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 Normal (Teste Nº 3, 16/01/07)

Notas:
O enunciado tem 3 questões, divididas em duas partes:

- Parte sem consulta (Parrte 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) Apresente os modos de funcionamento que conhece em que pode operar o protocolo IPSec. Ilustre ou represente um ou mais cenários de rede e explique nos cenários representados as diferenças entre esses modos.

b) 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 ?

c) Que tipos diferentes de certificados de autenticidade podem ser usados entre *endpoints* IPSec no tipo de carga de certificados no formato ISAKMP (ou formato de pacotes ISAKMP), de modo a estabelecerem autenticação mútua ?

d) 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 segurana em IPSec.

e) Explique a diferença dos papéis associados aos protocolos Oakley e ISAKMP na problemática da distribuição segura de chaves para associações IPSec.

f) 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?

Questão 2

a) 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 os campos que devem ser considerados com valor 0 (por serem considerados mutáveis) e os campos que podem entrar com o valor que possuírem em cadacaso, nas verificações de autenticidade e integridade, quando se tratarem de cabeçalhos IPV4. Justifique.
A2) Idem, no caso de cabeçalhos IPV6
A3) Idem, para campos de extensão do protocolo IPV6.

b) 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 ?

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.

Questão 3 A)
Sobre o Protocolo WHOPAY

a) Explique qual o princípio de funcionamento das assinaturas de grupo tal como são usadas pelos autores no âmbito do protocolo WHOPAY. Na síntese que elaborar para esta resposta, deve ficar claro qual o objectivo de uso desse tipo de assinaturas neste protocolo.
b) No caso do protocolo WHOPAY diga se considera que a propriedade de anonimato de utilizadores é integralmente garantida. Justifique adequadamente a sua resposta.

Questão 3 B) Sobre Segurança em comunicação multiponto (Secure Multicast Communication)

a) Quais as diferenças principais que caracterizam as diferentes abordagens de autenticação e distribuição de chaves em grupo, nomeadamente na sua caracterização segundo a tipologia seguinte. Apresente uma representação de diversos nós correspondentes a grupos de processos envolvidos num protocolo de comunicação em grupo (multiponto) para cada uma das tipologias.

i) Arquitecturas Centralizadas
ii) Arquitecturas Descentralizadas
iii) Arquitecturas Distribuídas