ROGÉRIO PEREIRA DIANA FILHO

UMA ABORDAGEM SOBRE SEGURANÇA EM REDES WIRELESS

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS

Orientador: Prof: Elio Lovisi Filho

BARBACENA

2003

ROGÉRIO PEREIRA DIANA FILHO

UMA ABORDAGEM SEGURANÇA EM REDES WIRELESS

Este trabalho de conclusão de curso foi julgado adequado à obtenção do grau de Bacharelado em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

Barbacena – MG, 09 de novembro de 2003.

_____

Prof. Elio Lovisi Filho - Orientador do Trabalho

_____

Prof. Emerson Rodrigo Alves Tavares- Membro da Banca Examinadora

_____

Prof. Eduardo Macedo Bhering - Membro da Banca Examinadora

AGRADECIMENTOS

Mãe,
dedico este trabalho a você que esteve ao meu lado nas horas que chorei e nas horas que sorri , nas horas que me lamentei e nas horas em que de uma forma ou de outra demonstrei total alegria... Por estar perto de você. Agradecer pelo sorriso diário, sem mágoas nem rancores , agradecer de peito aberto, de alma explosiva...

Hoje quero parar e agradecer, porque você fez , faz e fará sempre parte de minha história! Você é sempre maravilhosa..Eu-te-Amo.

RESUMO

Este trabalho tem como objetivo o estudo das principais características de segurança em redes wireless. Analisaremos o protocolo de comunicação WEP e o algoritmo de criptografia RC4, demonstrando as principais falhas. Será feito um estudo da ferramenta de gerenciamento para redes Wireless Orinoco, utilizada pela empresa Ferteco Mineração, vamos propor uma melhor configuração para que se melhore a segurança. Ao final vamos demonstrar que implementando alguns mecanismos de segurança a rede Wireless da empresa Ferteco Mineração pode se tornar segura e confiável.

Palavras-chave: Wireless, Segurança, Redes

SUMÁRIO

LISTA DE FIGURAS....8

LISTA DE TABELAS....11

LISTA DE SIGLAS....12

1 INTRODUÇÃO....13

2 COMUNICAÇÃO EM COMPUTAÇÃO MÓVEL....15

2.1 APLICAÇÃO DE COMUNICAÇÃO EM COMPUTAÇÃO MÓVEL....15
2.2 WIRELESS....16
2.2.1 Ataques a Redes Wireless....17
2.3 TIPOS DE INTRUSOS....18
2.3.1 Hackers....19
2.4 O FATOR HUMANO....21
2.5 REPLAY....24
2.6 RECUSA OU IMPEDIMENTO DE SERVIÇO....24
2.7 FOOTPRINTING....25
2.8 ALGUNS ERROS COMUNS DE SEGURANÇA:....26
2.9 VARREDURA....26
2.10 ENUMERAÇÃO....27

3 PADRÕES WIRELESS....28

3.1 ARQUITETURA....28
3.2 PADRÕES WIRELESS....29
3.2.1 Padrão IEEE802.11b....29
3.2.2 Padrão IEEE 802.11a....30
3.2.3 IEEE 802.11g....32
3.3 APLICAÇÕES DA REDES WIRELESS....33
3.3.1 WIRELESS LAN's – REDES LOCAIS SEM FIO....34
3.3.2 WIRELESS WANS – REDES GEOGRÁFICAMENTE DISTRIBUÍDOS SEM FIO....37

4 CRIPTOGRAFIA NAS REDES WIRELESS....40

4.1 CRIPTOGRAFIA E SEUS CONCEITOS....40

4.2 CHAVES....43
4.3 TIPOS DE CRIPTOGRAFIA....44
4.3.1 Criptografia por chave secreta....44
4.4 ALGORITMO RC4....48
4.4.1 Algumas fraquezas do RC4....48
4.5 RC4 E A SEGURANÇA....49
4.5.1 Precedentes de ataques no RC4....52

5 WEP E SUA SEGURANÇA....53

5.1 WEP....53
5.1.1 Confidencialidade....55
5.1.2 Integridade....57
5.1.3 Autenticação....57
5.2 QUEBRA DO PROTOCOLO WEP....62
5.2.1 Reutilização de uma Seqüência....62
5.2.2 Gerenciamento das Chaves WEP....64
5.2.3 Autenticação de Mensagens....65

6 PROPOSTA DE SEGURANÇA....68

6.1 ORiNOCO CL (CLIENT) MANAGER....68
6.1.1 Verificando a Qualidade da Comunicação....69
6.1.2 Funções do CL Manager....69
6.1.3 Wireless Orinoco X WEP....71
6.2 PROPOSTA DE SEGURANÇA PARA A REDE EXISTENTE....72
6.2.1 Segurança Orinoco....73
6.3 IMPLEMENTAÇÃO DE MECANISMOS DE SEGURANÇA....74
6.3.1 Autenticação RADIUS....75
6.3.2 Implementação CISCO....77

7 CONCLUSÃO....79

REFERÊNCIAS BIBLIOGRÁFICAS....81

ANEXO A – O PADRÃO IEEE 802.11....83

IEEE 802.11i....83
TKIP....85
AES-CCMP....86
IEEE 802.1X....88

LISTA DE FIGURAS

FIGURA 2.1 PROCURA DEMONSTRAR ALGUMAS MANEIRAS DE IMPLEMENTAÇÕES DAS REDES WIRELESS.[WECA,2003].....16

FIGURA 2.1 PROCURA DEMONSTRAR ALGUMAS MANEIRAS DE IMPLEMENTAÇÕES DAS REDES WIRELESS.[WECA,2003].....16

TABELA 2.1 – EXEMPLOS DOS OBJETIVOS DE ALGUNS INTRUSOS.[MCCLURE,2000].....19

FIGURA 2.3 AS ANTENAS PARA REDES WIRELESS TÊM UM ALCANCE DE 50 A 150 METROS.A ANTENA DE PRINGLES NÃO TÊM UM ALCANCE DETERMINADO.[PEIXOTO,2003].....21

TABELA 2.2 – TIPOS DE INFORMAÇÕES PROCURADOS NUM FOOTPRINT [MCCLURE,2000]...26

FIGURA 3.2 DEMONSTRA EXEMPLO REDE 802.11B.[MODULO,2003].....30

FIGURA 3.2 DEMONSTRA EXEMPLO REDE 802.11B.[MODULO,2003].....30

TABELA 3.2 COMPARAÇÕES ENTRE AS PRINCIPAIS TECNOLOGIAS WIRELESS[DAHAB,2003] 33

FIGURA 3.2 ANTENA DIRECIONAL[ORINOCO,2000].....35

FIGURA 3.3 EQUIPAMENTO AP-1000[ORINOCO,2000].....36

TABELA 3.2 COMPARAÇÃO ENTRE AS PRINCIPAIS APLICAÇÕES DAS REDES WIRELESS[ELLISON,2001].....39

FIGURA 4.3 CIFRAGEM E DECIFRAGEM DE UMA MENSAGEM.[TRINTA,1998].....43

FIGURA 4.3 CIFRAGEM E DECIFRAGEM DE UMA MENSAGEM.[TRINTA,1998].....43

FIGURA 4.2 – PROCESSO DE CRIPTOGRAFIA POR CHAVE SECRETA.[TRINTA,1998].....45

FIGURA 4.3 – COMUNICAÇÃO USANDO CHAVES SECRETAS.[TRINTA,1998].....46

FIGURA 4.4 – O CENTRO DE DISTRIBUIÇÃO DE CHAVES (KDC).[TRINTA,1998].....47

FIGURA 4.5 DEMONSTRA OS ALGORITMOS DE PROGRAMAÇÃO FUNDAMENTAL E O ALGORITMO DE GERAÇÃO PSEUDO-RANDOM[DAHA,2003].....52

FIGURA 5.4 TROCA DE SEGREDOS UTILIZADAS PELO PROTOCOLO WEP[MODULO,2003].....54

FIGURA 5.4 TROCA DE SEGREDOS UTILIZADAS PELO PROTOCOLO WEP[MODULO,2003].....54

FIGURA 5.5 COMPARAÇÃO ENTRE MODELO IEE 802.11 E O MODELO OSI[MODULO,2003].....54

FIGURA 5.3 DEMONSTRA A IMPLEMENTAÇÃO DA CONFIDENCIALIDADE NO 802.11[FERNANDES,2003].....56

FIGURA 5.4 FRAME WEP[FERNANDES,2003].....57

FIGURA 5.6 OPERAÇÃO LÓGICA DE OU-EXCLUSIVO PARA ENCRIPTAÇÃO. [WALKER,2002].59

FIGURA 5.7 AUTENTICAÇÃO NO 802.11[MODULO,2003].....60

FIGURA 5.8 UTILIZAÇÃO DE UM ROUTER PARA FILTRAGEM DOS ENDEREÇOS MAC[WALKER,2002].....61

FIGURA 5.9-SPOOFING – O INVASOR DIZ PARA A QUE ELE É B.[DAHA,2003].....62

FIGURA 6.6 TELA INICIAL FERRAMENTA ORINOCO CLIENTE MANAGER[ORINOCO,2000]....69

FIGURA 6.6 TELA INICIAL FERRAMENTA ORINOCO CLIENTE MANAGER[ORINOCO,2000]....69

FIGURA 6.2 DEMONSTRA O PONTO DE ACESSO MAIS PRÓXIMO[ORINOCO,2000].....70

FIGURA 6.3 DEMONSTRAÇÃO DA QUALIDADE DO LINK ENTRE USUÁRIO E AP. [ORINOCO,2000].....71

FIGURA 6.4 MOSTRA COMO A CRIPTOGRAFIA DESABILITADA(PADRÃO).[ORINOCO,2000]…72

FIGURA 6.5 PROCESSO DE ATIVAÇÃO WEP.[ORINOCO,2000].....74

FIGURA 6.6 MOSTRA UM EXEMPLO REDE NO PADRÃO 80211B COM AUTENTICAÇÃO RADIUS.[MODULO,2003].....76

FIGURA ANEXO 1 CÁLCULO DO MIC[FERNANDES,2003].....85

FIGURA ANEXO 2 FRAME 802.11I [FERNANDES,2003].....86

FIGURA ANEXO 3 CIPHER BLOCK CHAINING (CBC) [FERNANDES,2003].....87

FIGURA ANEXO 4 CRIPTOGRAFIA E INTEGRIDADE NO AES-CCMP[FERNANDES,2003].....87

FIGURA ANEXO 5 PILHA DE PROTOCOLOS 802.1X[FERNANDES,2003].....88

FIGURA ANEXO 6 COMPONENTES DO 802.1X[FERNANDES,2003].....89

FIGURA ANEXO 7 ESTRUTURA DO EAP[FERNANDES,2003].....89

LISTA DE TABELAS

TABELA 2.1 – EXEMPLOS DOS OBJETIVOS DE ALGUNS INTRUSOS.[MCCLURE,2000].....19

TABELA 3.2 COMPARAÇÕES ENTRE AS PRINCIPAIS TECNOLOGIAS WIRELESS[DAHAB,2003] 33

LISTA DE SIGLAS

AP – Ponto de Acesso
WLAN – Rede Local Sem Fio
WAN – Rede Geograficamente Distribuídas Sem Fio
GPS – Sistema de Posicionamento Global
ESSID – Código Alfanumérico de Identificação
TI – Tecnologia da Informação
TCP – Protocolo de Controle de transmissão
IP – Protocolo de Internet
UDP –
FHSS – Freqüência a ser Espalhada para Transmissão
DSMA-CA – Portador para Acesso Múltiplo Sem Colisão
SMR – Rádio Móvel Especializado
KDC – Centro de Distribuição de Chaves
PRGA – Algoritmo Gerador de Números Pseudo-Aleatórios
KSA - Algoritmo de Programação de Chave
WEP – Privacidade Equivalente à das Redes com Fios
ICV – Valor para Checar Integridade
CRC – Cheque de Redundância Cíclico
MAC – Controle de Acesso Médio

1 INTRODUÇÃO

O crescente desenvolvimento das tecnologias de telecomunicações e de informática, unido à necessidade do homem de estar cada vez mais informado esteja onde estiver, tem mostrado que as redes Wireless (sem fio) serão a próxima geração nas redes de computadores.

As redes sem fio/móveis, seria a quarta revolução na computação, Esta evolução conjunta da comunicação sem fio e da tecnologia da informática busca atender as necessidade do mercado, os dispositivos Wireless ficam cada dia mais populares.

Isso nos da uma idéia da importância da discussão sobre o assunto e as tecnologias existentes assim como as novas tendências. Neste trabalho procuramos, explicar como funciona uma rede Wireless, suas variações e aplicações, comparações e os cuidados que devemos ter com segurança.

Hoje é necessária uma visão precisa sobre as possibilidades e o uso de uma rede wireless, não basta, por exemplo, uma pessoa colocar um access point em sua LAN para que usuários de notebooks se conectem sem tomar alguns cuidados.

Com as tecnologias Wireless de hoje é extremamente necessário separar esta rede e ter um bom sistema de segurança, pois a área de acesso ultrapassa a área física, quebrando um paradigma do controle de acesso físico à rede. Ao final vamos propor meios a serem implementados, obtendo uma rede Wireless mais segura e confiável para a Empresa Ferteco Mineração S/A.

2 COMUNICAÇÃO EM COMPUTAÇÃO MÓVEL

2.1 APLICAÇÃO DE COMUNICAÇÃO EM COMPUTAÇÃO MÓVEL

Computação Móvel visa criar soluções de negócios usando computadores e comunicações para permitir aos usuários trabalharem fora dos ambientes fixos, onde normalmente operam. O ambiente móvel ou ambiente da computação móvel baseia-se, na capacidade que os usuários tem de munidos de um dispositivo móvel (Laptops, Notebook, etc), comunicarem com a parte fixa da rede, e possivelmente com outros dispositivos móveis, independentemente da sua localização.[YEMINI,1995]

A evolução conjunta da comunicação sem fio e da tecnologia da Informática busca atender muitas das necessidades do mercado. Serviços celulares, redes wireless, transmissão de dados via satélite, radio, modem,etc. A comunicação sem fio da suporte para computação móvel, que pode ser vista como uma área da comunicação sem fio, que por sua vez explora diferentes tecnologias de comunicação que serão inseridas em ambientes computacionais fixos e móveis.

Neste trabalho serão abordadas algumas das principais tecnologias da computação móvel, que são as redes Wireless, com intuito de propor uma solução segura e confiável para ser apresentada como solução para melhorias em uma rede wireless já implantada na empresa Ferteco Mineração S/A, esta mantém vários pontos isolados interligados por uma rede wireless no padrão 802.11b.

2.2 WIRELESS

"O termo Wireless - vem do inglês wire = fio, less = sem, logo conexão sem fio. É impulsionada pela possibilidade de executar transações e acessar informações em qualquer lugar e a qualquer momento".[WIRELESS,2003]

A rede Wireless é um sistema de transmissão de dados flexível que pode ser utilizada como alternativa para as redes cabeadas, é uma tecnologia que permite a conexão entre equipamentos sem uma conexão física direta.

O princípio de funcionamento das redes Wireless se baseia na transmissão de dados através do ar. Nos últimos anos esse tipo de rede tem crescido e tem ganho popularidade nos diversos setores, principalmente no que diz respeito as WLAN (Wireless Local Área Network).

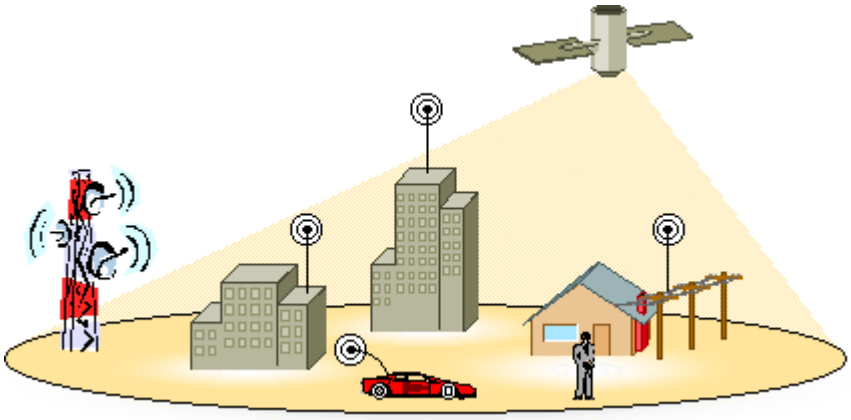


Figura 2.1 Procura demonstrar algumas maneiras de implementações das redes Wireless. [WECA,2003]

As redes wireless possuem uma importância grande para a disseminação da informação e para o acesso aos meios de comunicação. Porém, eles devem ser implantados de uma forma consciente e segura. A maior dúvida sobre o uso de redes sem fio recai sobre o fator segurança. Com um transmissor irradiando os dados transmitidos através da rede em todas as direções, como impedir que qualquer um possa se conectar a ela e ter acesso aos dados.

Um ponto de acesso provavelmente permitirá que um intruso a uma distância razoável consiga captar o sinal da sua rede, uma preocupação agravada pela popularidade que as redes sem fio vêm ganhando.[JESSEN,2003] .

A solução de segurança deve-se levar em consideração o sistema de computação a ser defendido. As soluções genéricas que são construídas para serem aplicadas a todas as empresas, não são as melhores. As boas soluções são desenvolvidas especialmente para a empresa alvo. Cada empresa tem a sua forma de trabalhar, tem a sua própria equipe e tem a sua metodologia.

Não adianta uma solução que vai obrigar uma equipe a usar uma metodologia de trabalho diferente da que já vem usando há anos. Essa metodologia nova tem muitíssima chance de não ser cumprida na sua totalidade. E, na maioria dos casos, uma metodologia que não é cumprida à risca é tão ineficaz quanto não ter metodologia nenhuma.

Agora, devemos ter em mente que a melhor solução é aquela que é baseada na modelagem de um provável ataque. Devemos pensar como se fossemos hackers, tendo assim, uma melhor visualização de todas as falhas do sistema da empresa.

2.2.1 ATAQUES A REDES WIRELESS

O intruso pode ter quatro comportamentos diferentes em relação às posições da origem e do destino da mensagem.[ELLISON,2001]

Na figura a seguir , veremos esses comportamentos:

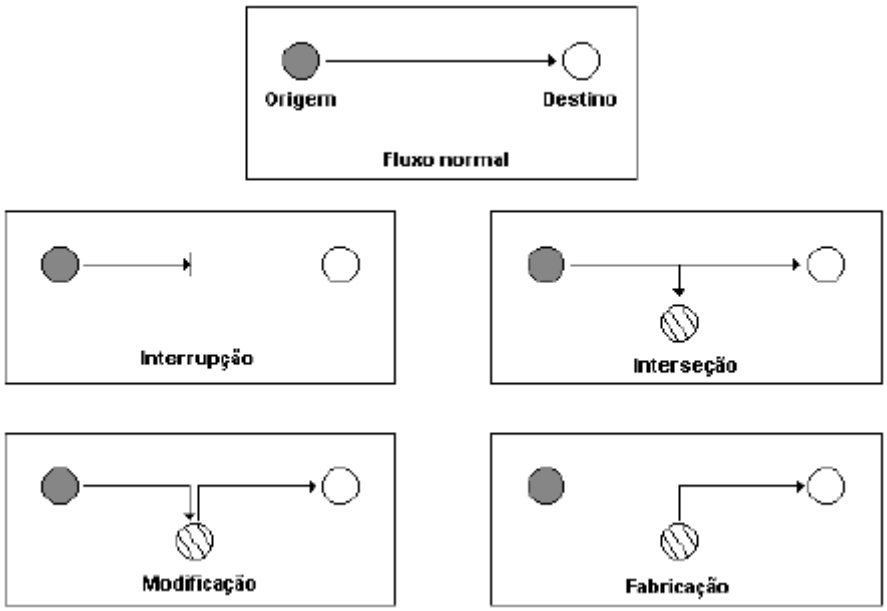


Figura 2.2 Posição do atacante em relação à origem e ao destino.[ELLISON,2001]

De acordo com Figura 2.2 teremos os seguintes comportamentos :

- **Interrupção:** O intruso objetiva interromper o fluxo de dados que parte da origem, deixando o dispositivo destino sem receber pacotes.
- **Interseção:** Nesse tipo de invasão o intruso objetiva apenas tomar conhecimento de todo fluxo de dados que trafega por essa conexão.
- **Modificação:** Aqui, o intruso além de escutar o tráfego , intercepta os dados e os modifica, enviando os para o destino.
- **Fabricação:** Na fabricação o intruso fabrica dados para enviar para o destino. O dispositivo destino não tem como saber quem está enviando esses dados.

2.3 TIPOS DE INTRUSOS

Intruso	Objetivos
Estudante	**Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas**

Hacker/Cracker	**Testar o sistema de segurança de alguém; ou roubar dados.**
Representante de vendas	**Tentar representar toda a Europa e não apenas a América**
Executivo	**Descobrir a estratégia de marketing do concorrente**
Ex-funcionário	**Vingar-se do ex-empregador**
Contador	**Desfalcar dinheiro de uma empresa**
Corretor de valores	**Causar prejuízo para lucrar no valor das ações**
Vigarista	**Roubar números de cartões de créditos e revendê-los**
Espião	**Descobrir a força militar do inimigo**
Terrorista	**Roubar segredos de guerra bacteriológica**

Tabela 2.1 – Exemplos dos objetivos de alguns intrusos.[MCCLURE,2000]

2.3.1 HACKERS

"É um invasor que tem a habilidade e conhecimentos profundos de tecnologia, plataformas tecnológicas, sistemas, redes, algoritmos e segurança digital para entrar em uma máquina ou rede de computadores, apoderar-se de dados e até paralisar sistemas. Um hacker conhece detalhes de linguagens de programação e pode, rapidamente e propositadamente, criar soluções inteligentes que interferem nos dados de outros usuários". [SPYMAN]

Nas redes de computadores tradicionais a proteção é feita usando dispositivos como firewalls que bloqueiam os ataques. Mas os hackers podem violar as indefesas redes wireless das companhias somente estando próximos com um laptop para capturar os sinais que transmitem os dados das empresas. As companhias estruturaram tão rapidamente as suas redes sem fio que negligenciaram a segurança das mesmas. Os especialistas apontam que a maioria possui pouca ou nenhum software de segurança ou qualquer outros meio de proteção para evitar invasões.

2.3.1.1 Tipos de ataques hackers:

"Wardriving consiste em percorrer as ruas e avenidas (e porque não auto-estradas) em busca de pontos de acesso. O que basicamente se faz, é pegar um laptop munido de

software apropriado para se conectar, e de uma boa placa local (wireless), então será só pesquisar as redes disponíveis". Os programas mais utilizados são no caso do windows. Os access Points anunciam a sua presença a intervalos certos (normalmente 100 milisegundos) através do 'brodcast' de um pacote que contém o seu SSID (nome identificador) e outro tipo de informações. Os programas acima vão fazer a listagem dos APs encontrados e, caso exista um GPS ligado ao computador, marcam o local onde ele se encontra.[PEIXOTO,2003]

"Warchalking: Ao pé da letra significa "Guerra do Giz",este termo surgiu na Europa, especificadamente em Londres, quando marcações feitas a giz apareceram pelas ruas da cidade indicando pontos onde era possível conectar-se em redes privadas wireless (sem fio) com um notebook e um amplificador de sinal".A febre espalhou-se rapidamente por todo o mundo e hoje, em grandes metrópoles principalmente, é possível achar símbolos (um X desconsertado) pelas ruas indicando pontos.

Como sempre, o investimento em métodos de segurança confiáveis, como criptografia, são muito baixos é possível conectar-se a redes de grandes corporações na rua, com apenas um notebook e antenas caseiras, feitas ate mesmo de latas de Pringles (figura 2.3) e Neston, que fazem os sinais ficarem cerca de 20x mais fortes.

Figura 2.3 As antenas para redes wireless têm um alcance de 50 a 150 metros.A antena de Pringles não têm um alcance determinado.[PEIXOTO,2003]

2.4 O FATOR HUMANO

As empresas devem considerar que as informações não pertencem somente à organização. Na verdade as informações pertencem sim, aos seus colaboradores. Desta forma o fluxo de informação sempre partirá do recurso humano. O ponto de origem sempre será a pessoa, independente do sistema tecnológico que a empresa utilize como ferramenta. A Tecnologia da Informação – TI é um dos grandes incentivadores do compartilhamento e transferência da informação. Nas redes digitais das organizações transitam todo e qualquer tipo de informação, tanto pela intranet – dentro para dentro, como de dentro para fora e de fora para dentro das empresas.[MCCLURE,2000]

A segurança total das informações é difícil, talvez até mesmo impossível. Para que exista uma real segurança do fluxo da informação e a identificação dos filtros do ambiente, há a necessidade deste sistema interagir com os usuários de alguma forma. [MODU,2003]

O fator humano é primordial, as pessoas geralmente não entendem de riscos. Elas podem entender, em um sentido geral, quando o risco é imediato. De acordo com [MODU,2003], podemos descrever os seguintes aspectos do fator humano:

1) Como as pessoas percebem os riscos: As pessoas não sabem como analisar o risco. O problema é que as pessoas que lidam com informações, dentro de uma organização não sabe o que tem nas mãos, ou seja ela não possui informações suficientes sobre a criticidade da informação.

2) Como as pessoas lidam com o que acontece muito raramente: Um perigo dos sistemas computadorizados é que eles cometam erros tão raramente que as pessoas não saibam como lidar com eles. Essa é a mentalidade “esse computador nunca comete um erro, e por isso você deve estar mentindo”. O fato é que os computadores cometem todos os tipos de erros o tempo todo, e hackers maliciosos ficam contentes em levar os computadores por um caminho repleto de erros e tirar proveito desses erros.

3) O problema da operacionalidade e da segurança: Já foi dito que o sistema mais desprotegido é aquele que não é usado. E, com freqüência, um sistema de segurança não é usado porque simplesmente é muito irritante. As pessoas querem segurança, desde que não mude sua rotina.

4) Engenharia social e por que é tão fácil para um hacker simplesmente pedir informações secretas: A engenharia social é o termo de hacker para um jogo de trapaça, persuadir a outra pessoa a fazer o que você deseja. Ela é muito eficiente. A engenharia social evita a criptografia, segurança de computador, segurança de rede e tudo o mais que for tecnológico. Ela vai diretamente para o elo mais fraco de qualquer sistema de segurança, o ser humano, sendo forçado a realizar seu trabalho e precisando de toda a ajuda que puder obter.

A maior parte da engenharia social é feita por telefone, isto faz com que fique mais difícil de se pegar o intruso, um hacker liga para a empresa e pede informações.

Todos esses ataques utilizam pessoas de baixo conhecimento das ameaças que uma rede está submetida ou por pessoas que, por boa fé, querem ajudar. Normalmente são secretárias, estagiários , funcionários novos na empresa.

O mais comum é o intruso, antes de tentar uma invasão, querer saber se a rede tem um firewall, qual é esse firewall, qual o sistema operacional que roda no roteador, qual o

nome, ou o número IP de alguma máquina específica, por exemplo, o servidor de banco de dados. Essas são algumas das informações muito úteis que um intruso pode querer saber antes de um ataque. Para saber o nome e o telefone do administrador da rede alvo do ataque, pessoa que certamente terá os dados que o atacante quer saber, basta dar uma olhada na Internet. Provavelmente esses dados estão na Home Page da empresa que contém a rede. Outro lugar de consulta pode ser a página do Registro.BR.[SPYMAN,2001]

O Registro.BR é a entidade que controla o registro de nomes de domínios na Internet no Brasil. É lá que você registra que o nome xxxx.com.br corresponde à rede 10.2.4.222. Ao registrar essa informação, o administrador da rede deve registrar também alguns de seus dados pessoais. Na maioria esmagadora dos casos, os dados ali registrados são verídicos, mesmo porque, o serviço de registro de nome de domínio é cobrado por essa entidade(Registro.BR) , e ela precisa saber os dados para onde mandar a fatura. Caso os dados estejam errados, a entidade registradora não faturar á o serviço e, automaticamente, remover á o registro. Logo, salvo os registros falsos, todos os administradores cadastram seus verdadeiros dados.

Os Ex-Funcionários merecem uma atenção especial, quando são demitidos muitos destes podem sair da empresa com informações vitais da empresa, e não é possível retirar dele os conhecimentos em que ele adquiriu quando estava trabalhando.[MCCLURE,2000]

A engenharia social trata esta situação como uma das principais para intrusos adquirirem informações sigilosas que possam ajudar nas invasões.

5) Indução para conquista de informações: Indução, pode ser definida como aquele processo que evita questões diretas e emprega um estilo de conversação para ajudar a reduzir desconfianças e suspeitas — tanto durante o contato quanto nos dias e semanas que se seguem — no interesse de maximizar o fluxo de informações. O propósito da indução é, então, obter a informação necessária que a concorrência necessita. O “alvo” não sabe o valor da informação que possui, por esta razão não saberá — ou até desconfiará — quem é o indutor. Tipicamente, envolve a coleta de informações sem fazer perguntas, ou quando as faz, faz com razões específicas como parte do plano de aproximação para a conversação.

O fator humano deve considerar que a comunicação efetiva raramente surge sem alguma organização, alguma coerência, talvez até algum rigor, caso contrário a conversação será inócua, não levará a lugar nenhum, deixando ambas as partes com um gosto de frustração. Profissionais em coletar dados procuram minimizar suspeitas e encorajar a abertura. Procuram ser mais efetivos, mais organizados, mais direcionados. Procuram a informação que um tomador de decisões precisa — a informação que pode lhe dar a liderança, ou o ponto de início num mercado rápido, volátil e competitivo.

A utilização dessas técnicas, de uma forma organizada aumenta significativamente a possibilidade de obter informações dos atores da rede, desprevenidos. Aprender a reconhecer essas técnicas também evita que a rede deixe passar informações quando esse tipo de conversação for empregado.

2.5 REPLAY

Uma mensagem, ou parte dela é interceptada, e posteriormente transmitida para produzir um efeito não autorizado.[SPYMAN,2001]

O sistema que está recebendo os pacotes vai ingenuamente receber os pacotes reenviados pelo intruso, acreditando que ele fora enviado pelo dispositivo origem.

2.6 RECUSA OU IMPEDIMENTO DE SERVIÇO

Também conhecido como DoS (Recusa de serviço). No seu uso mais comum esse ataque visa enviar para uma entidade, mais pacotes do que essa entidade suporta receber, fazendo com que ela passe a recusar mais pacotes.

Uma variação mais perigosa é o Impedimento de Serviço distribuído. Aqui o intruso utiliza-se de outros computadores, conhecidos como computadores zumbis, para aumentar a carga de pacotes (flood) a serem tratados pelo computador atacado. [MCCLURE,2000].

2.7 FOOTPRINTING

São técnicas de absorção de informações do sistema alvo, nada mais é do que a busca detalhada da maior quantidade de informações possíveis do alvo da invasão, sem cair e sem ser pego por ferramentas IDS's ou Firewalls, ou seja, ninguém que queria invadir sua rede vai ficar tentando uma invasão sem Ter uma estratégia definida, a partir do resultado obtido pelo FOOTPRINTING é que é traçado o plano/estratégia de invasão, há casos em que essa busca de informações, chega a durar meses. A tabela 2.2 mostra os tipos de informações em um Footprint.[MCCLURE,2000]

Tecnologia	Identifica
Internet	Nomes de domínio. Blocos de rede. Endereços IP específicos de sistemas atingíveis via Internet Serviços TCP e UDP executados em cada sistema identificado. Arquitetura do sistema (por exemplo, SPARC versus X86). Mecanismos de controle de acesso e listas de controle de acesso (ACLs, acess control lists) relacionadas. Sistemas de detecção de intrusos (IDSs).
Intranet	Enumeração de sistemas (nomes de usuários e de grupos, faixas de sistemas, tabelas de roteamento, informações de SNMP). Intranet Protocolos de rede em uso (por exemplo: IP, IPX, DexNET, etc...). Nomes de domínios internos. Blocos de rede. Endereços IP específicos de sistemas atingíveis por intermédio da internet. Serviços TCP e UDP executados em cada sistema identificado. Arquitetura do sistema (por exemplo, SPARC versus X86). Mecanismos de controle de acesso e listas de controle de acesso relacionadas. Sistemas de detecção de intruso. Enumeração de sistemas (nomes de usuários

Acesso remoto	Número de telefone analógicos/digitais. Tipo de acesso remoto. Mecanismo de autenticação.
Extranet	Origem e destino de conexões. Tipos de conexão. Mecanismos de controle de acesso.

Tabela 2.2 – Tipos de informações procurados num footprint [McCLURE,2000].

2.8 ALGUNS ERROS COMUNS DE SEGURANÇA:

- Postar mensagens em grupos de discussão ou usenet com o email da empresa onde trabalha detalhando o problema, a partir daí pessoas descobrem vulnerabilidades, ou seja, o que era para ajudar, acaba prejudicando[MCCLURE,2000];
- Informações importantes em páginas HTML, como telefones e nomes de usuários, a partir de nomes de usuários e contas de emails, é muito fácil descobrir informações no velho sistema;
- Nome da pessoa = senha, combinação de letras, data de nascimento....
- Servidores de correio com Relay aberto, o que é muito usado para ataques de engenharia social, qualquer pessoa que entenda um pouco, consegue mandar mensagens para qualquer pessoa e com qualquer nome, usando um servidor de email com problemas de Relay, o que pode ser usado para aquisição de senhas ou outros privilégios;
- Unidades de disco compartilhadas.

2.9 VARREDURA

Se o footprinting é o equivalente a cercar um lugar em busca de informações, a varredura (ou scanning) é equivalente a bater nas paredes para descobrir todas as portas e

janelas. O passo seguinte então é determinar quais sistemas estão ativos e alcançáveis a partir da Internet, usando uma série de ferramentas de descoberta automatizadas. É importante lembrar que um sistema (um endereço IP) descoberto utilizando o footprinting anterior não significa que esta máquina está ligada, ou mesmo se ela existe, por isso a varredura é necessária, ela que vai determinar os seus alvos.[MCCLURE,2000]

2.10 ENUMERAÇÃO

Existem muitas maneiras de se extrair contas válidas e recursos exportados de sistemas, um processo que chamamos de enumeração.[SPYMAN,2001]

A principal diferença entre técnicas de coleta de informações vistas e a enumeração está no nível de invasividade – a enumeração envolve conexões ativas e consultas dirigidas que podem ser registradas pelo sistema alvo.

O tipo de informação enumerada por atacantes pode ser classificada, de forma geral, nas seguintes categorias:

- Recursos de compartilhamento de rede;
- Usuários e grupos;
- Aplicativos e suas versões .

3 PADRÕES WIRELESS

Este capítulo faremos um estudo geral sobre as Tecnologias, arquiteturas, padrões ou protocolos que hoje temos disponíveis para o público consumidor.

3.1 ARQUITETURA

A arquitetura de redes sem fio, assim como de redes convencionais, é formada por níveis, interfaces e protocolos. Cada nível oferece um conjunto de serviços ao nível superior usando funções realizadas no próprio nível, e serviços disponíveis nos níveis inferiores. [ELLISON,2001].

Um nível pode ser um programa ou um processo implementado por hardware ou Software, que se comunica com processos correspondentes em outra máquina. As regras que governam a conversão de um nível qualquer são chamadas de protocolos de níveis.

Os limites entre cada nível adjacente são as interfaces. Na computação móvel a arquitetura lógica é separado em dois níveis.

1 – nível de fluxo de dados da aplicação

2 – nível de controle de sistema

Seguem o modelo de arquitetura da OSI. Embora as camadas do modelo OSI são identificadas, alguns componentes descritos nas caixas encorparam mais de uma camada. O objetivo é mostrar a simetria por níveis de processamento entre o cliente e o servidor que são completamente diferentes. Níveis de aplicação são implementadas tanto no cliente quanto no servidor.

3.2 PADRÕES WIRELESS

3.2.1 PADRÃO IEEE802.11B

“Este é um padrão projetado pelo IEEE (Institute of Electrical and Eletronics Engineers), este padrão é um dos principais focos deste estudo, por ser o padrão utilizado na maioria das redes wireless, baseia-se na tecnologia Direct Sequence Spread Spect rum (DSSS) que usa transmissão aberta (broadcast) de rádio e opera na freqüência de 2.4000 a 2.4835 GHz com uma capacidade de transferência de 11 Mbps, em ambientes abertos (~ 450 metros) ou fechados (~ 50 metros). Esta taxa pode ser reduzida a 5.5 Mbps ou até menos, dependendo das condições do ambiente no qual as ondas estão se propagando (paredes, interferências, etc)”. Por ser uma transmissão aberta, qualquer pessoa com um receptor operando na mesma freqüência pode captar as ondas. Assim como em um passeio de carro, conforme nos afastamos da estação de rádio transmissora o sinal começa a ficar cada vez mais fraco até que não possamos mais captá-lo. Conforme formos chegando mais perto da transmissora, o nosso receptor conseguirá mais facilmente captar o sinal até chegarmos no nível de clareza total na recepção. [MODULO,2003].

Possui as seguintes características :

- Tem conexão peer-to-peer ou baseada num ponto fixo de acesso;

- Opera na freqüência de 2,4GHz;
- Funciona com os dois métodos de espalhamento na freqüência: O FHSS (Frequency Hopping Spread Spectrum) e o DSSS (Direct Sequence Spread Spectrum). Além disso, funciona com infravermelho, que não utiliza nenhum desses dois métodos;
- Utiliza o protocolo de acesso CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance);
- Utiliza o WEP para autenticação e privacidade;

A figura abaixo mostra um exemplo de uma rede 802.11b, sua implementação e conexões.

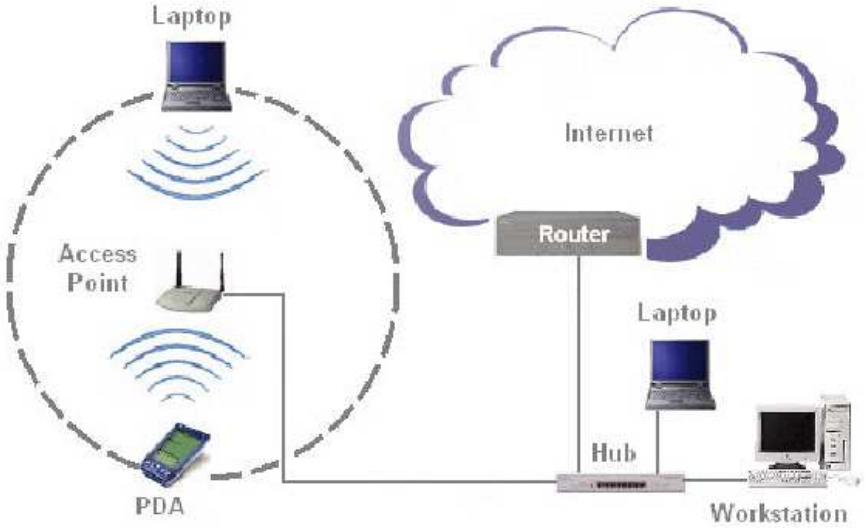


Figura 3.2 demonstra exemplo rede 802.11b.[MODULO,2003].

3.2.2 PADRÃO IEEE 802.11A

"O 802.11b utiliza a frequência de 2.4 GHz, a mesma utilizada por outros padrões de rede sem fio e pelos microondas, todos potenciais causadores de interferência. O 802.11a

por sua vez utiliza a freqüência de 5 GHz, onde a interferência não é problema. Graças à freqüência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo 54 megabits".[DAHAB,2003].

Note que esta é a velocidade de transmissão "bruta" que inclui todos os sinais de modulação, cabeçalhos de pacotes, correção de erros, etc. a velocidade real das redes 802.11a é de 24 a 27 megabits por segundo, pouco mais de 4 vezes mais rápido que no 802.11b.

Outra vantagem é que o 802.11a permite um total de 8 canais simultâneos, contra apenas 3 canais no 802.11b. Isso permite que mais pontos de acesso sejam utilizados no mesmo ambiente, sem que haja perda de desempenho.

O grande problema é que o padrão também é mais caro, por isso a primeira leva de produtos vai ser destinada ao mercado corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas.

Além disso, por utilizarem uma freqüência mais alta, os transmissores 8021.11a também possuem um alcance mais curto, teoricamente metade do alcance dos transmissores 802.11b, o que torna necessário usar mais pontos de acesso para cobrir a mesma área, o que contribui para aumentar ainda mais os custos.[MODULO,2003].

A diferença de custo vai se manter por um ou dois anos. É de se esperar então que as redes de 11 megabits continuem se popularizando no mercado doméstico, enquanto as de 54 megabits ganhem terreno no mercado corporativo, até que um dia o preço dos dois padrões se nivele e tenhamos uma transição semelhante à das redes Ethernet de 10 para 100 megabits.

Ao contrário do que o nome sugere, o 802.11a é um padrão mais recente do que o 802.11b. Na verdade, os dois padrões foram propostos pelo IEEE na mesma época, mas o 802.11b foi finalizado antes e por isso chegou ao mercado com mais de 6 meses de antecedência. Os primeiros periféricos 802.11a foram lançados em Novembro de 2001. [FERNANDES,2003]

3.2.3 IEEE 802.11G

Este é um padrão recentemente aprovado pelo IEEE, que é capaz de transmitir dados a 54 megabits, assim como o 802.11a.

"A principal novidade é que este padrão utiliza a mesma faixa de frequência do 802.11b atual: 2.4 GHz. Isso permite que os dois padrões sejam intercompatíveis. A idéia é que você possa montar uma rede 802.11b agora e mais pra frente adicionar placas e pontos de acesso 802.11g, mantendo os componentes antigos, assim como hoje em dia temos liberdade para adicionar placas e hubs de 100 megabits a uma rede já existente de 10 megabits."[DAHAB,2003].

A velocidade de transferência nas redes mistas pode ou ser de 54 megabits ao serem feitas transferências entre pontos 802.11g e de 11 megabits quando um dos pontos 801.11b estiver envolvido, ou então ser de 11 megabits em toda a rede, dependendo dos componentes que forem utilizados. Esta é uma grande vantagem sobre o 802.11a, que também transmite a 54 megabits, mas é incompatível com os outros dois padrões. [FERNANDES,2003]

Os primeiros produtos baseados no 802.11g devem chegar ao mercado a partir deste ano, um 2 anos depois da primeira leva do 802.11a, que é o concorrente direto. Isso significa que a popularidade do 802.11g será determinada pelo sucesso do concorrente. Se o 802.11a for rapidamente adotado e chegar a substituir o 802.11b até lá, os periféricos 802.11g terão pouca chance e talvez nem cheguem a ser lançados, já que seria uma guerra perdida.

Se por outro lado a maioria dos usuários preferir os dispositivos 802.11b, então o 802.11g terá chances de dominar o mercado. A tabela 3.1 veremos a comparação entre os principais tecnologias wireless.

Quadro de Comparação de Tecnologias Wireless			
PADRÕES WIRELESS	802.11	802.11a	802.11g
Popularidade	Amplamente usada. De fácil disponibilidade e mais usada hoje no	Nova tecnologia. Pouco usada no mercado.	Nova tecnologia com grande expectativa de crescimento no mercado.

	mercado.		
Velocidade	Até 11 Mbps (Obs: Nos serviços de cable modem dificilmente se atingem velocidades superiores a 5 Mbps.	Até 54 Mbps (5 vezes mais rápido que o padrão 802.11b).	Até 54 Mbps (5 vezes mais rápido que o padrão 802.11b).
Comparativo de Custos	Baixo custo	Custo Médio	Custo Médio
Freqüência	2.4 Ghz. Podem ocorrer conflitos com outros dispositivos 2.4 Ghz como telefones sem fio, microondas e outros.	5 Ghz. Não ocorre conflito com redes 2.4 Ghz.	2.4 Ghz.Podem ocorrer conflitos com outros dispositivos 2.4 Ghz como telefones sem fio, microondas e outros.
Alcance	Uso Indoor de 100 150 metros e externo depende do tipo de antena utilizada e da região onde é propagado o sinal.	Baixo alcance em relação aos padrões 802.11b & 802.11g, em uso indoor de 30 a 60 metros. Nas aplicações outdoor se restringe muito em relação aos padrões 802.11b & 802.11g cobrindo distancias bem menores.	Uso Indoor de 100 150 metros e externo depende do tipo de antena utilizada e da região onde é propagado o sinal

Tabela 3.2 Comparações entre as principais Tecnologias Wireless[DAHAB,2003]

3.3 APLICAÇÕES DA REDES WIRELESS

Neste tópico do trabalho procura-se definir dois dos principais modos de implementação das redes wireless que são WIRELESS LAN's e WAN'S, esta é uma das aplicações mais populares para a tecnologia wireless, em que se utiliza ondas de rádio para interligação de pontos de redes locais (LANs). Esta tecnologia permite que a rede vá para lugares onde as redes cabeadas não podem ir, desta forma usuários podem acessar informações compartilhadas e administradores de rede podem ajustar e gerenciar a rede sem se preocupar com instalações de cabos, outra vantagem é que a instalação das WLANs podem ser rápidas e fáceis eliminando a necessidade de se instalar uma quantidade muito grande de cabos internamente as paredes.[ELLISON,2001]

3.3.1 WIRELESS LAN'S – REDES LOCAIS SEM FIO

3.3.1.1 CARACTERÍSTICAS

Redes locais têm se tornado padrão na conectividade física entre PC's, Workstations e servidores. Na maioria dos casos, o uso de cabos (fibra ótica, cobre), é uma necessidade inevitável para realizar esta conectividade física. A instalação é uma atividade cara, consumidora de tempo, e laboriosa. Entretanto usuários móveis (profissionais executivos tomando decisões longe do ambiente do escritório, vendedores) exigem flexibilidade na sua liberdade de se moverem. Neste contexto redes locais sem fio encontram um importante foco de aplicação em negócios.[MODULO,2003]

Existem três cenários de conectividade, onde redes locais sem fio são usadas comumente:

1 – Redes sem fio verdadeiras

Para mudanças e movimentos constantes, provê conexões rápidas locais. Este tipo de redes é muito usado em ambientes muito dinâmicos, interior de edifícios, tais como escritórios de advocacia.

2 – Redes locais sem fios flexíveis

Para situações em que o usuário precisa sair fora do ambiente do edifício. O objetivo pode ser executado economicamente através do uso de conexões sem fio para Hosts ou servidores

3 – Conexões LAN-LAN

As conexões LAN – LAN envolvem conexões entre edifícios, universidades, filiais de lojas onde o cabeamento será possível, porém cara, conexões entre edifícios distanciadas de alguns quilômetros e conexões entre edifícios em áreas rurais.

3.3.1.2 COMPONENTES

Os componentes essenciais de LAN's sem fio são os mesmos ou similares aos das LAN's convencionais. A mudança maior está na substituição de cartões de interface de redes Ethernet e Token Ring com seus similares nas LAN's sem fio, e a ausência de conectores de cabo.[ORINOCO,200]

Os componentes principais são:

1. Cartões de Interface de rede -NIC's (Network Interface Cards). Este deve ser da forma PCMCIA para notebooks ou cartões padrão ISA para desktops.

2. Antenas para captar e difundir sinais de rádio, onde diversos tipos de antenas são utilizadas.

- .Antenas Direcionais que levam sinais de rede para longas distâncias tais como edifício para edifício. Eles são montados em postes ou mastros em telhados para assim aumentar o alcance. Esta antena é usada pela Empresa Ferteco Mineração para interligar vários pontos da rede wireless.

Figura 3.2 Antena Direcional[ORINOCO,2000]

- .Antenas Unidirecionais - em áreas de cobertura são fixados para acessar pontos onde a mobilidade é requerida.

3. Equipamento AP-1000/500 - ORINOCO AP-1000/500 Access Point é o ponto de acesso wireless 802.11 compatível com a solução ORINOCO Enterprise Solution. Amplia o alcance de sua rede Ethernet cabeada, fornecendo um acesso fácil à rede para usuários móveis e para localizações difíceis de serem cabeadas. A arquitetura única utiliza dois slots para PC Cards. Esta solução Orinoco é utilizada pela Empresa Ferteco Mineração para distribuição do sinal da rede wireless.[ORINOCO,2000]

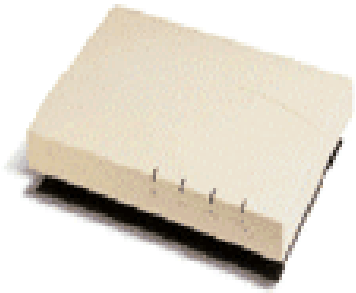


Figura 3.3 Equipamento AP-1000[ORINOCO,2000]

3.3.1.3 FUNCIONAMENTO

Para melhor entender o funcionamento das redes locais sem fio alguns conceitos serão mostrados:[ORINOCO,2000]

Ponto de acesso ou hub – Na terminologia normal, ponto de acesso ou hub permite a múltiplas estações se conectarem com servidores, ou entre si. No caso de redes sem fio o ponto de acesso tem três funções:

- Prover conectividade para dispositivos móveis ou backbone de uma rede,
- Estender o alcance das redes locais sem fio colocando pontos de acesso em lugares estratégicos.
- Prover aos usuários móveis a capacidade de roaming.

Os pontos de acesso são conectados via cabo ás LAN's, assim como estações base estão ligadas por backbones ás WAN's. O número de usuários suportados por um ponto de acesso não é limitado pelo hardware e sim pelo trafego da rede.

Pontes de Redes Sem fio – Conectam LAN's individuais a outras LAN's dentro de edifícios ou com outras LAN's em outros edifícios. O tipo de antena para esse caso varia de acordo com a distância coberta, e aos requisitos físicos do lugar.

3.3.2 WIRELESS WANS – REDES GEOGRÁFICAMENTE DISTRIBUÍDOS SEM FIO

3.3.2.1 CARACTERÍSTICAS E COMPONENTES

"WAN's – *Wide Área Networks*, surgiram da necessidade de compartilhar recursos especializados por uma maior comunidade de usuários geograficamente dispersos. Geralmente são redes públicas, pois o custo da comunicação é bastante elevado por usarem circuitos de satélites e enlaces de microondas. Neste sentido a transmissão de dados se dará da mesma forma que as transmissões de rádio. Tem em comum as estações rádio base, repetidores, e ás vezes raios infravermelhos ou laser".[WIRELESSWANS,2003].

3.3.2.2 FUNCIONAMENTO

Uma conexão de aplicação da computação móvel consiste de vários segmentos de comunicação. Tipicamente só a conexão entre o dispositivo móvel e as estações da rede é que são sem fio.

Desde que os sinais de rádio são carregados no espaço, os seguintes fatores devem ser levado s em consideração.

a) Métodos de transmissão pelos engenheiros de rádio:

- Ponto a ponto,
- Linha de vista,

- Unidirecionais.

O método de transmissão depende da distancia e a área de cobertura. Barulhos de diferentes tipos são sempre um fator. Estes distúrbios podem resultar na transmissão do sinal.

b) Os sinais diminuem muito quando atravessam determinados materiais, e aumentam na força quando atravessam condutores.

c) Chuva ou neve pode absorver alguns dos sinais transmitidos em algumas bandas de freqüências.

Como várias estações compartilham o mesmo meio de transmissão, é necessário métodos para disciplinar este comportamento, métodos como multiplexação de freqüência (FDM), Multiplexação de tempo (TDM), multiplexação por divisão do espaço (SDM). [ELLISON,2001].

O método SDM pode ser realizado de duas formas:

- Utilização de antenas direcionais que emitem sinais de rádio de alta freqüência concentrados em feixes usados por sistemas de rádio,

- Utilização de células em que há uma rápida diminuição da potência do sinal de rádio, á medida que se propagam, usadas nos sistemas celulares.

As redes sem fio geralmente utilizam freqüência altas em suas transmissões (915 MHz 2.46 GHz). Parte das ondas de rádio nessas freqüências são refletidos quando entram em contato com objetos sólidos, o que implica na formação de diferentes caminhos entre o emissor e o receptor.

3.3.2.3 ALGUNS EXELPLOS DE REDES WAN's SEM FIO

1- REDES SEM FIO QUE UTILIZAM SINAIS DE RÁDIO

- .SMR (Specialized Mobile Radio) – Estes sistemas provem

Serviços nos Estados Unidos para mais de um milhão de usuários de rádio

- .Redes de paging,
- .Redes radio mail,

A tabela 3.2 teremos a comparação das principais aplicações das redes wireless e algumas configurações.

	WLANs	LAN-LAN	WWANs	WMANs	WPANs
Área Coberta	Prédios ou Campos	Prédio-Prédio	Além das Metropolitanas	Área Metropolitana	Distâncias curtas
Função	Extensão ou alternativa para LAN (com cabo)	Alternativa para conexão com cabo	Extensão de LAN	Extensão de LAN (com cabo)	Ponto – Ponto Alternativa p/ cabo
Vazão (Throughput)	1 – 10 Mbps	2 - 10 Mbps	1 – 32 Kbps	10 – 100 Kbps	0.1- 4Mbps

Tabela 3.2 Comparação entre as principais aplicações das redes wireless[ELLISON,2001]

4 CRIPTOGRAFIA NAS REDES WIRELESS

Em toda solução Wireless, a segurança é um dos fatores de maior importância, pois os dados que trafegam pala rede devem ser mantidos em sigilo total, sem riscos de cair ao conhecimento de pessoas indevidas.

Neste capitulo abordarei o que é criptografia, seus tipos e como é implementada nas redes Wireless, e também um dos principais algoritmos de criptografia que é o RC4 que é o algoritmo utilizado pelo protocolo WEP, que é o protocolo utilizado nas redes Wireless pela Empresa Ferteco Mineração S/A, apresentado no estudo de caso do próximo capítulo.

4.1 CRIPTOGRAFIA E SEUS CONCEITOS

A criptografia representa a transformação de informação inteligível numa forma aparentemente ilegível, a fim de ocultar informação de pessoas não autorizadas, garantindo principalmente o sigilo.

“A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia) e define a ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamada comumente de texto cifrado, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza, no processo inverso, a decifragem”. [TERADA,2000].

Há duas maneiras básicas de se criptografar mensagens: através de códigos ou através de cifras. A primeira delas procura esconder o conteúdo da mensagem através de códigos predefinidos entre as partes envolvidas na troca de mensagens. Imagine o exemplo onde em uma guerra, um batalhão tem duas opções de ação contra o inimigo: atacar pelo lado direito do inimigo ou não atacar. A decisão depende da avaliação de um general posicionado em um local distante da posição de ataque deste batalhão. É acertado que se for enviado uma mensagem com a palavra "calhau", o exército deverá atacar pela direita; se for enviada uma mensagem com a palavra "araçagy", não deve haver ataque. Com isso, mesmo que a mensagem caia em mãos inimigas, nada terá significado coerente. O problema deste tipo de solução é que com o uso constante dos códigos, eles são facilmente decifrados. Outro problema é que só é possível o envio de mensagens predefinidas. Por exemplo: não há como o general mandar seu exército atacar pela esquerda.

O outro método usado para criptografar mensagens é a cifra, técnica na qual o conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original. A mensagem é decifrada fazendo-se o processo inverso ao ciframento. Os principais tipos de cifras são [TERADA,2000]:

1. Cifras de Transposição: método pelo qual o conteúdo da mensagem é o mesmo, porém com as letras postas em ordem diferente. Por exemplo, pode-se cifrar a palavra "CARRO" e escrevê-la "ORARC";

2. Cifras de Substituição: neste tipo de cifra, troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição. As cifras de substituições podem ser subdivididas em:

3. Cifra de substituição simples, monoalfabética ou Cifra de César: é o tipo de cifra na qual cada letra da mensagem é substituída por outra, de acordo com uma tabela baseada geralmente num deslocamento da letra original dentro do alfabeto. Ela é também chamada Cifra de César devido ao seu uso pelo imperador romano quando do envio de mensagens secretas. César quando queria enviar mensagens secretas a determinadas pessoas, substituía cada letra "A" de sua mensagem original pela letra "D", o "B" pelo "E", etc., ou seja, cada letra pela que estava três posições a frente no alfabeto.

4. Cifra de substituição polialfabética: consiste em utilizar várias cifras de substituição simples, em que as letras da mensagem são rodadas seguidamente, porém com valores diferentes.

5. Cifra de substituição de polígramos: utiliza um grupo de caracteres ao invés de um único caractere individual para a substituição da mensagem. Por exemplo, "ABA" pode corresponder a "MÃE" e "ABB" corresponder a "JKI".

6. Cifra de substituição por deslocamento: ao contrário da cifra de César, não usa um valor fixo para a substituição de todas as letras. Cada letra tem um valor associado para a rotação através de um critério. Por exemplo, cifrar a palavra "CARRO" utilizando o critério de rotação "023", seria substituir "C" pela letra que está 0(zero) posições a frente no alfabeto, o "A" pela letra que está 2 (duas) posições a frente, e assim por diante, repetindo-se o critério se necessário.

A principal vantagem das cifras em relação aos códigos é a não limitação das possíveis mensagens a serem enviadas, além de ser tornarem mais difíceis de serem decifradas.

As cifras são implementadas através de algoritmos associados a chaves, longas seqüências de números e/ou letras que determinarão o formato do texto cifrado.

4.2 CHAVES

O conceito de chave apresentado é um tanto abstrato, mas se pensarmos no criptosistema como um conjunto de algoritmos, as chaves são elementos fundamentais que interagem com os algoritmos para a cifragem/decifragem das mensagens. A figura 4.1 ilustra bem esta relação.[TRINTA,1998]

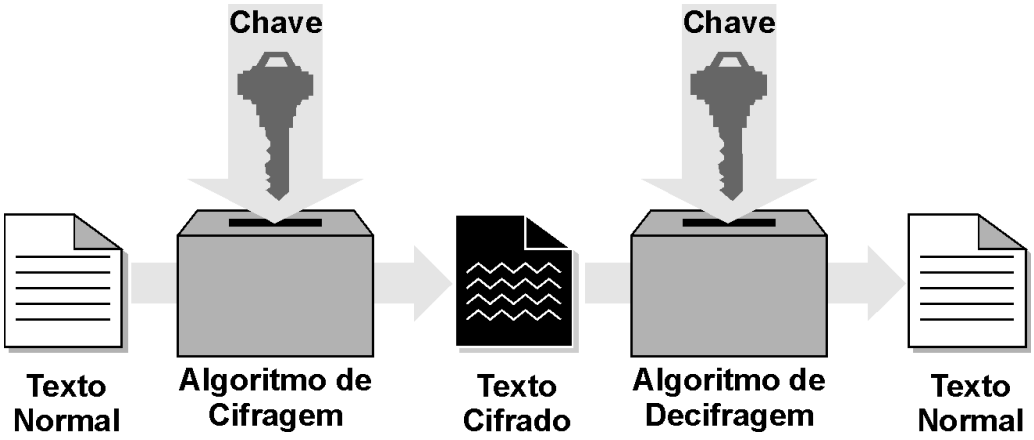


Figura 4.3 Cifragem e decifragem de uma mensagem.[TRINTA,1998]

“Para entender melhor o conceito de chave, considere o exemplo de cifras de substituição por deslocamento descrito anteriormente. Nele, o critério utilizado para a cifragem das mensagens não é nada mais que a chave usada pelo algoritmo. No caso também da cifra de substituição simples, poderia-se dizer que o algoritmo de cifragem seria algo do tipo "deslocamento de *n* letras à frente", onde *n* seria a chave”.[TRINTA,1998]

Do ponto de vista do usuário, as chaves de criptografia são similares as senhas de acesso a bancos e a sistema de acesso a computadores. Usando a senha correta, o usuário tem acesso aos serviços, em caso contrário, o acesso é negado. No caso da criptografia, o uso de chaves relaciona-se com o acesso ou não à informação cifrada. O usuário deve usar a chave correta para poder decifrar as mensagens.

Tomando-se ainda a comparação aos sistemas de acesso a computadores, senhas dos serviços descritos acima podem possuir diferentes tamanhos, sendo que quanto maior for a senha de um usuário, mais segurança ela oferece. Assim como estas senhas, as chaves na

criptografia também possuem diferentes tamanhos, e também seu grau de segurança está relacionado com sua extensão.

Na criptografia moderna, as chaves são longas seqüências de bits. Visto que um bit pode ter apenas dois valores, 0 ou 1, uma chave de três dígitos oferecerá $2^3 = 8$ possíveis valores para a chave. Sendo assim, quanto maior for o tamanho da chave, maior será o grau de sigilo da mensagem.

4.3 TIPOS DE CRIPTOGRAFIA

Há basicamente dois tipos de criptografia em relação ao uso de chaves. Quando podemos cifrar e decifrar uma mensagem usando a mesma chave tanto para o ciframento quanto para o deciframento, dizemos estar usando um sistema de criptografia por chave simétrica ou chave secreta. Caso estas chaves sejam diferentes, fala-se de um sistema de chaves assimétricas ou chave pública. No estudo seguir, veremos com mais detalhes a criptografia por chave simétrica que é a utilizada pelo algoritmo RC4 que é o centro de nossos estudos neste capitulo.

4.3.1 CRIPTOGRAFIA POR CHAVE SECRETA

No caso do uso de chave secreta, tanto o emissor quanto o receptor da mensagem cifrada devem compartilhar a mesma chave, que deve ser mantida em segredo por ambos. A figura 4.2 ilustra o processo de criptografia por chave secreta, mostrando que a mesma chave que atua para a cifragem da mensagem, é utilizada para sua posterior decifragem. [TERADA,2000].

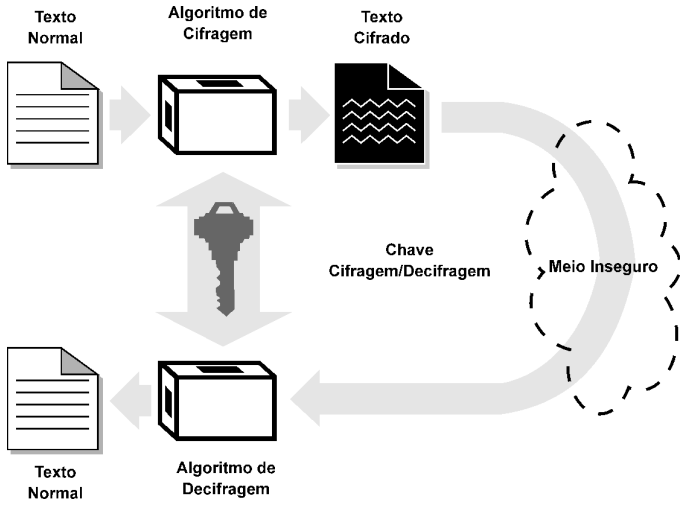


Figura 4.2 – Processo de criptografia por chave secreta.[TRINTA,1998]

Se uma pessoa quer se comunicar com outra com segurança, ela deve passar primeiramente a chave utilizada para cifrar a mensagem. Este processo é chamado distribuição de chaves, e como a chave é o principal elemento de segurança para o algoritmo, ela deve ser transmitida por um meio seguro. Porém, se existe um meio seguro de se enviar a chave, por que não enviar a própria mensagem por este meio? A resposta para esta questão é que meios seguros de comunicação são geralmente caros e mais difíceis de serem obtidos e utilizados, sendo então razoável sua utilização uma única vez, mas não continuamente.

Existe outro problema no processo de distribuição das chaves. Imaginando-se o caso de três pessoas – A, B e C – que queiram se comunicar utilizando chaves secretas. Serão necessárias 3 (três) chaves: uma compartilhada entre A e B, outra entre A e C, e a última entre B e C, como descrito pela figura 4.3.

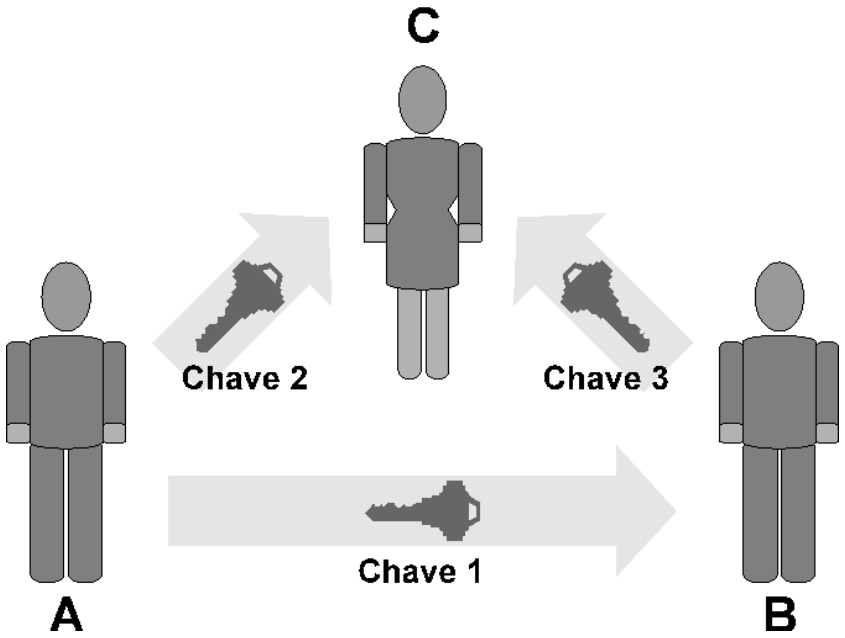


Figura 4.3 – Comunicação usando chaves secretas.[TRINTA,1998]

Se mais pessoas forem inclusas neste sistema de comunicação, mais chaves serão necessárias. No caso de mais duas pessoas, mais sete chaves serão necessárias. Em geral, se *n* pessoas querem se comunicar utilizando chave secreta, serão necessárias $\frac{(n)(n-1)}{2}$ chaves, gerando um grande problema para o gerenciamento de chaves entre grandes grupos de usuários.

Uma das tentativas de solucionar o problema da distribuição das chaves secretas foi a criação de um centro de distribuição de chaves(Key Distribution Center - KDC), que seria responsável pela comunicação entre pessoas aos pares. Para isto, o KDC deve ter consigo todas as chaves secretas dos usuários que utilizam seus serviços. Por exemplo, imagine a situação descrita pela figura 4.4, onde A quer mandar uma mensagem secreta para B. Para isto, ele manda a mensagem para o KDC usando sua chave secreta. O KDC recebe esta mensagem, decifrando com a chave secreta de A, depois o KDC a cifra novamente usando agora a chave secreta de B, e a envia para o mesmo.[TERADA,2000]

O maior problema em torno do KDC, é que este constitui um componente centralizado, além de ser gerenciado por pessoas que podem, casualmente, serem corrompidas.

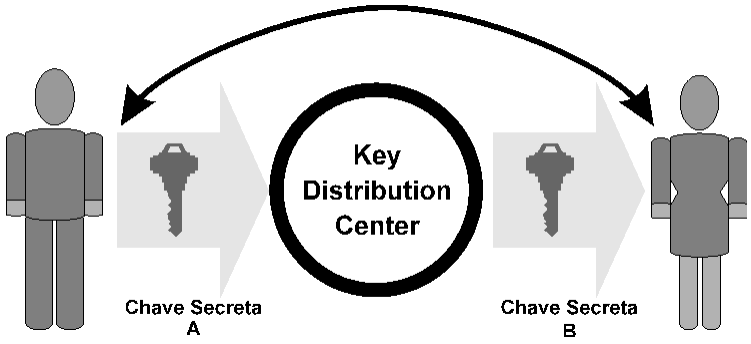


Figura 4.4 – O Centro de Distribuição de Chaves (KDC).[TRINTA,1998]

Em relação ao uso das cifras, os algoritmos de chaves secretas utilizam dois tipos de cifra:

- **Cifras de corrente**: quando se cria uma chave aleatória com o mesmo tamanho do texto a ser cifrado, e combina-se a chave com a mensagem a ser enviada.

- **Cifras de Bloco**: aceita um grupo de bits ou bloco de dados, podendo ser utilizados em cadeia. São geralmente usados para grandes quantidades de dados.

4.4 ALGORITMO RC4

"O RC4 foi criado por Ronald Rivest em 1987, e foi mantido em sigilo. O algoritmo era propriedade da RSA Security. Em 1994, alguém enviou, anonimamente, para uma lista de discussão da Internet, um algoritmo, afirmando que aquele era o RC4. Este fato foi confirmado empiricamente, e o que era segredo industrial virou domínio público, da noite para o dia. Felizmente, como um bom algoritmo criptográfico, o RC4 é seguro independente de seu algoritmo ser público ou não".[DAHA,2003]

O RC4 é, na verdade, uma maneira de se gerar bytes aleatórios, a partir de uma chave de tamanho variável. Estes bytes serão usados para encriptar uma mensagem através da operação lógica XOR. O destinatário executará o RC4 como o remetente, obtendo os mesmos bytes aleatórios, podendo assim desencriptar a mensagem. A principal vantagem do RC4 é que ele é um algoritmo defluxo. O algoritmo de fluxo é chamado assim, pois concatena a string gerada com a mensagem pura à medida que esta ultima é gerada.

4.4.1 ALGUMAS FRAQUEZAS DO RC4

"O RC4 tem o estado interno secreto, que é uma permutação de todos os $N = 2^n$ possíveis *n* bits de letras, permitindo dois índices nele. Na pratica a aplicação n=8, e assim o RC4 tem um estado $\log_2 (2^8! \text{ X } (2^8)^2 = 1700$".[TRINTA,1998].

Algumas das fraquezas do "Key Scheduling Algorithm" (KSA) o estado inicial de uma chave, variável do tamanho, e descrever duas significantes fraquezas deste processo. A fraqueza da existência de classes grandes de chaves fracas, em que uma parte pequena da chave secreta determina um número grande bits do estado inicial da permutação KSA de saída. Além do "Pseudo Random Generation Algorithm" (PRGA) a tradução destes testes padrões na permutação inicial em testes padrões prefixo do "stream" de saída, e assim RC4 tem a propriedade indesejável que são as chaves fracas, suas saídas iniciais são desproporcionalmente afetadas por um pequeno número de bits da chave. Estas chaves fracas têm o comprimento que é $l = 2^q m$ para algum $q > 0$[1].

Quando o RC4n usa uma chave fraca de l palavras, fixando n + q (l – 1) + 1 bit de K (um teste padrão particular) determina q (N) bits da permutação inicial com probabilidade de metade da determina vários prefixos de saída do stream com várias probabilidades (dependendo de seu comprimento).

A segunda fraqueza está relacionada com a vulnerabilidade de chave relacionado, que se aplica quando a parte da chave apresentada ao KSA é exposta ao atacante.Consiste na observação de quando a mesma parte secreta da chave é usada com números diferentes valores expostos, um ataque pode derivar a parte secreta para analisar a palavra inicial do keystreams com relativamente pouco trabalho. Esta concatenação de uma parte secreta a longo prazo com uma peça visível do atacante é uma modalidade geralmente usada no RC4, e particularmente usada no protocolo WEP, que protege muitas redes wireless. O novo ataque nesta modalidade é prático para todo o tamanho de chave e para qualquer modificação de tamanho, incluindo os 24 bits recomendados originalmente no WEP e 128 bits recomendado e revisado no WEP2.

4.5 RC4 E A SEGURANÇA

"RC4 consiste em duas partes (descritas na figura 4.5). Um "Key Scheduling Algorithm" KSA que gire uma chave aleatória (cujo tamanho típico seja 40-256 bits) em uma permutação inicial de *S* de (0,...,N – 1) e uma parte de geração de saída do PRGA com usuários que a permutam para gerar uma pseudo-randômica seqüência de saída". [TRINTA,1998]

A PRGA inicializa dois índices de *i a j para 0*, e então loops sobre as quatro operações incrementando *i* ao contador, incrementando *j* pseudo randomicamente, trocando os dois valores de *S* apontado para *i* e *j*, e a saída do valor de *S* apontado para $S[i] + S[i]^2$. Note que cada entrada de S é trocado ao menos uma vez (possivelmente com ele mesmo) dentro de muitos *N* com círculos consecutivos, e assim a permutação de *S* envolve com razoável rapidez a duração da geração do processo de saída. O KSA consiste de *N* loops que são similares a rodar uma operação PRGA.

Inicializando S para ser o identificador da permutação de i e j para 0, e aplica o PRGA rodando na operação em um tempo N , passando de i através de S, e atualizando j adicionando S[i] na seguinte palavra da chave (em ordem cíclica). Nós chamamos cada ciclo do KSA de uma etapa.

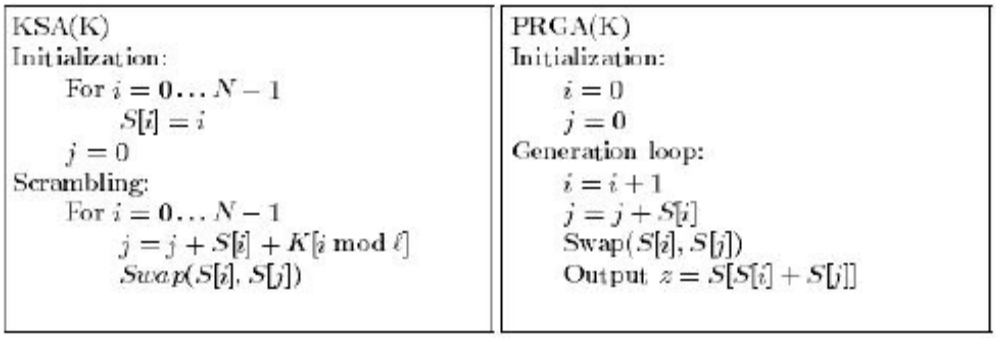


Figura 4.5 Demonstra os algoritmos de programação fundamental e o algoritmo de geração Pseudo-Random[DAHA,2003]

4.5.1 PRECEDENTES DE ATAQUES NO RC4

"Devido à enorme chave efetiva de RC4, atacar o PRGA parece ser impossível (melhor ataque conhecido nesta parte requer tempo que excede 2^{700}). O único resultado prático relatado no PRGA é o negocio de distinguir construções. Pesquisadores descreveram como distinguir saídas randômicas no RC4 com strings de 2^{30}".[TRINTA,1998]

Porém, só poderiam ser usados para montar um ataque parcial em RC4 em aplicativos difundidos. Em particular, foi descoberto dentro de uma classe de chaves fracas que reduzem o tamanho efetivo delas em cinco bits, os pesquisadores, demonstraram que dentro de chaves grandes, cujo tamanho está perto de *N* palavras, o RC4 é vulnerável a ataque.

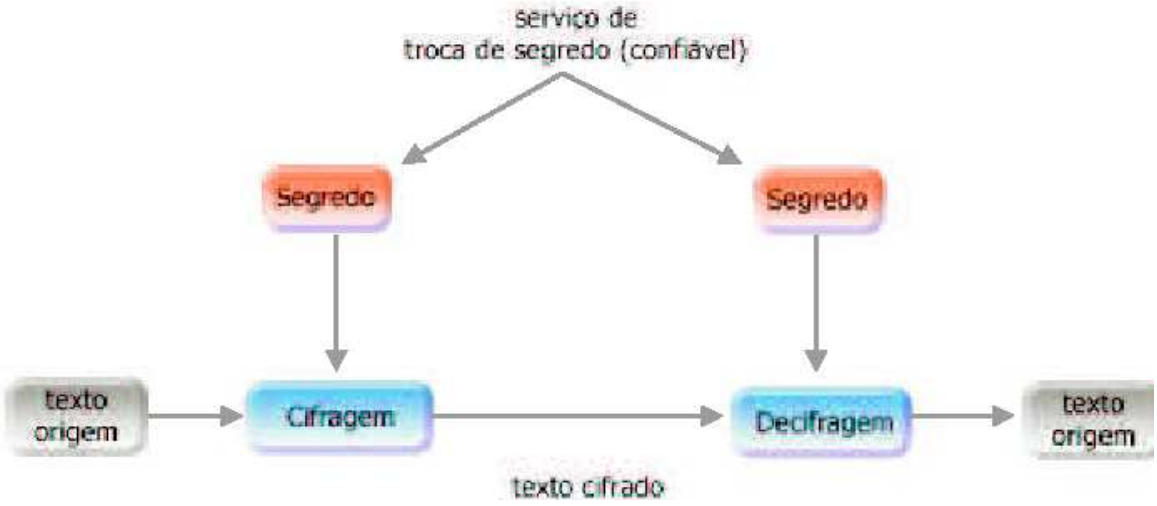
5 WEP E SUA SEGURANÇA

Neste capitulo apresentamos os conceitos sobre WEP(Wired Equivalent Privacy), que é um protocolo de segurança usado em redes 802.11 que tenta prover segurança semelhante à redes com fio, através de criptografia e autenticação no nível do enlace wireless. Seu principal objetivo é manter a confidencialidade dos dados do usuário. Porém, ao longo deste trabalho iremos analisar sua eficiência e tentar descobrir se o WEP é de fato um protocolo seguro e se seu uso realmente garante confidencialidade, autenticidade e integridade aos dados transmitidos.

5.1 WEP

As redes sem fio, como a IEEE 802.11b, possuem um conjunto adicional de elementos de segurança, chamado WEP, que não está disponível no mundo cabeado. O WEP possui um serviço de troca de mensagens , a partir da troca de segredos(chaves), a figura 4.1 demonstra esta troca de segredos.[WALKER,2002]

Figura 5.4 Troca de segredos utilizadas pelo protocolo WEP[MODULO,2003]



O WEP atua na camada de enlace entre estações e o ponto de acesso (AP), oferecendo, basicamente, três serviços: confidencialidade, integridade e autenticação. A figura a seguir faz uma comparação entre modelo IEE802.11 e o modelo OSI, suas camadas e representações.

Figura 5.5 Comparação entre modelo IEE 802.11 e o modelo OSI[MODULO,2003]

5.1.1 CONFIDENCIALIDADE

A implementação da confidencialidade da transmissão é opcional, ou seja, pode ser habilitada ou não. Quando habilitada, a confidencialidade é garantida pela técnica de criptografia de chave simétrica, utilizando o algoritmo RC4.[FERNANDES,2003]

"O RC4, projetado por Ron Rivest em 1987, é um algoritmo de chaves secreta, amplamente utilizada em aplicações comerciais, especialmente em transações na Internet que utilizam SSL".[FERNANDES,2003]

Para que seja possível o ciframento dos frames, os participantes devem compartilhar a mesma chave secreta. A configuração das chaves é feita manualmente em cada estação. Um dos grandes problemas no WEP é a ausência de um mecanismo de gerência de chaves, o que introduz uma série de vulnerabilidades e não garante escalabilidade ao modelo. Por exemplo, se a chave secreta de uma estação for roubada, todas as estações terão que ter suas chaves alteradas.[FERNANDES,2003].

Para enviar uma mensagem, a estação transmissora, inicialmente, concatena a sua chave secreta (shared key) a um vetor de inicialização (IV). O resultado serve de entrada para o algoritmo gerador de números pseudo-aleatórios (PRNG) definido pelo RC4. O PRNG gera uma seqüência de bits do mesmo tamanho que a informação a ser cifrada, ou seja, o frame MAC incluindo o CRC. Um XOR (OU exclusivo) é realizado entre o frame e a seqüência de bits, gerando o frame cifrado. Finalmente, o frame é enviado juntamente com o IV para que o receptor possa fazer o processo inverso (Fig.5.3).

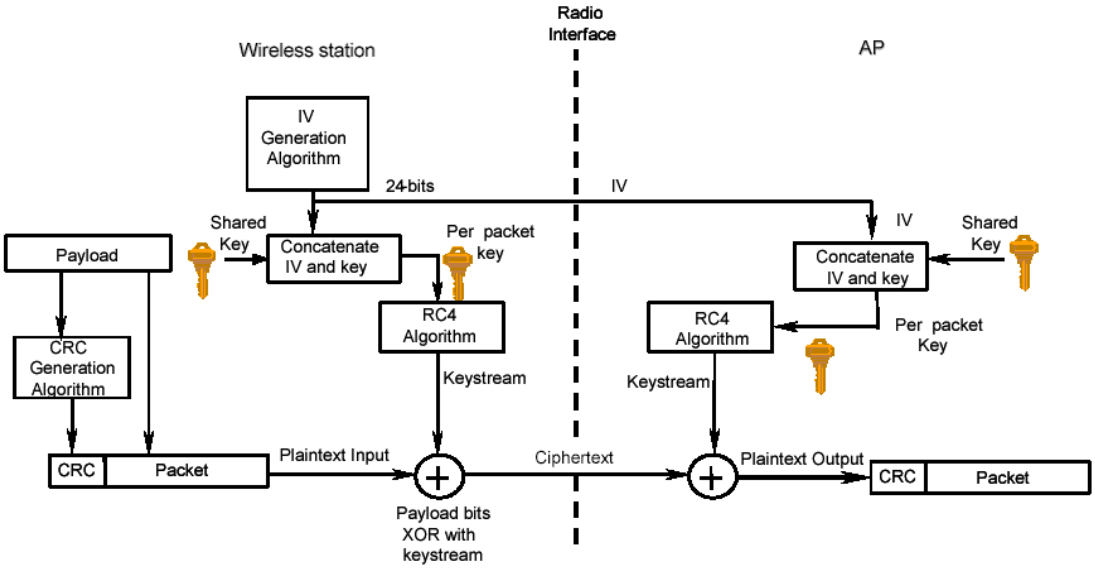


Figura 5.3 Demonstra a implementação da confidencialidade no 802.11[FERNANDES,2003].

O WEP utiliza um vetor de inicialização (IV) de 24 bits para proteger a chave secreta utilizada no processo de criptografia. A cada frame enviado, o IV é gerado e concatenado à chave secreta, fazendo com que a chave utilizada no ciframento do frame (keystream) mude a cada novo frame. O vetor de inicialização faz com que o tamanho de chave passe de 40 bits para 64 bits e de 104 bits para 128 bits, porém como IV é passado em claro para a estação destino para realizar a decriptografia, os tamanhos das chaves continuam 40 bits e 104 bits para fins de criptografia. De qualquer forma, quanto maior o tamanho da chave criptográfica, mais seguro é processo de criptografia.Um dos grandes problemas na implementação da confidencialidade no WEP é o esquema de geração das chaves criptográficas utilizadas pelo algoritmo RC4. O RC4 utiliza uma nova chave a cada frame enviado, sendo que a chave é formada por uma parte fixa (chave secreta) e uma variável (IV). O problema está na parte variável da chave, que possui apenas 24 bits e pode repertir-se em pouco tempo, comprometendo a chave como um todo. Em uma rede com grande fluxo de mensagens, é possível derivar chaves de 128 bits após o envio de cerca de quatro milhões de frames ou depois de quatro horas de monitoramento da rede. Apesar desta vulnerabilidade, o RC4 continua sendo utilizado na maioria das aplicações Web com base no SSL, mas implementando um outro esquema de geração de chaves.[FERNANDES,2003]]

5.1.2 INTEGRIDADE

"A integridade de um frame, ou seja, a garantia que o frame não seja alterado entre o transmissor e o receptor é implementada a partir da técnica de CRC-32 (Cyclic Redundancy Check), que gera um ICV (Integrity Check Value) para cada frame enviado. Ao receber o frame, o destinatário executa a mesma função de CRC e compara o ICV obtido com ICV recebido. Caso o valor do ICV calculado for igual ao ICV recebido, a mensagem está integra, caso contrário, o frame sofreu alguma alteração" (Fig.4.4).[FERNANDES,2003]

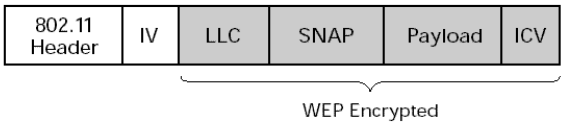


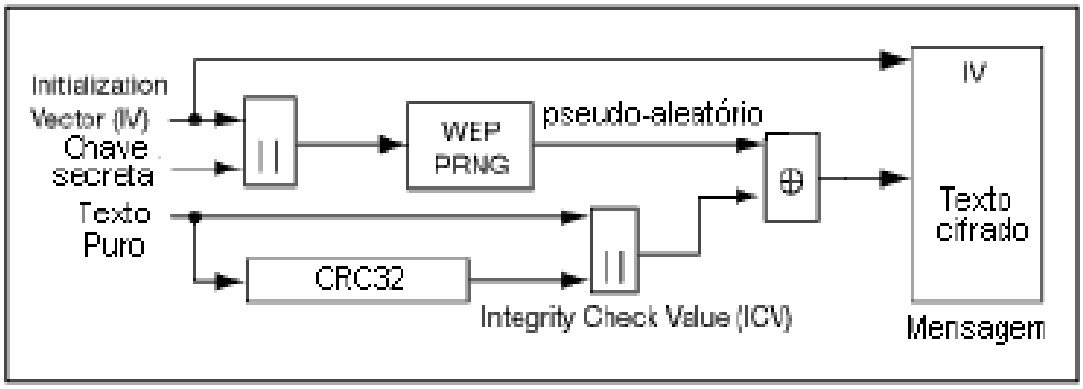
Figura 5.4 Frame WEP[FERNANDES,2003]

A utilização da técnica de CRC para gerar a integridade do frame, torna o WEP vulnerável à ataques do tipo replay e bit-flipping.

5.1.3 AUTENTICAÇÃO

O WEP utiliza a mesma chave para encriptar e desencriptar os pacotes. Veja como o algoritmo de encriptação do WEP funciona:

Figura 5.5 Funcionamento do algoritmo de encriptação[RIVEST,2003]



Dois processos são aplicados sobre o texto puro. Um deles é o processo de encriptação e o outro é um processo que visa proteger quanto uma alteração não autorizada no texto durante a transmissão.

"A chave secreta tem 40 bits e é concatenada com um Vetor de Inicialização (IV) de 24 bits, formando a chave composta que será responsável por chegar a string pseudo aleatória de bits. A chave composta é inserida no algoritmo de PRNG (Pseudo-random Number Generator). O PRNG é baseado no algoritmo RC4 (Ron's Cipher 4), que vimos no capítulo 3 desse trabalho. A saída do algoritmo PRNG é uma seqüência pseudo-aleatória de bits, baseada na chave composta. Esta saída é utilizada para encriptar o texto puro através de uma operação binária de XOR. O resultado da encriptação é exatamente do tamanho do texto puro. A este resultado é concatenado, no início do pacote, o vetor de inicialização, e no final do pacote, 4 bytes (32 bits) resultado de um processo de ICV (integrity check value). O algoritmo de ICV é o CRC32. Esse conjunto, texto encriptado, IV e ICV são enviados pelo canal inseguro. O CRC32 é utilizado para proteger os dados contra uma modificação não autorizada".[DAHA,2003]

A estação destino, que de antemão já sabe o valor da chave secreta, usa o IV que vem no inicio do pacote para criar a mesma string gerada pelo PRNG e desencriptar o texto cifrado. Então ele roda o CRC32 sobre esse texto desencriptado e recebe um novo valor de ICV. Ele compara esse novo valor de ICV com o valor que veio no final do pacote transmitido. Se os

valores forem diferentes, o pacote é descartado, pois se tem certeza que a sua integridade foi quebrada.

Esquema do pacote cifrado que é transmitido pelo canal inseguro

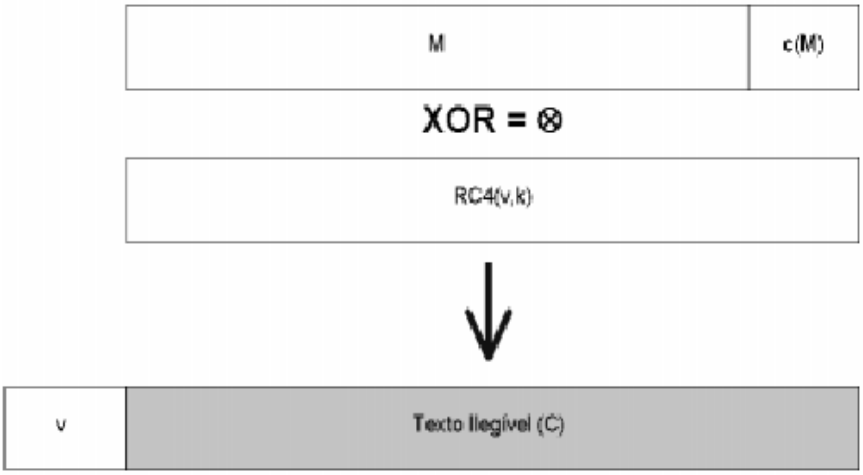


Figura 5.6 Operação lógica de Ou-exclusivo para encriptação. [WALKER,2002]

"No WEP, a mesma chave que é utilizada para encriptar e desencriptar é também utilizada para autenticar uma estação. Ter a mesma chave para encriptar e autenticar é um risco de segurança. Existe também um método onde as estações que o ponto de acesso pode utilizar o WEP sozinho sem compartilhar autenticação de chaves,essencialmente utilizando o WEP como encriptador".[DAHA,2003]

O PRNG (RC4) é o componente mais crítico do processo WEP, já que é o real responsável pela encriptação. O vetor de inicialização estende a vida da chave secreta e provê a auto-sincronização do algoritmo. A chave secreta continua constante e o IV se altera periodicamente. O IV pode variar a cada envio de pacote.

"No WEP existe dois tipos de autenticação no padrão IEE 802.11: sistema aberto (open system) e chave compartilhada (shared key). A autenticação por sistema aberto é a opção default e, na verdade, funciona apenas como mecanismo de identificação, devendo ser

evitado. Se o mecanismo de criptografia não estiver habilitado, qualquer dispositivo poderá ter acesso ao AP(Acess Point) e, conseqüentemente, acesso à rede. Se a criptografia estiver habilitada e o cliente não possuir uma chave secreta, o cliente não conseguira transmitir mensagens através do Acess Point e nem recebê-las, mesmo que a estação seja autenticada.A autenticação com base em chave compartilhada utiliza a técnica de challenge-response. Neste mecanismo, o ponto de acesso não é autenticado, apenas a estação".[FERNANDES,2003]

Na Fig.5.7 , a estação sem fio (wireless station) está solicitando ao Acess Point sua autenticação (authentication request). O Acess Point gera um número aleatório (challenge) e o envia para a estação. A estação recebe o número, criptografa-o utilizando o algoritmo RC4 e o envia de volta (response). O AP decripta a resposta e a compara com o número enviado. Se a comparação for positiva, o AP envia para a estação um mensagem confirmando o sucesso da autenticação.

Figura 5.7 Autenticação no 802.11[MODULO,2003]

Um grande problema neste esquema de autenticação é que o processo de challenge-response é vulnerável a ataques do tipo man-in-the middle, que refere-se a qualquer ataque em que um segundo elemento (pessoa, sistema ou aplicação) faz a comunicação mascarando-se como o destino pretendido. Como é possível capturar tanto o texto cifrado como o texto original, a chave criptográfica pode ser facilmente derivada.

Uma alternativa para autenticação seria por endereço MAC (Medium Access Control) é uma outra forma de autenticação, porém não é padrão IEEE, mesmo sendo oferecida por alguns fabricantes. Neste esquema, existe um servidor de autenticação que verifica, a partir de uma lista de endereços MAC, se a estação cliente está autorizada ou não a ter acesso à rede. Este mecanismo não oferece segurança, pois os endereços MAC podem ser interceptados e forjados, permitindo ataques do tipo spoofing.[FERNANDES,2003]

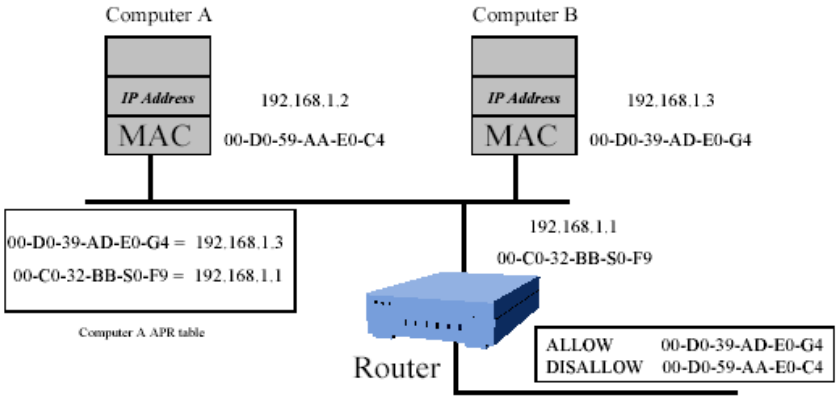


Figura 5.8 Utilização de um Router para filtragem dos endereços MAC[WALKER,2002]

Muitos problemas podem ser gerados na autenticação na figura 4.9 temos um exemplo de como um invasor pode entrar na rede se passando por outro usuário, tendo assim acesso a dados confidenciais.

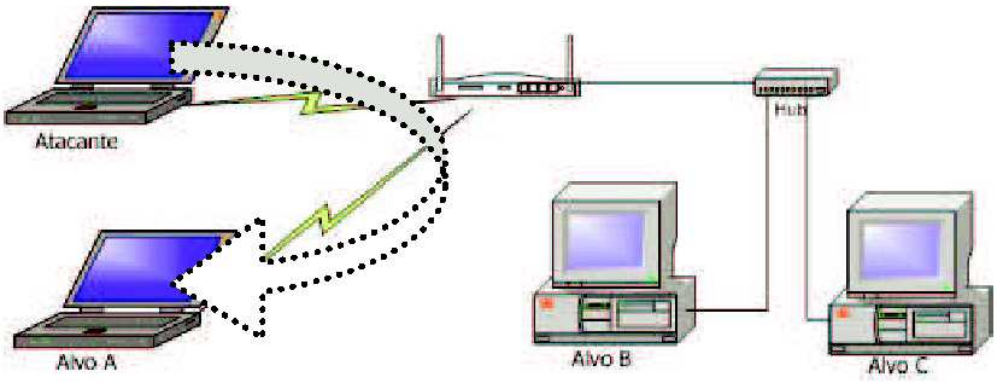


Figura 5.9-Spoofing – O invasor diz para A que ele é B.[DAHA,2003]

5.2 QUEBRA DO PROTOCOLO WEP

A Intel, foi um dos primeiras a demonstrar que a chave WEP não é segura independente do seu tamanho, uma pesquisa feita por Nikita Borisov, Ian Goldberg e David Wagner da UC Berkeley7, foi possível quebrar uma chave WEP de 40 bits em 4 horas usando 250 computadores. Também demonstraram que é possível quebrar chaves de 128 bits.

"Foi provado que é possível ter acesso à chave utilizada na criptografia o que provocou surgimento de diversas ferramentas para quebra do WEP na Internet.Apresentaremos algumas falhas que contribuíram para quebra do WEP". [WALKER,2002]

5.2.1 REUTILIZAÇÃO DE UMA SEQÜÊNCIA

A criptografia WEP, ao utilizar o algoritmo RC4 permite que a mesma seqüência aleatória se repita de vez em quando. Isso, é um ponto muito desfavorável para o aspecto de segurança do protocolo, mostraremos a seguir, o que pode ocorrer ao reutilizarmos uma seqüência RC4(v,k)[WALKER,2002].

Suponha que C1 e C2 são dois pacotes cifrados com o mesmo vetor de inicialização e a mesma chave secreta.Então temos a seguinte situação:

$$C1 = P1 \otimes RC4(v,k)$$
$$C2 = P2 \otimes RC4(v,k)$$
$$C1 \otimes C2 = (P1 \otimes RC4(v,k)) \otimes (P2 \otimes RC4(v,k))$$
$$= P1 \otimes P2$$

Ou seja, podemos observar que, com dois pacotes cifrados com a mesma seqüência, é possível recuperar um xor (ou exclusão) dos dois textos planos sem conhecer a chave secreta e o vetor de inicialização. Isso só foi possível pois houve um cancelamento da seqüência RC4, que por sua vez ocorreu devido ao fato dos dois pacotes terem sido igualmente cifrados. Esse resultado permite uma série de ataques ao protocolo uma vez que se um dos dois textos é conhecido, imediatamente o outro torna-se conhecido. Mas conhecer um pacote não é tarefa tão difícil, afinal muitos pacotes possuem conteúdo previsível (ex: cabeçalho). Além disso, muitos textos possuem redundância, o que torna mais fácil descobrir seus conteúdos através de várias técnicas conhecidas. (ex: análise da freqüência).

Para evitar este tipo de ataque, o WEP utiliza um vetor de inicialização diferente para cada pacote, e então, apesar da chave ser a mesma para todos os pacotes, a seqüência gerada pelo RC4 será diferente para cada pacote.

No entanto, apesar de existir a recomendação de se utilizar um vetor de inicialização diferente para cada pacote, o protocolo WEP não especifica a maneira como devem ser selecionados os VI´s, e isso causa deficiência no protocolo já que a chance de serem utilizados dois VI´s iguais, a que chamaremos de colisão, existe e nem sempre é pequena.

Algumas placas geram os vetores de inicialização de maneira seqüencial começando do zero e incrementando seu valor a cada pacote enviado. Além disso, resetam seu valor para zero cada vez que um cartão é reinserido na máquina. Isso faz com que baixos valores de VI´s ocorram mais freqüentemente que os outros, aumentando a chance de haver colisão entre eles.

“Além disso, a própria arquitetura do protocolo permite a ocorrência de colisões. Suponha por exemplo que estamos transmitindo numa taxa de 5Mbps (o máximo seria 11Mbps) pacotes de 1500 bytes. Com isso podemos transmitir aproximadamente 416 pacotes por segundo. Como os VI´s possuem 24 bits, a quantidade de pacotes diferentes que podem ser enviados é 2^{24} , ou seja podemos no melhor caso ficar 11 horas e 12 minutos sem enviar pacotes repetidos. No entanto esse cálculo é otimista, pois uma colisão pode acontecer mais freqüentemente. Uma implementação que usa um VI aleatório de 24 bits por pacote, terá de acordo com o “Paradoxo do Aniversário”, 50% de chance de repetir um VI depois de apenas 4823 pacotes, o que significa alguns poucos minutos”.[WALKER,2002].

5.2.2 GERENCIAMENTO DAS CHAVES WEP

“Uma outra vulnerabilidade do protocolo, se encontra no gerenciamento das chaves de criptografia. Se na transmissão, já é mandado o vetor de inicialização sem proteção alguma, é importante que a chave seja confidencial, caso contrário qualquer um que possua a chave estará apto a descobrir a seqüência RC4(v,k)”.[DAHA,2003]

Então, o protocolo realiza uma distribuição global das chaves através de um mecanismo externo onde cada mensagem tem um campo IK que identifica uma entre as quatro possibilidades de chave. Porém, na prática acaba-se usando a mesma chave k para a rede inteira. Se no entanto, a rede é grande, utilizada por muitas pessoas, então, a chave será conhecida por muitas pessoas e quanto mais gente tiver conhecimento da chave, maior será a probabilidade dela deixar de ser confidencial.

Além disso, o fato da chave ser a mesma para a rede inteira aumenta as chances de ocorrer uma colisão, o que é extremamente desfavorável.

Para evitar este tipo de problema, uma das soluções seria a troca periódica das chaves, porém, essa troca seria manual e no caso de termos uma rede muito grande, a realização da troca de centenas ou milhares de chaves seria um tanto quanto trabalhosa e até mesmo insana.

Uma outra medida que muitos administradores de rede tomam para tentar diminuir esse risco de descoberta da chave k é simplesmente fazer diretamente a configuração das chaves nos próprios dispositivos, dessa forma o usuário final não tem conhecimento de k. Essa medida diminui o risco, mas não resolve o problema visto que as chaves continuam guardadas nos dispositivos remotos.

5.2.3 AUTENTICAÇÃO DE MENSAGENS

Como já citamos anteriormente, no protocolo WEP utiliza-se um algoritmo (CRC-32) para detectar possíveis erros de transmissão que por ventura tenham modificado o conteúdo dos dados. No entanto, como trata-se de um código linear, mostraremos a seguir que esse código não é eficiente contra ataques maliciosos que podem fazer modificações controladas no pacote e não despertar suspeita.

"O usuário para poder fazer parte da rede sem fio, envia para o AP (ponto de acesso) um pedido de autenticação. Este retorna para o usuário uma espécie de desafio, ao qual o usuário deve cifrar utilizando o RC4 e a chave que ele posssui, e então, enviar de volta o desafio cifrado para o AP que vai utilizar a chave k para decifrar o conteúdo. Se o conteúdo recuperado pelo AP for igual ao original, significa que o usuário utilizou a chave k correta e portanto poderá ser autenticado e receberá uma confirmação do AP".[DAHA,2003]

No entanto, vamos mostrar que é possível violar a integridade dos dados, interceptando uma mensagem e modificando seu conteúdo. Isso só é possível devido ao fato do checksum e do RC4 serem funções lineares. Suponhamos então que C é um texto cifrado capturado por um atacante malicioso que deseja inserir um ruído r no pacote. Então, ao inserir este ruído, o atacante modificará o texto cifrado C para C´da seguinte maneira:

$$
\begin{aligned}
C' &= C \otimes (r, c(r)) \\
&= RC4(v,k) \otimes (M, c(M)) \otimes (r, c(r)) \\
&= RC4(v,k) \otimes (M \otimes r, c(M) \otimes c(r)) \\
&= RC4(v,k) \otimes (M', \otimes c(M \otimes r)) \\
&= RC4(v,k) \otimes (M', \otimes c(M'))
\end{aligned}
$$

Portanto, provamos ser possível inserir um ruído numa mensagem alterando não só a mensagem original como também o checksum da mensagem original, fazendo isso, provamos que o CRC-32 não foi capaz de manter a integridade dos dados. Além de modificar uma mensagem, é possível também inserir na rede uma nova mensagem, violando novamente o controle de acesso a rede. Mostraremos que isto é possível, devido ao fato do checksum ser uma função que não possui chave alguma. Então, basta conhecer um texto plano P para que junto com o texto cifrado C a seqüência RC4 seja descoberta:

$$P \otimes C = P \otimes (P \otimes RC4(v,k)) = RC4(v,k)$$

A partir desta seqüência, é possível injetar na rede um novo pacote cifrado de uma nova mensagem M´:

$$C´= (M´,c(M´)) \otimes RC4\ (v,k)$$

Com isso, um atacante estará apto a enviar para o AP o desafio cifrado corretamente e conseqüentemente receberá a confirmação de autenticação na rede.

É importante lembrar que isso só é possível se usarmos o mesmo VI da mensagem original. Mas apesar do protocolo recomendar que não se reutilize o VI, ele não exige que os VI´s sejam trocados a cada pacote.

Uma das possíveis soluções para este problema seria utilizar um código de autenticação de mensagem (MAC) com chave, uma função de Hash por exemplo que evitasse que o ICV fosse alterado por algum intruso.[DAHA,2003]

Um outro possível ataque seria através de uma redireção de IP. Este tipo de ataque é possível quando o AP atua como roteador de uma conexão da Internet.

Nesse caso, a idéia principal seria capturar um pacote cifrado no ar e utilizar por exemplo a técnica descrita acima para modificar seu conteúdo, no caso fazer uma modificação no endereço de destino deste pacote para um novo endereço conhecido pelo atacante. Dessa maneira, estaríamos usufruindo do AP que faria todo o processo de decriptar o pacote e então enviaria este pacote decriptado para o endereço especificado pelo atacante. Através desse tipo

de ataque, explora-se a capacidade do AP de decifrar os pacotes, para enviá-los da rede sem fio para a Internet.

6 PROPOSTA DE SEGURANÇA

Neste capítulo, apresentamos uma solução que pode deixar uma rede wireless mais segura e confiável. Propomos aqui uma reestruturação da segurança na rede wireless local (WLAN) da Empresa Ferteco Mineração S/A, baseada em uma ferramenta que empregamos na empresa e adição de alguns mecanismos de segurança.

6.1 ORINOCO CL (CLIENT) MANAGER

Neste tópico procuramos apresentar um estudo feito sobre as características gerais e de segurança que podem ser implementadas sobre a ferramenta ORiNOCO CL Manager, responsável pelo gerenciamento, controle e implementações na rede wireless da empresa Ferteco Mineração S/A. A figura 6.1 mostra a tela inicial do sistema de gerenciamento da rede wireless da empresa Ferteco Mineração S/A.

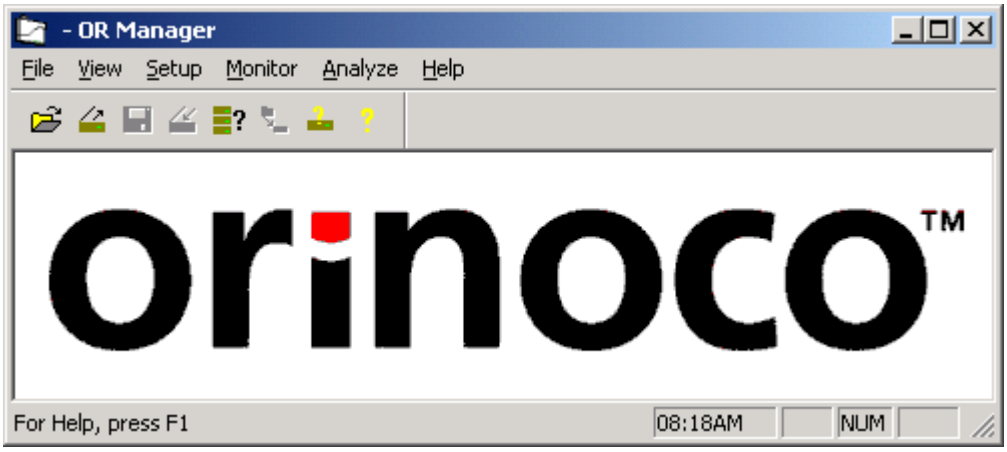


Figura 6.6 Tela inicial ferramenta Orinoco Cliente Manager[ORINOCO,2000]

6.1.1 VERIFICANDO A QUALIDADE DA COMUNICAÇÃO

Com o emprego da ferramenta ORiNOCO CL Manager o usuário pode verificar a qualidade da comunicação, testando a qualidade da ligação entre sua estação ORiNOCO e outros aparelhos sem fio aos quais esteja conectado.[ORINOCO,2000]

Também se pode usar o CL Manager para conferir a cobertura no prédio, identificar padrões de cobertura, selecionar freqüências alternativas, localizar e neutralizar interferência de Rádio freqüência e personalizar a segurança do acesso à rede.

6.1.2 FUNÇÕES DO CL MANAGER

6.1.2.1 Perfis de configuração

Para facilitar aplicações e alterações online,antes se podia dispor de 4 configurações, mas com a introdução da Edição de Verão do Software este número aumentou para 99. O que facilita o roaming entre domicílio, escritório e locais de muito público. [ORINOCO,2000]

6.1.2.1.1 Indicador de comunicações

Usuários em trânsito recebem informações gráficas em tempo real sobre o nível da qualidade da comunicação entre suas estações ORiNOCO e o ponto de acesso mais próximo. A figura 6.2 mostra todos os pontos de acesso disponíveis, através do scan conseguimos rastrear todos os pontos de acesso do local.

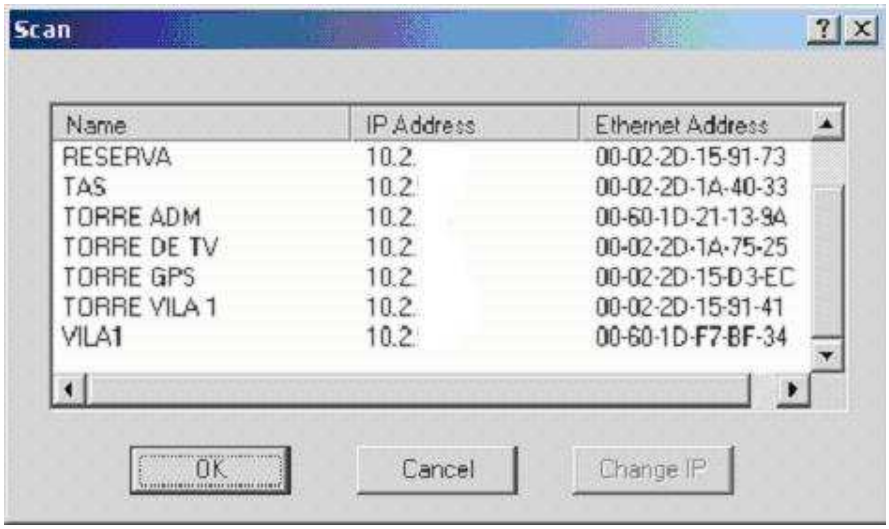


Figura 6.2 Demonstra o ponto de acesso mais próximo[ORINOCO,2000]

6.1.2.1.2 Site Monitor

Confirma a posição ideal para os seus AP-1000 (Equipamento de capitação e distribuição de sinal wireless). À medida que o usuário vai caminhando pelas dependências, o Site Monitor exibe a qualidade da comunicação em todos os pontos de acesso disponíveis no ambiente (domínio) da rede. Com o ORiNOCO Site Monitor fica fácil identificar 'pontos mortos' de rádio ou fontes de interferência, o que ajuda a melhorar o rendimento da estrutura sem fio ao otimizar a colocação dos AP-1000.[ORINOCO,2000]

6.1.2.1.3 Link Test

Utilizado para conferir o caminho de comunicação entre sua estação ORiNOCO e uma estação vizinha ou entre ela e o ponto de acesso no âmbito de uma célula sem fio. A ferramenta dá informações a respeito de onde colocar os AP-1000 para cobertura ideal. Além

disso, o Link Test demonstrado na figura 6.3, mede detalhes referentes à razão sinal-ruído e ao número de pacotes bem recebidos no aparelho local e no remoto.

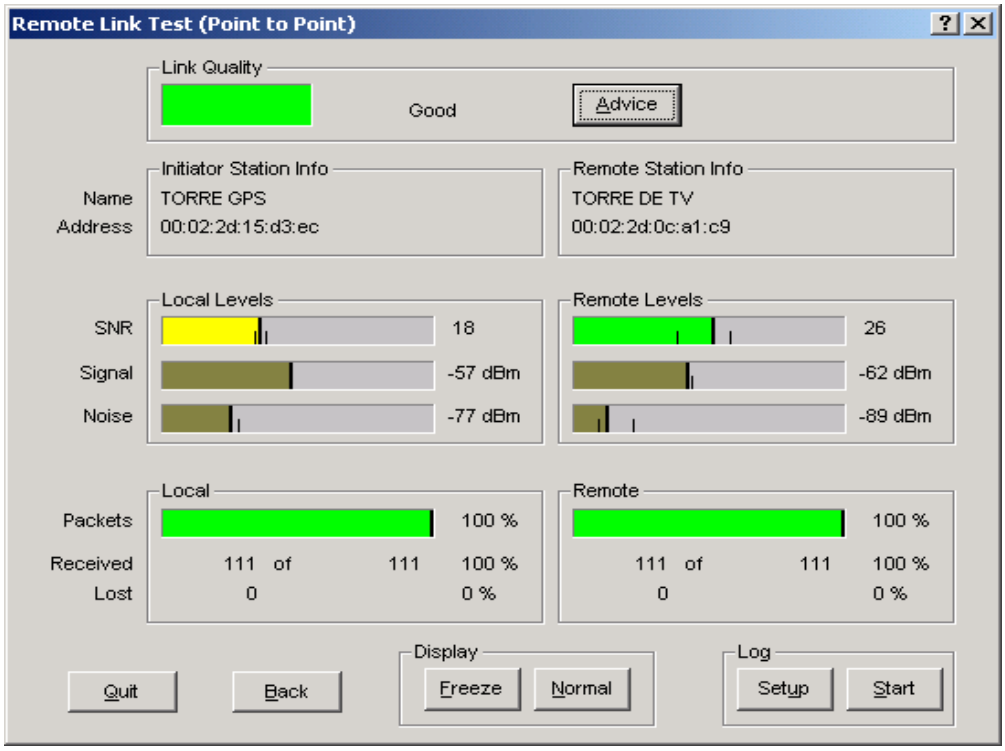


Figura 6.3 Demonstração da qualidade do link entre usuário e AP.[ORINOCO,2000]

6.1.3 WIRELESS ORINOCO X WEP

Para prover o nível mais alto de segurança na transmissão dos dados em uma rede wireless (Orinoco) podemos empregar a privacidade do protocolo de criptografia WEP. [ORINOCO,2000]

A WEP usa chave de 5 caracteres para a criptografia, baseado no RC4 algoritmo que será usado para encriptar e desencriptar todos os dados transmitido pela rede sem fio Orinoco.

O sistema de ORiNOCO pode apoiar simultaneamente até quatro chaves diferentes. Isto está conforme o 802.11 padrão que define quatro chaves.

Não é obrigatório que ambos os lados (tipicamente AP-1000 e cliente) tenham o mesmo jogo ativo de 4 chaves. Contanto que haja que uma chave em comum para que eles possam se comunicar .

A opção para usar 4 chaves diferentes para decifrar dados sem fios, lhe permite mudar suas chaves de WEP a intervalos regulares sem afetar desempenho de rede regular, este recurso vem desabilitado como padrão, a figura 6.4 mostra como esta opção vem desabilitada por padrão .

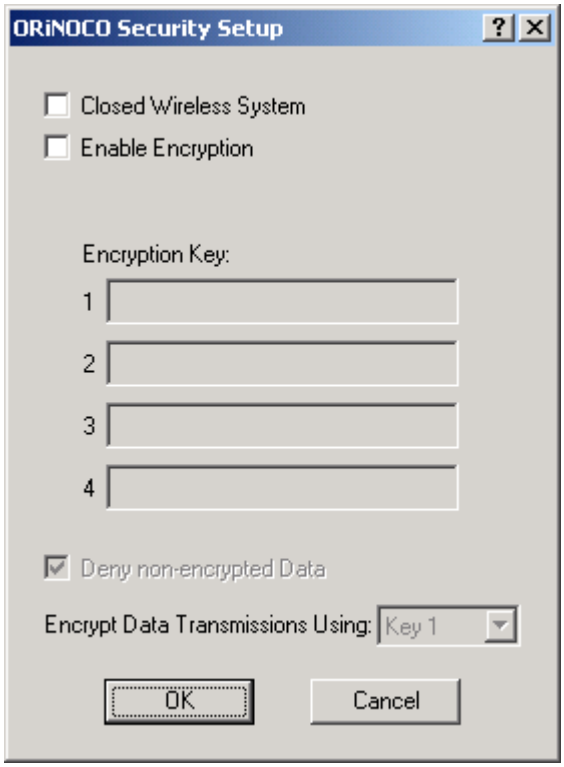


Figura 6.4 mostra como a criptografia desabilitada(padrão).[ORINOCO,2000]

6.2 PROPOSTA DE SEGURANÇA PARA A REDE EXISTENTE

Dividimos este item em dois, primeiramente falaremos sobre serviços que deveram ser habilitados ou desabilitados na própria ferramenta Orinoco Client Manager para melhorar a segurança, em seguida será proposto um sistema de segurança extra para ser implementado na rede wireless da Empresa Ferteco Mineração S/A.

6.2.1 SEGURANÇA ORINOCO

Para garantir a segurança, existem varias configurações que podem ser habilitados ou desabilitadas, na própria ferramenta Orinoco Client Manager.

6.2.1.1 ESSID

A primeira linha de defesa é o ESSID (Extended Service Set ID), um código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede. Cada fabricante utiliza um valor default para esta opção, mas você deve alterá-la para um valor alfanumérico qualquer que seja difícil de adivinhar.[ORINOCO,2000]

Geralmente estará disponível no utilitário de configuração do ponto de acesso a opção "broadcast ESSID". Devemos desabilitar esta opção evitando o broadcast na rede, devemos configurar manualmente o código ESSID em todos os micros.

Se deixarmos esta opção ativada o ponto de acesso envia periodicamente o código ESSID da rede, permitindo que todos os clientes próximos possam conectar-se na rede sem saber préviamente o código. Ativar esta opção significa abrir mão desta camada de segurança, em troca de tornar a rede mais "plug-and-play”.

6.2.1.2 Ativando WEP

Apenas o ESSID, oferece uma proteção muito fraca. Mesmo que a opção broadcast ESSID esteja desativada, já existem sniffers que podem descobrir rapidamente o ESSID da rede monitorando o tráfego de dados.[ORINOCO,2000]

Temos então o WEP, abreviação de Wired-Equivalent Privacy, que como o nome sugere traz como promessa um nível de segurança equivalente à das redes cabeadas. Na prática o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o ESSID sozinho.

O WEP vem desativado na grande maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração. O mais complicado é que você

precisará definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede. A figura 6.5 demonstra como podemos ativar o Wep usando até jogo de 4 chaves, como foi descrito acima.

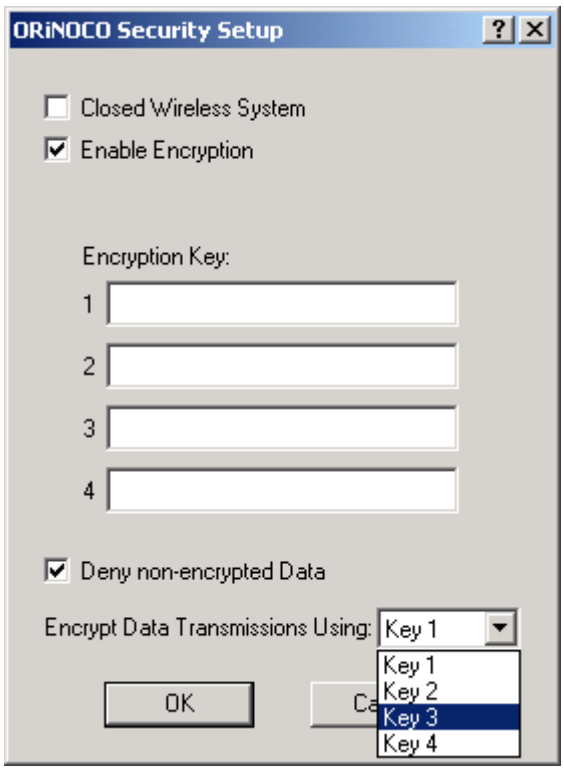


Figura 6.5 Processo de ativação WEP.[ORINOCO,2000]

6.3 IMPLEMENTAÇÃO DE MECANISMOS DE SEGURANÇA

A solução que será proposta é o resultado de todos os estudos e análises feitas durante a elaboração deste trabalho, o resultado foi a união de autenticação forte (servidor RADIUS) e equipamentos Wireless CISCO(Cisco Aironet Wireless).

6.3.1 AUTENTICAÇÃO RADIUS

"RADIUS é um padrão de encriptação proprietário que utiliza chaves de encriptação de 128 bits reais, o que o torna muito mais seguro que o WEP, provê um sistema de segurança Cliente/Servidor aberto e escalonável. O servidor RADIUS pode ser adaptado facilmente para trabalhar com produtos de segurança de terceiros ou em sistemas de segurança proprietário. Qualquer mecanismo de comunicação, seja um software ou um hardware que utilize o protocolo cliente RADIUS pode se comunicar com um servidor RADIUS".[MICROSOFT,2003]

6.3.1.1 Funcionamento

O RADIUS autentica através de uma série de comunicações entre o cliente e o servidor. Uma vez que o usuário é autenticado, o cliente proporciona a ele, o acesso aos serviços apropriados. Os passos envolvidos no processo do RADIUS estão descritos a seguir. [MICROSOFT,2003]

1. PortMaster cria um pacote de dados com as informações e o chama de "pedido de autenticação". Este pacote inclui a informação que identifica o PortMaster específico que envia o pedido de autenticação, a porta que está sendo usada para a conexão de modem, identificação do usuário e a senha. Para proteger os dados de hackers que possam estar escutando a conexão, o PortMaster age como um cliente RADIUS e codifica a senha antes que seja enviada em sua jornada ao servidor RADIUS.

2. Quando um pedido de autenticação é recebido, o servidor de autenticação valida o pedido e então decifra o pacote de dados para ter acesso a identificação do usuário e senha. Esta informação é passada para o sistema de segurança apropriado.

3. Se o usuário e senha estiverem corretos, o servidor envia um reconhecimento de autenticação que inclui informação sobre o usuário e as exigências dos serviços. Por exemplo, o servidor RADIUS contará para o

PortMaster que um usuário precisa do Protocolo PPP (ponto-a-ponto) para se conectar à rede. O reconhecimento pode também, conter filtros, com informações sobre os limites de acesso do usuário para os recursos específicos na rede. Se o usuário e a senha não estiverem corretos, o servidor RADIUS envia um sinal ao PortMaster e o usuário terá o acesso negado à rede.

4. Uma vez que a informação é recebida pelo PortMaster, o servidor RADIUS envia uma chave de autenticação, ou assinatura, se identificando para o cliente RADIUS e permitindo então, a configuração necessária para que os serviços de envios e recepções personalizados, funcione para o usuário autenticado.

A figura 6.6 demonstra um servidor Radius interligado a uma rede wireless,ilustrando assim todo o processo que foi descrito acima.

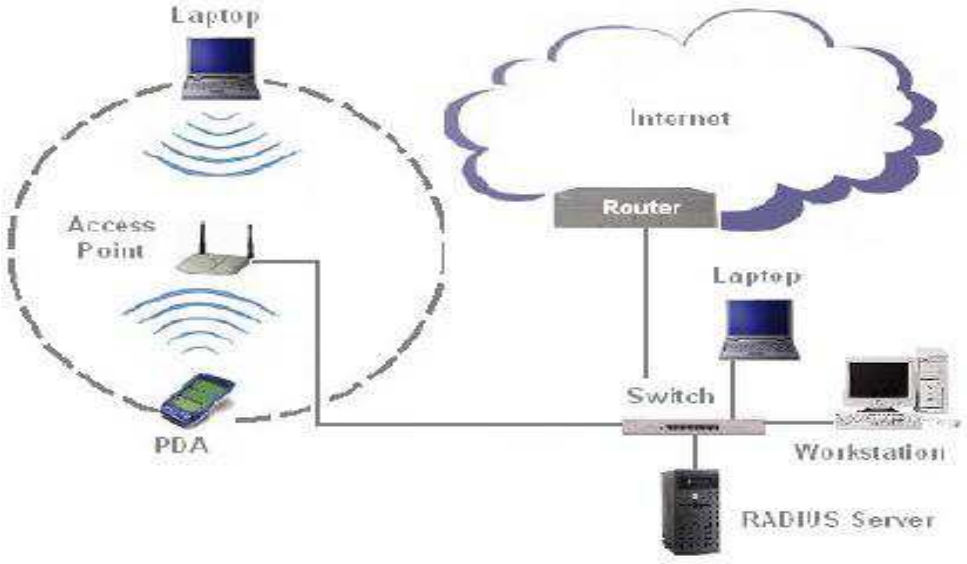


Figura 6.6 mostra um exemplo rede no padrão 80211b com autenticação RADIUS. [MODULO,2003]

6.3.2 IMPLEMENTAÇÃO CISCO

Vamos mostrar como a Cisco resolveu o problema que seus produtos teriam com segurança se oferecessem somente o WEP,e com este padrão a solução CISCO atende perfeitamente as expectativas esperadas de segurança para rede wireless DA Empresa Ferteco Mineração S/A.

6.3.2.1 Autenticação Mútua

"Os produtos Cisco para redes sem fio, conhecidos como Cisco Aironet Wireless oferecem um serviço de autenticação mútua. Isso consiste no ato da autenticação do cliente no ponto de acesso e o ponto de acesso no cliente. A Cisco criou o protocolo de autenticação EAP(este protocolo foi explicado capitulo 4) para assegurar a autenticação mútua entre o cliente e o servidor RADIUS".[CISCO,2003]

6.3.2.2 Tratamento de chaves CISCO

- Derivação da chave secreta:Originalmente o WEP utiliza a chave secreta para encriptar e desencriptar, e também para a autenticação. Os produtos Cisco não utilizam a chave secreta para autenticar, ao invés disso, eles utilizam uma chave derivada para essa mútua autenticação.

- Chaves do WEP escolhidas dinamicamente:Como falamos anteriormente a chave do WEP costuma ser fixa, seja porque não é política da empresa trocar essas chaves, ou seja, porque o usuário é remoto e não tem conhecimento para trocar essa senha, sem auxílio do administrador. A Cisco oferece em seus produtos um sistema para troca das chaves a cada novo usuário e a cada nova conexão. Se o mesmo usuário tentar fazer uma nova conexão este receberá uma nova chave secreta. Assim, a Cisco impede ou dificulta que o invasor fique escutando strings aleatórias geradas pela mesma chave por muito tempo.

6.3.2.3 Política de reautenticação

"A política de reautenticação é forçar o usuário depois de um certo tempo, uma nova autenticação, e a nova autenticação determinará uma nova chave secreta, assim, mesmo que não se t roque usuário e nem se troque uma sessão (como num processo de FTP), o cliente será obrigado a encriptar e desencriptar com outra chave secreta".[CISCO,2003]

6.3.2.4 Alteração do Vetor de Inicialização

Como todas as implementações, os produtos da Cisco também incrementam o Vetor de Inicialização a cada pacote enviado. A diferença é que o vetor de inicialização começará a cada sessão a contagem a partir de um número escolhido aleatoriamente e não do zero como é em outras implementações.

7 CONCLUSÃO

As redes wireless ainda enfrentam problemas graves de segurança, mas é evidente que o seu uso seja cada vez mais disseminado e que caminhamos para a utilização cada vez maior deste tipo de dispositivo.

Apesar de parecer um desafio prover segurança para equipamentos sem fio,profissionais de Segurança da Informação podem reutilizar muitas das medidas usadas nas redes com fios, assim como foi na época do laptop com modem para acesso discado à empresa.Não devem ser usadas as configurações default nos equipamentos wireless. Será como um convite para hackers entrarem na rede. Deve- se considerar o uso de mecanismos de alta segurança como controle de acesso, criptografia ponto- a- ponto, EAP e RADIUS , especialmente em ambientes corporativos. WEP por si só não deve ser considerado como uma solução de segurança.

A política de segurança deve definir com clareza as restrições sobre a comunicação em WLANs (quais equipamentos são permitidos, que tipo de dados podem ser transferidos na rede e se é obrigatório o uso de métodos de criptografia e autenticação, etc), bem como o uso indevido de Access Point’s.

Em conjunto com as medidas de segurança citadas neste trabalho, outras devem ser consideradas para garantir a segurança da rede sem fio, embora durante o estudo deste documento chegou se a conclusão que o padrão 802.11b, que é o mais utilizado pelo mercado brasileiro deve ser urgentemente substituído, pois mesmo em conjunto com dispositivos de segurança Wireless ainda apresenta falhas graves.

Para estudos futuros estamos propondo a implementação de uma arquitetura WStrike para rede Wireless da Empresa Ferteco Mineração S/A, arquitetura WStrike propõe a integração de Acess Point, Firewall, Servidor Web e Gateway VPN na mesma rede. O WStrike possui as funcionalidades de ponto de acesso de uma rede sem fio 802.11b, possui um firewall para controle de acesso das estações clientes, um servidor web capaz de servir páginas através das quais os clientes da rede sem fio devem se autenticar e um gateway VPN capaz de autenticar e criptografar todas as transações eletrônicas entre as estações e o AP.

REFERÊNCIAS BIBLIOGRÁFICAS

TANENBAUM, Andrew S. **Redes de Computadores.** Tradução da 3º edição.*Rio de Janeiro*, RJ: CAMPUS, 1997.

DAHAB, Ricardo. **Segurança em Redes Sem Fio**, 2003. Monografia - Curso de especialização em Redes de Computadores, UNICAMP, São Paulo.

MCCLURE, Stuart;**SCAMBRAY**,Joel. **Hackers Expostos:Segredos e Soluções para a Segurança de Redes.** Tradução **ANTUNES**, Álvaro.*São Paulo*, **SP**: MAKRON BOOKS, 2000

TERADA,Roto**.Segurança de dados:Criptografia de Redes de Computadores.**.*São Paulo*, SP: EDGARD, 2000.

YEMINI, Yechiam**.The NetWork Book.** Tradução 1º edição.*São Paulo*, SP: NOVA ERA, 1995.

SPYMAM, Hacking**. Guia de Consulta e Aprendizagem.**.*São Paulo*, SP: BOOK EXPRESS, 2001.

ELLISON, C. **Exploiting and Protecting 802.11b Wireless Networks**.In: ExtremeTech.sep.4,2001.2001

RIVEST, R. RSA Security Response to Weaknesses in Key Scheduling Algorithm. <http://www.rsasecurity.com>, acessado em: 07 out 2003.

TRINTA, Fernando Antonio Mota. **Um Estudo sobre Criptografia e Assinatura Digital** . Artigo apresentado para Departamento de Informática , UFP, set 1998.

PEIXOTO, Roney de Castro. Tecnologias Wireless demandam cuidados extras. <**http://www.csalaw.com.br/pdf/Art_dig11.pdf**>, acessado em: 18 out 2003.

MICROSOFT. **RADIUS**. <http:// www.technetbrasil.com.br/> Acesso em: 08 out. 2003.

FERNANDES, José. **Métodos de Acesso em Redes Wireless**. <http://www.gta.ufrj.br/seminarios/semin2003_1/fernandes/MAC_1.htm> Acesso em: 20 out. 2003.

WECA.**WLAN'S**. <http:// www.weca.net> Acesso em: 20 out. 2003.

WIRELESS, Wireless.**Redes Wireless Padrões e Adaptações**. <http://www.wireless.com.pt> acessado em: 03 nov 2003.

JESSEN,E. **Cartilha de Segurança** <http://www.nbso.nic.br/docs/cartilha/cartilha-05-wireless.html> acessado em 21 out 2003.

MODULO, Modulo Segurança. **Protegendo Redes wireless**. <http:// www.modulo.com.br> Acesso em: 20 out. 2003.

CISCO, Cisco. **Implementações Cisco Wireless**. <http:// www.cisco.com.br> Acesso em: 22 out. 2003.

WALKER,Jessé.**802.11 Security Series:The Temporal Key Integrity Protocol(WEP),** Universidade of Texas, <http://cedar.intel.com/media/pdf/security/80211_part3.pdf>, acessado em: 10 nov 2002.

ORINOCO, Lucent Technologies. **Orinoco Manager Suite: User's Guide**,<http://www.lucent.com>acessado em: 20 out 2003.

ANEXO A – O PADRÃO IEEE 802.11

IEEE 802.11I

"O padrão IEEE 802.11i será o substituto do protocolo WEP. O novo padrão está em discussão no Task Group i (TGi) e tem previsão de ser finalizado no final deste ano. Seu objetivo é resolver os diversos problemas encontrados no protocolo WEP, ligados a garantia da confidencialidade e integridade da comunicação, como apresentados anteriormente". [FERNANDES,2003].

Desde quando o grupo de trabalho do 802.11i iniciou o seu estudo alguns fabricantes tem implementado algumas pré normas no mercado para prevenir alguns tipos de vulnerabilidade, como:

- **Ataque de dicionário ao EAP:** O frame 802.11 é facilmente capturado, possibilitando que um intruso descubra uma senha usando o mecanismo de força bruta baseado em dicionário. É recomendado que seja utilizado

métodos de autenticação como, EAP (Extensible Authentication Protocol) TLS, SRP TTLS and PEAP.

- **Ataque a chave default:** Como 802.11 não implementa um mecanismo de troca de chaves aleatório, como isso descobrir a chave é questão de tempo. É extremamente recomendado que se use algum mecanismo de troca dinâmica de chaves como SNMPv3 ou SSH.

- **Ataque de DOS baseado no frame EAPOL-Logoff:** Como esse tipo de frame não é autenticado, alguém pode enviar um frame EAPOL logoff e desconectar um usuário. Pode-se filtrar esse tipo de solicitação no ponto de acesso (AP).

- **Ataque de DOS baseado no frame EAPOL-Styart:** O atacante pode fazer um envio maciço de frames EAPOL start para sobrecarregar o ponto de acesso (AP) e tira-lo de serviço. Isso pode ser evitado fazendo com que o AP não gaste muito recurso com o atendimento desse tipo de frame.

- **Ataque de DOS baseado no espaço de identificação do EAP:** O atacante pode consumir o espaço de identificação do EAP, que vai de 0 a 255, e tirar o ponto de acesso for a de serviço.

- **Ataque de DOS baseado no envio antecipado do pacote de sucesso do EAP:** O atacante pode enviar um pacote de sucesso do EAP antecipado para permitir que uma estação possa vista na rede antes que o ponto de acesso complete o processo de autenticação.

- **Ataque de DOS baseado no pacote de falha do EAP:** O atacante pode enviar um pacote de falha do EAP antecipado para não permitir que uma estação seja vista na rede antes que o ponto de acesso complete o processo de autenticação.

- **Ataque de DOS baseado na alteração do pacote EAP:** O atacante pode modificar o conteúdo do pacote EAP. Para evitar esse tipo de ataque deve-se utilizar protocolos de criptografia como TLS, PEAP ou TTLS.

Basicamente, o 802.11i oferece dois esquemas de criptografia, que eliminam os problemas encontrados no WEP. O TKIP e o CCMP podem ser utilizados simultaneamente na mesma rede, permitindo que exista uma negociação entre o cliente o AP para definirem qual protocolo criptográfico será utilizado.

TKIP

O TKIP (Temporal Key Integrity Protocol), também chamado de WEP2, foi projetado para resolver os problemas apresentados pelo WEP, ao mesmo tempo que mantém a compatibilidade com a base instalada. O TKIP pemite eliminar os problemas de confidencialidade e integridade apresentados pelo WEP.

A integridade no TKIP é garantida atravé do MIC (Message Integrity Code), que tem a função de evitar ataques do tipo bit-flipping aplicados no WEP. O MIC é um campo do frame 802.11i (Fig, 14), calculado a partir de diversas informações contidas no próprio frame (Fig. 13), como, por exemplo, os endereços MAC de origem (SA) e destino (DA). O MIC é calculado a partir de uma função de hashing, conhecida como Michael.

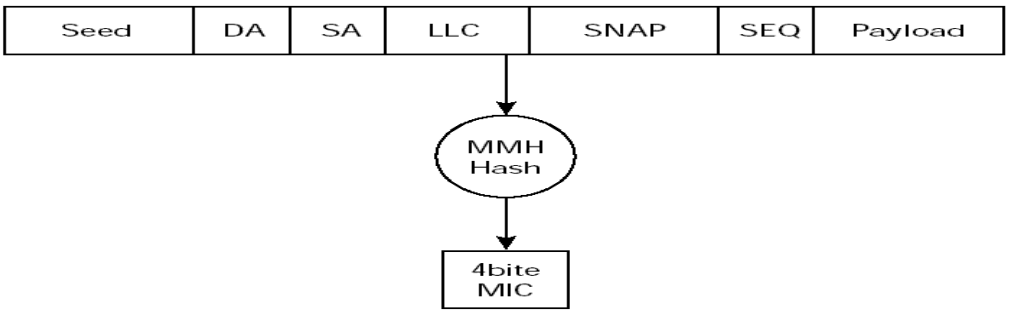


Figura Anexo 1 Cálculo do MIC[FERNANDES,2003]

Além do campo MIC, o TKIP implementa um campo de seqüência (SEQ) no frame 802.11i (Fig. 14), para evitar ataques do tipo replay. O número de seqüência é

incrementado a cada frame enviado, sendo que o AP irá descartar frames que estejam fora de ordem enviados por um mesmo cliente.

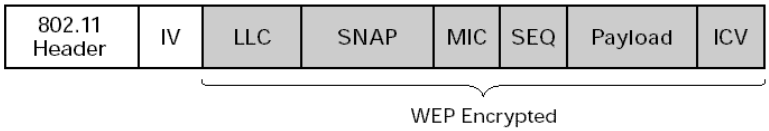


Figura Anexo 2 Frame 802.11i [FERNANDES,2003]

O TKIP utiliza um vetor de inicialização (IV) de 48 bits, ao contrário dos 24 bits utilizados no WEP. Com 48 bits é possível enviar 2^{48} frames sem que o IV se repita, o que permiti ampliar o tempo de vida da chave temporal, tornando desnecessária a geração de uma nova chave.

AES-CCMP

O protocolo CCMP (CCM Protocol) utiliza o novo padrão para criptografia simétrica AES (Advanced Encryption Standard), aprovado pelo NIST (National Institute of Standardsand Technology) em 2002. O AES trabalha com blocos de 128 bits e, no caso do 802.11i, chaves de 128 bits.

O AES trabalha com diferentes modos de operação, que alteram a forma como o processo de criptografia é realizado. Os modos de operação têm o objetivo de previnir que uma mesma mensagem quando criptografada gere o mesmo texto cifrado. O CCM utiliza o modo de operação conhecido como CBC (Cipher Block Chaining). Neste modo de operação, o texto cifrado no passo anterior é utilizado como entrada no processo de criptografia subsequente. No primeiro passo, como ainda não existe um texto cifrado, é utilizado o vetor de inicialização, figura abaixo.

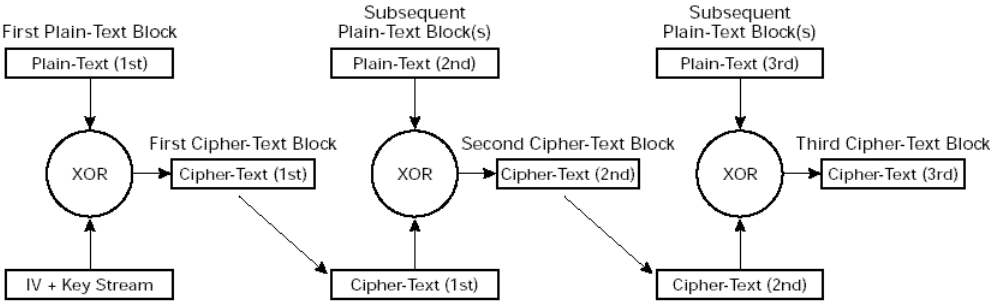


Figura Anexo 3 Cipher Block Chaining (CBC) [FERNANDES,2003]

O CCM é, na verdade, uma combinação de dois modos de operação: o CBC-CTR (Cipher Block Chaining Counter mode) e CBC-MAC (Cipher Block Chaining Message Authenticity Check), sendo que o CBC-CTR oferece criptografia, enquanto o CBC-MAC oferece integridade.

A Figura abaixo apresenta os mecanismos de criptografia e integridade, implementados AES-CCMP. O mecanismo de criptografia utiliza o vetor de inicialização (IV), sendo que o IV é incrementado a cada bloco criptografado, gerando uma chave única para cada bloco. A integridade é implementada através do MIC, gerado a partir do IV e informações contidas no header do frame.

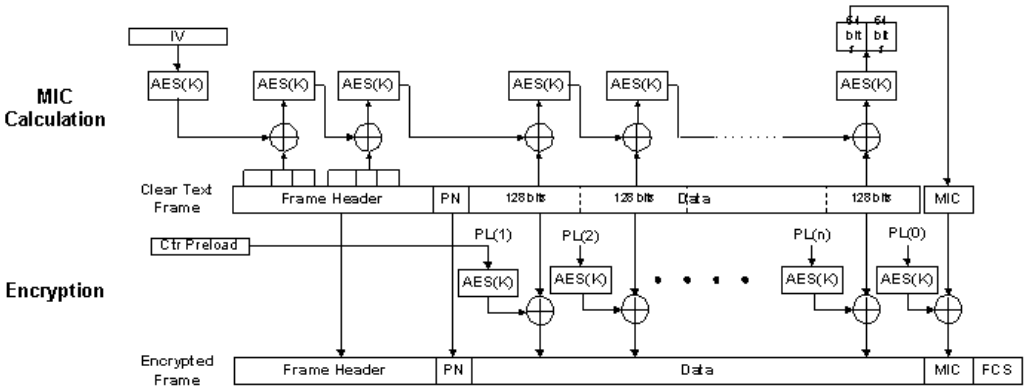


Figura Anexo 4 Criptografia e integridade no AES-CCMP[FERNANDES,2003]

IEEE 802.1X

O padrão IEEE 802.1X foi concebido para oferecer autenticação, controle de acesso e distribuição de chaves criptográficas em redes locais com e sem fio. É importante destacar que o 802.1X não está ligado apenas ao padrão IEEE 802.11, mas a todos os padrões de redes locais e metropolitanas patrocinados pelo IEEE 802. Além disso, o padrão pode ser utilizado em conjunto com diversos protocolos de autenticação localizados nas camadas superiores (Fig.). O grupo de trabalho 802.11i definiu que o mecanismo de autenticação a ser utilizado no IEEE 802.11 deverá seguir o modelo do IEEE 802.1X.

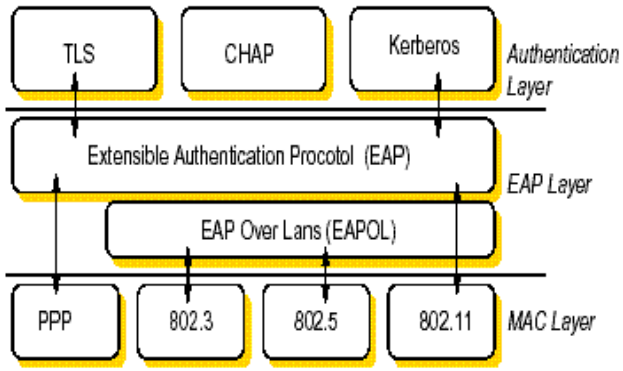


Figura Anexo 5 Pilha de protocolos 802.1X[FERNANDES,2003]

A autenticação no IEEE 802.1X é realizada nos dois sentidos (mutual autentication) e utiliza o esquema de challenge-response. Existem três componentes a serem considerados no padrão: autenticador, supplicant e servidor de autenticação (Fig.). Em uma rede sem fio, o autenticador é geralmente o AP (Access Point) e o supplicant uma estação que deseja conectar-se ao AP. O servidor de autenticação é o verdadeiro responsável por autenticar o supplicant, com base nas informações oferecidas por ele. O padrão não especifica qual servidor de autenticação deve ser utilizado, podendo ser, por exemplo, um servidor RADIUS (Remote Authentication Dial-In User Service). Na verdade, o servidor de autenticação não precisa ser necessariamente um elemento externo, podendo fazer parte do próprio AP.

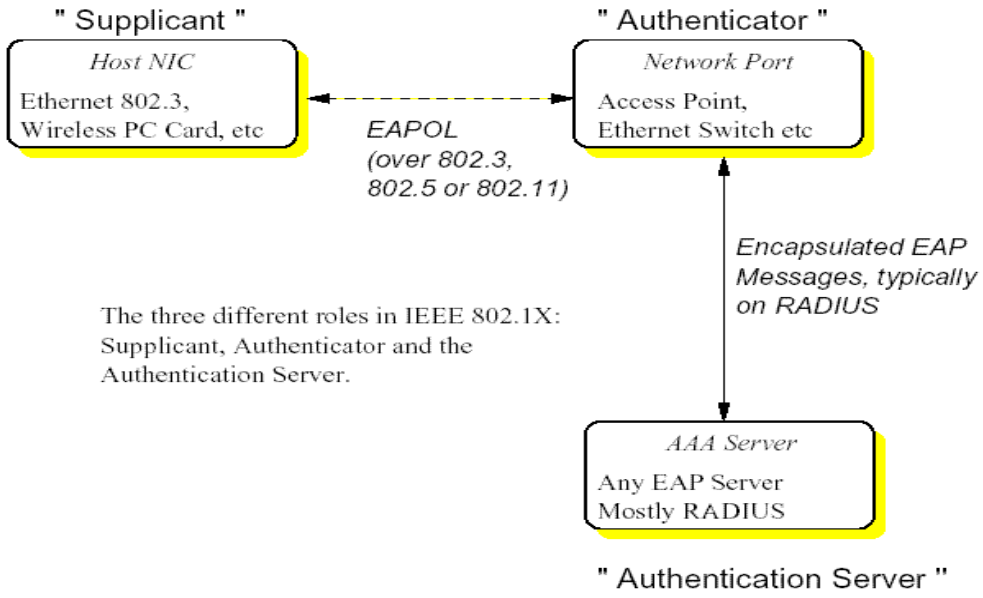


Figura Anexo 6 Componentes do 802.1X[FERNANDES,2003]

O IEEE 802.1X implementa o protocolo EAP (Extensible Authentication Protocol), em conjunto com o EAP over LAN (EAPOL). O EAP permite o encapsulamento de diversos protocolos de autenticação oferecidos nas camadas superiores e, consequentemente, não definidos pelo 802.1X (Fig.). Estes protocolos oferecem diferentes métodos de autenticação, como Kerberos, senhas, certificados digitais e chaves públicas. Desta forma é possível que o usuário também seja autenticado e não apenas a estação.

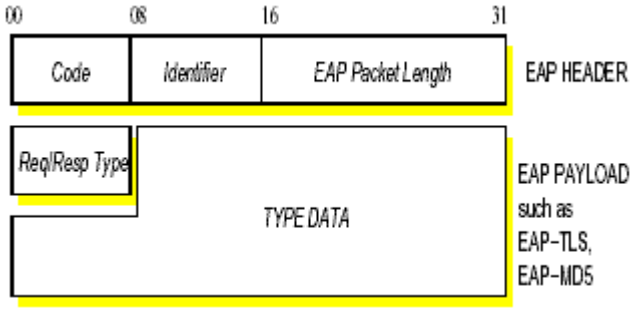


Figura Anexo 7 Estrutura do EAP[FERNANDES,2003]

O IEEE 802.1X, apesar de ser uma iniciativa de oferecer autenticação forte, apresenta algumas vulnerabilidades em função de alguns protocolos que fazem parte do padrão. Em são apresentados ataques do tipo man-in-the middle.