

Segurança Operacional

Redes sem Fio

Gustavo Vilar

- Mini – CV
 - PPF / DPF – Papiloscopista Policial Federal
 - Pós-Graduado em Docência do Ensino Superior – UFRJ
 - Graduado em Ciência da Computação e Processamento de Dados – ASPER/PB
 - Aprovações: PRF 2002, PF 2004, MPU 2010, ABIN 2010

Gustavo Vilar

- Contatos:

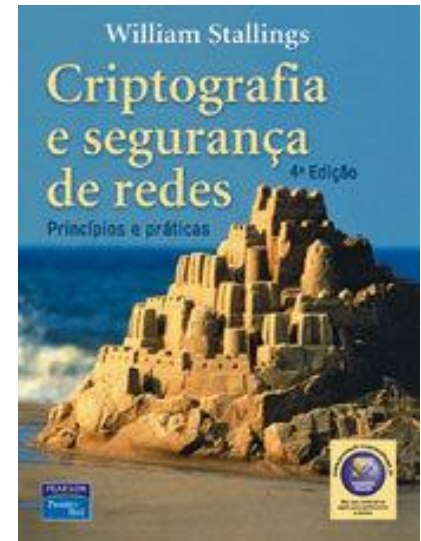
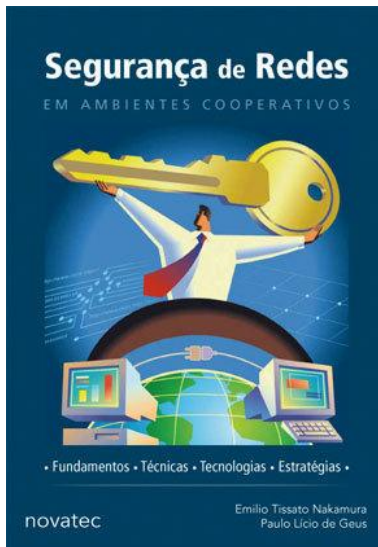
- gustavopintovilar@gmail.com
- p3r1t0f3d3r4l@yahoo.com.br



Escopo

- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais freqüentes.
- Abordar as metodologias de resolução de questões das principais bancas

Bibliografia



Segurança Operacional 03 de 03 – Carga Horária

- **10 vídeo aulas (03h47m / 00h22m40s)**

- Conceitos Iniciais, Modos Ad-hoc e PCF, Serviços, Mesh, CSMA-CA
- 802.11A, 802.11B, 802.11G, 802.11N
 - Características principais, semelhanças e diferenças entre os padrões
- WEP
 - Características, processo de cifração e decifração, fragilidades
- WPA
 - Características, inovações, pontos fracos
- WPA 2
 - Características, protocolos envolvidos
- Considerações finais sobre ambientes sem fio
- Primeira bateria de questões de aprendizagem
- Segunda bateria de questões de aprendizagem
- Terceira bateria de questões de aprendizagem



Segurança Operacional

Módulo 3 – 802.11*

Conceitos Iniciais

- Rede em que os meios de transmissão não usam cabos físicos
 - Vantagens:
 - Facilidade de conexão
 - Mobilidade
 - Flexibilidade
 - Manutenção reduzida: reduz o custo do enlace, em comparação ao custo de uma rede tradicional



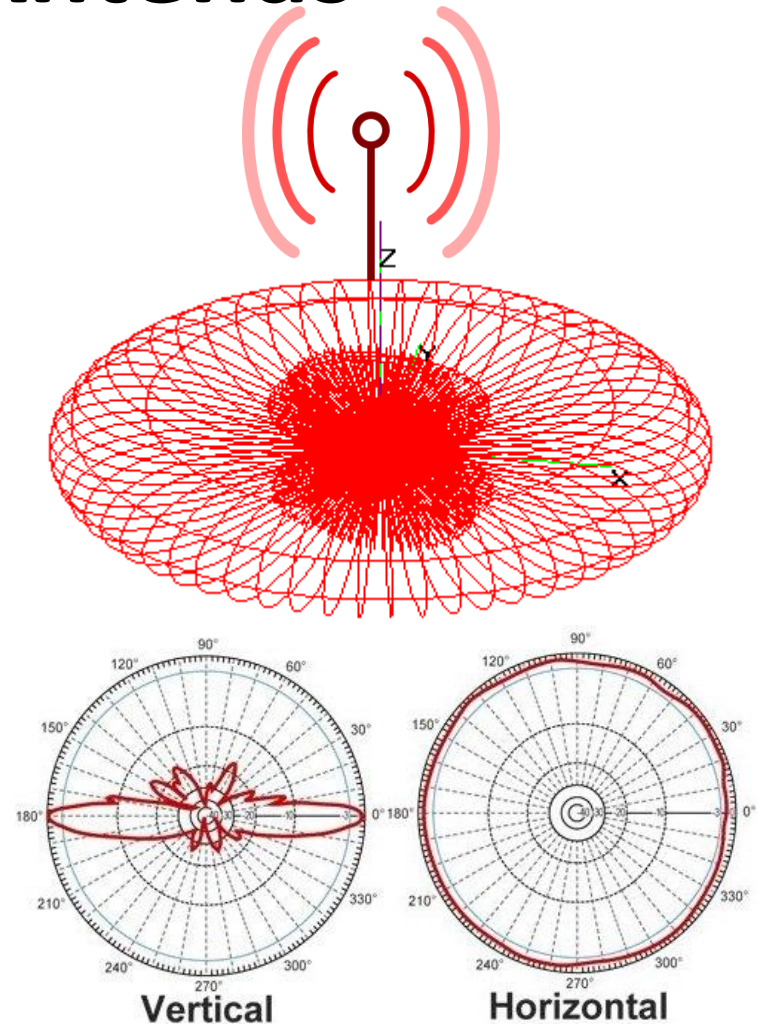
Conceitos Iniciais

- Rede em que os meios de transmissão não usam cabos físicos
 - Desvantagens:
 - Tamanho da banda
 - Interferência
 - Alcance do Sinal
 - Força do sinal decrescente
 - **Segurança**
 - Maior problema atual em redes sem fio
 - suscetível a interceptações
 - Necessidade de protocolos de segurança



Espécies de Antenas

- Omnidirecional
 - Transmitem em todas as direções (360°)
 - Ex. WiFi tradicional



Espécies de Antenas

- Setorial
 - Transmitem em uma única direção, mas com ângulo de irradiação aberto
- Ex. Celulares

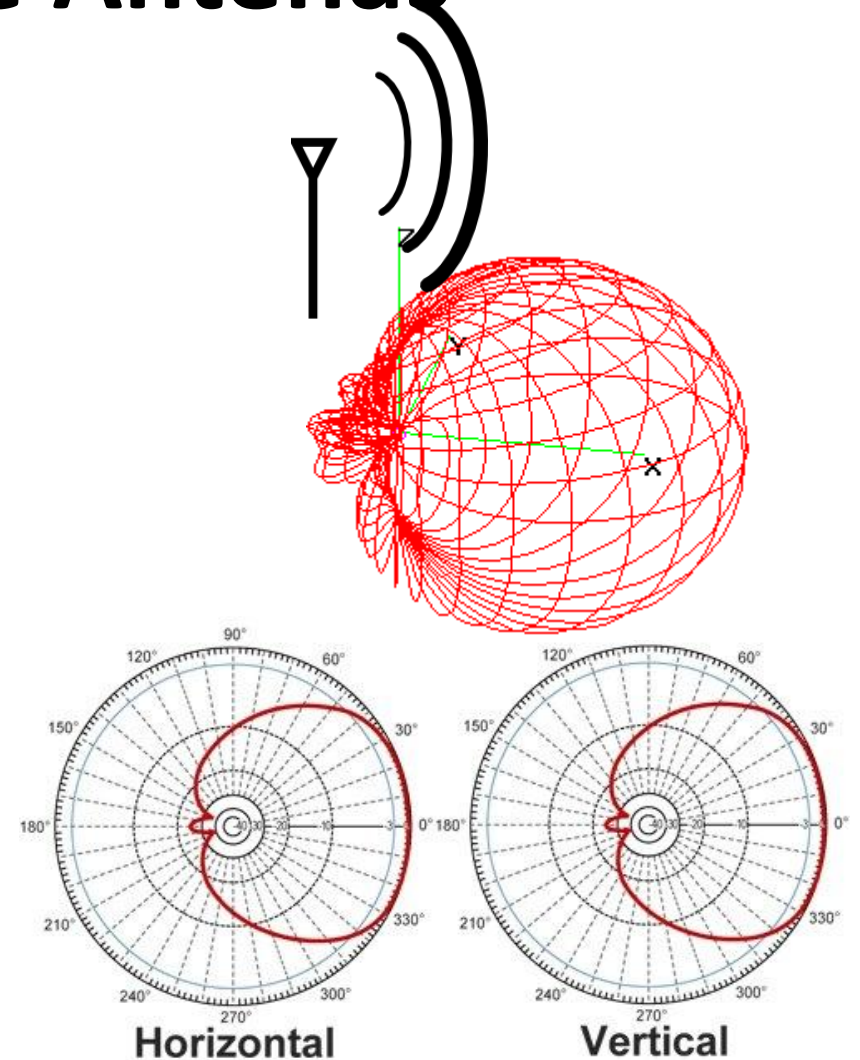


Imagem de uma antena setorial



Espécies de Antenas

- Direcional
 - Transmitem em uma única direção, com ângulo de irradiação fechado
- Ex. Parabólicas



Modos de Operação das redes Wifi

- DCF (Distributed Coordination Function)
 - *Sem estação base*
 - *Ad hoc*
 - *DCF*
 - As estações competem entre si pelo meio
 - Uso de CSMA/CA
 - Modo obrigatório



Modos de Operação das redes Wifi

— Redes Ad-hoc

- Não há controle centralizado
- Análogo à ligação direta de dois computadores com cabo crossover
- Máquinas podem se comunicar livremente, desde que dentro do alcance de sinal
- Alcance do sinal é menor, pois antenas dos dispositivos são menos potentes
- Usado apenas em redes de pequeno porte
- Conceito de IBSS (Independent)
- BSS sem um AP
- Uma das estações pode assumir a função de coordenação



Modos de Operação das redes Wifi

- PCF (Point Coordination Function)
 - *Com estação base*
 - *PCF*
 - *Opcional*
 - *sem colisão*
 - *Infraestrutura*
 - É opcional
 - AP escuta estações em turnos para verificar se há frames
 - Elimina colisões
 - Estação-base efetua o polling



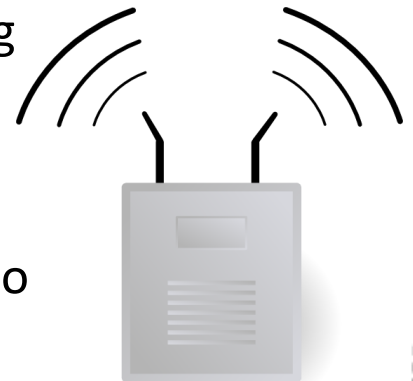
Modos de Operação das redes Wifi

- Infraestrutura
 - Utiliza dispositivos centralizadores
 - Access Points, intermedeiam as comunicações
 - Um AP é análogo a um hub sem fio



Tipos de serviços básicos - BSS

- BSA (Basic Service Area)
 - Área em que os dispositivos móveis podem comunicar
- BSS (Basic Service Set)
 - Área coberta por um AP chama-se célula, composta por BSSs
 - Basic Service Set é o conjunto de serviços básicos de uma célula
- ESS (Extended Service Set)
 - Um conjunto de BSS
 - Em uma rede ESS, é comum o acontecimento de roaming
- IBSS (Independent Basic Service Set)
 - BSS sem um AP (Redes Ad-hoc)
 - Uma das estações pode assumir a função de coordenação



Identificadores dos serviços

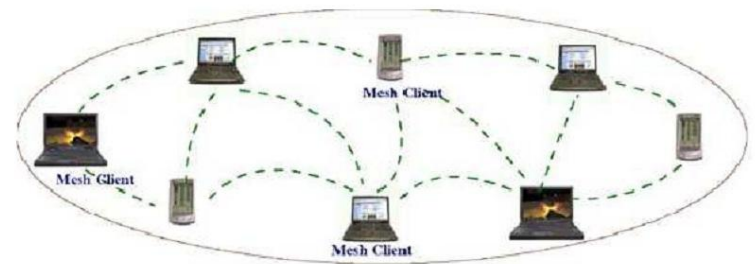
- “Identificação da rede”
- Basic Service Set Identifier (BSSID)
 - Identificador da célula. Valor é o MAC do AP
 - Composto por 12 algarismos Hexa
 - Um BSS possui um único BSSID
- Service Set Identifier (SSID)
 - Nome da rede, com caracteres alfanuméricos e tamanho máximo de 32 caracteres
 - Uma rede possui um único SSID, Mesmo que possua mais de um AP (ESS) - Extended Service Set



Especializações de redes Wifi

- Redes Mesh

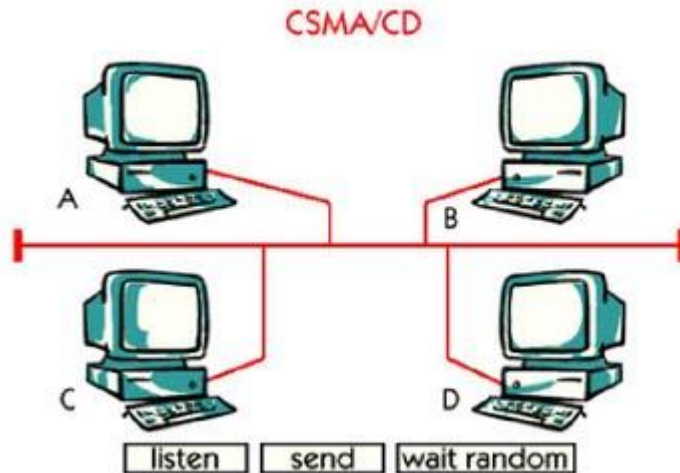
- Tipo de rede Ad-hoc em que os nós são fixos
- Protocolos em uso devem aproveitar a não mobilidade dos nós
- Limitado a curtas distâncias
- Nós afastados tem performance pior



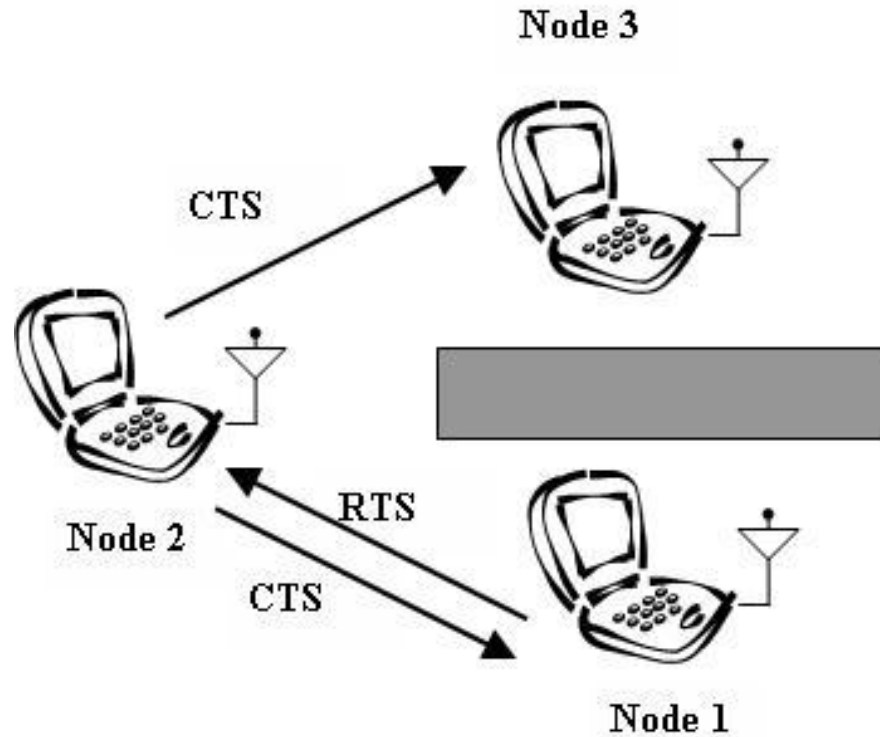
Métodos de acesso ao meio – CSMA/CA

- Dispositivo “escuta” o meio e...
 - Se o meio estiver livre por tempo determinado (DIFS) ; transmite;
 - Senão backoff
- Tempo de backoff é randômico, para evitar colisões
- Uso de ACK para verificar entrega
- Todo quadro deve ser confirmado
- Prevenção de colisão
- Operação atômica

Métodos de acesso ao meio – CSMA/CD X CSMA/CA



Entendendo o CTS/RTS



Padrão 802.11a

- Opera na faixa de frequência 5 GHz
 - Maior perda de sinal a 5 GHz porque a esta frequência o sinal é absorvido com mais facilidade
 - Alcance mais curto
 - Taxa de transmissão teórica: 54 Mbps
 - Taxa real é menor, perto da metade
 - 64 utilizadores por Ponto de Acesso (AP)
 - incompatibilidade com os padrões no que diz respeito a Access Points
- 802.11 b e g,
- Menos suscetível a interferência do meio porque a frequência é usada por poucos aparelhos
 - Necessário mais energia a 5 GHz (bateria)
 - Opera em SHF e não UHF como os demais padrões de wi-fi

Padrão 802.11b

- Opera na faixa de frequência 2.4 GHz
- Taxa de transmissão teórica: 11 Mbps
- 32 utilizadores por ponto de acesso
- Primeiro padrão a disseminar no Brasil
- alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz
- Alcance médio indoor: 35mt
- Muito suscetível a interferência
 - Opera na faixa de frequência de vários aparelhos
 - Bluetooth; Fornos de micro-ondas; telefones sem fio; equipamentos médicos

Padrão 802.11g

- Opera na faixa de frequência 2.4 GHz
 - 802.11 g interopera com 802.11 b
- Taxa de transmissão teórica: 54 Mbps
- Padrão mais comum na atualidade
- 32 utilizadores por ponto de acesso
- Muito suscetível a interferência
 - Mesma forma do padrão 802.11b
- Suporta comunicação com dispositivos 802.11b, com velocidade setada pelo padrão inferior
- Pode alcançar até 108Mbps com uso de compactação proprietária
- Alcance médio indoor: 25mt

Padrão 802.11n

- 2,4 GHz e/ou 5 GHz
 - Alcance 2 X maior
 - Várias antenas
 - Menos suscetível a interferência
 - 64 utilizadores por ponto de acesso
 - Padrão já definido
 - Fabricantes usaram por certo tempo draft, Atualmente existem versões comerciais operando em tais velocidades
 - 65 Mbps a 600 Mbps
 - Necessidade de atualização de firmware
 - Alcance médio aparentemente maior
- que os padrões anteriores
- Uso do MIMO (multiple-input multiple-output)
 - Diversos fluxos de transmissão: (2x2), (2x3), (3x3), (4x4)
 - Velocidade nominal subiu de 54 para 300 megabits (600 megabits nos APs 4x4, capazes de transmitir 4 fluxos simultâneos)
 - Uso de múltiplos fluxos de transmissão torna o alcance do sinal quase duas vezes maior.



WEP – Wired Equivalent Privacy

- Primeira tentativa de se criar um protocolo eficiente de proteção de redes Wi-Fi
 - Tipos
 - 104 bits: soma-se a este valor os 24 bits do IV
 - 40 bits (padrão): soma-se a este valor os 24 bits do IV
- Métodos de autenticação
 - Sistema aberto
 - Chave compartilhada



WEP – Wired Equivalent Privacy

- Algoritmo Criptográfico: RC4
 - Keystream - Sequencia pseudo-aleatória
 - Mesma chave no emissor e receptor
 - RC4 não valerá para a parte da rede cabeada, somente para a rede sem fio (característica do RC4)



Pacote WEP

- Vetor de Inicialização
 - É transmitido em claro
 - Curto: 24 bits
- Key ID Byte: Key Stream
- CRC-32
 - Faz a verificação da integridade dos dados
 - A segurança sugerida não pode ser considerada segura
 - Garante integridade sob ruído

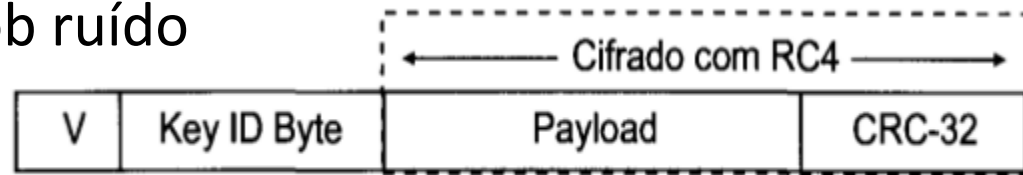
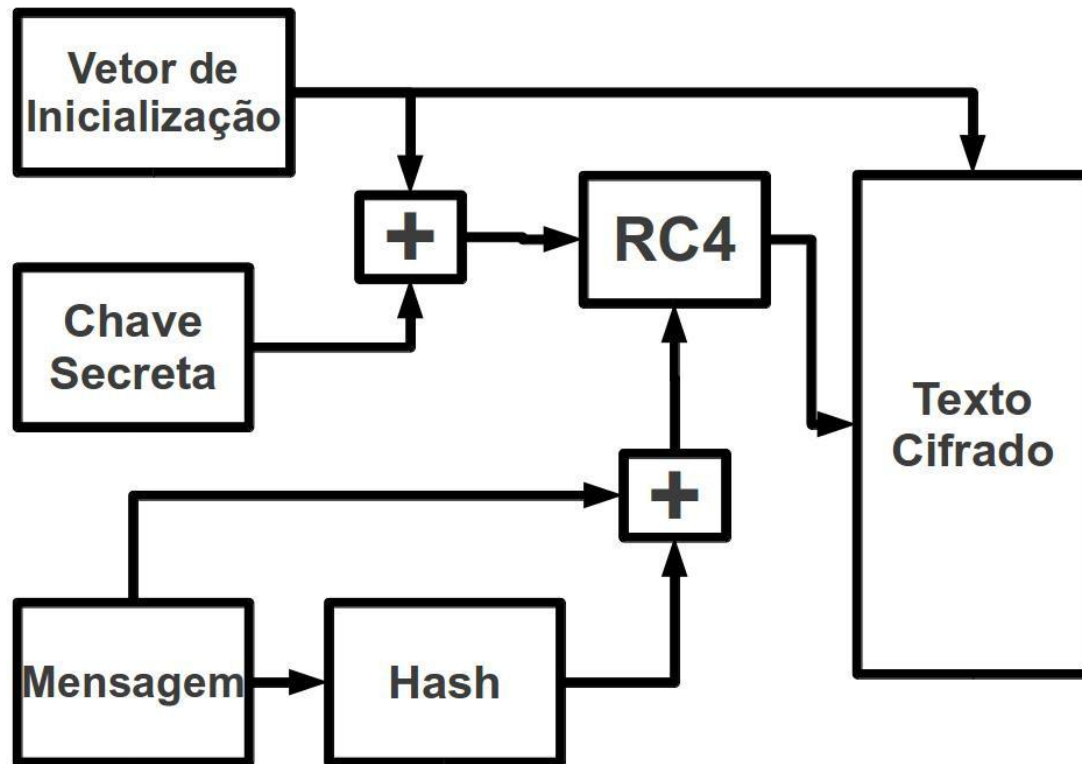


Figura 5.24 Pacote padrão IEEE 802.11.

Pacote WEP - Cifração

- Chave Secreta (K) + VI
 - Chave de 40 bits compartilhada
 - Vetor de inicialização de 24 bits diferente para cada pacote
- KVI submetido ao RC4 gerando um KEY STREAM
- Rodado o CRC-32 sobre a mensagem gerando um ICV
 - Integrity Check Value
- ICV concatenado à Mensagem
- Texto Cifrado = (Texto Claro + ICV) XOR (Key Stream)
- O Texto Cifrado é transmitido junto com o Vetor de Inicialização(que vai em claro)

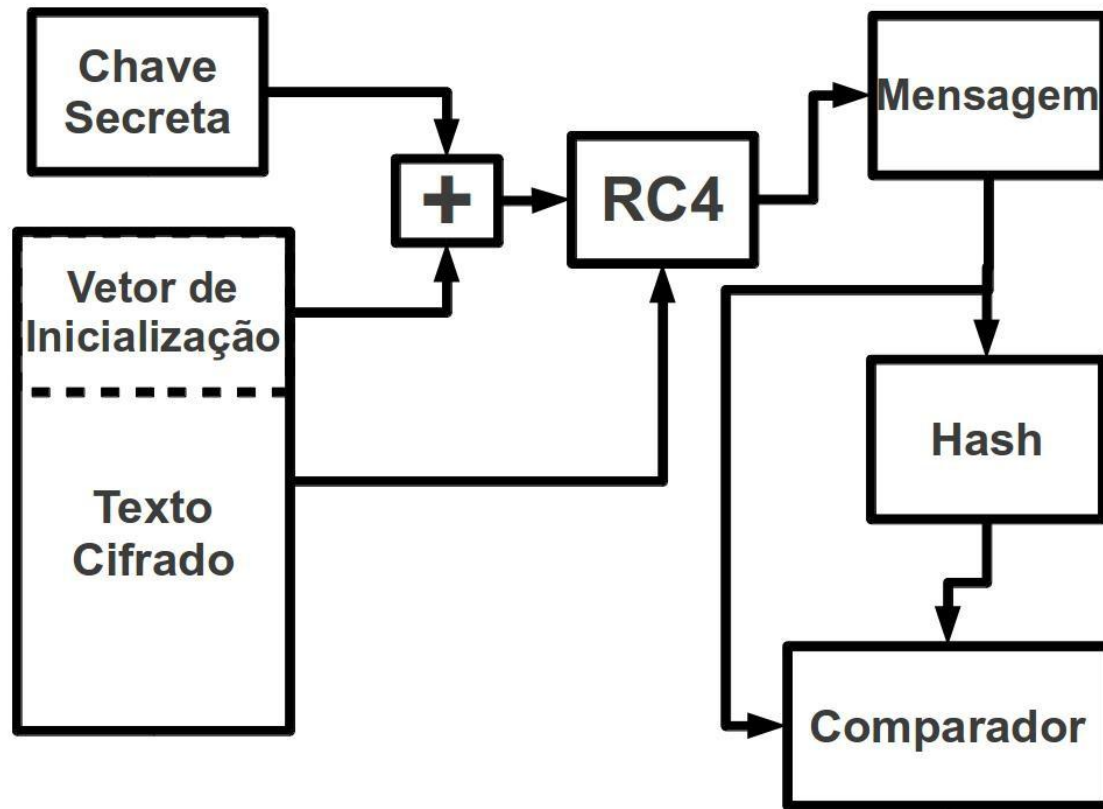
Pacote WEP - Cifração



Pacote WEP - Decifração

- Chave Secreta (K) + VI
- KVI submetido ao RC4 gerando um KEYSTREAM
- O Keystream passa por um XOR com o Texto Cifrado, para gerar o Texto Original
- É realizada a checagem da integridade do texto decifrado. gerando um novo ICV
- O ICV calculado é comparado com o ICV recebido, que estava concatenado com o texto recebido
- Se os dois ICVs forem iguais, o texto pode ser considerado íntegro.

Pacote WEP - Decifração



WEP - Vulnerabilidades

- **Vetor de Inicialização**
 - É enviado em claro
 - Seu espaço de 24 bits é relativamente curto
 - Vetores voltam aos seus valores iniciais quando uma placa é reinicializada (aumentando as possibilidades de colisões)



WEP - Vulnerabilidades

- **Chave WEP**
 - Muitos usuários usam a mesma chave WEP durante um período relativamente grande
 - 40 ou 104 bits
 - Não existe protocolo de gerenciamento de chaves
 - Impossibilita a troca dinâmica
 - Chave cadastrada manualmente
 - Cada estação tem uma chave secreta compartilhada com a estação base
- Uma vez autenticado o usuário pode sniffar os pacotes de outros usuários como em uma rede aberta



WEP - Vulnerabilidades

- **CRC-32**

- É fácil pegar um texto qualquer e gerar um CRC válido, independente do conhecimento da chave WEP
- Esse texto será aceito pelo AP e retransmitido para a estação da Vítima
- Contudo, o texto recebido não fará nenhum sentido (Pois esse texto fará parte de uma decifragem com uma chave desconhecida pelo atacante)
- O texto decifrado será lixo
- O atacante poderá provocar um ataque DOS, por exercício de sequências de dados inválidos
- CRC-32 não detecta erros que não modifiquem ICV - Integrity Check value



WEP - Vulnerabilidades

- **Sobre chaves e IV**
 - $40(24)=64$ ou $104(24)=128$ bits.
Onde 24 dinâmicos
 - Taxa 4000 por segundo
 - 300.000 quadros para descoberta: 64
 - 1.000.000 de quadros para descoberta: 128
 - Chave estática (dicionário e força bruta) + componente dinâmico
 - Chave WEP não é atualizada, Keystreams semelhantes



WEP - Vulnerabilidades

- Protocolo de autenticação ineficiente
 - Desafio passado em claro
 - Resposta criptografada
 - Hacker possuirá os 2 (XoR)

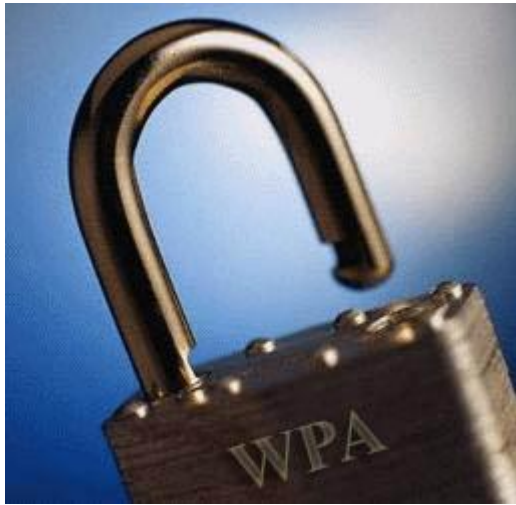


WPA / Wi-Fi Protected Access / WEP2 / TKIP



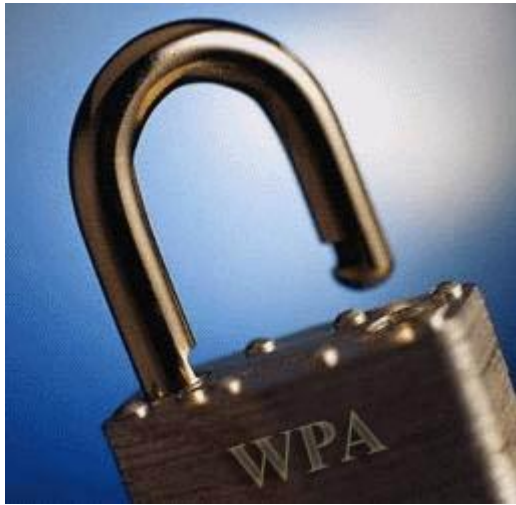
- Solução para resolver os problemas do WEP
- WEP melhorado. Também chamado de WEP2, ou TKIP
- método de criptografia que se utiliza de hierarquia e gerenciamento de chaves para remover a previsibilidade das chaves do WEP
- Aumento da chave para 128 bits

WPA / Wi-Fi Protected Access / WEP2 / TKIP



- 4 novos algoritmos em relação ao WEP
 - Message Integrity Code(MICHAEL)
 - Se dois pacotes não passarem pelo teste no mesmo minuto, a sessão é terminada, a chave da sessão é jogada fora e uma nova chave é gerada
 - Key Mixing por pacote
 - objetivo de acabar com os ataques a chaves “fracas”
 - Uma chave única para cada pacote
 - Mecanismo de mudança de chaves
 - Chaves atualizadas periodicamente
 - Novo sequenciamento dos IV
 - A sequenciação dos vetores de inicialização faz com que cada pacote tenha um código sequencial de 48 bits
 - Não são mais enviados as claras como no WEP

WPA / Wi-Fi Protected Access / WEP2 / TKIP



- Sua autenticação é realizada através de um framework IEEE 802.1X
 - IEEE 802.1X(EAPoL)
 - Componentes
 - Suplicante
 - Autenticador
 - Servidor de autenticação
 - Pre-Shared Key (PSK)

WPA / Wi-Fi Protected Access / WEP2 / TKIP



- Principais diferenças em relação ao WEP
 - Codificação do vetor de inicialização sequencial
 - Um novo tipo de método para gerar chaves
 - Troca da chave periodicamente de maneira automática

WPA / Wi-Fi Protected Access / WEP2 / TKIP

- Vulnerabilidades



- Fraqueza no algoritmo de combinação de chaves
- Susceptibilidade a ataques de dicionário
- Negação de serviços
 - MIC possui mecanismo de proteção para evitar ataque de força bruta
 - 2 erros em menos de 1 min = AP cancela a conexão por 60 seg e altera a chave de integridade
 - Injeção de pacotes mal formados

WPA 2 / 802.11i

- Solução a longo prazo para a segurança
- WPA2 = WPA + AES
- Criptografia simétrica AES
 - 128/192/256 bits
 - Criptografia de bloco/byte



WPA 2 / 802.11i

- Suporte a diferentes protocolos de privacidade
- CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
 - Privacidade: Modo counter (CTR)
 - Frame encriptado
 - Cabeçalho não muda
 - IV único por pacote (Nonce)
 - MIC enviado encriptado



WPA 2 / 802.11i

- Integridade: CBC-MAC
 - AES em modo CBC-MAC -> cálculo do MIC
 - Entradas: quadro a ser enviado e a TK
 - O MIC será enviado para o receptor aonde será recalculado e comparado com o valor enviado



WPA 2 / 802.11i

- Protocolo de privacidade e integridade baseado no AES
 - Chave de 128, 192 e 256 bits
- Numeração de pacote de 48 bits
- Preocupação com roaming
 - PMK (Pairwise Master Key) caching
 - Preautenticação



WIFI – Panorama Geral

- **Vantagens:**
 - Facilidade de conexão
 - Mobilidade
 - Flexibilidade
- **Problemas:**
 - Tamanho da banda
 - Interferência
 - Alcance do Sinal
 - SEGURANÇA
- Maior problema atual em redes sem fio
- suscetível a interceptações
- Necessidade de protocolos de segurança



WIFI – Ataques e ferramentas

- **DoS**

- Ataque contra a disponibilidade
- Ataque aos CRCs através da geração de quadros válidos
- Inundação de RTS/CTS com tempo grande
- Não tem como se livrar totalmente desse tipo de ataque

- Uso de APs Rogue

- **Soluções**

- Balanceamento de carga através de access points redundantes
- Controle do “tamanho” da rede (mapas topológicos)



WIFI – Ataques e ferramentas

- Ferramentas de descoberta

- Wireshark
- TCPDump
- Kismet
- Netstumbler
- Nmap
- Quebra de senha/fingerprint
- Cálculo Manual do Sinal Ruído /Shannon



WIFI – Ataques e ferramentas

- Ferramentas de ataque

- Airtraf
- Aircrack
- Aircrack-ng
- BSD Airtels



WIFI – Segurança



- **Confidencialidade**
 - proteção contra acesso não autorizado
 - Criptografia, esteganografia
- **Integridade**
 - Proteção contra modificação não autorizada
 - CRC
- **Disponibilidade**
 - Garantia de acesso ao serviço, sob demanda
 - Access point sempre operante
 - De dados é obtida através de backup

WIFI – Segurança



- **Autenticidade**
 - Prova de identidade
 - TKIP, CCMP
 - O que sei, o que porto, o que sou
- **Não-repúdio**
 - Garantia de irretratabilidade

WIFI – Segurança



- Não publicação do SSID da rede
- Limitação do alcance do sinal
- Filtragem MAC para associações
- Desligamento do equipamento em horários de não uso
- Inibir acesso físico ao aparelho
- Criptografia
- Autenticação
- Mudança do usuário e senha padrão

Bateria de questões de aprendizagem 1

Segurança Operacional – Módulo
III/III

BADESC – FGV 2010 – Analista de Sistemas – Suporte Técnico

1. A figura a seguir ilustra um roteador wireless da linha IEEE- 802.11, em que o ponto de acesso incorpora o que há de mais atual em tecnologia de rede, para aumentar a velocidade, alcance e performance.



Este dispositivo utiliza três antenas externas para aumentar a cobertura de dados wireless. Ele permite a clientes wireless se conectarem a taxa de dados de até 300 Mbps. Este ponto de acesso opera na frequência de 2,4GHz e criptografia WEP e WPA para transmissões seguras de dados wireless. Velocidade turbinada e throughput elevado fazem desse produto a solução perfeita para aplicações multimídia.

Esse padrão é compatível com o IEEE-802.11/g, sendo denominado:

- A. IEEE-802.11a
- B. IEEE-802.11g
- C. IEEE-802.11m
- D. IEEE-802.11n
- E. IEEE-802.11b

MPU – FCC 2007 – Analista Banco de Dados

2. No que diz respeito exclusivamente à segurança das conexões em rede local wireless, pode-se associar o termo

- A. Centrino.
- B. WLAN.
- C. Hotspot.
- D. WPA.
- E. IEEE 802.11.

3. No planejamento de uma rede sem fio, é comum que o administrador configure o roteador de modo que ele gerencie um pool de endereços IP e informações sobre os parâmetros de configuração do cliente, tais como gateway padrão, nome de domínio, servidores de nome, etc.

Nessas condições, o roteador será, também, um servidor

- A. TKIP
- B. WEP
- C. WAP
- D. HTTP
- E. DHCP

4. Assinale a alternativa que indica o protocolo que acrescenta o maior nível de segurança a uma rede sem fio 802.11.

- A. Filtro de MAC (MAC Filtering).
- B. IPv4.
- C. NAT.
- D. WEP.
- E. WPA.

5. Com relação à segurança em redes sem fio, é correto afirmar:

- A. O protocolo WPA implementa o padrão 802.11i em sua totalidade.
- B. WPA é um protocolo criptografado frequentemente usado em conexões 802.11, apesar de poder ser facilmente decodificado por terceiros.
- C. WEP é um protocolo criptografado frequentemente usado em conexões 802.11, apesar de poder ser facilmente decodificado por terceiros.
- D. O protocolo WEP foi criado com explícita motivação de remediar a vulnerabilidade do protocolo WPA.
- E. A diferença entre os protocolos WPA e WPA2 reside nos métodos criptográficos utilizados em cada um deles

6. Com relação aos protocolos de segurança para redes sem fio, julgue os itens seguintes.

[87] O WPA é um termo utilizado para proteção de redes sem fio. A sua principal implementação foi o WEP (wired equivalent Privacy).

[88] O WPA2 implementa os elementos mandatórios especificados pelo padrão IEEE 802.11i.

[89] O EAP foi definido para autenticação extensível em redes e está relacionado ao controle de acesso, em que o protocolo IP não está disponível, no primeiro momento.

[90] No WPA2, é previsto o uso do protocolo RC4, que é considerado robusto e eficiente para redes sem fio.

INFRAERO – FCC 2011 – Analista Superior III Segurança da Informação

7. Representam fragilidades de segurança em redes sem fio, EXCETO:

- A. A maioria dos concentradores vem com serviço SNMP habilitado, e isso pode ser usado por um atacante, pois revela uma vasta gama de informações sobre a rede em questão.
- B. A maioria dos equipamentos saem de fábrica com senhas de administração e endereço IP padrão. Caso estes não sejam trocados, poderão permitir a um atacante que se utilize delas em uma rede-alvo.
- C. A alta potência dos equipamentos pode permitir que um atacante munido de uma interface de maior potência receba o sinal a uma distância não prevista pelos testes.
- D. O posicionamento de determinados componentes de rede pode comprometer o bom funcionamento da rede e facilitar o acesso não autorizado e outros tipos de ataque.
- E. Os métodos de segurança WEP são completamente vulneráveis por possuírem chaves WEP pré-configuradas que não podem ser modificadas.

TRT 23 – FCC 2011 – Analista Judiciário Tecnologia da Informação

8. Para tornar confidenciais as mensagens nas redes de comunicação sem fio, os protocolos WEP, WPA e WPA2 se baseiam, respectivamente, entre outros componentes, no algoritmo de criptografia:

- A. RC4, RC4 e AES.
- B. RC4, RC4 e RC4.
- C. AES, AES e RC4.
- D. AES, AES e AES.
- E. RC4, AES e AES.

TRT 23 – FCC 2010 – Analista do MP Gestão e Análise de Projeto

9. A chave criptográfica usada no WEP (Wired Equivalent Privacy) pelo algoritmo RC4 (semente WEP) é formada por uma chave simétrica ou raiz e por um vetor de inicialização de
- A. 24 bits.
 - B. 48 bits.
 - C. 24 bytes.
 - D. 48 bytes.
 - E. 96 bits.

10. O primeiro protocolo de criptografia disponível para redes Wi-Fi é baseado em um algoritmo chamado

- A. RC4, que é um codificador de fluxo.
- B. RSA, que é um decodificador de chave pública.
- C. WAP, que é um protetor de arquivos transmitidos.
- D. NAT, que é um decodificador de fluxos.
- E. WPA, que é um protetor de arquivos transmitidos.

Gabarito

1. D

2. D

3. E

4. E

5. C

6. E, C, C, E

7. E

8. A

9. A

10.A

Bateria de questões de aprendizagem 2

Segurança Operacional – Módulo
III/III

AL/SP – FCC 2010 – Agente Técnico Legislativo – Segurança de Redes

1. Com relação à robustez do método criptográfico utilizado, a ordem do protocolo mais vulnerável para o menos vulnerável é

- A. TKIP, WPA e WEP.
- B. WPA, TKIP e WEP.
- C. TKIP, WEP e WPA.
- D. WEP, TKIP e WPA.
- E. WEP, WPA e TKIP.

2. O protocolo que fornece autenticação e criptografia de dados entre hospedeiros e um ponto de acesso em redes sem fio, num esquema baseado em chaves simétricas compartilhadas, é o(a)
- A. algoritmo de troca de chaves na Internet (IKE).
 - B. privacidade equivalente sem fio (WEP).
 - C. protocolo de autenticação de cabeçalho (AH).
 - D. protocolo de segurança de encapsulamento de carga útil (ESP).
 - E. protocolo extensível de autenticação (EAP).

3. O mecanismo de segurança para redes sem fio IEEE 802.1i que define os formatos de mensagens fim-a-fim utilizadas nas interações entre clientes e servidor de autenticação é denominado
- A. protocolo de aplicação sem fio ou WAP (Wireless Application Protocol).
 - B. privacidade equivalente sem fio ou WEP (Wired Equivalent Privacy).
 - C. vetor de inicialização.
 - D. protocolo extensível de autenticação ou EAP (Extensible Authentication Protocol).
 - E. WAP2.

4. Julgue os itens seguintes, acerca das características de redes locais sem fio

[87] A utilização do algoritmo WEP é insuficiente para a garantia dos mecanismos de autenticação e de privacidade definidos na especificação do padrão IEEE 802.11i.

[88] Os padrões IEEE 802.11a e IEEE 802.11g, que são padrões para tecnologias de redes locais sem fio, operam na mesma faixa de frequência não licenciada de 2,4 GHz a 2,485 GHz e utilizam modulação do tipo OFDM.

5. Com relação a redes sem fio, segundo o padrão IEEE 802.11, julgue os itens seguintes

- [95] Logical link control (LLC) e media access control (MAC) são parte da camada de enlace do padrão IEEE 802.11.
- [96] WEP, WPA e WPA2 são protocolos que proveem criptografia na camada de transporte em redes sem fio.
- [97] O padrão IEEE 802.11b e o IEEE 802.11g possuem suporte a taxas de conexão de 1 Mbps, 2 Mbps, 5 Mbps e 11 Mbps, com frequência de 5 GHz.
- [98] No modo de funcionamento AdHoc, o ponto de acesso (access point) tem a função de fornecer o roteamento com o protocolo OLSR (optimized link state routing).

6. A respeito das características básicas de redes sem fio em que se adota o padrão IEEE 802.11, julgue os itens a seguir

- [114] Frequency hopping spread spectrum (FHSS) e direct sequence spread spectrum (DSSS) são tecnologias de espalhamento do sinal usadas no padrão IEEE 802.11.
- [115] O protocolo WPA2 suporta o algoritmo de criptografia AES com 128 bits.
- [116] Um problema comum em redes WLAN é a propagação multipath, que ocasiona variações no tempo, no atraso e na atenuação.
- [117] A partir da introdução do WEP, as redes sem fio tornaram-se mais seguras no que se refere à prevenção de acessos indevidos.

7. São protocolos de criptografia utilizados em redes sem fio:

- A. WEP e WPA2.
- B. 3DES e SHA1.
- C. RSA e AES.
- D. SHA1 e WPA.
- E. 3DES e WEP.

8. Julgue os itens que se seguem, a respeito das redes sem fio

[105] O padrão WPA2 utiliza a cifra AES no modo de operação CCMP e apresenta conformidade com o padrão IEEE 802.11i.

[106] O tamanho máximo dos pacotes de dados transferidos nas redes no padrão IEEE 802.11 tem o mesmo valor que nas redes ethernet.

9. Considerando o âmbito de Wi-Fi, o WPA foi criado como um remendo do protocolo WEP

- A. para tentar corrigir o problema do vetor de inicialização longo.
- B. para tentar corrigir o problema do vetor de inicialização curto.
- C. para uso em intranets com alcance não superior a quinhentos metros.
- D. porque o WEP não podia ser utilizado em redes sem fio com mais de cinco roteadores.
- E. porque o WEP não podia ser usado em redes com mais de cinquenta estações.

Gabarito

1. D

2. B

3. D

4. C, E

5. C, E, E, E

6. C, C, C, E

7. A

8. C, E

9. B

Bateria de questões de aprendizagem 3

Segurança Operacional – Módulo
III/III

1. A respeito dos sistemas, das tecnologias e dos protocolos de redes sem fio, julgue os itens que se seguem.

[89] A conexão de um cliente que usa o padrão IEEE 802.11b a um ponto de acesso que usa o padrão IEEE 802.11g pode proporcionar ao cliente um desempenho com maior velocidade.

[90] Embora os padrões WPA e WPA2 utilizem TKIP, ambos são diferentes com relação à cifra utilizada. Enquanto o primeiro usa o RC4, como o WEP, o último usa AES.

[91] O padrão IEEE 802.1x tem por base o EAP, um protocolo para troca de mensagens no processo de autenticação.

EMBASA – CESPE 2010 – Assistente de Informática

2. A respeito das redes sem fio (wireless), julgue os próximos itens

- [67] Quanto maior a distância a ser coberta por uma rede wireless, maior é o consumo de energia. Bluetooth, HomeRF, IrDA e o padrão IEEE 802.15 são exemplos de tecnologias WPAN disponíveis para uso em distâncias curtas e pouco consumo de energia.
- [68] Em uma rede no padrão IEEE 802.11a, na faixa de 5 GHz, é possível se transmitir até 54 Mbps, com codificação OFDM (orthogonal frequency-division multiplexing).
- [69] Os modelos atuais de aparelhos celulares não são capazes de executar sistemas de informações da área empresarial, a exemplo dos notebooks ou PDAs, apesar de incorporarem cada vez mais tecnologias.
- [70] As informações que trafegam nas redes wireless, por serem transmitidas pelo ar, são mais difíceis de serem interceptadas em comparação às que trafegam em fibra óptica ou por conexões com fio.

3. Se o roteador tiver antena sem fio, os computadores instalados nas proximidades, quando dotados de antena para conexão de rede sem fio, estarão conectados à Internet e também à rede interna. NÃO se trata de uma ação, após instalar o roteador de banda larga, para evitar tal situação:
- A. alterar a senha administrativa.
 - B. habilitar o gerenciamento remoto.
 - C. atualizar o firmware do roteador, com a versão mais nova, para mantê-lo livre de falhas conhecidas.
 - D. desabilitar a funcionalidade de rede sem fio, caso não seja usada.
 - E. habilitar ou alterar a criptografia para WPA-2, tanto no roteador quanto nos computadores da rede.

AL/SC – FEPESE 2010 – Técnico em Hardware

4. Considere a possibilidade de executar as seguintes configurações no AP (access point) de uma rede local sem fio, padrão IEEE 802.11g.

I. Habilitar o broadcast do SSID.

II. Trocar o SSID e a senha padrão configurados pelo fabricante.

III. Utilizar preferencialmente o protocolo WEP (Wired Equivalent Privacy) para criptografar os dados transmitidos.

IV. Utilizar preferencialmente WPA (Wi-Fi Protected Access) para autenticação e proteção de dados.

V. Utilizar o canal de frequência mais alto que estiver disponível.

Assinale a alternativa que enumera corretamente as configurações citadas acima que são capazes de aumentar a segurança da rede.

A. Apenas as configurações I e III.

B. Apenas as configurações I e V.

C. Apenas as configurações II e III.

D. Apenas as configurações II e IV.

E. Apenas as configurações IV e V.

5. Com relação aos conceitos e aos protocolos utilizados em redes sem fio, julgue os itens.

[80] A autenticação em redes sem fio é realizada, no padrão IEEE 802.1x, por meio de três componentes: o autenticador, o requerente e o servidor de autenticação.

[81] O WPA2 usa o protocolo RC4 como algoritmo de criptografia principal, e o radius como protocolo de acesso ao meio.

[82] De maneira geral, o padrão IEEE 802.1x se baseia no EAP (extensible authentication protocol), cujo papel é transportar as informações de identificação dos utilizadores.

6. Com relação aos conceitos e aos protocolos utilizados em redes sem fio, julgue os itens.

[83] O vetor de inicialização do WEP tem 24 bits e é enviado em texto claro como parte da mensagem. Esse é um dos motivos de esse protocolo ser considerado inseguro.

[84] O WPA não utiliza PSK (pre-shared key).

[85] A taxa máxima de transmissão de dados no padrão IEEE 802.11b é de 54 Mbps e o acesso ao meio é do tipo CSMA/CD.

7. A respeito das tecnologias de redes sem fio, julgue os próximos itens.

[155] O WPA originalmente implementou integralmente a especificação IEEE 802.11i, particularmente TKIP.

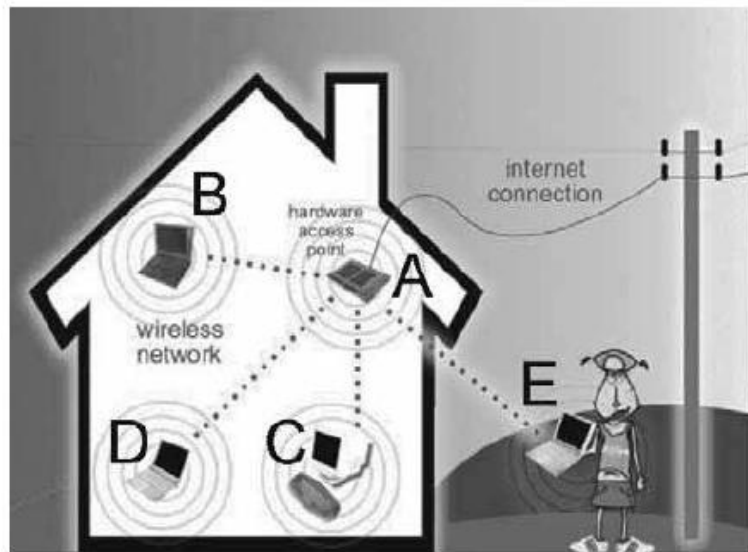
[156] O WEP, especificado no padrão IEEE 802.11b é embasado na cifra de fluxo RC4, não determina como devem ser gerados os vetores iniciais, o que propicia que as implementações os reúsem, causando, assim, vulnerabilidades de segurança.

[157] O padrão IEEE 802.1x, incorporado pelo WPA2, envolve três componentes: o suplicante, que deseja se autenticar; o autenticador, que recebe o pedido do suplicante e o repassa ao serviço de autenticação; e o servidor de autenticação, que suporta o serviço de autenticação.

CEHAP/PB – CESPE 2009 – Analista de Sistemas

8. O projeto 802 é um conjunto de normas de comunicação para redes LAN e WAN implementados pelo IEEE (Institute of Electrical and Electronics Engineering) e que envolve a camada de enlace de dados. Com relação ao padrão IEEE 802.11, assinale a opção incorreta.
- A. Em relação ao WEP (Wired Equivalent Privacy) a norma utiliza criptografia de dados de forma a permitir um nível de segurança entre os usuários de uma rede sem fios e possíveis intrusos.
 - B. A norma 802.11a utiliza a frequência de rádio de 5 GHz, o que permite o aumento da velocidade de transferência para cerca de 54 Mbps.
 - C. A norma 802.11b, conhecida como Wi-Fi pode alcançar 54 Mbps de transferência de dados e utiliza a frequência de 2,4 GHz, o que pode provocar interferências com outros aparelhos que utilizem a mesma faixa de frequência.
 - D. A norma 802.11i acrescentou o serviço denominado TKIP (Temporal Key Integrity Protocol) e estabeleceu o uso de chaves de 128 bits, implicando chaves de criptografia mais complexas do que as usadas no serviço WEP (Wired Equivalent Privacy).

TCE/GO – CESPE 2009 – Analista de Controle Externo Informática – processamento de dados



9. A figura acima, obtida de www.websafecrackerz.com, apresenta um cenário de uso de redes IEEE 802.11, no qual os dispositivos B, C, D e E se conectam ao dispositivo A. Acerca desse tipo de rede de computadores, julgue os itens seguintes.

I Se A funciona conforme o protocolo IEEE 802.11g, então os dispositivos B, C, D e E transmitem e recebem mensagens através de A usando sinais de rádio na frequência de 2,4 GHz.

II Se A funciona conforme o protocolo IEEE 802.11i, então, para a criptografia da carga útil dos pacotes que transitam entre B e A, é usado o algoritmo AES, que é um protocolo de criptografia simétrica.

III Se A funciona conforme o protocolo IEEE 802.11b e com segurança

WEP, então, entre A e qualquer dos dispositivos a ele conectados através da rede sem fio, serão trocados vetores de inicialização com comprimento de 24 bits e chaves secretas précompartilhadas com comprimento de pelo menos 40 bits.

IV O dispositivo A usualmente dissemina, várias vezes por segundo, um sinal contendo o SSID do ponto de acesso, empregando, nesse caso, o modelo de rede sem fio denominado ad hoc.

V Se A funciona conforme o protocolo IEEE 802.11i, então, a fim de evitar colisões de pacotes com outras redes sem fio que porventura estejam na proximidade de A, este dispositivo faz dispersão do sinal pelas centenas de canais disponíveis na faixa de frequência pertinente ao protocolo 802.11i, por meio da técnica de spread spectrum.

Estão certos apenas os itens

- A. I, II e III.
- B. I, II e IV.
- C. I, III e V.
- D. II, IV e V.
- E. III, IV e V.

Gabarito

1. E, C, C

8. C

2. C, C, E, E

9. A

3. B

4. D

5. C, E, C

6. C, E, E

7. E, C, C