	Departamento de Informática Faculdade de Ciências e Tecnologia UNIVERSIDADE NOVA DE LISBOA

Mestrado em Engenharia Informática

Segurança em Sistemas Informáticos Distribuídos

2º Semestre 2005/2006

Avaliação de Conhecimentos (Exame – Época Normal, 5/Julho/2006)

Notas:

- O enunciado tem 5 questões, divididas em duas partes:
  - **Parte sem consulta** (Questão 1): 45 min
  - **Parte com consulta** (Questão 2) : 45 min
- Leia completamente e com atenção cada questão antes de responder. A interpretação do enunciado é um factor de avaliação.

---------- A preencher pelos alunos ----------

Nº de aluno: _____ Nome: _____

Nº Total de páginas entregues: _____ (numere as páginas na forma Pág / TOTAL)

Classificação (a preencher pelo docente):

PARTE 1 (sem consulta)	**PARTE 2 (com consulta)**

1)	**2)**	**3) TP3**
a)	a)	a)
b)	b)	b)
c)	c)	
d)	d)	
e)	e)	
f)	f)	

Questão 1)

a) Os serviços de segurança suportados ao nível IPSEC abarcam as seguintes dimensões ou propriedades de segurança:

- S1 - Controlo de Acessos
- S2 - Autenticação da Origem dos Dados
- S3 - Integridade sem orientação para conexão (ou connectionless integrity)
- S4 - Rejeição ou descarte de pacotes com retransmissão ilegal (para protecção de replying ou como forma de prevenção contra integridade de sequência parcial)
- S5 - Confidencialidade dos pacotes IP
- S6 - Confidencialidade limitada de fluxos de tráfego IP

Estes serviços são suportados por cada um dos sub-protocolos ou serviços especializados que constituem a pilha IPSec, protocolo AH e as variantes do protocolo ESP. Organize um quadro em que refira quais dos serviços acima são suportados por cada uma destes protocolos (ex: serviços S1, S2, ... etc nas colunas e protocolos e variantes nas linhas).

b) Uma associação de segurança IPSec é unicamente identificada por três parâmetros principais: um índice de parâmetros de segurança, o endereço IP destino e um identificador de protocolo. Qual o significado de cada um destes parâmetros

c) Indique que tipo de parâmetros adicionais (tentando enumerá-los o mais completamente possível) fazem parte de uma associação de segurança em IPSec. Tente indicar para cada um deles um breve resumo do seu significado e objectivo em termos de controlo de processamento IPSec

d) Indique se a seguintes afirmações são VERDADEIRAS ou FALSAS e justifique a sua resposta adequadamente.

D1) "Em IPSec podem usar-se dois modos, designados respectivamente por modo transporte e por modo túnel. Quando se usa o modo túnel (numa SA em modo túnel) não se pode usar o modo ESP pois este modo origina que todo o pacote IP interno do encapsulamento IP/IP é totalmente cifrado".

D2) "Quando se usa o protocolo AH no modo transporte (numa SA em modo transporte), apenas a carga ou payload de cada pacote IP são protegidos do ponto de vista de autenticação com base em HMACs (sejam HMAC-MD5-96 ou HMAC-SHA-1-96)

e) Em ESP está normalizado o uso de *padding*, incluindo-se no pacote ESP um campo com o tamanho do padding adicionado. No entanto, no AH não existe esse suporte. Porque é que esse suporet existe no ESP e não no AH ? Justifique.

f) Diga em que consistem as noções de *Iterated Tunneling* (ou modo túnel iterado) e *Transport Adjacency* (ou adjacência em modo transporte) e discuta como podem as duas noções serem combinadas, com que vantagens ou desvantagens.

Questão 2

a) Em ESP está normalizado o uso de *padding* garantindo-se que:

- Um algoritmo de cifra pode requerer que um pacote total (*plaintext*) tenha que ser múltiplo do bloco básico de cifra desse algoritmo;
- O tamanho de todo um pacote ESP seja sempre múltiplo de 32 bits (pressupondo-se que o tamanho do *padding* efectivamente usado seja indicado num campo *PAD Length* de16 bits e o campo "*Next Header*" tenha igualmente 16 bits.

Dado que existe o campo PAD Length, podem ter-se diferentes dimensões de *padding* dado um mesmo pacote ESP. Que interesse há nisso ?

b) Os campos potencialmente mutáveis do cabeçalho de um pacote IP que viaja através da Internet não são sujeitos a autenticação e teste de integridade por parte do protocolo AH da pilha IPSec. Na verdade apenas são processados para efeitos de autenticação em AH, os campos do cabeçalho do próprio AH e alguns campos (considerados imutáveis) do cabeçalho do pacote IP que se pretende autenticar. Por exemplo, em IPV4, os campos TYPE OF SERVICE, FLAGS, FRAGMENT OFFSET, TTL e HEADER CHECKSUM são considerados para efeitos de autenticação com AH. Também o campo PAYLOAD LENGHT do cabeçalho AH é sujeito a autenticação.

Ora, acontece que um pacote IP pode eventualmente ser sujeito a fragmentação durante o seu encaminhamento. Tal obriga a que quer a informação FRAGMENT OFFSET (do cabeçalho IPV4) quer a informação PAYLOAD LENGTH (do AH) podem ter que ser modificados durante o encaminhamento do pacote.

Isso constitui algum obstáculo ao uso do protocolo AH em relação ao processamento de autenticação de pacotes genéricos IP em IPSec ? Justifique adequadamente a sua resposta.

c) Existe algum problema em considerar o endereço IP destino de um pacote IP como um dos campos imutáveis que deve ser incluído na computação de autenticação e integridade de um pacote IP em IPSec (AH) ? Se sim, como se suporte a possibilidade de o IPSec (AH) funcionar bem mesmo quando há possibilidade de se usar *source-routing* em IPV4ou IPV6 em qualquer um dos nós de encaminhamento **?**

d) Suponha que numa aplicação cliente/servidor, um host H1 está a enviar mensagens TCP ao host H2. H1 e H2 estão a usar IPSec. A aplicação em H2, que estava à espera de uma mensagem de ACK após o envio de uma mensagem M1 para H1 não recebeu esse ACK num certo tempo (time-out definido na aplicação). Essa aplicação foi programada para que, neste caso, a reenvia a mensagem M1 a H1 esperando novamente por novo ACK. A

implementação de IPSec de H1 deverá detectar alguma retransmissão do pacote IPSec que transporta essa mensagem TCP como potencial duplicado **?**

Discuta a resposta no caso de H1 e H2 estarem a usar AH ou ESP nas suas associações de segurança IPSec

e) Suponha que no protocolo IPSec era o transmissor a assignar o SPI (*Security Parameter Index*) a uma SA e não o receptor, como está definido. Isto seria mais, menos ou igualmente adequado ? Justifique eventuais vantagens ou desvantagens que esta opção implicava.

f) Que vantagens ou desvantagens encontra em usar IPSec em modo transporte ou em modo túnel no caso de ter sob sua responsabilidade uma infra-estrutura de rede ligada à Internet através de uma Firewall. Suponha que o sistema Firewall que vai usar possui suporte para NAT e é encadeado com um sistema que detecta e filtra a entrada de vírus embebidos no protocolo HTTP e SMTP, sendo esses os únicos protocolos associados ao tráfego que atravessam a Firewall, de fora (Internet) para dentro da sua organização. Suponha ainda que nessa organização você não controla os computadores que funcionam como postos de trabalho, e a gestão destes (configurações, sistemas operativos e sua instalação, *patching*, instalação de aplicações ou auditoria) estão fora do âmbito da sua responsabilidade ou controlo.