Sistemas de Comunicação

Segurança em Redes IEEE 802.11

Prof. Paulo Gonçalves
pasg@cin.ufpe.br
www.cin.ufpe.br/~pasg
CIn/UFPE

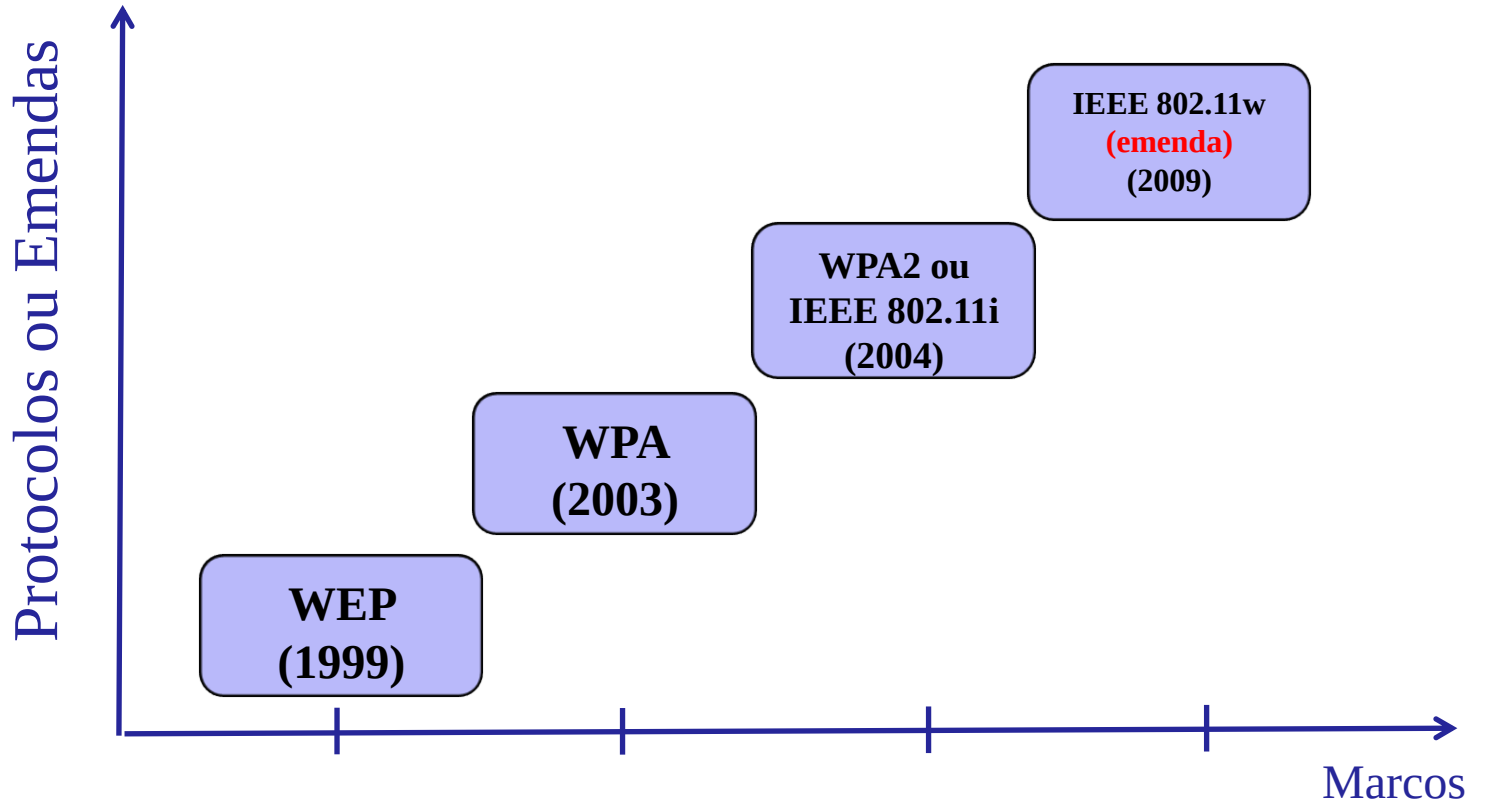
Segurança em Redes IEEE 802.11

- Tema vasto!
- Cobriremos os seguintes tópicos
  - Protocolos de Segurança
  - Auditoria de Redes IEEE 802.11
  - Rogue APs
  - Honeypots e Honeynets

PROTOCOLOS DE SEGURANÇA

Segurança em Redes IEEE 802.11

- Protocolos de Segurança ou emendas

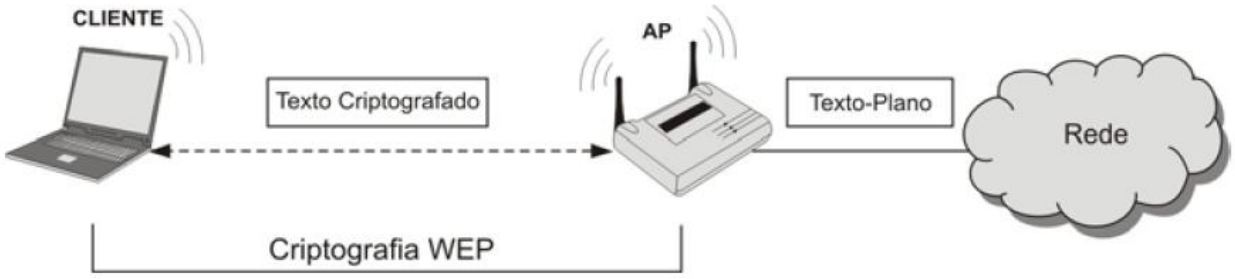


Segurança em Redes IEEE 802.11

- Protocolos de Segurança
  - WEP
  - WPA
  - IEEE 802.11i ou WPA2
  - IEEE 802.11w

WEP *(Wireless Equivalent Privacy)*

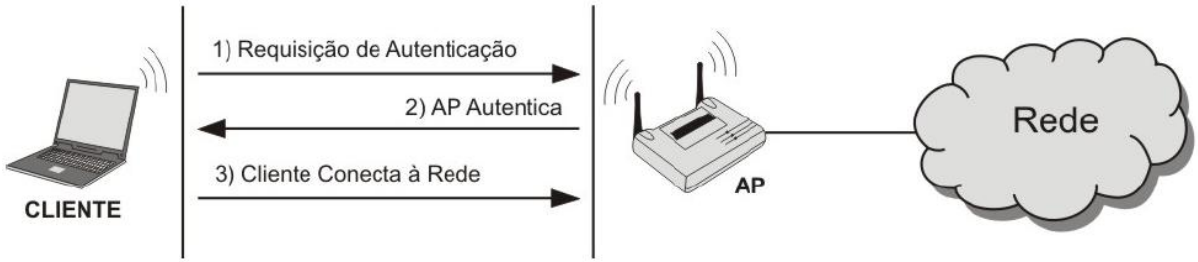
- Primeiro protocolo (1999) de proteção para redes IEEE 802.11
- Ideia: Prover proteção equivalente a de um cabo



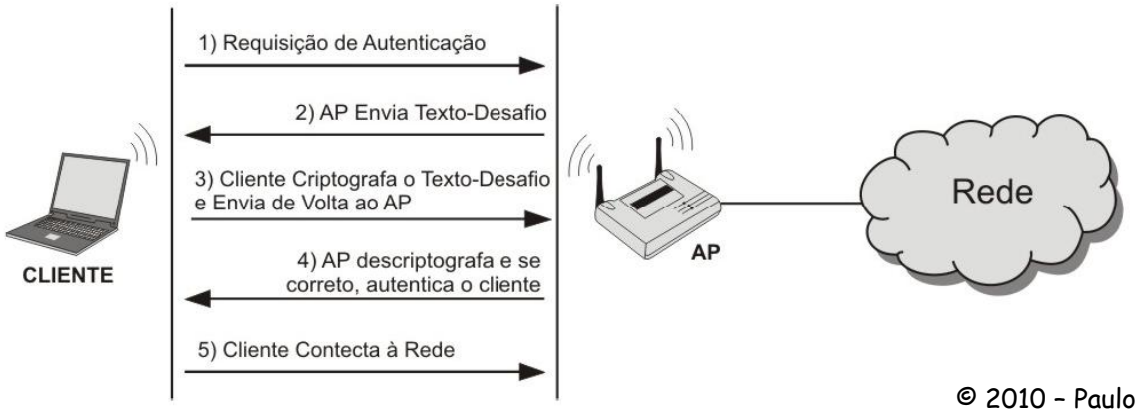
WEP: Autenticação

Pode-se combinar esses métodos de autenticação com filtragem de endereços MAC

- Objetivo: verificação de autorização de acesso à rede
- 1º Tipo: Sistema Aberto ou Rede Aberta
  - Autenticação nenhuma é feita na prática. Qualquer cliente ou estação é aceito na rede
  - Basta informar o SSID da rede (obtido através de beacons ou conhecido previamente pelo cliente)

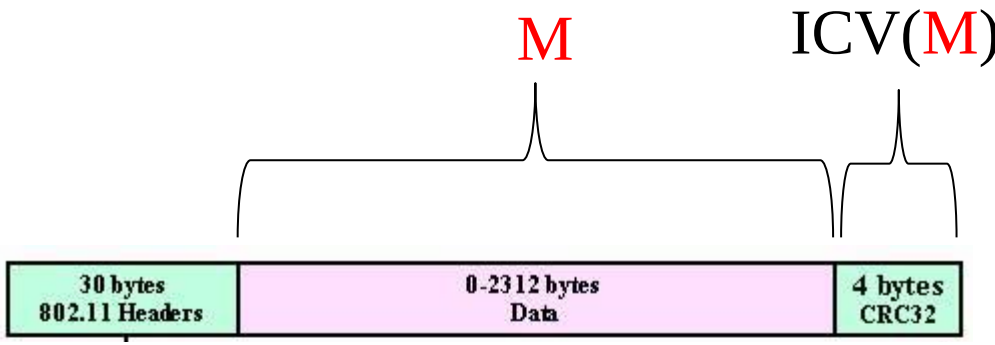


- 2º Tipo: Por chave pré-compartilhada
  - Uso de chave pré-compartilhada entres os clientes e o ponto de acesso. A chave é utilizada na criptografia de dados
  - Uso de texto-desafio



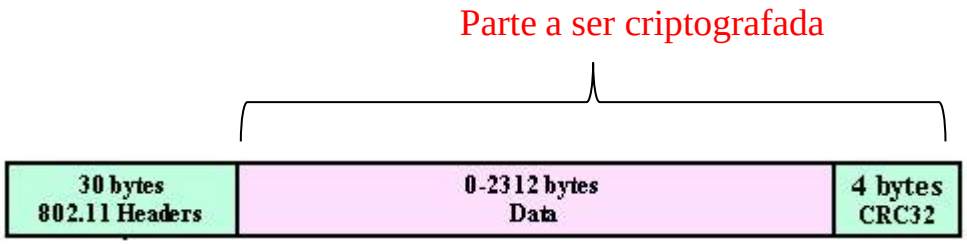
WEP: Integridade

- Objetivo: Detectar modificações/alterações nas mensagens recebidas (*e.g.* erro de transmissão ou manipulação)
- O WEP adiciona à mensagem a ser enviada um ICV (Integrity Check Value)
- O ICV nada mais é do que um CRC-32 informado no campo ICV da mensagem



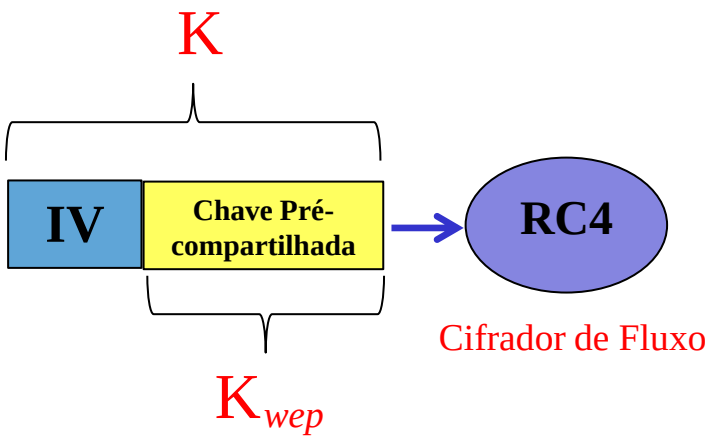
WEP: Confidência

- Objetivo: decodificação de mensagens por clientes autorizados
- Baseado no uso de uma chave secreta pré-compartilhada entre os dispositivos da rede
- Criptografa apenas parte do quadro de dados na camada enlace



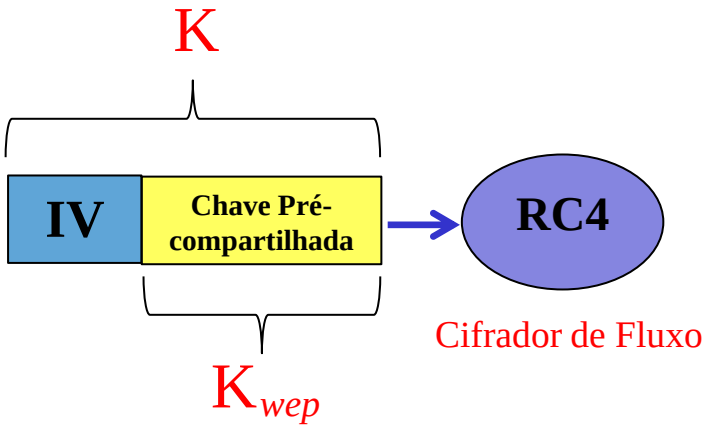
WEP: Confidência

- Criptografia ...
  - Uso do cifrador de fluxo RC4
    - Cifrador de fluxos amplamente utilizado. Exemplo: SSL (Secure Socket Layer)
  - Chave de entrada para o RC4 = concatenação da chave secreta com um modificador denominado vetor de iniciação ou IV (Initialization Vector)
  - Chave secreta possui tipicamente 104 bits e o IV possui tamanho fixo de 24 bits
  - Existem versões que suportam chaves secretas de apenas 40 bits



WEP: Confidência

- Criptografia ...
  - O uso de um modificador da chave criptográfica – o IV – se justifica por razões de segurança
  - Cada quadro deve ser criptografado usando uma chave diferente. Por isso o IV deve ser modificado a cada quadro
  - O WEP não especifica como os IVs devem ser modificados
  - Decisão de modificação deixada para fabricantes
    - Alguns iniciam o IV em zero e o incrementam de uma unidade a cada quadro
    - Outros geram os IVs de forma randômica
    - Alguns filtram certos IVs para tentar evitar certos ataques de recuperação de chaves



WEP: Funcionamento do RC4

- RC4
  - Como dito ... cifrador de fluxos amplamente utilizado. Exemplo: SSL (Secure Socket Layer)
  - É composto de duas partes
    - Um Algoritmo de Escalonamento de Chaves (KSA – Key Scheduling Algorithm)
    - Um Algoritmo de Geração Pseudo-Aleatória (PRGA – Pseudo-Random Generation Algorithm)
- Funcionamento ...

WEP: Funcionamento do RC4

- RC4
  - K = chave secreta pré-compartilhada concatenada com IV atual
  - PRGA recebe vetor S[] resultante do KSA

KSA(K)

Iniciação:
for $i \leftarrow 0$ **to** $N-1$
$S[i] \leftarrow i$
$j \leftarrow 0$
Embaralhamento:
for $i \leftarrow 0$ **to** $N-1$
$j \leftarrow (j + S[i] + K[i \bmod l]) \bmod N$
Troca$(S[i], S[j])$

PRGA(S)

Iniciação:
$i \leftarrow 0$
$j \leftarrow 0$
Loop de Geração:
$i \leftarrow (i+1) \bmod N$
$j \leftarrow (j + S[i]) \bmod N$
Troca$(S[i], S[j])$
Saída $z \leftarrow S[S[i] + S[j]) \bmod N]$

K: chave de entrada (40 a 256 bits)
l: Tamanho da chave de entrada

S[]: vetor
N: número de posições do vetor S[].
Tipicamente N = 256

WEP: Funcionamento do RC4

- KSA
  - Após fase de iniciação
    - S[0]= 0 , S[1]= 1 , S[2] = 2 ... S[N-1] = N-1
    - i e j representam índices do vetor S
    - Ambos possuem valor zero antes do embaralhamento
  - Embaralhamento
    - percorre-se os i elementos de S ao mesmo tempo em que se atualiza o valor de j com o seu próprio valor anterior adicionado ao i-ésimo elemento de S e ao elemento da chave K que ocupa a posição ***i mod l***
    - A computação do valor final de j é feita usando **módulo N**
    - Troca-se a posição dos elementos i e j do vetor S

KSA(K)

Iniciação:

for $i \leftarrow 0$ **to** $N-1$

$S[i] \leftarrow i$

$j \leftarrow 0$

Embaralhamento:

for $i \leftarrow 0$ **to** $N-1$

$j \leftarrow (j + S[i] + K[i \bmod l]) \bmod N$

Troca$(S[i], S[j])$

K: chave de entrada (40 a 256 bits)
l: Tamanho da chave de entrada

S[]: vetor
N: número de posições do vetor S[].
Tipicamente N = 256

WEP: Funcionamento do RC4

- PRGA
  - O vetor S[] vindo do KSA define seu estado interno inicial
  - i e j representam índices do vetor S
  - Ambos possuem valor zero antes do embaralhamento
  - Loop de Geração -> Loop infinito que produz o keystream
    - Incrementa i de uma unidade enquanto j é incrementado com o i-ésimo elemento do vetor S[]. Respeita-se o módulo N em ambos.
    - Troca-se os elementos i e j de S[] de posição entre si
    - Computa-se o **keystream z**

PRGA(S)

Iniciação:

$i \leftarrow 0$

$j \leftarrow 0$

Loop de Geração:

$i \leftarrow (i+1)\ mod\ N$

$j \leftarrow (j + S[i])\ mod\ N$

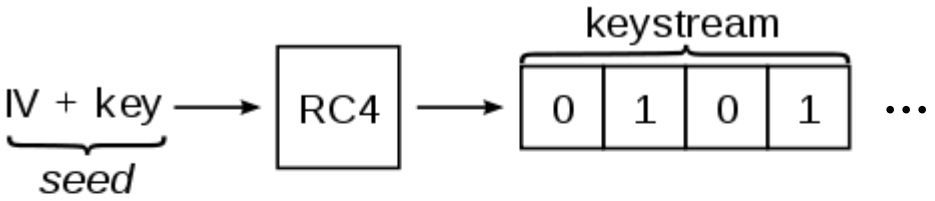
Troca$(S[i], S[j])$

Saída $z \leftarrow S[S[i] + S[j])\ mod\ N]$

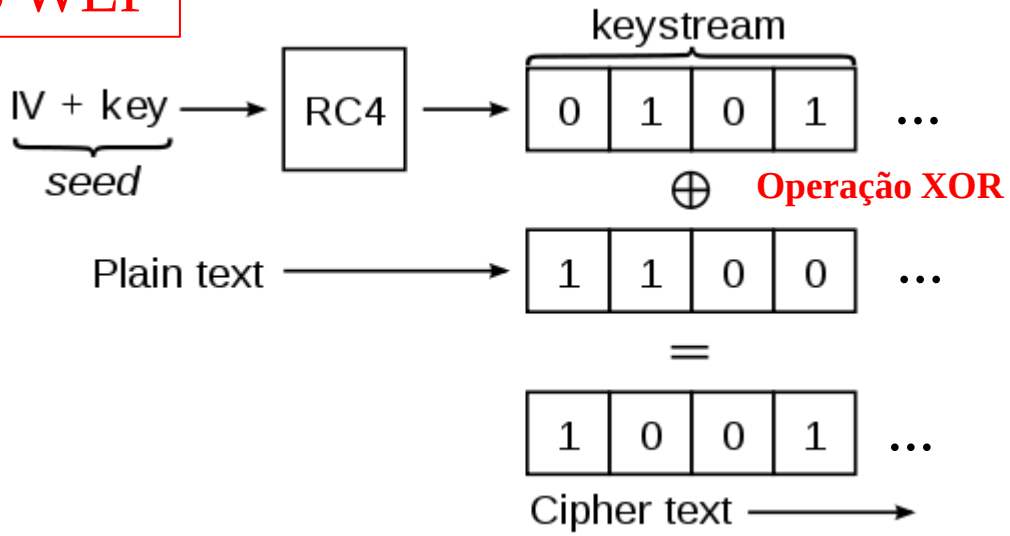
S[]: vetor
N: número de posições do vetor S[].
Tipicamente N = 256

Keystream e Encriptação no WEP

Keystream

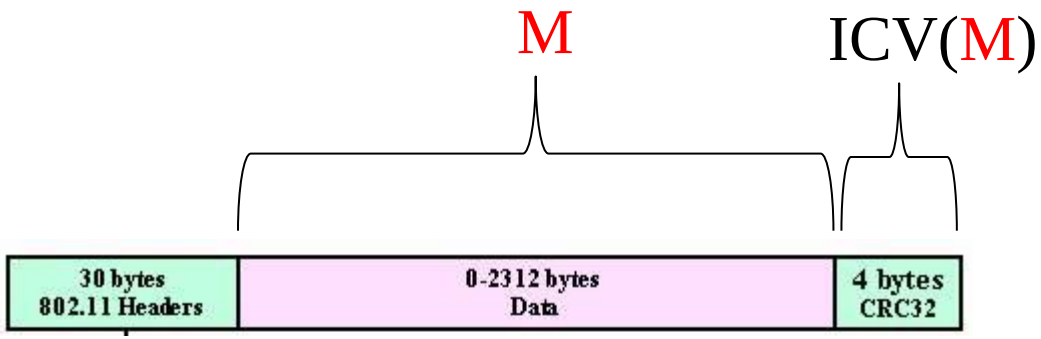


Encriptação no WEP



WEP: Encriptação

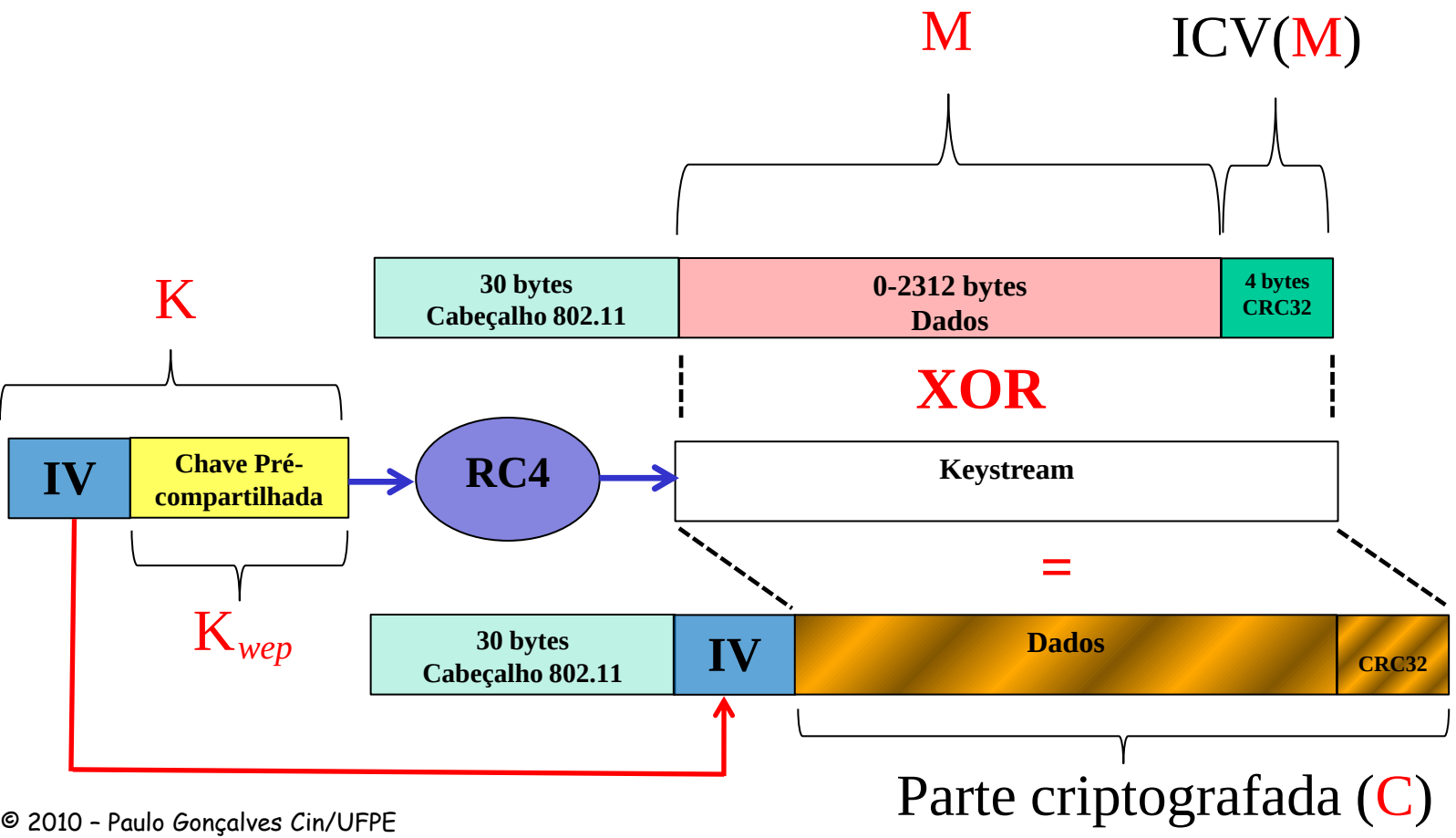
- Cifragem de apenas uma porção do quadro de dados usando o RC4
- A porção (M) desejada, em texto plano, é criptografada com o seu *checksum* correspondente, o ICV (Integrity Check Value)
- O ICV nada mais é do que um CRC32 (soma linear previsível)



$$C = [M||ICV(M)] \oplus [RC4(IV||K_{wep})]$$

WEP: Encriptação

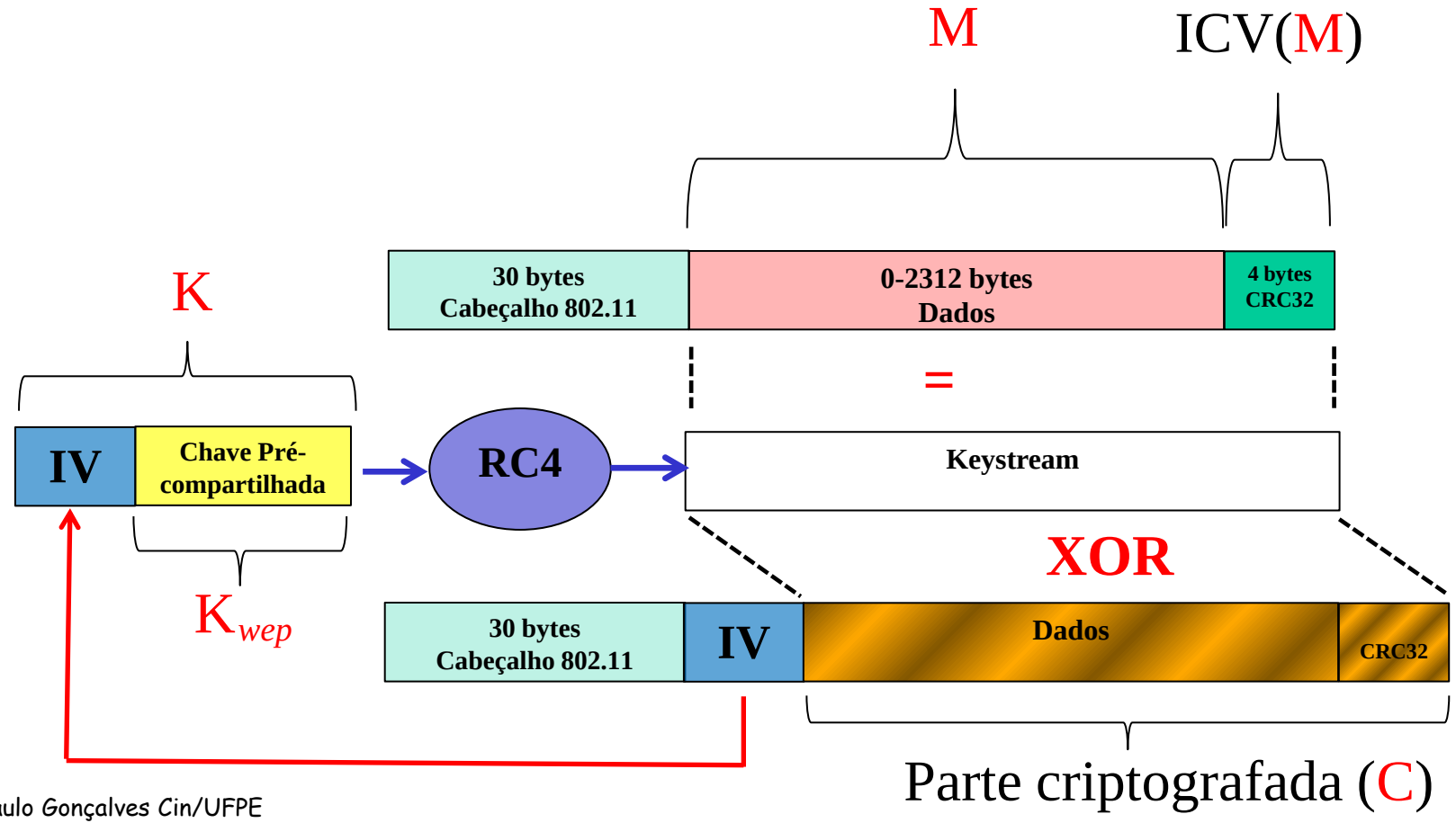
- A chave K é a concatenação da chave secreta WEP com o IV atual
- Para cada quadro um novo IV deve ser escolhido



$$M||ICV(M) = [C] \oplus [RC4(IV||K_{wep})]$$

WEP: Desencriptação

- Note que é importante que o receptor conheça o IV atual para decifrar o quadro
  - Por isso o IV é enviado em claro no cabeçalho do quadro
  - Este foi o maior erro do WEP !



WEP: Vulnerabilidades

- Não foi projetado por especialistas em criptografia e logo se mostrou vulnerável (2000)
- Ao longo dos anos surgiram diversos ataques contra o WEP
  - MAC Spoofing
  - Possibilidade de usar chaves pré-compartilhadas de 40 bits (ataque de força bruta em tempo factível)
  - Reuso de chaves (poucos IVs distintos -> 2^(24) = 16,7 milhões)

WEP: Vulnerabilidades

- Ao longo dos anos surgiram diversos ataques contra o WEP ...
  - Gerenciamento de Chaves (sem mudanças dinâmicas ao longo do tempo)
  - IV passado em claro (parte da chave!)
  - Autenticação falha (basta capturar o texto-desafio e o equivalente cifrado para obter um keystream válido e usá-la para criar resposta válida a qualquer texto-desafio) – (Plain text attacks)
  - CRC-32 é uma função linear (insegura em termos criptográficos)

WEP: Vulnerabilidades (Cont.)

- Ao longo dos anos surgiram diversos ataques contra o RC4, o WEP e redes Wi-Fi em geral
  - Ataques de Negação de Serviço (DoS): e.g. autenticação/desautenticação
  - Desencriptação de mensagens sem uso da chave WEP que protege a rede (ataque chopchop)
  - Reinjeção de pacotes
  - Ataques estatísticos de recuperação de chave
    - Exploram problemas do RC4
  - Ufa! Tem mais?

WEP: Ataques estatísticos

- Diversos ataques estatísticos contra o WEP foram propostos
  - Diferem em eficiência em número de mensagens (Ivs) necessárias(necessários) para a quebra da chave secreta e, consequentemente, no tempo necessário para a recuperação dessa chave

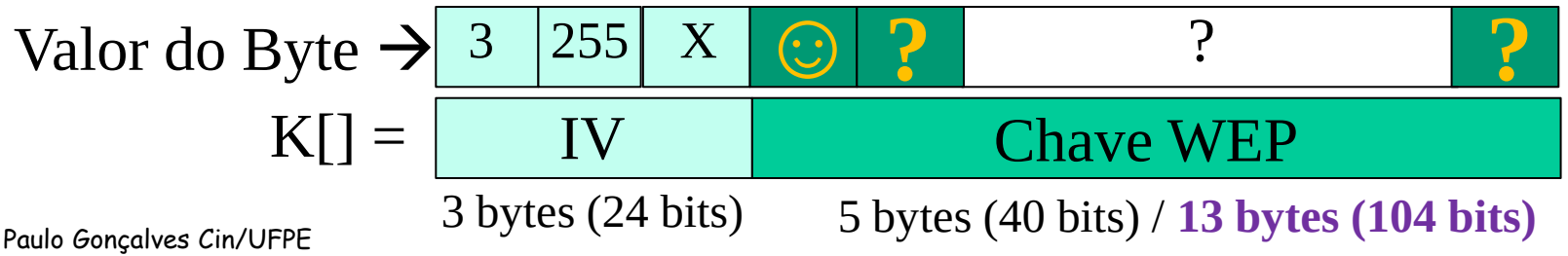
- Ataques estatísticos de recuperação de chave WEP surgiram após descoberta de falhas do RC4
  - Chaves de entrada do KSA que respeitam determinados padrões permitem a ocorrência de padrões fixos no *keystream* do PRGA. Tais chaves são denominadas "chaves fracas"
  - O conhecimento de uma pequena parte dessas chaves é suficiente para se determinar grande parte do estado interno do RC4
  - O conhecimento de alguns bytes da chave de entrada do KSA traz informações sobre os bytes restantes da chave (IV -> maior fraqueza do WEP)

WEP: Principais ataques de recuperação de chaves

- FMS (2001)
- Otimizações do FMS (2004)
- Família de 17 ataques KoreK (2004)
- PTW (2007)

WEP: Ataque Teórico FMS

- Estudo teórico que mostrou como atacar o WEP (2001)
- Utiliza apenas a primeira palavra de saída da sequência pseudo-aleatória do PRGA
  - Chamaremos de P1
- Se os IVs possuem o padrão [B+3 | 255 | X] (0 <= B < **13** e X qualquer)
  - O byte K[B+3] da chave utilizada no KSA pode ser encontrado
- Para encontrar o primeiro byte da chave WEP basta procurar por quadros com IVs que possuam o padrão [3 | 255 | X] e saber o valor de P1



WEP: Ataque Teórico FMS

- Ok. Mas como é possível ?
- Acompanhe a sequência de eventos no KSA

KSA(K)

Iniciação:
for $i \leftarrow 0$ **to** $N-1$
$S[i] \leftarrow i$
$j \leftarrow 0$
Embaralhamento:
for $i \leftarrow 0$ **to** $N-1$
$j \leftarrow (j + S[i] + K[i \bmod l]) \bmod N$
Troca$(S[i], S[j])$

Vetor S após Iniciação do KSA

0	1	2	3	4	5	6	···
0	1	2	3	4	5	6	···

Primeira Troca: $i = 0,\ j = 3$

0	1	2	3	4	5	6	···
3	1	2	**0**	4	5	6	···

Segunda Troca: $i = 1,\ j = 3$

0	1	2	3	4	5	6	···
3	**0**	2	**1**	4	5	6	···

Terceira Troca: $i = 2,\ j = 5 + X$

0	1	2	3	4	···
3	0	**5+X**	1	4	···

Quarta Troca: $i = 3,\ j = 6 + X + K[3]$

0	1	2	3	4	···
3	0	5+X	**S_3[6+X+K[3]]**	4	···

$S_3[d]$ representa o elemento de S na terceira troca cujo índice é d

Sequência de eventos no KSA

WEP: Ataque Teórico FMS

KSA(K)

Iniciação:
for $i \leftarrow 0$ **to** $N-1$
$S[i] \leftarrow i$
$j \leftarrow 0$
Embaralhamento:
for $i \leftarrow 0$ **to** $N-1$
$j \leftarrow (j + S[i] + K[i \bmod l]) \bmod N$
Troca$(S[i], S[j])$

- Ok. Mas como é possível ?
- Agora suponha o seguinte
  - Alguns valores do vetor S, durante a operação do KSA, permaneçam em posições inalteradas
  - Esta suposição é a base dos ataques estatísticos contra o WEP

Vetor S após Iniciação do KSA

0	1	2	3	4	5	6	···
0	1	2	3	4	5	6	···

Segunda Troca: $i = 1,\ j = 3$

0	1	2	3	4	5	6	···
3	**0**	2	**1**	4	5	6	···

Primeira Troca: $i = 0,\ j = 3$

0	1	2	3	4	5	6	···
3	1	2	**0**	4	5	6	···

Terceira Troca: $i = 2,\ j = 5 + X$

0	1	2	3	4	···
3	0	**5+X**	1	4	···

Quarta Troca: $i = 3,\ j = 6 + X + K[3]$

0	1	2	3	4	···
3	0	5+X	S_3**[6+X+K[3]]**	4	···

$S_3[d]$ representa o elemento de S na terceira troca cujo índice é d

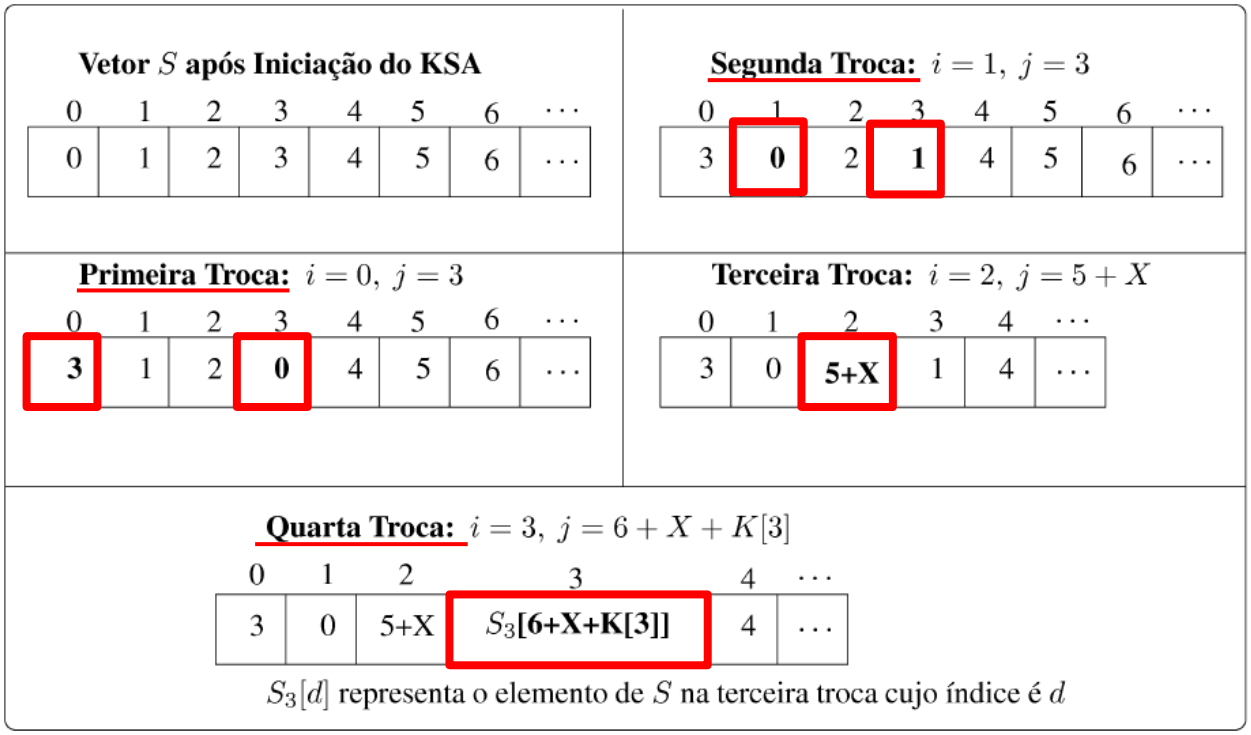
Sequência de eventos no KSA

WEP: Ataque Teórico FMS

KSA(K)

Iniciação:
for $i \leftarrow 0$ **to** $N-1$
$S[i] \leftarrow i$
$j \leftarrow 0$
Embaralhamento:
for $i \leftarrow 0$ **to** $N-1$
$j \leftarrow (j + S[i] + K[i \bmod l]) \bmod N$
Troca$(S[i], S[j])$

- Ok. Mas como é possível ?
- Probabilidade da suposição ser verdadeira
  - Implica na probabilidade de sucesso do ataque
  - Com probabilidade de ≈ 5%, S[0], S[1], S[3] permanecerão inalterados a partir da quarta troca no KSA



Sequência de eventos no KSA

Note que tenho K[3] em S_3

WEP: Ataque Teórico FMS

PRGA(S)

Iniciação:

$i \leftarrow 0$

$j \leftarrow 0$

Loop de Geração:

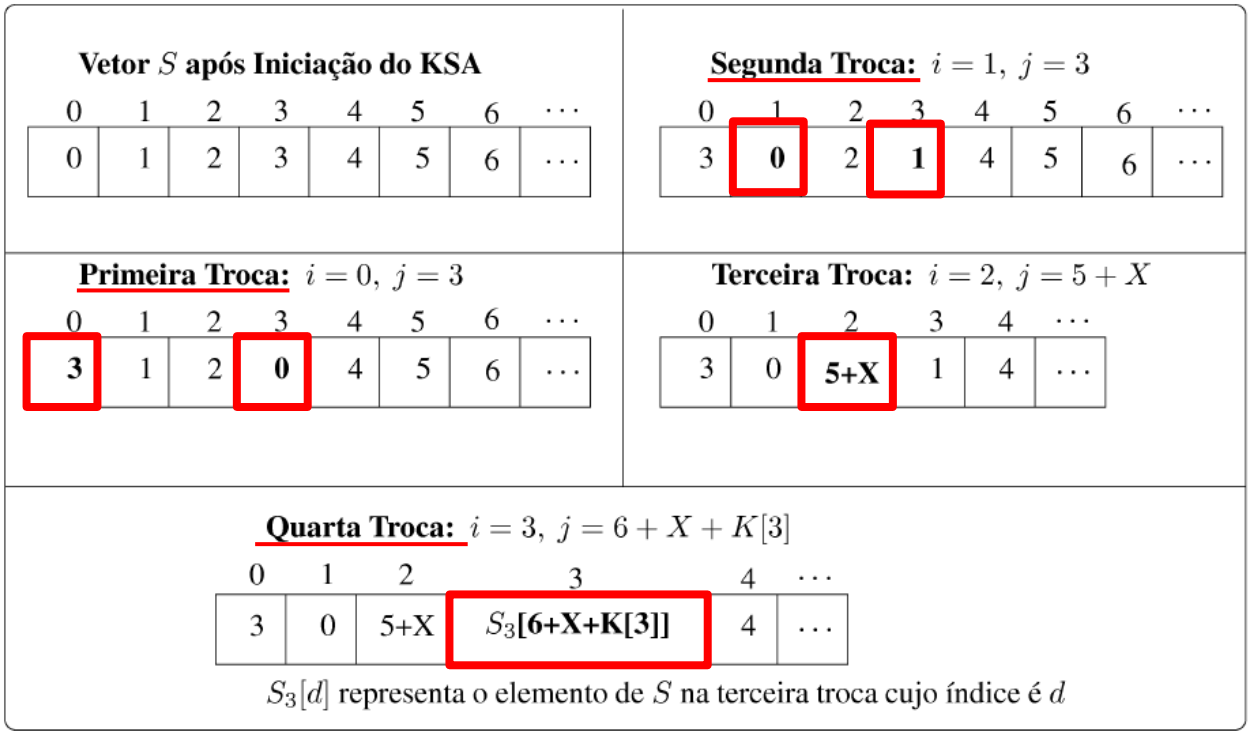
$i \leftarrow (i+1)\ mod\ N$

$j \leftarrow (j + S[i])\ mod\ N$

Troca$(S[i], S[j])$

Saída $z \leftarrow S[S[i] + S[j])\ mod\ N]$

- Ok. Mas como é possível ?
- Ao se utilizar S no PRGA
  - S[0] e S[1] trocarão de posição entre si dado que S[1] = 0
  - Assim, o primeiro byte de saída do PRGA será **P1** = S[S[0]+S[1]] = S[0+3] = S3[6+X+K[3]]
  - K[3] possui provavelmente o valor que torna a igualdade verdadeira (Mas quem é **P1** ?)



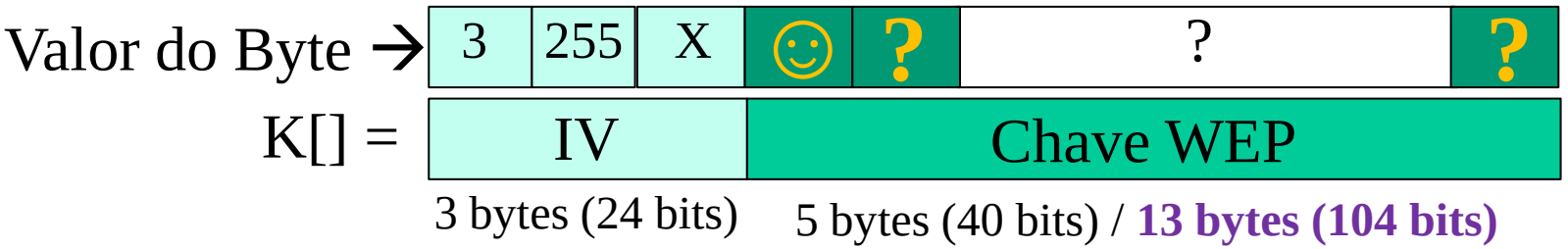
Sequência de eventos no KSA

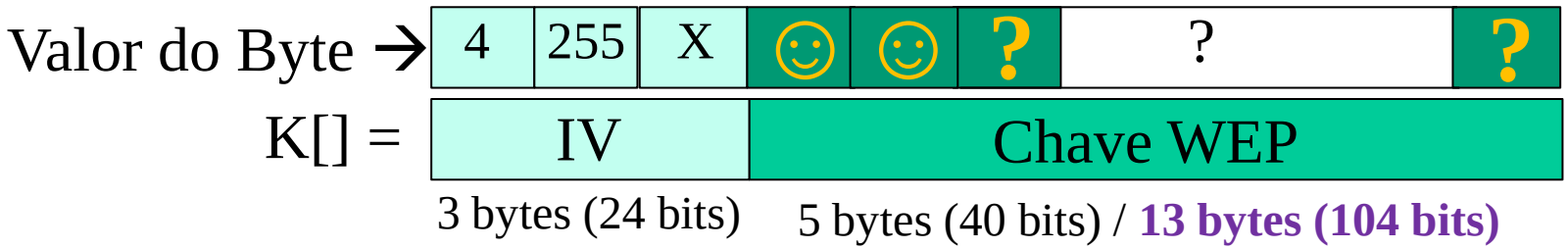
WEP: Ataque Teórico FMS

- Como determinar P1 (o primeiro byte do *keystream*)?
  - A porção inicial criptografada de um quadro de dados IEEE 802.11 é praticamente constante
  - Começa com o cabeçalho LLC (Logic Link Control) seguido por um cabeçalho SNAP (Subnetwork Access Protocol)
  - Os dois cabeçalhos correspondem aos 8 primeiros bytes criptografados de um quadro
  - Tanto para pacotes IPv4 quanto para ARPs, o primeiro byte no cabeçalho LLC será 0xAA
- Para encontrar P1, basta fazer um XOR entre 0xAA e o primeiro byte da porção criptografada do quadro

WEP: Ataque Teórico FMS

- Para se conhecer os outros bytes da chave WEP ataca-se sequencialmente do segundo ao último byte da chave, um byte por vez





WEP: Ataque Teórico FMS

- Lembre-se: o ataque é estatístico
  - Existe a necessidade de se capturar vários IVs ou quadros para cada byte que se deseja encontrar
  - Vários bytes candidatos vão surgir e votos serão acumulados para cada um deles
  - Aquele que receber mais votos é provavelmente o byte procurado da chave

- Na teoria
  - Preciso de em torno de 4 milhões de IVs ou quadros para recuperar a chave secreta (contador de IVs *little indian*)
  - Preciso de em torno de 1 milhão de IVs ou quadros para recuperar a chave secreta (contador de IVs *big indian*)

Little indian: byte de ordem mais baixa é incrementado mais rápido

Big indian: byte de ordem mais alta é incrementado mais rápido

WEP: Principais ataques de recuperação de chaves

- FMS (2001)
- Otimizações do FMS (2004)
- Família de 17 ataques KoreK (2004)
- PTW (2007)

WEP: Ataque Prático e Otimizado FMS

- Somente em 2004 que o ataque FMS foi testado na prática e otimizado
- Encontraram mais casos resolvidos
  - Nos casos encontrados, um byte da chave secreta é obtido com probabilidade de ≈13% ao invés de ≈5%
- O ataque FMS é construído byte a byte
  - Predição do byte seguinte depende da correta predição do byte anterior
  - Descobriram que casos resolvidos ocorrem com maior probabilidade para os últimos bytes da chave secreta
  - Descobriram que dependendo da forma como os IVs são gerados, é mais provável que casos resolvidos para vários bytes da chave ocorram antes daqueles necessários para a predição dos bytes iniciais

WEP: Ataque Prático e Otimizado FMS

- O ataque FMS é construído byte a byte (cont.)
  - Desta forma, foi proposto utilizar os casos resolvidos para diminuir o leque de possibilidades dos primeiros bytes da chave secreta
  - Para testar bytes candidatos dentro de um leque de possibilidades, é verificado se o *checksum* de um quadro decifrado revela-se correto (CRC é um função linear)
  - No caso de empate entre dois ou mais bytes candidatos, prioriza-se respectivamente letras minúsculas, letras maiúsculas, números, símbolos e outros bytes.
  - Otimização baseada no fato de que geralmente chaves WEP em formato ASCII são empregadas

WEP: Ataque Prático e Otimizado FMS

- Na prática descobriram que para recuperar uma chave WEP de 104 bits
  - FMS precisa de 4 milhões a 6 milhões de IVs ou quadros capturados
  - FMS otimizado precisa de 1 milhão a 2 milhões de IVs ou quadros capturados

- Alguns APs e placas Wi-Fi deixaram de utilizar IVs vulneráveis ao ataque FMS (filtragem de IVs)

- Mas ...

WEP: Principais ataques de recuperação de chaves

- FMS (2001)
- Otimizações do FMS (2004)
- Família de 17 ataques KoreK (2004)
- PTW (2007)

WEP: Ataques KoreK

- Hacker KoreK desenvolveu 17 ataques estatísticos contra o WEP (2004)
- Os ataques são uma generalização do ataque FMS
  - O que importa é como os IVs fazem o KSA e o PRGA se comportarem e não mais como alguns IVs que seguem determinados padrões fazem isso
- KoreK conseguiu encontrar comportamentos do KSA e PRGA que permitem revelar um byte da chave secreta com probabilidade de ≈5% e ≈ 14%
- Na prática
  - Requer em torno de 500 mil IVs ou quadros capturados para se encontrar uma chave WEP de 104 bits
- Não adiantava mais filtrar IVs ...

WEP: Principais ataques de recuperação de chaves

- FMS (2001)
- Otimizações do FMS (2004)
- Família de 17 ataques KoreK (2004)
- PTW (2007)

WEP: Ataque PTW

- Ataque especializado ao RC4 utilizado contra o WEP
- Em 2007 encontraram uma função que permite estimar os bytes da chave secreta à condição de que vários bytes dessa chave sejam previamente conhecidos
- Para funcionar, é necessário obter os bytes iniciais de uma quantidade "suficiente" de keystreams
  - Isso é feito através da captura de requisições e respostas ARP criptografadas pelo WEP
  - Pacotes ARPs são pequenos e de tamanho fixo
  - Pacotes ARPs possuem vários bytes fáceis de serem advinhados !
- ARP
  - Primeiros 16 bytes: 8 bytes fixos do cabeçalho LLC/SNAP 802.11 (AA:AA:03:00:00:00:08:06) seguidos de 8 bytes específicos à mensagem ARP
  - Se requisição: os 8 bytes são iguais a (00:01:08:00:06:04:00:01)
  - Se resposta: os 8 bytes são iguais a (00:01:08:00:06:04:00:02)

WEP: Ataque PTW

- Distinção entre requisições e respostas ARP
  - Se requisição: enviada para endereço broadcast da rede (em claro no quadro)
  - Se resposta: enviada para endereço unicast (em calro no quadro)
- Recupera-se os primeiros 16 bytes do *keystream* com a realização de um XOR entre o ARP criptografado capturado e o seu padrão inicial fixo de bytes em texto-plano
- A recuperação do IV associado ao *Keystream* é simples (está em claro)
- Resultados teóricos mostram que
  - PTW possui 50% de chance de recuperar um chave WEP de 104 bits com a captura de 40 mil quadros !
  - Para ter sucesso em 95% dos casos, são necessários 85 mil quadros

WEP: Ataque PTW

- No PTW, cada byte da chave é computado de forma independente e por isso o ataque pode ser executado mais rápido

- Teste realizado pelos autores do ataque permitiu encontrar uma chave WEP de 104 bits em menos de 60 segundos !
  - Coletaram pouco mais de 40 mil keystreams nesse teste

- Mas precisa obter muitos ARPs para conseguir vários *keystreams* !
  - Posso esperar de forma passiva por ARPs passando pela rede (pode demorar!)
  - Posso fazer um ataque ativo, reinjetando na rede pacotes ARPs previamente capturados

- PTW não consegue encontrar todas as chaves possíveis
  - Mas encontra a grande maioria e ainda existem os outros ataques!

- PTW nem sempre é tão rápido (depende da existência de ARPs)
  - Mas pode durar apenas alguns minutos

WEP: Principais ataques de recuperação de chaves

- Principais ataques de recuperação de chaves
  - FMS (2001)
  - Otimizações do FMS (2004)
  - Família de 17 ataques KoreK (2004)
  - PTW (2007)

- Ataques mais eficientes e disponíveis em ferramentas de domínio público
  - PTW
  - Versão combinada de ataques: FMS, KoreK e Força-Bruta

- Força-Bruta nesse caso consiste em testar todas as possibilidades para algum byte

WEP: Exemplos de Ataques

- Versão combinada de ataques: FMS, KoreK e Força-Bruta

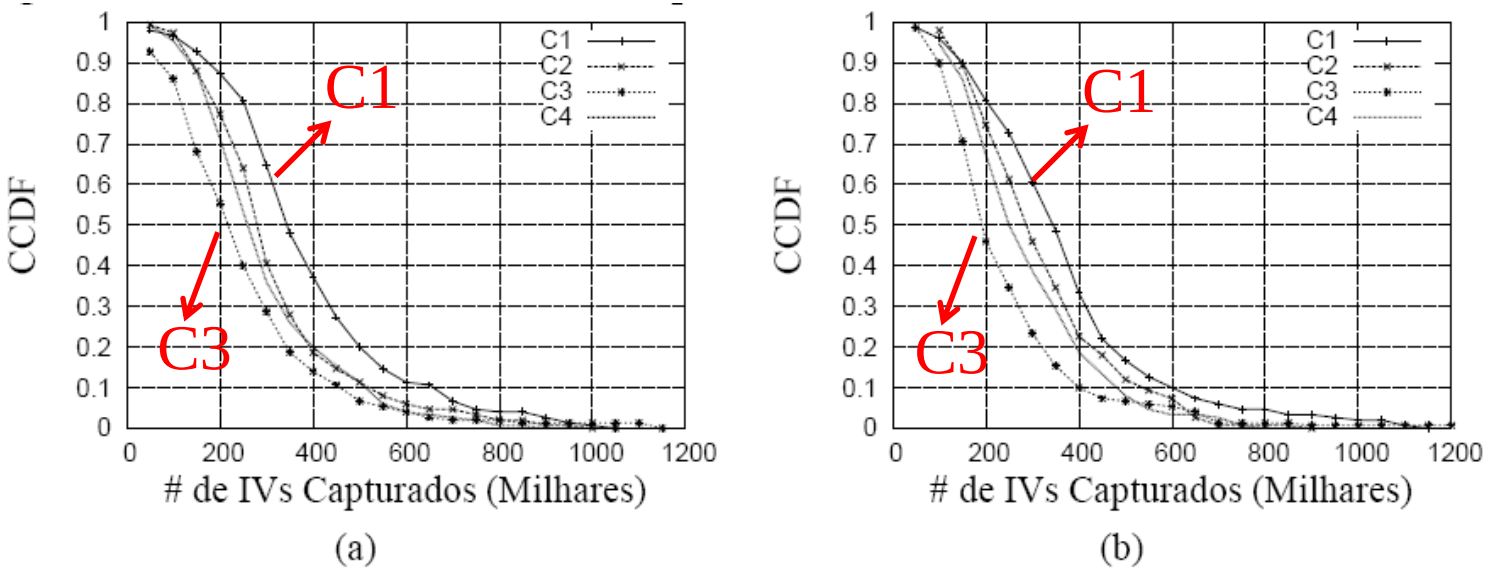


Figura 1. Gerador de IVs: (a) Tipo 2 (b) Tipo 3

Chave 1 (C1): sTo4hOuh176la
Chave 2 (C2): c-i*S3ia+ri2p
Chave 3 (C3): Sw6##leCrO+2=
Chave 4 (C4): aaaaaaaaaaaa

Tipo 2: incrementa os IVs seguindo a convenção *little endian e não* utiliza o o IVs zero nem os IVs propensos ao ataque FMS

Tipo 3: incrementa os IVs seguindo a convenção *little endian* e também não utiliza o IV zero

WEP: Exemplos de Ataques

- Versão combinada de ataques: FMS, KoreK e Força-Bruta

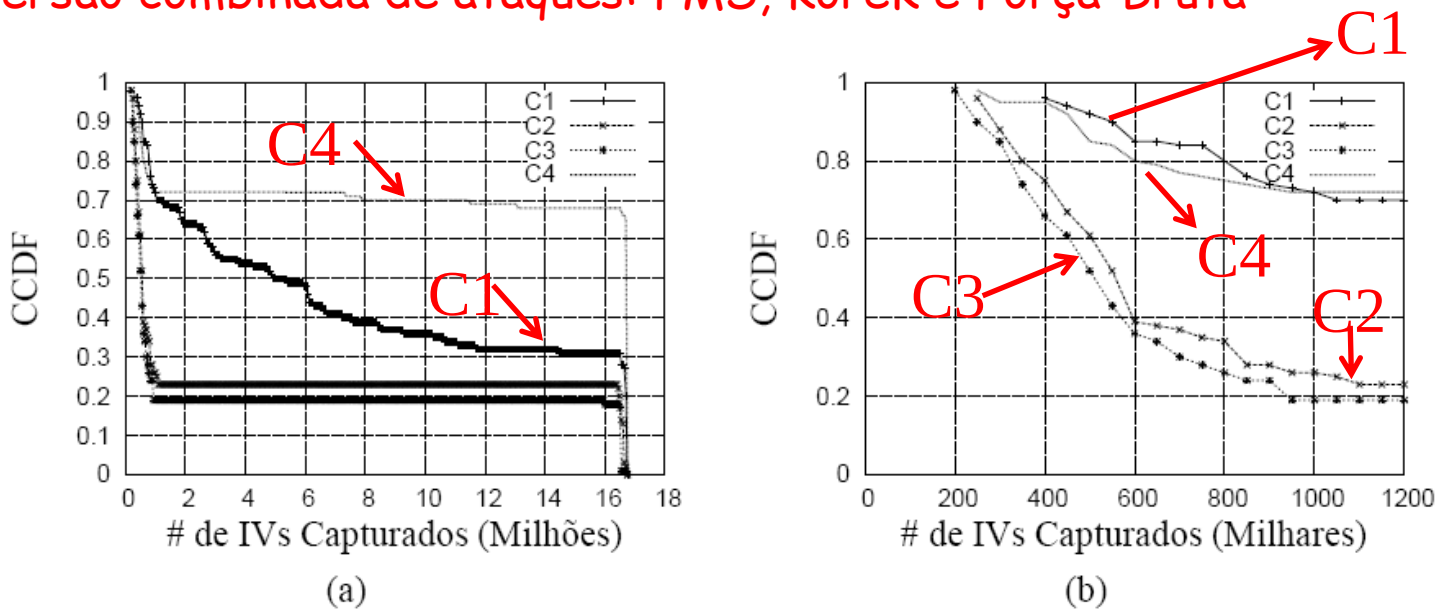


Figura 2. Gerador de IVs Tipo 1

Chave 1 (C1): sTo4hOuh176la
Chave 2 (C2): c-i*S3ia+ri2p
Chave 3 (C3): Sw6##leCrO+2=
Chave 4 (C4): aaaaaaaaaaaa

Tipo 1: incrementa os IVs seguindo a convenção *big endian* e o IV zero não é utilizado

WEP: Exemplos de Ataques

- Versão combinada de ataques: FMS, KoreK e Força-Bruta

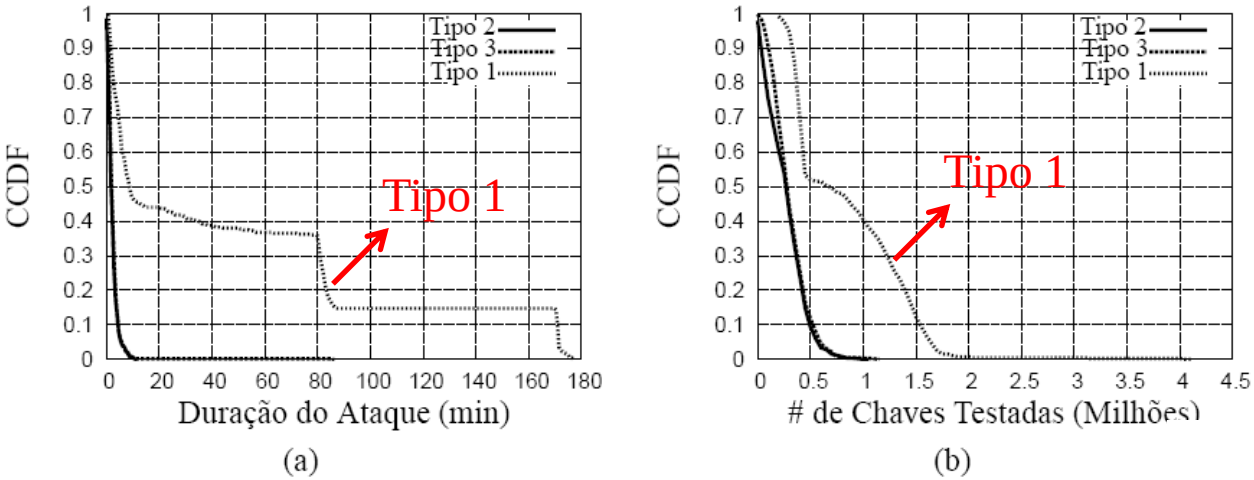


Figura 4. Avaliações de acordo com tipos de contadores de IVs

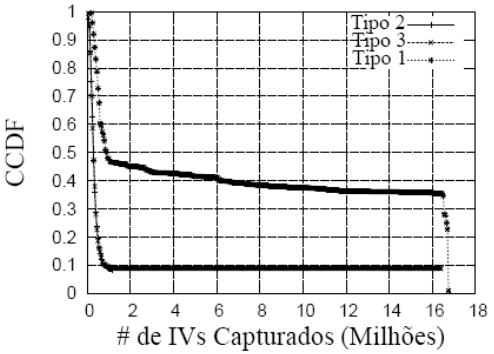


Figura 3. Impacto da forma de incrementação dos IVs

Tipo 1: incrementa os IVs seguindo a convenção *big endian* e o IV zero não é utilizado
Tipo 2: incrementa os IVs seguindo a convenção *little endian e não* utiliza o o IVs zero nem os IVs propensos ao ataque FMS
Tipo 3: incrementa os IVs seguindo a convenção *little endian* e também não utiliza o IV zero

WEP: Exemplos de Ataques

- PTW Ativo (em uma plataforma de testes)

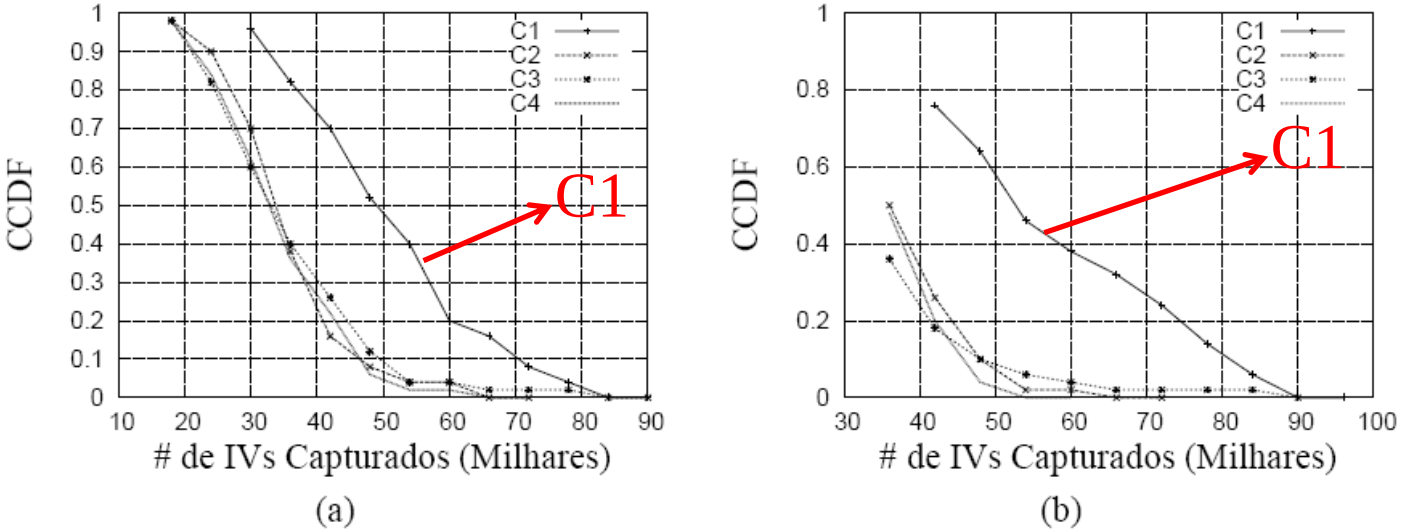


Figura 5. Cenários: (a) Início imediato e (b) Início postergado em 120 segundos

Chave 1 (C1): sTo4hOuh176la
Chave 2 (C2): c-i*S3ia+ri2p
Chave 3 (C3): Sw6##leCrO+2=
Chave 4 (C4): aaaaaaaaaaaa

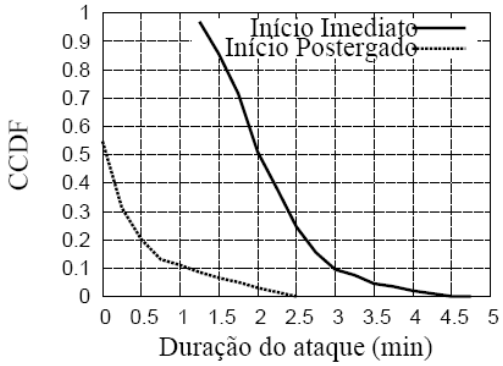


Figura 6. Avaliação do PTW ativo

WEP: Exemplos de Ataques

- PTW Ativo (em uma rede real)

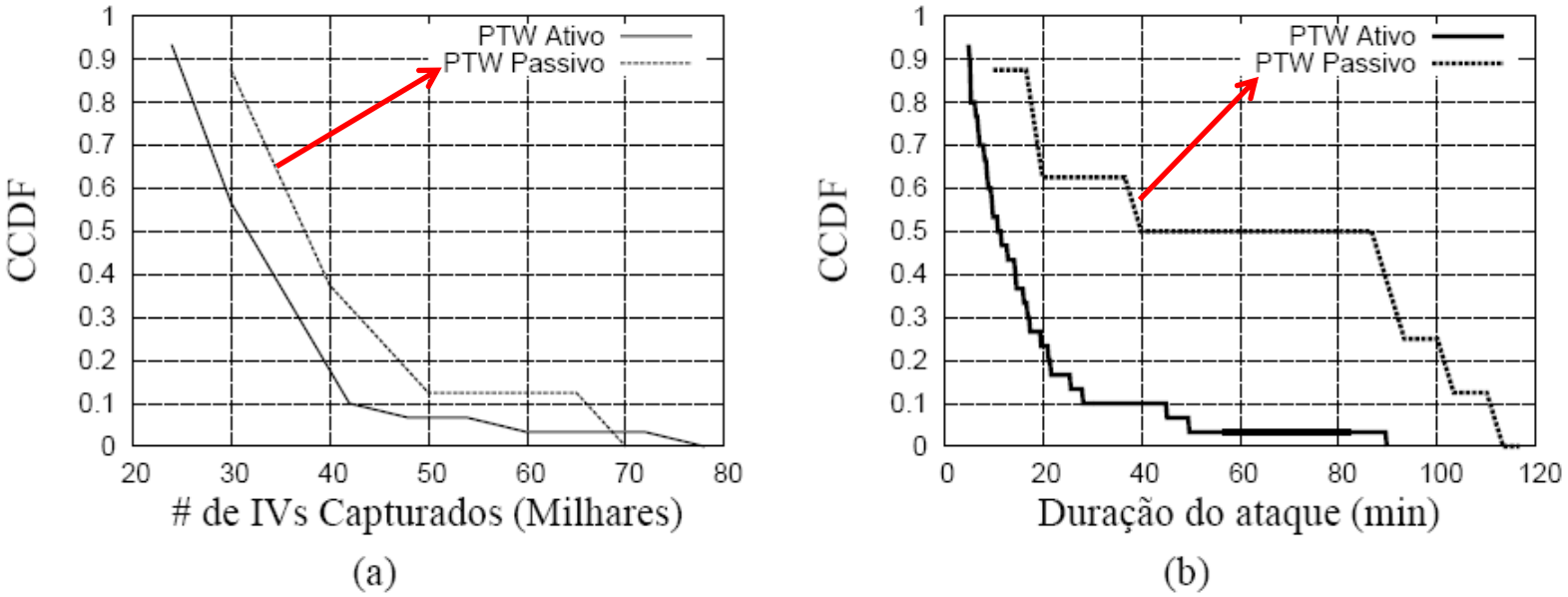


Figura 7. Avaliações: (a) Número de IVs capturados (b) Duração do ataque.

As chaves WEP podem ser fornecidas como uma sequência curta de caracteres em ASCII (*e.g.* 13 caracteres – 104 bits) ou como uma sequência longa de números em hexadecimal (26 caracteres). A rede em questão usava uma chave WEP em hexadecimal

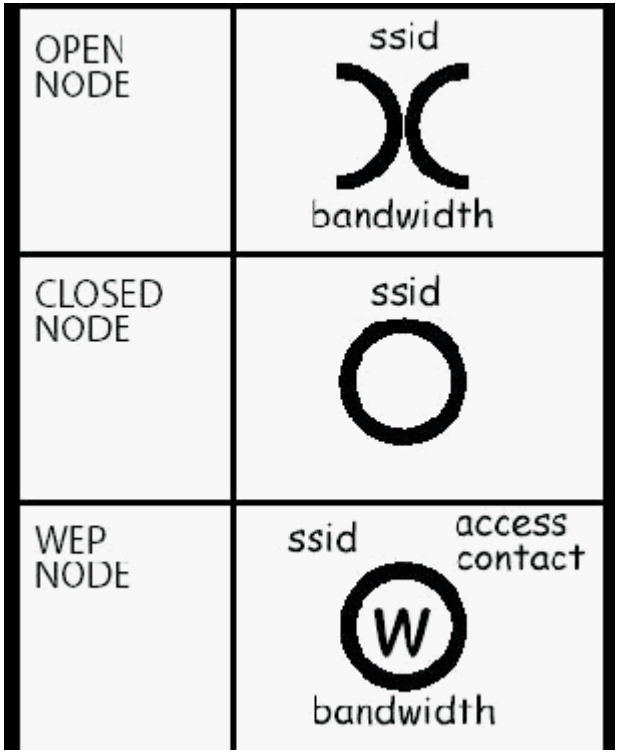
(PARÊNTESES)

CURIOSIDADE

Warchalking

- Ato de desenhar símbolos em lugares públicos de forma a avisar as pessoas sobre redes Wi-Fi na região
- Criação atribuída (na Internet) ao *webdesigner Matt Jones*
  - Alusão à linguagem de sinais usada por mendigos e viajantes para indicar lugares com comida grátis, cama confortável, confusão ...
- Símbolos indicam a presença da rede sem fio, sua banda passante e seu SSID

Símbolos Originais

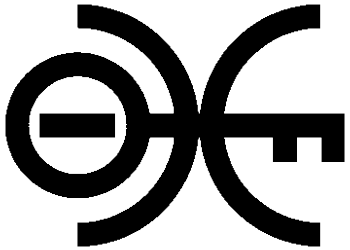


Warchalking

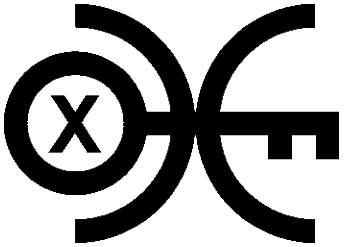
- Exemplos

Warchalking

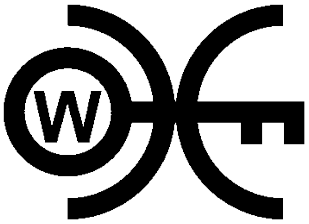
- Novos Símbolos



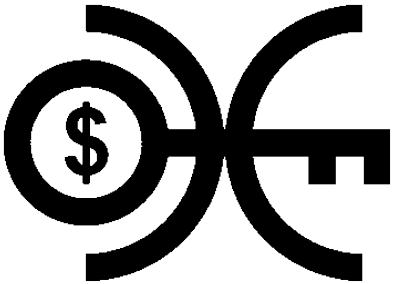
Nó Invisível
(Não divulga SSID)



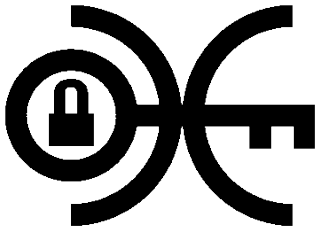
Nó Fechado



Nó usando criptografia



Rede Paga



Nó usando controle de acesso via endereço MAC

Segurança em Redes IEEE 802.11

- Protocolos de Segurança
  - WEP
  - WPA
  - IEEE 802.11i ou WPA2
  - IEEE 802.11w

WPA (Wi-Fi Protected Access)

- Motivação: vulnerabilidades do WEP
  - Grupo de trabalho do IEEE inicia desenvolvimento de novo protocolo de segurança: IEEE 802.11i
  - IEEE -> lento!

- Enquanto isso ...
  - Tentativa de resposta rápida da Wi-Fi Alliance
  - Wi-Fi Alliance apresenta em 2003 um novo protocolo de segurança denominado WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access)

- Principais Características
  - Baseado no RC4 e em um subconjunto de especificações apresentadas em uma versão preliminar (rascunho/draft) do IEEE 802.11i
  - Mudanças no IV
    - Antes ... IV era de 24 bits -> ~16 milhões de IVs, facilitando repetições
    - Agora ... IV de 48 bits → 2^(48) > 280 trilhões !
    - Agora ... introdução de regras para a escolha e verificação de IVs (para impedir a reijenção de pacotes)
  - Distribuição e Derivação de Chaves
    - Deriva e distribui automaticamente chaves que serão utilizadas para a criptografia e verificação de integridade de dados
    - Resolve o problema da chave estática do WEP

WPA (Wi-Fi Protected Access)

- Principais Características
  - Usa conceito de chaves temporais
    - Há uma chave principal denominada PMK (Pairwise Master Key), da qual se derivam outras chaves como a chave de criptografia e integridade de dados
    - PMK não é usada para criptografar!
  - Novo código de verificação de mensagens
    - Insere o campo de 64 bits MIC (*Message Integrity Code*)
    - Permite verificar se quadro de dados possui alterações por erros de transmissão ou manipulação de dados
    - MIC é obtido através do algoritmo Michael (usa chave)
  - Não há suporte para redes Ad Hoc como no WEP
  - Implementação através de uma atualização de firmware nos equipamentos WEP

WPA: Autenticação

- O WPA define dois métodos de autenticação
  - Corporativo
  - Pessoal ou PSK

Autenticação: WPA Pessoal

Lembrete

PMK é a chave mestra da rede

- WPA Pessoal ou WPA-PSK (Pre-Shared Key)
  - Usado caso seja impossível ou indesejável o uso de um servidor de autenticação
  - Usado tipicamente em redes residências e de pequenos escritórios (redes SOHO – Small Office/Home Office)
  - Clientes e AP compartilham uma chave denominada PSK (Pre-Shared Key)
  - PSK possui **256 bits** e pode ser diretamente fornecida ou calculada com base em uma *passphrase*
    - Diretamente fornecida: através de 64 dígitos hexademais (0 a 9 e A a F) (**256 bits** ao todo)

$$PMK = PSK$$

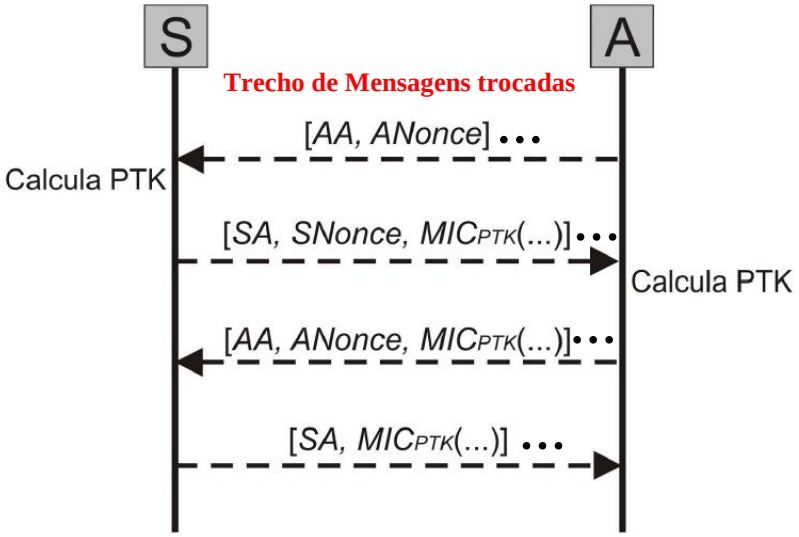
    - Calculada: através de uma passphrase de 8 a 63 caracteres ASCII "imprimíveis". Nesse caso, é necessária sua conversão para **256 bits** através do uso de uma função derivativa PBKDF2

$$PMK = PSK = PBKDF2(passphrase, ssid, ssidLength, 4096, 256)$$

4096 iterações através de uma função *hash* HMAC-SHA1

Autenticação: WPA Pessoal

- Autenticação ocorre durante o 4-Way Handshake entre o cliente e o AP
- Durante o 4-Way Handshake entre um cliente e o AP ocorre a derivação de uma chave PTK (*Pairwise Transient Key*) comum e exclusiva a eles
  - A PTK representa na prática um conjunto hierárquico de chaves temporárias
  - A PTK serve para a criptografia de dados, verificação de integridade, etc



Legenda

S: Cliente
A: Ponto de Acesso (AP)
AA: Endereço MAC do AP
AS: Endereço MAC do Cliente
ANonce: *nonce* do Cliente
SNonce: *nonce* do AP
MIC_{PKT}: campo de 64 bits para verificação de integridade

Autenticação: WPA Pessoal

- Cálculo/Derivação da PTK é feito/feita utilizando-se uma PRF (*Pseudo Random Function*)

PTK = PRF(PMK, "Pairwise key expansion", *Min*(AA,AS) || *Max*(AA,AS) || *Min*(ANonce, SNonce) || *Max*(ANonce, Snonce))

Legenda

S: Cliente
A: Ponto de Acesso (AP)
AA: Endereço MAC do AP
AS: Endereço MAC do Cliente
ANonce: nonce do Cliente
SNonce: nonce do AP

Lembrete

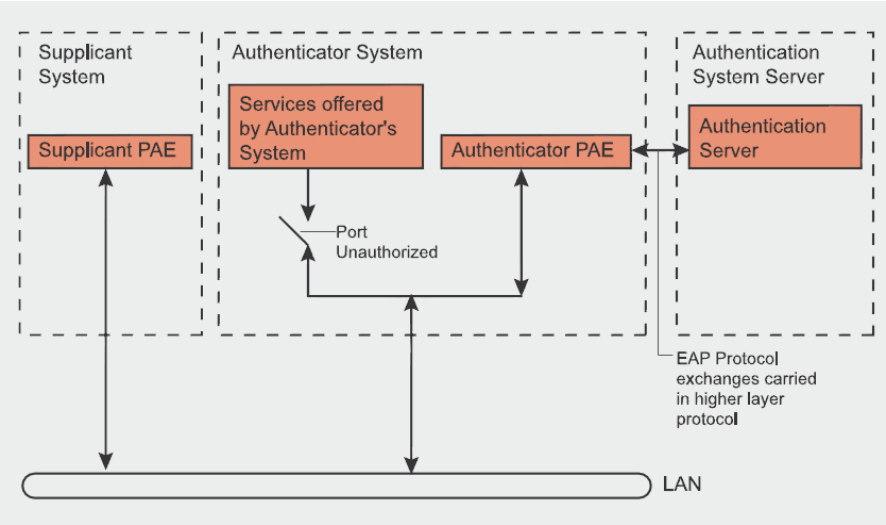
PMK é a chave mestra da rede

Autenticação: WPA Corporativo

- WPA Corporativo
  - Uso de um servidor de autenticação
  - Arquitetura/Protocolo IEEE 802.1X com algum tipo de EAP (*Extensible Authentication Protocol*)

Autenticação: WPA Corporativo

- IEEE 802.1X
  - aka *Port-Based Network Access Control*
  - *Framework* originalmente para redes cabeadas
  - Provê
    - Mecanismos de Autenticação
    - Mecanismos de Autorização
    - Mecanismos de distribuição de chave
    - Implementa controle de acesso de usuários à rede
  - Arquitetura composta por 3 entidades
    - Supplicant - cliente/usuário que se associa à rede
    - Servidor de Autenticação - toma decisões sobre autorização (e.g. RADIUS)
    - Autenticador - provê controle de acesso (dispositivo entre os dois componentes acima)
  - Há pequenas modificações para redes sem fio
    - Considera possibilidade de roubo de identidade
    - Incorpora autenticação de mensagem



PAE: *Port Access Entity*

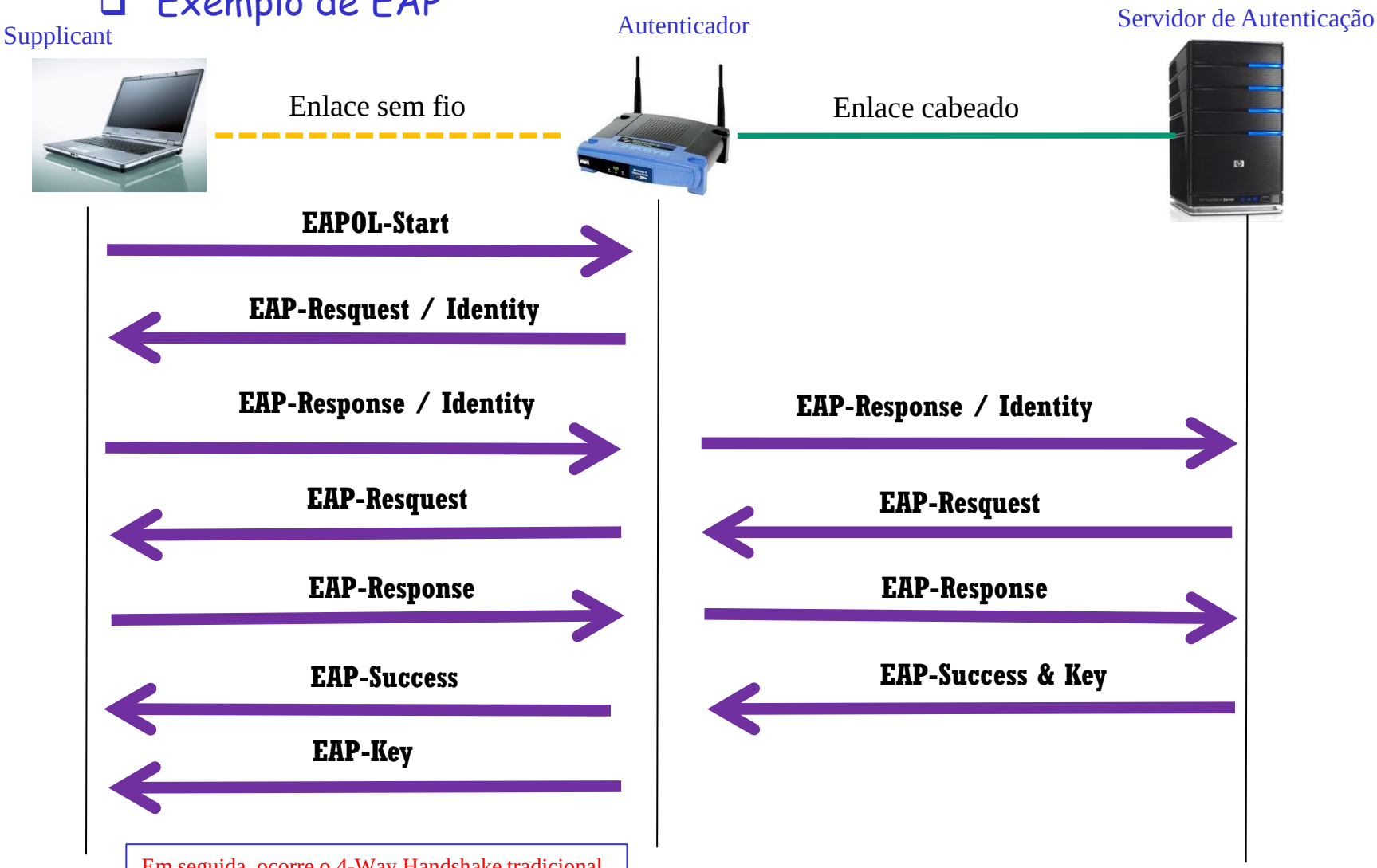
garante que *supplicant* e autenticador calculem suas chaves secretas e habilitem a criptografia antes de acessarem a rede

Autenticação: WPA Corporativo

- EAP (*Extensible Authentication Protocol*)
  - *Framework* para o transporte de vários métodos de autenticação
  - Permite um número limitado de mensagens *(Request, Response, Success, Failure)* com outras mensagens intermediárias de acordo com o método de autenticação usado *(e.g. EAP-TLS, EAP-TTLS)*
- Comunicação entre *supplicant* e autenticador
  - usa protocolo do tipo EAP
- Comunicação entre autenticador e servidor de autenticação
  - Prossegue usando o protocolo EAPOL (EAP Over LAN)
  - EAPOL transporta dados utilizando protocolos de camadas mais elevadas como o Radius

Autenticação: WPA Corporativo

- Exemplo de EAP



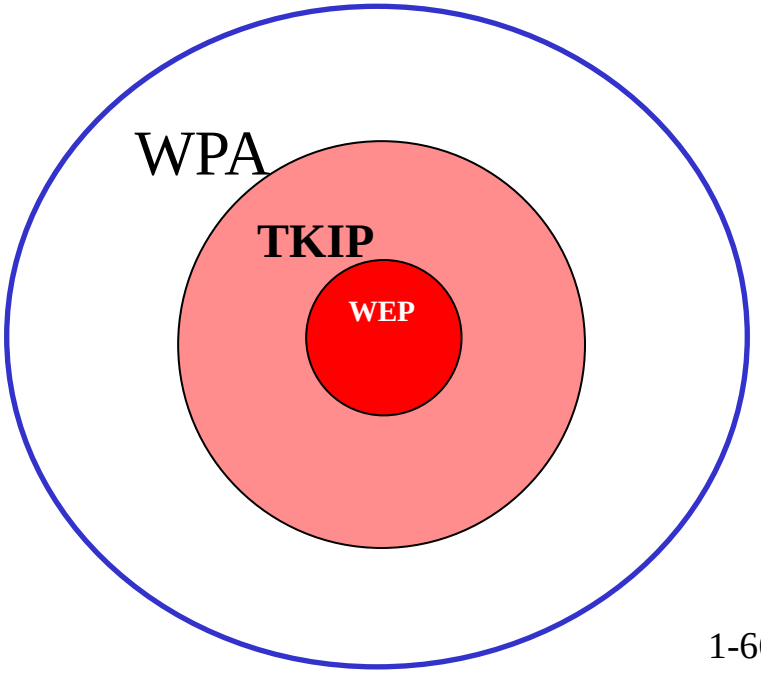
Em seguida, ocorre o 4-Way Handshake tradicional

Autenticação: WPA Corporativo

- Tipos de EAP incluídos na certificação Wi-Fi de 2010
  - EAP-TLS
  - EAP-TTLS/MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - PEAP-TLS
  - EAP-SIM
  - EAP-AKA
  - EAP-FAST
- Existem outros outras variantes na literatura

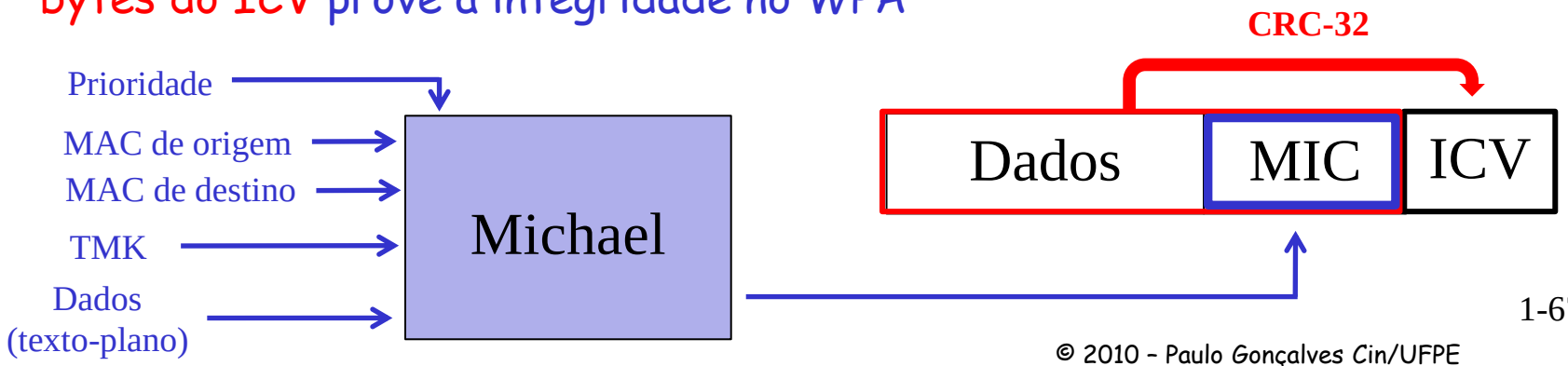
WPA: Integridade e Confidência

- A base do WPA é o protocolo TKIP (*Temporal Integrity Protocol*) e o WEP
- O TKIP pode ser visto como um invólucro envolta ("wrapper around") do WEP
  - Objetivo: Prover melhor segurança dadas as restrições de projeto (usar mesmo hardware e manter bom desempenho)
- O TKIP é composto por 4 componentes
  - Algoritmo de verificação de integridade Michael (MIC) – acabar com alterações maliciosas
  - Nova disciplina de sequenciamento dos IVs – acabar com "replay attacks"
- O TKIP é composto por 4 componentes (*cont.*)
  - Um algoritmo de combinação de chaves (*key mixing function*) por pacote – acabar com a correlação entre os IVs públicos e chaves fracas
  - Um mecanismo de renovação de chaves – acabar com reuso de chaves

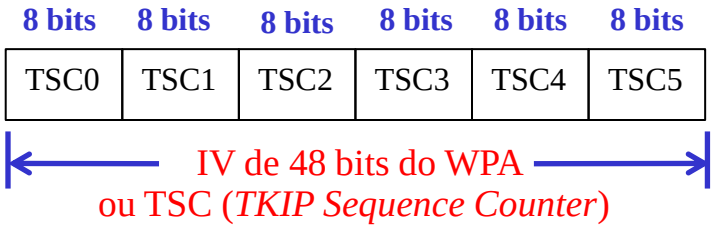


WPA: Integridade

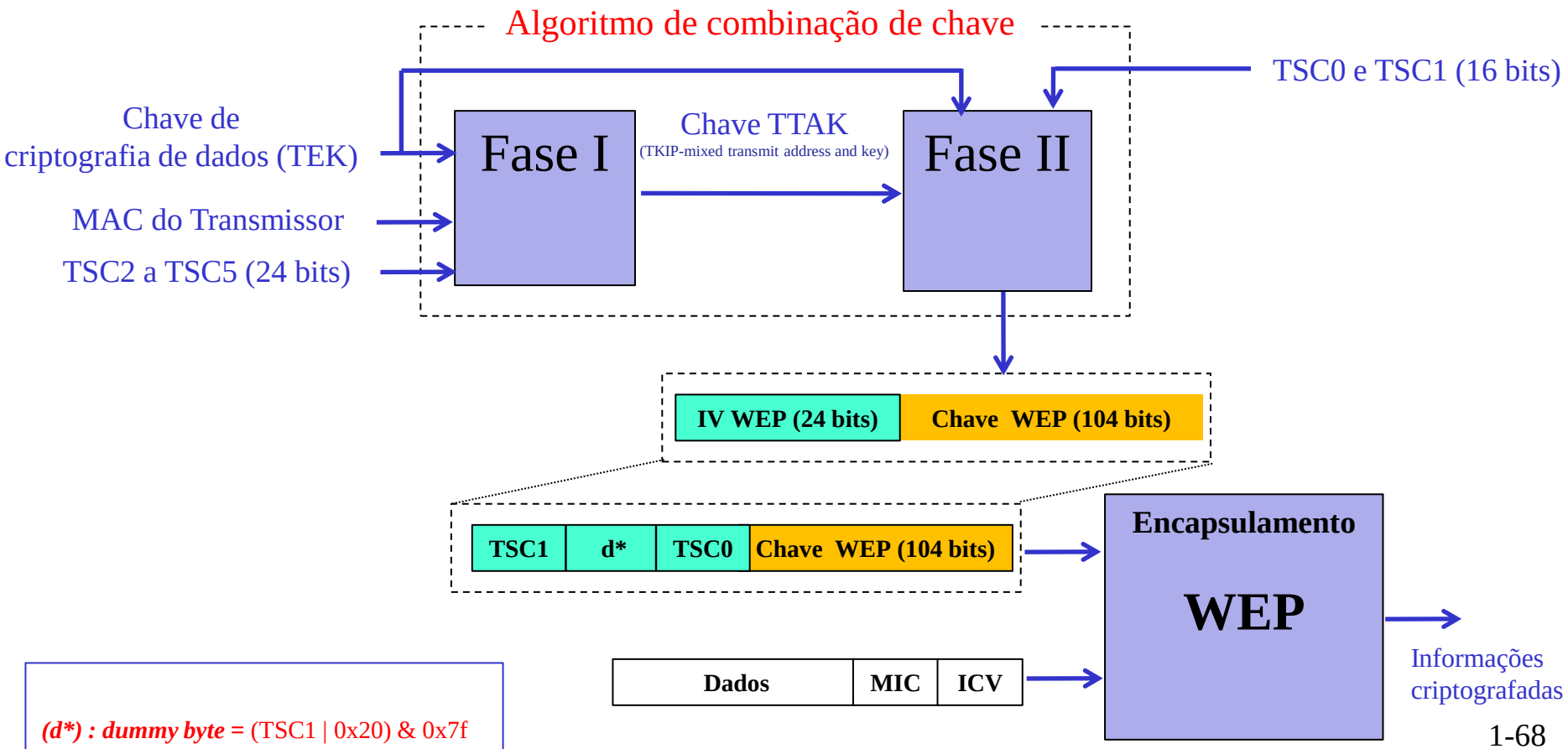
- Usa o ICV e o MIC
- O Michael (MIC) é uma função hash não-linear
  - Mais seguro do que CRC-32
- Recebe os seguintes parâmetros
  - Endereço MAC de destino
  - Endereço MAC de origem
  - Prioridade (definida como zero mas deve ser usada "futuramente" para suporte ao IEEE 802.11e)
  - Dados em texto-plano
  - Chave de integridade TMK (*Temporal MIC Key*) – compõe a PTK
- A saída do Michael corresponde à 8 bytes (MIC) que juntamente com os 4 bytes do ICV provê a integridade no WPA



WPA: Confidência



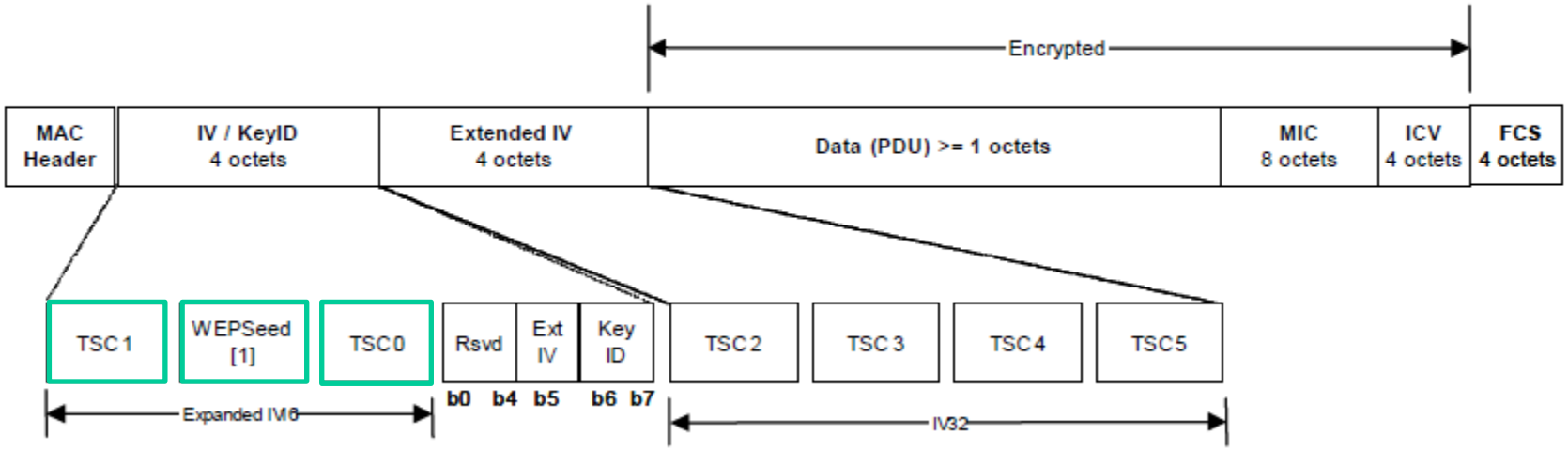
- Usa o WEP
  - Principal diferença está na chave que irá alimentar o RC4
  - Essa chave é o resultado de um algoritmo de combinação de chave
  - A chave é única por pacote!



(d*) : dummy byte = (TSC1 | 0x20) & 0x7f

WPA: Quadro

- quadro conforme especificação do TKIP (802.11i-2004 - amendment 6)



TSC0...5: TKIP Sequence Counter ou IV do WPA (48 bits)

WEPSeed[1]: (TSC1 | 0x20) & 0x7f → ***dummy byte d****

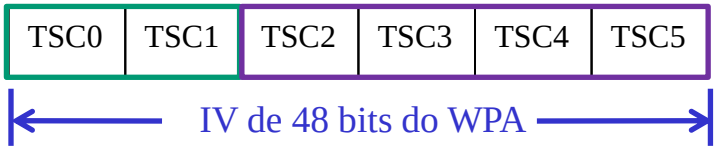
FCS: *Frame Check Sequence* (para detecção de erro – ruído)

ExtIV: indica presença/ausência de IV estendido

KeyID: índice da chave

WPA: Regras e Contra-medidas

- Regras para o TKIP Sequence Counter (TSC)
  - Incrementado a cada quadro transmitido
  - Incrementa-se os 16 primeiros bits de 0x0000 a 0xFFFF
  - Ao se zerar novamente os 16 primeiros bits, incrementa-se os últimos 32 bits de 1 unidade



  - TSC é zerado ao se mudar a PTK

- FCS, ICV e TSC são verificados primeiro
  - FCS e ICV provêem verificação de erros apenas
  - TSC fora de ordem é considerado "replay attack" (há exceções → retransmissões)
  - Se tudo está ok, só então o MIC é verificado

WPA: Regras e Contra-medidas

- Regras para o MIC
  - Se dois erros de MIC são detectados em menos de 60 segundos, assume-se que o MIC está sendo atacado
  - Em caso de ataque ao MIC, AP deleta as chaves temporárias, desassocia a estação e aguarda 1 minuto para a sua reassociação
- Tempo para renovação "normal" de chaves no TKIP
  - Default: 3600 segundos
  - Pode ser configurado pelo administrador para um tempo menor

WPA: Vulnerabilidades?

- Passphrase da rede (WPA-PSK) precisa ter mais de 20 caracteres
  - Senão ... sujeito a ataques de dicionário
  - Basta capturar informações durante o 4-way-handshake
- Ataque (impraticável ... ainda)
  - Tendo conhecimento de algumas chaves RC4 (menos de 10) geradas por IVs cujos 32 bits mais significativos são os mesmos, é possível achar a chave de criptografia e integridade de dados
  - Complexidade de Tempo: O(2^(105)) em vez de O(2^(128)) quando realizado ataque de força-bruta pura
- Negação de Serviço
  - Se 2 erros de MIC detectados em menos de 1 minuto, AP cancela a conexão por 60 segundos e altera as chaves
  - Ao se reinjetar pacotes mal formados ... consegue-se um ataque de negação de serviço
- Não há proteção dos quadros de gerenciamento
  - Sujeito aos mesmos ataques de negação de serviço do WEP

WPA: Vulnerabilidades?

- Descobriram recentemente (2009) um ataque (*Beck and Tews*) que explora fraquezas do Michael (MIC) e do TKIP
  - Um atacante com acesso à rede por 12-15 minutos pode decifrar uma requisição ou resposta ARP e enviar 7 pacotes "customizados" para a rede
  - E qual o problema? Pode-se injetar pacotes maliciosos na rede (serão aceitos como legítimos)
  - Há pré-requisitos: IEEE 802.11e ... mas a versão estendida desse ataque proposta por *Ohigashi e Morii* (2009) elimina esse pré-requisito (o ataque é do tipo *man-in-the-middle*)
- Ataque *Beck and Tews* foi melhorado pelo próprio *Tews* (fev 2010)
  - Permite reinjetar pacotes maiores e em quantidade maior do que antes

Soluções para os três ataques de reinjeção de pacotes maliciosos?

Segurança em Redes IEEE 802.11

- Protocolos de Segurança
  - WEP
  - WPA
  - IEEE 802.11i ou WPA2
  - IEEE 802.11w

WPA2 (Wi-Fi Protected Access 2) ou IEEE 802.11i

- Especificação aprovada em 2004
- Retro-compatível com o WPA
  - Lembre-se que o WPA é um baseado em um rascunho do IEEE 802.11i
- Principais avanços em relação ao WPA
  - Novos algoritmos de criptografia e integridade
  - CTR with CBC-MAC Protocol (CCMP)
    - Provê confidência, autenticação adicional, integridade e proteção contra "replay attacks"
    - Baseado no algoritmo de criptografia AES (*Advanced Encryption Standard)* no modo de operação CCM
- Observações
  - Requer hardware mais "poderoso"
  - Não dá para fazer via upgrade de *firmware*
  - IV continua com 48 bits

WPA2 - Autenticação

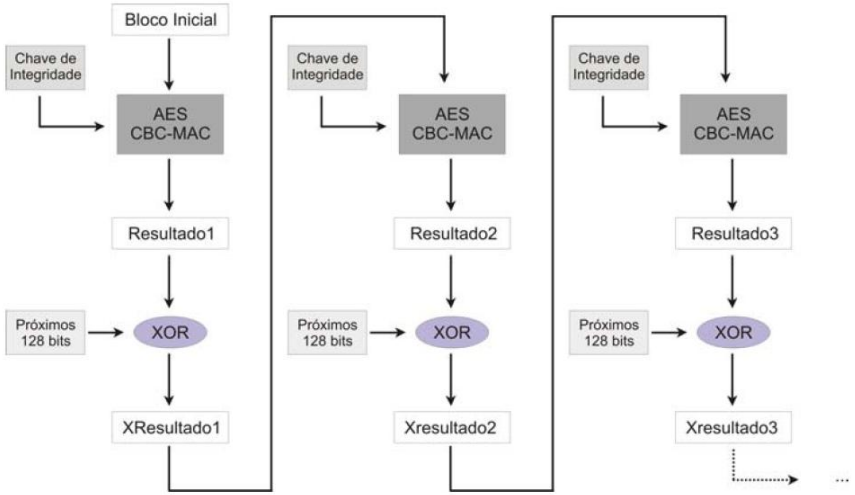
- Similar ao WPA mas introduz AAD
  - AAD (*Additional Authentication Data*) – Dados que não são criptografados mas estão "criptograficamente" protegidos (mais a seguir …)

- Preocupação com *roaming*
  - PMK Caching
    - AP guarda informações sobre autenticação de clientes
    - diminui número de mensagens trocadas para re-autenticações
  - Preauthentication
    - cliente se associa à vários APs previamente

WPA2 – Integridade

- Uso do protocolo CCMP *(Counter Mode with Cipher Block Chaining Message Authentication Protocol)* para prover integridade e confidência

- O CBC-MAC *(Cipher Block Chaining Message Authentication Code)* é responsável pela integridade dos quadros
  - Baseado no AES
  - Blocos e chaves de 128 bits
  - Saída de 128 bits mas usa-se os 64 bits mais significativos no campo MIC

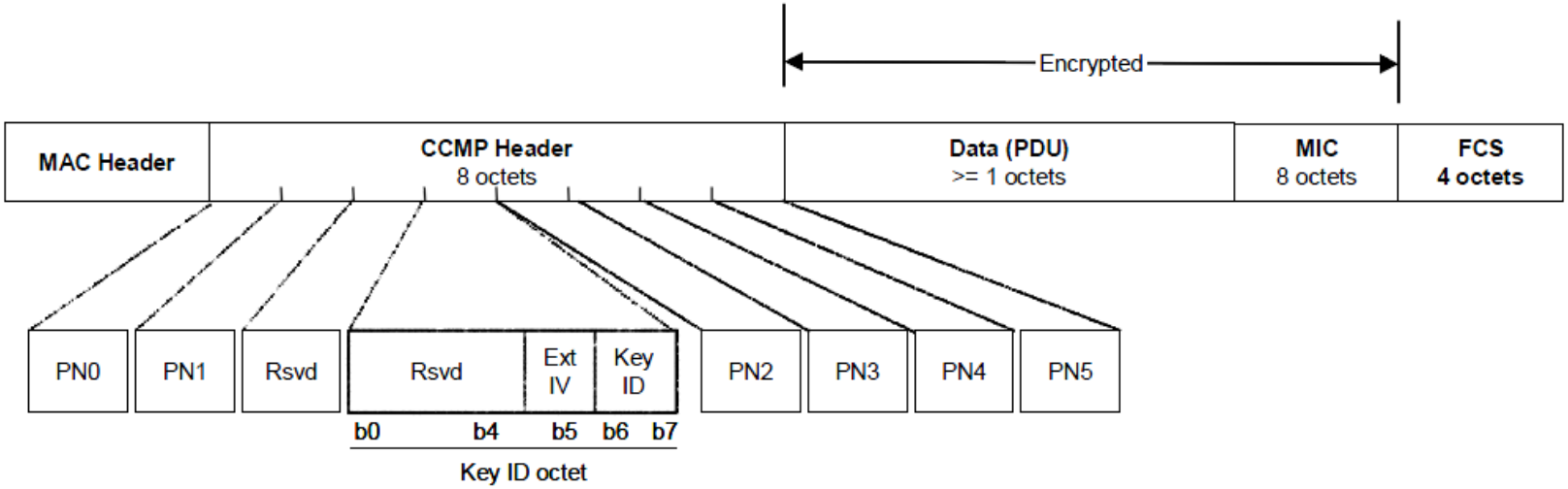


WPA2 – Confidência

- Uso do protocolo CCMP *(Counter Mode with Cipher Block Chaining Message Authentication Protocol)* para prover integridade e confidência
- Usa conceito de chaves temporais como TKIP
- A partir da PMK são geradas as chaves de criptografia e integridade
- Criptografia de quadros com o AES Counter Mode (CTR)
  - Chave simétrica de 128 bits

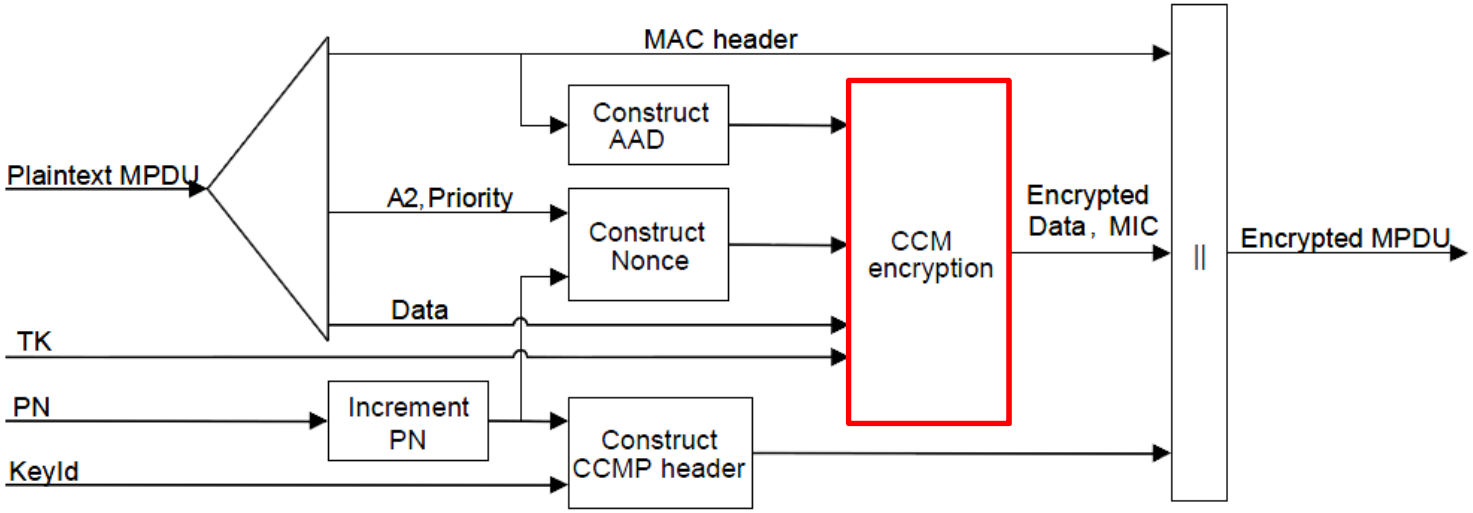
WPA2 - Quadro

- quadro conforme especificação do CCMP (802.11i-2004 - amendment 6)



PN: Packet Number ou IV do WPA2 (48 bits)

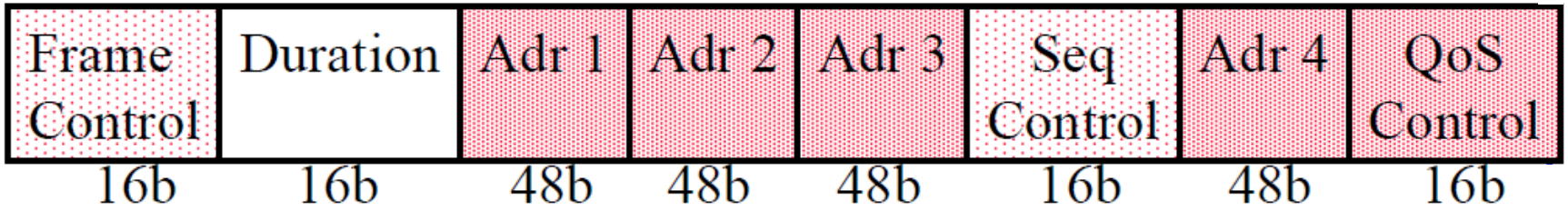
WPA2 – Encapsulamento CCMP



PN: Packet Number ou IV do WPA2 (48 bits)
TK: Chave de criptografia de dados
A2: MPDU Address 2
Priority: uso reservado (setado para zero)
AAD: *Additional Authentication Data*

WPA2 – AAD (Additional Authentication Data)

- AAD
  - Dados que não são criptografados mas estão "criptograficamente" protegidos
- AAD é incluído no cálculo do MIC
  - Alguns bits do "Frame Control" e "Seq. Control" são zerados e "Duration" não é incluído
  - Não consegue-se alterar endereço MAC (MAC Spoofing)



WPA2 - Vulnerabilidades

- Passphrase da rede pequena (WPA-PSK) -> 20 caracteres
- Negação de serviço (e.g. desautenticação)
- Sem proteção nos quadros de gerenciamento

Segurança em Redes IEEE 802.11

- Protocolos de Segurança
  - WEP
  - WPA
  - IEEE 802.11i ou WPA2
  - IEEE 802.11w

IEEE 802.11w

- É uma emenda ao WPA e ao WPA2
- Provê "Alteração/Correção" que adiciona proteção aos quadros de gerenciamento
  - Bye bye ataques de negação de serviço do tipo de-authentication/desautenticação
- Padrões IEEE 802.11v, 802.11k e 802.11r estendem funcionalidades dos quadros de gerenciamento
  - Agora podem conter informações "sensíveis" sem problemas (e.g. recursos de rádio, identificadores de localização, dados para execução de *handoffs*)
- Protocolo recente
  - Especificação saiu em 2009
  - Vulnerabilidades? E os quadros de controle?

Futuro: WEP, WPA e WPA2

- WPA2 é retro-compatível com o WPA
  - Permite operar com TKIP somente (WPA), AES somente ou mixed TKIP/AES (negocia com cada cliente qual utilizar)
- Transição para um mundo Wi-Fi puramente AES em 2014 !
  - A partir de 1º de janeiro de 2011, TKIP e WEP não serão, ao poucos, mais suportados em novos dispositivos Wi-Fi para obterem certificação
  - Retirada do suporte será em fases e durará 3 anos (até 1º de janeiro de 2014)
  - Em 2012 -> acaba suporte ao TKIP em novos *adaptadores Wi-Fi*
  - Em 2013 -> acaba suporte ao WEP em novos *APs*
  - Em 2014 -> acaba suporte ao mixed TKIP/AES em novos *APs*
  - Em 2014 -> acaba suporte ao WEP em novos *adaptadores Wi-Fi*
- Padrão IEEE 802.11n especifica suporte somente ao AES
  - Se estiver usando produto 802.11n configurado com WEP ou TKIP, quer dizer que ele está funcionando no modo de operação 802.11g (54 Mbps)

Recomendações

- Modo de Autenticação Pessoal
  - o quão importante é a segurança da sua rede e de seus dados pra você?
  - sempre que possível use WPA2 com AES ... mas pode não ser possível ou desejável
    - (hardware não suporta, consumo mais rápido da bateria do handset/notebook, etc)
  - quando não for possível ou desejável
    - previna-se com eventuais "workarounds" ... sim, eles são importantes e necessários até a transição para o mundo Wi-Fi puramente AES em 2014 somente!
- Modo de Autenticação Corporativo
  - É o melhor caminho para empresas e instituições
  - Tradicionalmente mais seguro do que o Método de Autenticação Pessoal
  - Servidor de autenticação (Manutenção/Administração)
  - Nenhuma vulnerabilidade conhecida?
- Uso de redes abertas (e.g. lugares públicos, restaurantes, aeroportos, shoppings)
  - Acesso pode ser direto à Internet ou pode precisar de verificação de credenciais (e.g. login e senha ou CPF)
  - Não há criptografia na camada enlace. Use https (camdada aplicação) sempre que possível. Caso contrário, evite acesso a sites "sensíveis"

AUDITORIA DE REDES IEEE 802.11

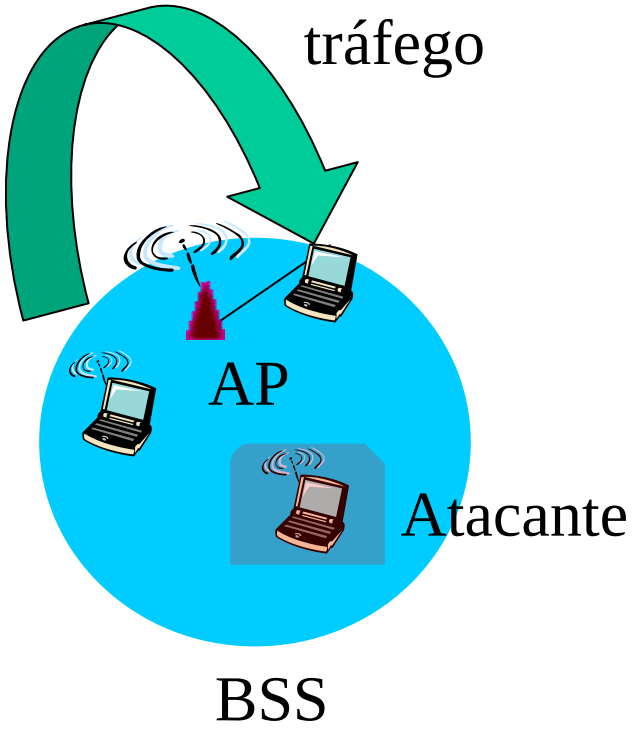
Auditoria de Redes IEEE 802.11

- Existem diversas ferramentas de domínio público para isso
  - Aircrack
  - coWPAtty
  - Airsnarf

- Um pouco mais sobre o Aircrack (http://www.aircrack-ng.org)
  - Conjunto de ferramentas para auditar [ou atacar] redes Wi-Fi
  - Airmon-ng
    - coloca interface wireless em modo monitor
  - Airodump-ng
    - Possui diversas funções, entre elas capturar "IVs" do WEP
  - Aireplay-ng
    - 0: Desautenticação;
    - 3: Reinjeção de requisição ARP;
  - Airdecap-ng
    - Tenta decifrar chave WEP ou WPA a partir de informações no arquivo.cap obtido

Auditoria de Redes IEEE 802.11: Parte Prática

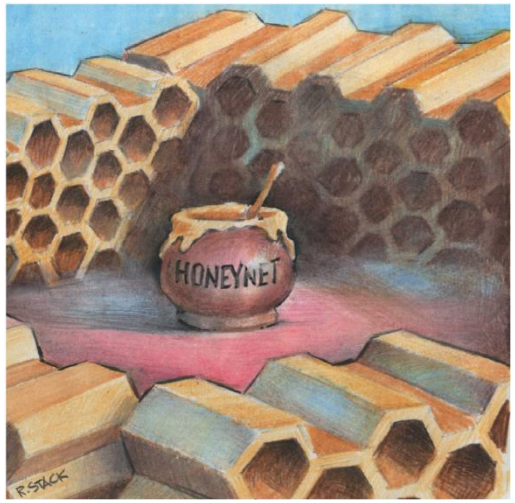
- Infra-estrutura de teste



ROGUE APS
HONEYPOTS E HONEYNETS

Outros Tópicos em Segurança de Redes IEEE 802.11

- Honeypots e Honeynets
  - Objetivo: atrair invasores para uma rede falsa e coletar informações sobre eles
  - Projetados para parecerem sistemas reais



- Rogue AP ou AP falso/não autorizado
  - Objetivo: Roubo de informações de usuários de redes sem fio
  - Como combater?

Apresentações

- Honeypots e Honeynets
  - Wireless honeypots: survey and assessment (ISTA 2009)
- Rogue AP
  - A Measurement Based Rogue AP Detection Scheme (INFOCOM 2009)
  - A Passive Approach to Rogue Access Point Detection (GLOBECOM 2007)
  - Rogue access point detection and localization (Personal Indoor and Mobile Radio Communications (PIMRC), 2012)
  - A passive approach to wireless device fingerprinting (DNS 2010)
  - Detecting protected layer-3 rogue Aps (Broadnets 2007)
- Autenticação
  - **Um Mecanismo de Autenticação Baseado em EDCH para Redes IEEE 802.11 (SBSeg 2010)**
    - http://www.cin.ufpe.br/~pasg/gpublications/SoGo10.pdf

Projeto

- Demonstre um ataque de dicionário a uma rede protegida pelo WPA2
- Apresente a solução para que este ataque se torne impraticável e estimativa de tempo para encontrar a chave

- Apresentação dia 24/09 (15 minutos por grupo)