo IKE na pilha IPSec ?

b) Em IPSec o subprotocolo ESP-AE suporta Autenticação, Confidencialidade e Integridade de pacotes IP. Utiliza criptografia assimétrica e assinaturas digitais para a autenticação da origem dos pacotes IP? Justifique.

c) Uma VPN para suportar um cliente remoto a aceder a vários servidores numa rede empresarial com endereçamento privado pode ser suportada em IPSec em modo transporte? Justifique.

Questão 6

a) Num sistema de controlo de acesso de tipologia DAC (*Discretionary Access Control*), qual a diferença na representação de permissões usando listas de controlo de acesso e usando capacidades (ou *capability tickets*)? Exemplifique esquematicamente como representaria as permissões de acesso a ficheiros, num e noutro caso.

b) Num sistema de controlo de acessos do tipo ABAC (*Attribute-Based Control*), dê exemplos de diferentes tipos de atributos que podem ser usados no controlo de permissões.

Parte II - Resposta podendo usar elementos individuais de consulta

Questão 7. Num acordo Diffie-Hellman (DH) anónimo , Alice e Bob estão a usar uma raiz primitiva = 2 e um número primo 7. Alice computou o par DH (privado,público) tendo enviado a Bob um valor = 4. Bob por sua vez, calculou o seu par de valores (privado, público), tendo enviado para Alice o valor = 1

a) Indique o valor que representa a chave de sessão que Alice e Bob estabelecerão no acordo? Justifique.

b) Apenas com os dados fornecidos, qual o valor privado que Alice calculou na geração do par? Justifique.

Questão 8

a) Pretende usar-se em TLS uma das seguintes *ciphersuites* envolvendo computações com base no algoritmo de Diffie-Hellman. Em que medida a conexão TLS estará protegida de um eventual ataque à autenticação por parte de um atacante do tipo "homem no meio" em cada uma das *ciphersuites* consideradas ?

Opção *ciphersuite* 1: TLS_DH_RSA_WITH_AES_128_CBC_SHA256
Opção *ciphersuite* 2: TLS_EDH_DSS_WITH_3DES_EDE_CBC_SHA
Opção *ciphersuite* 3: TLS_DH_Anon_WITH_AES_256_CBC_SHA

b) Refira-se ao maior ou menor nível de segurança de cada uma das ciphersuites, considerando que todas as chaves RSA e DSA envolvidas têm 2048 bits e os númerous públicos/privados de Diffie Hellman que possam estar envolvidos são gerados sobre uma raiz primitiva e o número primo relacionado, tendo este uma representação de 1024 bits.

Questão 9

a) O protocolo TLS não tem nos seus objetivos a cobertura de contra-medidas contra ataques de negação de serviço. Estes podem ser desencadeados, por exemplo, por atacantes que lançam ataques do tipo "SYN-Flooding" sobre servidores HTTPS (provocando abertura incompleta de conexões TCP no processo de *3-way handshake* na abertura de conexões TCP). Estes ataques são ainda mais amplificados no caso do estabelecimento de sessões TLS ? Sim ou Não ? Justifique.

b) Numa implementação TLS/TCP como está subjacente ao protocolo HTTPS, uma vez que o transporte TCP já garante controlo de sequenciamento de segmentos TCP, qual a relevância de haver controlo de sequenciamento ao nível do processamento TLS? Não é neste caso uma situação de *overhead* que poderia ser evitada? Argumente.

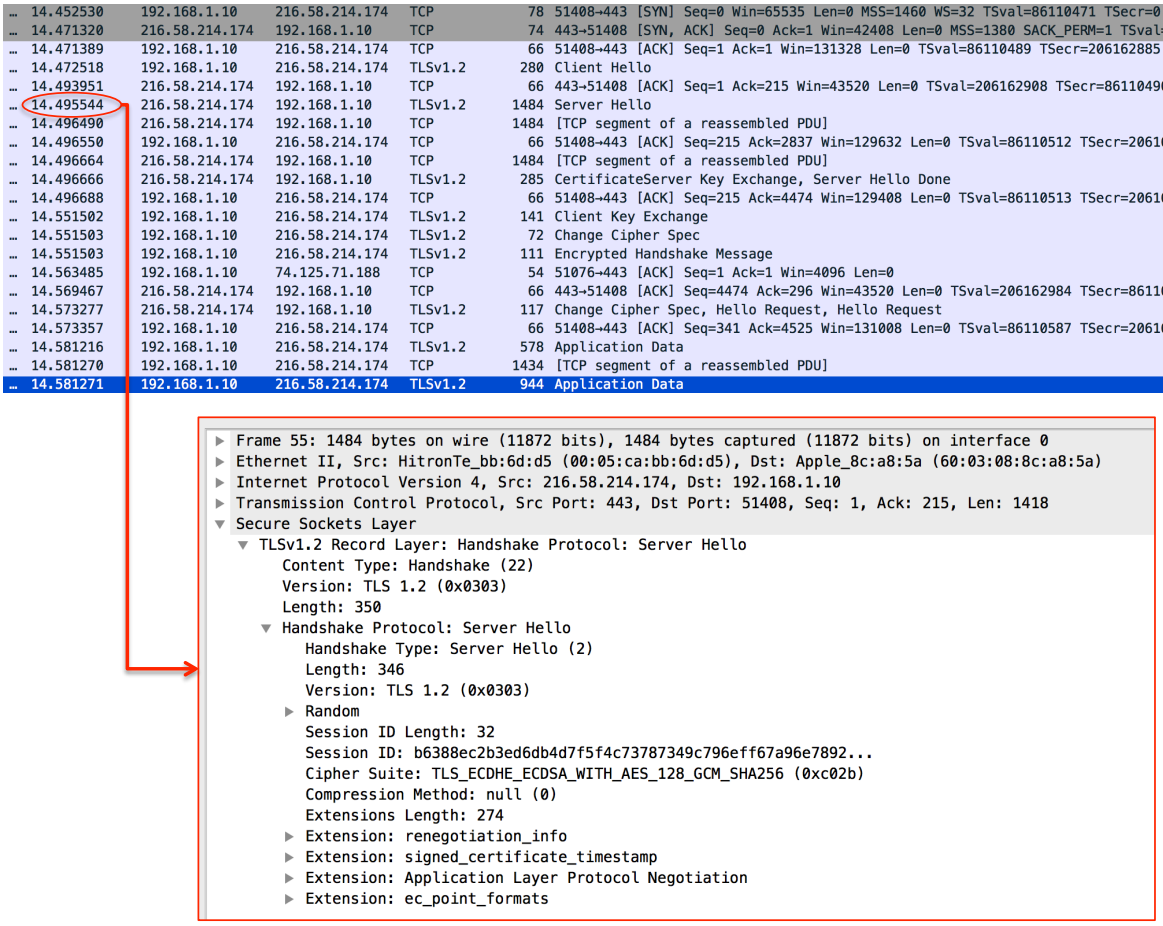
c) O traço seguinte (capturado pela ferramenta *wirehsark*) mostra um trecho de tráfego (21 pacotes TCP – alguns dos quais encapsulando TLSv1.2) trocados entre um computador numa rede privada doméstica, com endereço 192.168.1.10, e um servidor HTTPS com endereço público 216.58.214.174, correspondente ao nome DNS mad01s26-in-f174.1e100.net). Responda às seguintes questões:

- **B1)** O modo de autenticação TLS visível no traço é cliente-*only*, server-*only* ou mutual cliente/server? Porquê?
- **B2)** Que porto TCP está a ser usado pelo cliente para enviar records TLS (*Record Layer Protocol*) no protocolo TLS ?
- **B3)** Após qual dos pacotes no traço indicado o servidor já calculou a chave de sessão e está apto a receber records RLP cifrados enviados pelo cliente ? Porquê ?
- **B4)** Sabendo que o detalhe da mensagem trocada no instante ... 14.495544 é a que consta no anexo, diga qual a *ciphersuite* que vai ser adoptada pelo cliente e servidor neste *handshake* e qual a chave de sessão que no final irá suportar a troca de mensagens do protocolo HTTPS. Justifique.

d) No *handshake* TLS um dos elementos determinantes da complexidade computacional imposta aos *endpoints* é a necessidade de computações envolvendo exponenciais modulares (ou exponenciais-módulo), com números de grande dimensão (conforme as dimensões de chaves envolvidas).

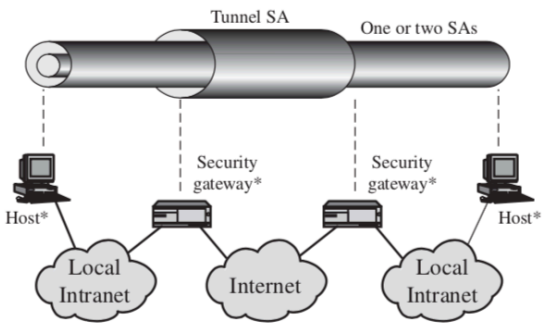
De acordo com o *handshake*, quantas exponenciais modulares foram feitas pelo cliente e pelo servidor, para concluírem o *handshake*? Justifique.

e) Porque é que no processamento TLS (ao nível do subprotocolo RLP – *Record Layer Protocol*) a compressão (que é opcional) é feita na ordem estipulada e não pode ser aplicada após o cálculo da prova de autenticidade e integridade com MAC ? Justifique.



Questão 10.

a) Tenha em conta uma parametrização para *bundling* de associações de segurança (SAs) em IPSec com sobreposição de modo túnel iterado (iterated tunneling) e modo transporte, como se representa na figura. Os dois hosts representados possuem uma ligação IPSec em modo transporte, usando ESP só com encriptação no layer interior e AH no layer exterior. Para o túnel entre gateways usa-se ESP com autenticação e encriptação, como forma de reforçar a proteção contra Traffic-Confidentilaity ao nível do encaminhamento Internet. Para lá da proteção desta forma de bundling vê algum inconveniente nesta utilização, tendo em vista que está a usar gateways que implementam firewalls e detecção de intrusões com filtragem de tráfego susceptível de transportar vetores de ataque? Argumente.



b) Em teoria, é possível usar *IPSec bundling* combinando os protocolos AH e ESP num mesmo fluxo *end-to-end*. No entanto, combinando esses dois protocolos apenas uma dada ordem na forma de processar o *bundling* pode fazer sentido: processar ESP antes do AH no envio de pacotes. Porquê ?

Dica: analise a ordem de modo a que se garantam as condições de segurança associadas e tendo em conta que pode ser importante facilitar a detecção rápida, pelo receptor, de possíveis ataques de replaying ou de envio de pacotes "bogus". Tenha em conta a mitigação pelo receptor de ataques de negação de serviço, bem como permitir que o processamento do receptor possa ser o mas otimizado possível do ponto de vista de performance.

Questão 11.

a) Como é sabido, existe nos sistemas UNIX um utilizador com nome *root*; processos associados a este utilizador têm todos os privilégios; processos pertencentes a outros utilizadores têm muito menos privilégios. Quais são os perigos associados a esta situação e diga, justificadamente se, ou em que condições, o princípio dos mínimos privilégios é neste caso aplicado.

b) Como é que faria para estabelecer permissões para um dado programa executável que lhe pertence como utilizador com *uid*=120 e *username* u, pudesse ser executado com os privilégios efetivos desse utilizador uma vez mandado executar pelo utilizador com *uid*=130 e *username* alice. Explique que tipo de mecanismo de permissões usaria e o que deveria fazer para o fim pretendido.