DI/FCT/UNL - Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores - 1º Semestre, 2019/2020
Teste de frequência nº 2 (9/Dezembro/2019)

T2A001209 - PARTE I Sem Consulta

Questão 1

Considere o contexto e definições da *framework* X.800, nomeadamente a tipologia de ataques (passivos e ativos) bem como propriedades, mecanismos e serviços de segurança. Considere por outro lado a proteção que é assegurada pelas soluções ***IPSec*** e ***TLS***.

Preencha a seguinte tabela colocando ***V***, ***X*** ou ***P*** nas células em que considera ter as garantias de proteção indicadas nas linhas, com o seguinte significado:

V: A proteção indicada é garantida

X: A proteção indicada não é garantida

P: A proteção indicada é parcialmente garantida, dependendo das condições de configuração ou parametrização

A pergunta não carece de justificações mas se entender que alguma clarificação seja útil para justificar algum critério na sua seleção, pode complementar a sua resposta com essa justificação.

Questão 2

Considere que se tem uma ***VPN*** para suportar acessos de uma rede sem fios doméstica (suportada em ***WLAN IEEE 802.11g***) onde se suporta ***IPv4*** com endereçamento privado (ex., 192,168.1.0/24 ou *mask* 255.255.255.0). A ***VPN*** será usada para aceder a uma rede IP institucional que usa internamente endereços privados ***IPv4***.

Para suportar a ***VPN*** utilizar-se-á ***IPSec*** em modo túnel. A ideia é que o túnel possa ser utilizado entre qualquer dispositivo wireless da rede doméstica (ex., computadores, *tablets* ou *smartphones*), através do *router* wireless doméstico com acesso à *Internet* e do *router* de acesso I*nternet* da instituição.

Nas ligações *Internet* os *routers* usarão endereçamento público ***IPv6*** e encaminhamento de pacotes ***IPv6***.

a) Se a ideia for garantir autenticação, confidencialidade, integridade e privacidade de todos os pacotes IPV4 enviados pelo túnel, qual deverá ser o subprotocolo da pilha *IPSec* que deve ser estabelecido para suportar o túnel ? Justifique.

b) Quantas associações de segurança são precisas para suportar o túnel e o tráfego *inbound*/*outbnoud* em cada *router*? Justifique.

c) Numa solução como a que se preconiza em a) indique, justificando, como considera estar protegido o tráfego internet na interligação dos dois *routers*:

C1) confidencialidade, autenticação e integridade de pacotes mas não confidencialidade do tráfego

C2) confidencialidade, autenticação e integridade de pacotes e confidencialidade parcial de tráfego

C3) confidencialidade, autenticação e integridade de pacotes e confidencialidade completa de tráfego

d) No suporte da referida ***VPN***, poderia ainda usar-se uma solução de túnel iterado. Para o túnel iterado faria sentido usar o subprotocolo ***IPSec AH*** ? Justifique a resposta com base no que se acrescentaria em termos de propriedades de segurança, a partir do que indicou em a).

Questão 3

a) Considerando um atacante do tipo *homem-no-meio* num canal TLS (seja suportado em UDP, seja suportado em TCP) e que foi estabelecido entre dois *endpoints*. Porque é que não será possível a esse atacante desencadear ataques do tipo *message replaying* ou desordenação de pacotes IP, segmentos TCP ou *datagramas* UDP que suportam a comunicação? Justifique a resposta discutindo que mecanismos evitam esse ataque e porque é que não é possível ao atacante contrariar essa defesa, independentemente da parametrização do *handshake* TLS ser feito com autenticação mútua ou unilateral.

b) Na negociação clienet/servidor (*handshake*) ***TLSv1.3***, comparativamente às versões anteriores em uso (***TLSv1.1*** e ***TLSv1.2***), são evitadas ou descartadas da negociação as *ciphersuites* que não envolvam negociação de chaves simétricas de sessão usando o método *Diffie-Hellman* em modo efémero, com assinaturas de curva elíptica calculando assinaturas RSA ou DSA). Este é o caso das seguintes que se ilustram como exemplo, entre outras (neste caso impressas a partir da ferramenta ***openssl***):

```
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-
POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384
```

Esta decisão torna obsoletas as assinaturas RSA com *padding* PKCS#1 ou PSS, mesmo que usando chaves muito grandes (2048 ou 4096 bits), que não estejam associadas assinaturas de números públicos Diffie Hellman.

Questão: Que racional encontra para explicar esse reforço do TLSv1.3 ? Argumente.

T2A001209 - PARTE II Com Consulta

Questão 4

Estava a usar-se o protocolo *Neuman-Stubblebine* com cifras simétricas, de modo a estabelecer uma *ciphersuite* para propriedades de segurança de um canal entre dois *peers* A e B, suportado em transporte TCP.

A *ciphersuite* requerida usa cifras AES com chave de sessão *Ks* de 256 bits, *padding* PKCS#7 e modo *GCM*, adopta sínteses *SHA-256* e autenticadores *HMAC* com base em sínteses *SHA-512*, usando por sua vez chaves *Kmac* geradas a partir da síntese *SHA-512* do resultado XOR das duas meias partes (128 bits) da chave *Ks*. Suponha que uma vez estabelecidos os parâmetros de segurança, o canal será usado por A e B corretamente com as anteriores construções criptográficas, para garantir propriedades de autenticação, integridade e confidencialidade de mensagens (ou seja dos segmentos TCP trocados e respetivos *payloads)*.

Como sabe o protocolo *Neuman Stubblebine* utiliza um KDC (*Key Distribution Center*) com chaves mestras pré-partilhadas entre o KDC e cada *Peer* (A, B, ... etc), usando apenas criptografia simétrica. No entanto houve uma evolução na infraestrutura e passou-se a dispor de uma solução *PKI*. A e B têm agora certificados de chave pública (chaves RSA) emitidos numa cadeia de certificação X509v3, sendo a raiz de confiança nessas cadeias correspondente a um certificado de autoridade da PKI, confiável por A, B e todos os outros *Peers*.

Revisitando o protocolo *Neuman-Stubblebine* e beneficiando da PKI podemos agora evitar as mensagens das duas rondas iniciais (para além da mensagem inicial de intenção de A em interagir com B) e alcançar as mesmas garantias, apenas modificando a partir da terceira mensagem. Deste modo podem manter-se as propriedades de segurança requeridas para o canal mas apenas "pagando-se o custo de latência" de no máximo 1 *RTT* entre A e B. Além disso, as garantias de segurança podem ainda ser reforçadas com autenticação mútua, *peer-authentication*, independência de sincronização de relógios e garantia de segurança futura e passada perfeitas, desde que a nova solução obtida pela evolução do anterior modelo *Neuman Stubblebine* for bem desenhada.

Proponha uma solução para alcançar estas vantagens. Concentre-se na última mensagem / última ronda Neuman-Stubblebine), já que se deverão descartar as duas primeiras mensagens do protocolo original. Apresente a sua proposta de protocolo num diagrama temporal de sequência, legendando de forma clara as construções criptográficas usadas nas partes das mensagens que seriam necessárias.

Questão 5

Considere o protocolo *handshake* TLS (tendo em conta as mensagens trocadas entre o cliente e o servidor e as quatro fases em que decorre o protocolo até ao estabelecimento da sessão TLS e suas associações de segurança.

a) Em que circunstâncias o servidor não envia no *handshake* na fase 2 os seus certificados ao cliente?

b) Em que circunstâncias o cliente pode enviar a mensagem *cliente-key-exchange* sem que necessite de enviar antes o seu certificado na fase 3?

c) Nas condições de b) e se estiver a ser usado *Ephemeral Diffie-Hellman* (como método para estabelecimento da chave de sessão), que garantias de autenticidade pode o servidor esperar dos números públicos DH enviados pelos clientes ? Isso reduz de alguma forma a segurança do acordo DH e consequente geração da chave de sessão ? Argumente.

d) Em que fase (1,2,3,4) e em que mensagem do protocolo *handshake* envia o servidor ao cliente o número público de DH que gerou, no caso de se estar a usar EPHEMERAL-DIFFIE-HELLMAN ?

e) Um *endpoint* que atua como servidor no *handshake* TLS, tem que atuar necessariamente como servidor que atende a conexão TCP (num *socket*) quando se está a suportar TLS/TCP. Verdadeiro ou Falso ? Justifique.

Questão 6

a) Considere o processamento do protocolo IPSec num fluxo unidirecional entre um emissor e um receptor de mensagens (em pacotes) IPSec. Nas entradas de definição da *Security Policy Database* do receptor, o protocolo UDP no acesso ao porto 500 (que suporta o protocolo IKE) deve estar sempre associado a uma ação BYPASS. Porquê ?

b) No mecanismo de proteção contra *replaying* usado pelo IPSec, o que acha ser determinante no dimensionamento adequado da janela deslizante do controlo feito pelo receptor? São as falhas na transmissão de pacotes IP encaminhados entre o emissor e receptor ou a probabilidade de desordenação dos pacotes IPSec enviados e recebidos ? Justifique.

Questão 7

a) Como é que se pode suportar a utilização de IPSec em modo transporte *end-to-end* (usando ESP com autenticação e confidencialidade) para suportar segurança do tráfego entre clientes remotos (emissores de pacotes IP) e recursos na rede de uma organização (servidores ou receptores de pacotes IP) que apenas usam endereços privados ? Justifique.

b) Sendo possível usar a solução que propõe em *a)*, considera que essa solução é interessante para uma organização que implementa mecanismos de defesa de perímetro para detecção e prevenção de intrusões para filtrar a possível injeção de conteúdos ou código malicioso que possam viajar como *payloads* dos pacotes IPSec ? Justifique.

c) De acordo com as suas observações em *b)*, que outro tipo de configuração é mais indicada para a proteção da referida organização e recursos disponibilizados ? Configurações iPSec com combinações de associações de segurança em túneis iterados ou combinação com asso