



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

Licenciatura em Engenharia Informática  
Mestrado em Engenharia Informática  
**Segurança em Sistemas Informáticos Distribuídos**  
**1º Semestre 2006/2007**  
Prova de Exame / Época de Recurso (10/2/07)

Notas:

O enunciado tem 3 questões, divididas em duas partes:

- Parte sem consulta (Parte I, Questão 1): até 60 min
- Parte com consulta (Parte II, Questões 2 e 3): até 90 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: \_\_\_\_\_

Numere as folhas na forma Nº / TOTAL e coloque em cada uma o seu nome e apelido

Nº Total de FOLHAS entregues sem contar com esta capa: \_\_\_\_\_

Classificação (a preencher pelo docente):

PARTE 1 (s/consulta)	PARTE 2 (com consulta)
-------------------------	---------------------------

1)	2)	3)
a)	a)	
b)	b)	
c)	c)	
d)	d)	
e)	e)	

## Parte I

### Questão 1

- a) Que serviços e propriedades de segurança são suportados por cada um dos sub-protocolos AH, ESP da pilha IPSec nas suas diferentes variantes de uso ?
- b) Explique a diferença entre as noções de adjacência de transporte (ou *Transport Adjacency*) e de túneis iterados (ou *Iterated Tunneling*) ao nível do suporte de associações de segurança em IPSec.
- c) Explique a diferença dos papéis e funcionalidades subjacentes aos protocolos Oakley e ISAKMP na problemática da distribuição segura de chaves para associações IPSec.
- d) Indique o tipo de parâmetros que identificam as associações de segurança no contexto de suporte de IPSec na ligação entre dois Hosts A e B, quando ambos actuam como emissores e receptores de mensagens. Os parâmetros que indicou têm que ser os mesmos nos dois computadores ? Quantas associações de segurança IPSec têm que estar definidas em cada um dos hosts mencionados?
- e) Na discussão do processamento do sub-protocolo AH da pilha IPSec, alguns dos campos de cabeçalho dos pacotes IP (seja IPV4 ou IPV6) não podem ser incluídos na autenticação abrangida por MACs para cálculo de verificação de autenticação e de integridade.

**A1)** Indique que campos devem ser considerados com valor 0 e porquê quando se tratarem de cabeçalhos IPV4. Justifique.

**A2)** Idem, no caso de cabeçalhos IPV6

**A3)** Idem, para campos de extensão do protocolo IPV6.

## Questão 2

- a) Considere o protocolo IPSec tal como a norma define a criação de SAs e a associação de SPIs a essas SAs. Que implicações haveria em que fosse o emissor a *assignar* (inicializar e propor) o parâmetro SPI e não o receptor ? Considera que isso teria vantagens ou desvantagens ? Porquê ?
- b) Suponha que trabalha na equipa de segurança de infraestruturas TCP/IP de uma organização. Suponha que se pretende usar nessa organização IPSec em modo transporte para permitir acessos remotos (suportados em IPSec) entre computadores pessoais de utilizadores que trabalham em casa (ex., em teletrabalho) e que precisam de aceder por uma VPN (IP/IPSec) directamente a um servidor de partilha de ficheiros na intranet dessa organização. Antes que uma tal solução fosse instalada, que considerações faria para se opor a uma tal solução em favor de uma solução baseada em IPSec em modo túnel.
- c) A autenticação extremo-a-extremo e a confidencialidade, são propriedades de segurança suportadas entre dois computadores comunicando com base no suporte IPSec. Apresente e legende de forma clara figuras, usando uma representação nos moldes semelhantes ao tipo de representação que o autor W. Stallings utiliza na bibliografia de base da disciplina, para ilustrar o uso de combinações possíveis de SAs ou associações de segurança IPSec. As suas figuras, legendas ou textos auxiliares de explicação das figuras devem clarificar como se suportam as seguintes combinações de SAs:
  - B1)** Adjacência de Transporte com Confidencialidade aplicada de forma prévia à Autenticação
  - B2)** Uma associação de segurança de Transporte combinada com Túnel, com autenticação aplicada de forma prévia à confidencialidade
- d) Na arquitectura IPSec, quando duas SAs em modo Transporte são combinadas de forma a permitirem o suporte dos sub-protocolos AH e ESP no mesmo fluxo de dados extremo-a-extremo, deve-se sempre aplicar confidencialidade (ESP e cifra dos dados) antes da prova de autenticação (processamento AH). Porque é que isto parece ser recomendável e não o inverso ? Justifique adequadamente a sua resposta.
- e) Considere o estabelecimento de chaves segundo o protocolo Oakley numa troca de chaves no modo tipo agressivo. Indique quais os parâmetros de cada mensagem e em que campos da carga ISAKMP esses parâmetros são colocados.

*Sugestão:* Represente primeiro a troca de chaves Oakley no modo agressivo e, para cada parâmetro, das mensagens representadas, diga em que campo do formato ISAKMP são esses parâmetros colocados.