

NOME DO PROFESSOR(A)
Frederico Sauer

DISCIPLINA
Redes sem-fio

AValiação
AV2

DATA
26/02/2014

NOME: _____ Matrícula: _____

INSTRUÇÕES

- **Leia com atenção cada questão antes de responder**
- Tire as dúvidas no momento da leitura da prova feita pelo Professor.
- Procure rasurar o mínimo à prova e não use corretivo. Identifique as rasuras com: ANULADO
- Mediante ocorrência de “COLA”, o aluno ficará com zero na PROVA correspondente
- Favor escrever com letra legível, caso o professor não identifique a resposta, a questão será anulada.
- A revisão da prova será na próxima aula.
- **Esta folha de questões não será retornada ao aluno.**

1ª. Questão: (valor 1,0 ponto) - Assinale a alternativa CORRETA:

- A. O protocolo de segurança WEP utiliza o algoritmo RC4 com chaves de 64 ou 128 bits;
ERRADA: As chaves efetivas são de 40 ou 104 bits
- B. O protocolo de segurança WEP criptografa o vetor de inicialização usado em conjunto com a chave para criptografar o fluxo
ERRADA: O IV é enviado em claro
- C. **O protocolo de segurança WEP possibilita os modos de autenticação “Open” ou “Shared”. Em ambos não há garantias efetivas de autenticação do usuário CERTA !**
- D. Nenhuma das alternativas acima está correta
- E. Todas as alternativas acima estão corretas

2ª. Questão: (valor 1,0 ponto) - Assinale a alternativa INCORRETA:

- A. A solução de segurança proposta pelo IEEE para redes sem fio foi o 802.11i, que, dentre outras coisas, adotou o mecanismo EAP (enterprise)
CERTA !
- B. O WPA, implementação parcial do IEEE 802.11i, propôs entre outras coisas o uso do MIC (Message Integrity Code) cujo algoritmo é denominado Michael
CERTA !
- C. **Apesar de usar o mesmo tamanho de vetor de inicialização que o WEP, no WPA o mesmo é permutado aleatoriamente, impedindo a sua captura ERRADA ! O IV dobra de tamanho no WPA (48 bits)**
- D. Nenhuma das alternativas acima está incorreta
- E. Todas as alternativas acima estão incorretas

3ª. Questão: (valor 1,0 ponto) - Assinale a alternativa INCORRETA:

- A. O WPA2 tem como uma das principais diferenças para o WPA o suporte ao CCMP (AES com chaves de 128, 192 ou 256 bits)
CERTA !
- B. No WPA2 podem ser usadas chaves compartilhadas ou o uso de um login e senha para cada usuário diferente (802.1x – EAP)
CERTA !
- C. O WPA2 cumpre todas as especificações do 802.11i
CERTA !
- D. **Nenhuma das alternativas acima está incorreta**
- E. Todas as alternativas acima estão incorretas

NOME DO PROFESSOR(A)
Frederico SauerDISCIPLINA
Redes sem-fioAVALIAÇÃO
AV2DATA
26/02/2014

NOME: _____ Matrícula: _____

4ª. Questão: (valor 1,0 ponto) - Assinale a alternativa CORRETA:

- A. O principal problema de segurança do WEP está na facilidade de se quebrar a chave, seja por bruta força ou por análise estatística;
CERTA !
- B. O protocolo WEP usa vetores de inicialização que, além de serem transmitidos em claro, repetem-se rapidamente em função de seu tamanho pequeno
CERTA !
- C. O protocolo WPA introduziu maior robustez nas redes sem fio, direcionando esforços para corrigir os problemas do WEP, como a facilidade de quebrar a chave e a dificuldade de garantir integridade das mensagens
CERTA !
- D. Nenhuma das alternativas acima está correta
- E. **Todas as alternativas acima estão corretas**

5ª. Questão: (valor 3,0 pontos)

Correlacione as colunas

A	Protocolo de segurança que usa o RC4 com chaves temporárias	(B)	WPA2
B	Protocolo que usa modos de operação CBC ou CTR c/AES	(A)	WPA
C	Protocolo que usa o RC4 com IV de 24 bits	(C)	WEP

6ª. Questão: (valor 3,0 pontos)

Imagine o seguinte cenário: você precisa instalar uma rede sem fio na sua empresa, mas é requisito desta implementação que:

- a) Cada usuário tenha o seu próprio login/senha
- b) Os dados que trafegam na rede estejam o mais seguro possível; e
- c) Possa ser usado um algoritmo criptográfico cuja chave possa aumentar de tamanho até 256 bits. A solução mais indicada é ? (especifique a solução para AUTENTICIDADE E CONFIDENCIALIDADE)

Resposta: Confidencialidade: **AES** Autenticidade: **EAP**

Glossário:

WEP – Wired Equivalent Privacy

WPA – Wireless Protected Access

AES – Advanced Encryption Standard

IEEE – Institute of Electrical and Electronic Engineers

IV – Initialization Vector

CCMP - Counter Cipher Mode with block chaining message authentication code Protocol

EAP – Extensible Authentication Protocol

RC4 – RSA Cipher 4

CBC – Cipher Block Chaining

NOME DO PROFESSOR(A)
Frederico Sauer

DISCIPLINA
Redes sem-fio

AValiação
AV2

DATA
26/02/2014

NOME: _____ **Matrícula:** _____

CTR – Counter Mode