Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Carlos Eduardo Malafaia Silva

Segurança em redes Wi-Fi Corporativas: Estudo de caso na Marinha do Brasil.

Rio de janeiro

2010

Carlos Eduardo Malafaia Silva

Segurança em redes Wi-Fi Corporativas: Estudo de caso na Marinha do Brasil.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientadora:

Prof. Mônica Ferrreira da Silva, D.Sc., UFRJ, Brasil.

Rio de Janeiro

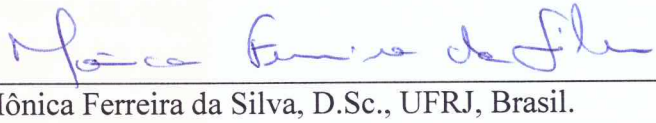
2010

Carlos Eduardo Malafaia Silva

Segurança em redes Wi-Fi Corporativas: Estudo de caso na Marinha do Brasil.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em setembro de 2010.



Prof. Mônica Ferreira da Silva, D.Sc., UFRJ, Brasil.

RESUMO

SILVA, Carlos Eduardo Malafaia, **Segurança em redes Wi-Fi Corporativas: Estudo de caso na Marinha do Brasil.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

O principal objetivo deste trabalho é o estudo de caso de como foram resolvidos os problemas de vulnerabilidade de redes Wi-Fi na Marinha do Brasil. Serão abordados os requisitos de segurança, uma análise das principais soluções disponíveis no mercado e a solução encontrada pela Marinha do Brasil para evitar os ataques as suas redes sem fio.

O Método de pesquisa utilizado foi o de Estudo de Caso, visto que este estudo buscou se aprofundar em um caso recente. A Marinha do Brasil foi escolhida já que somente neste semestre começou a implementar infraestruturas sem fio em algumas de suas sedes.

Esta pesquisa aborda o caso do Centro de Reparos e Suprimentos Especiais do Corpo de Fuzileiros Navais, que recentemente implementou uma solução sem fio para a administração de seus estoques de sobressalentes. Este trabalho descreve a solução de segurança implementada e analisa as vantagens e os possíveis óbices encontrados.

ABSTRACT

SILVA, Carlos Eduardo Malafaia, **Segurança em redes Wi-Fi Corporativas: Estudo de caso na Marinha do Brasil.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

The main purpose of this work is to study how the Wi-Fi vulnerability problems were solved by the Brazilian Navy. The security requirements, the available security solutions assessment and the Brazilian Navy solution for their Wi-Fi security problem will be highlighted.

The research method used was the Case Study, as this research is based on a recent case. The Brazilian Navy was chosen because they nearly started to implement Wi-Fi infrastructures in some of their bases.

This research is about the Brazilian Marines Special Supplies and Repairs Center case, which has nearly implemented a Wireless solution for the management of its supplies. This work will describe the security solution they have implemented and will analyze the advantages and the possible disadvantages of it.

LISTA DE FIGURAS

Página

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Objetivos

Este estudo tem por finalidade analisar as soluções de segurança para redes sem fio corporativas encontradas no mercado e analisar a solução encontrada pela Marinha do Brasil para evitar os ataques as suas redes sem fio.

Esta pesquisa visa responder a seguinte pergunta: quais as características da solução de segurança implantada na Marinha do Brasil e as razões de sua escolha?

1.2 Relevância

Os avanços da comunicação nos últimos anos possibilitaram o surgimento de várias tecnologias que, desde então, procuram atender a real necessidade de seus usuários, com a melhor qualidade possível. No início eram máquinas mono-usuário, e muito se teve que evoluir até chegar as redes de computadores atuais. Hoje em dia, o mercado está apostando numa das mais novas e revolucionárias tendências tecnológicas: A comunicação por redes sem fio (wireless networks).

A vida do ser humano pós-moderno é agitada, exige mobilidade, agilidade e liberdade. Esses seres humanos também precisam, cada vez mais, se comunicar onde quer que estejam. Então, os dispositivos de comunicação móvel tornam-se cada vez mais comuns. Os telefones celulares, PDAs, Notebooks, entre outros, são dispositivos acessórios que a cada dia são mais comuns. O custo vem caindo a cada ano e alguns modelos de PDA são objetos de promoção de vendas de assinatura de jornais e revistas, distribuídos em grande quantidade para o público em geral. Já as empresas prestadoras de serviço, que comercializam serviços específicos para dispositivos móveis começaram a surgir só no início do ano passado, e ainda são modestas e prestam serviços básicos, mas só enquanto a demanda por mais serviços não aumentar. Idéias para novos serviços há muitas.

A tendência mundial é a de criarmos cada vez mais redes mistas, com trechos mais distantes ou de difícil acesso utilizando-se redes sem fio e as redes locais utilizando-se as redes cabeadas. Salvo casos atípicos, onde, por exemplo, uma rede local é instalada em um prédio ou lugar de valor histórico, que, por isso, não se pode passar cabos pelas paredes (já fragilizadas com ação do tempo). Também se vem falando muito na criação das redes pessoais (PAN), que seriam as redes formadas pelos aparelhos pessoais, como o telefone celular ou o PDA. Essas redes, por serem formadas por aparelhos tão móveis quanto os seus usuários, só fazem sentido se usarem tecnologia sem fio. Entretanto, o diâmetro máximo da rede como essa não ultrapassa os 9 ou 10 metros, devido a limitações tecnológicas. De outro lado, segurança sempre foi uma preocupação constante do homem. Uma boa definição de segurança temos a seguir :

> *"Segurança são procedimentos para minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos, onde vulnerabilidade é qualquer fraqueza que pode ser explorada para violar um sistema ou as informações que ele contém".* (Soares,1995).

Antes de tratar da infra-estrutura de tecnologias que compreendem uma rede corporativa, é necessário que se avalie, detalhadamente, a amplitude daquilo que se pretende proteger. O primeiro passo consiste em realizar um levantamento e a classificação dos ativos da empresa. É preciso avaliar o grau de risco e de vulnerabilidade destes ativos, testar suas falhas e definir o que pode ser feito para aperfeiçoar sua segurança.

O segundo passo diz respeito a uma política de segurança que basicamente estabelece a elaboração de normas e procedimentos dentro da organização. Este trabalho normalmente é monitorado por um grupo especialmente criado para esse fim. A infra-estrutura de tecnologias é a terceira fase deste planejamento, envolvendo desde aquisição de ferramentas, até configuração e instalação de soluções, criação de projetos específicos e recomendações de uso.

Ao delimitar estes processos, o profissional de tecnologia de redes deve partir para a fase de gerenciamento, passando pela análise de infra-estrutura da empresa, auditoria de processos, testes regulares de ataques a vulnerabilidades, revisões e acompanhamento de políticas e tratamento de incidentes.

O tráfego de informações através de redes sem fio ainda é objeto de estudo de quanto às soluções de segurança da informação. A facilidade de se trafegar dados dispensando a necessidade de conexão a qualquer tipo de rede de cabos tem atraído cada vez mais usuários em todas as partes do mundo. Entretanto, o fato é que, em termos práticos, este meio de comunicação ainda não está totalmente protegido de invasões e fraudes, realidade que está diretamente relacionada ao desenvolvimento dos padrões de comunicação dessas redes.

2 REFERENCIAL TEÓRICO

2.1 Conceitos básicos

Segundo Pinheiro (2005), um Programa de Segurança bem estruturado deve prever o combate a ameaças que possam afetar os sistemas de informação da empresa. Entre elas podemos citar as ameaças do ambiente (fogo, enchente, etc.), erros humanos, fraudes, indisponibilidade, falhas em sistemas ou nos diversos ambientes computacionais, etc. Para cumprir esses objetivos, um Programa de Segurança da Informação deve seguir quatro paradigmas básicos:

Integridade: garante que as informações ou os recursos da informação estão protegidos contra modificações não autorizadas;

Confidencialidade: informações não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono;

Disponibilidade: possibilidade de acesso por aqueles que necessitam das informações para o desempenho de suas atividades;

Legalidade: estado legal da informação, ou seja, em conformidade com os preceitos da legislação em vigor.

Classificando as informações

Um aspecto importante que deve ser considerado na elaboração de um Programa de Segurança é a classificação das informações. É preciso que a informação seja claramente classificada para que seja possível controlar o acesso aos dados, evitando, dessa forma, que pessoas não autorizadas tenham acesso a ela. Para tanto, é preciso classificar todas as informações segundo grau de importância e teor crítico.

Informações Confidenciais: são aquelas que devem ser disseminadas somente para indivíduos previamente definidos;

Informações Corporativas: devem ser disseminadas somente dentro da empresa;

Informações Públicas: podem ser divulgadas dentro e fora da empresa.

Aplicações

Algumas aplicações já fazem parte da rotina das empresas. Dentre elas destacam-se:

Antivírus: faz a varredura de arquivos maliciosos disseminados pela Internet ou correio eletrônico. Basicamente, sua função está atrelada à ponta do processo, isto é, ao usuário que envia e recebe dados. Uma das últimas tendências deste tipo de ameaça são os chamados "vírus polimórficos", que possuem a capacidade de mudar constantemente para driblar a vítima e dificultar sua remoção;

Balanceamento de carga: as ferramentas de balanceamento estão relacionadas à capacidade de operar de cada servidor da empresa. Elas permitem que, em horários de grande utilização da rede, se determine a hierarquia do que trafega, bem como o equilíbrio da carga disseminada entre os servidores;

Firewall: cumprem a função de controlar os acessos. São soluções que, uma vez estabelecidas suas regras, passam a gerenciar tudo o que deve entrar e sair da rede corporativa. Muitas vezes, recomenda-se a adoção do firewall para separar a intranet da companhia de seus clientes externos ou de servidores e serviços públicos. Basicamente, o firewall é um software, mas também pode incorporar um hardware especializado;

Autenticações: cartões, senhas numéricas e randômicas, recursos de identificação como biometria, RFID, etc. Trata-se do recurso utilizado para validar um acesso, identificando de acordo com normas estipuladas pela empresa;

Detector de Intrusão (IDS): estas ferramentas têm a função de monitorar o tráfego contínuo da rede, identificando ataques que estejam em execução. Como complemento do firewall, o IDS (Intrusion Detection System) se baseia em dados dinâmicos para realizar sua varredura, como por exemplo, pacotes de dados com comportamento suspeito, códigos de ataque e outros;

Varredura de vulnerabilidades: produtos que permitem realizar verificações regulares em determinados componentes de rede como servidores e roteadores. O objetivo destas ferramentas é encontrar brechas de sistemas ou configurações;

Rede Privada Virtual (VPN): uma das alternativas mais adotadas pelas empresas na atualidade, as VPN's são canais que utilizam túneis para trafegar dados criptografados entre divisões de uma mesma companhia, parceiros de negócios etc;

Criptografia: é utilizada para garantir a confidencialidade das informações. Trata-se de uma codificação que usa um processo de decifração para restaurar os dados ao seu formato original. As chaves criptográficas podem ser simétricas (privada) ou assimétricas (pública);

Autenticação: são processos de identificação para disponibilizar acesso. A autenticação e conseqüente autorização de manipulação dos dados se baseiam em algo que o indivíduo sabe (uma senha, por exemplo), algo que ele tem (dispositivos como tokens, cartões inteligentes, etc) e o que ele é (leitura de íris, linhas das mãos, etc);

Integradores: permite centralizar o gerenciamento de diferentes tecnologias que protegem as operações da rede. Mais que uma solução, trata-se de um conceito.

Elaborar um Programa de Segurança é uma tarefa complexa. Seus custos são aparentemente elevados, ele precisa ser constantemente monitorado, revisado e atualizado e seus resultados só poderão ser notados a médio e longo prazo.

Pela complexidade de cada uma das etapas que compreende um projeto de segurança, recomenda-se que a empresa desenvolva a implementação baseada em projetos independentes. Análise de logs das ferramentas, backup de base de dados, auditoria, manutenção e atualização constante das ferramentas são os passos seguintes. Uma vez que se tenha completado este ciclo, entende-se que a rede estará pronta para ser gerenciada adequadamente e colocada em funcionamento com um grau maior de segurança.

Objetivos do intruso

Tabela 2.1 – Exemplos dos objetivos de alguns intrusos. (Tanenbaum,1997).

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

Ataques

Segundo Veríssimo (2002), o intruso pode ter quatro comportamentos diferentes em relação às posições da origem e do destino da mensagem. Na figura 2.1 veremos esses comportamentos:

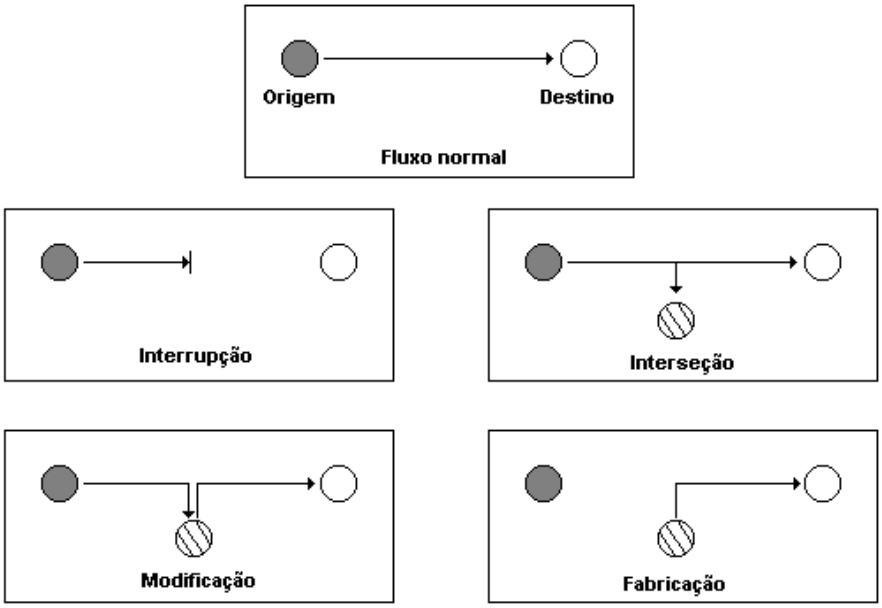


Figura 2.1 – Posição do atacante em relação à origem e ao destino

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.

Adiante vamos falar sobre como são os ataques e os tipos de ataque.

O elo mais fraco

O elo mais fraco de um sistema de segurança é o ser humano. Não tem como se controlar o comportamento de um ser humano. Na frente falaremos sobre a engenharia social, uma técnica ut ilizada pelo hacker para descobrir as informações necessárias a um ataque.

É comum ouvirmos os especialistas dizerem que o único sistema 100% seguro é aquele que fica o tempo todo desligado. Ora, como um intruso pode invadir um computador

desligado? Simples, ele pode pedir para alguém ligar o sistema. Pedir a alguém alguma coisa é uma das ferramentas da Engenharia Social.

Engenharia Social

O termo engenharia social foi dado ao grupo de procedimentos que se toma para convencer alguém a tomar atitudes que você não pode, ou não quer tomar. A engenharia social é considerada um tipo de ataque a uma rede. Todos esses ataques utilizam pessoas com 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, e que querem mostrar serviço. 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.

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 999.999.999.0. Ao registrar essa informação, o administ rador 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 faturará o serviço e, automaticamente, removerá o registro. Logo, salvo os registros falsos, todos os administradores cadastram seus verdadeiros dados. Existirá uma possibilidade de, se você telefonar para o administrador, não o encontrar,

e em seu lugar, encontrar o seu estagiário. Aí, o intruso pode usar de toda a sua malícia contra o estagiário, que na maioria das vezes, é uma pessoa jovem, sem experiência, e doido para mostrar serviço ao chefe. O intruso liga identificando-se como algum controlador de tráfego do backbone ou de algum órgão do governo, lamenta-se por não encontrar o administrador, e duvida da capacidade do estagiário de lhe dar informações tão específicas, ou seja, desafia o estagiário a mostrar a sua capacidade de dar as informações. Na sua ingenuidade, o estagiário dará todas as informações que ele puder para provar que é capaz, acreditando, assim, ter feito um bom trabalho. Terminará o telefonema feliz, por ter conseguido prestar um bom serviço ao chefe, e deixará o intruso ainda mais contente.

Ex-funcionários

Uma atenção especial deve ser dada à ex-funcionários que saíram contrariados da empresa. Não há como remover os conhecimentos específicos da empresa que foram dados ao ex-funcionário, durante o tempo que ele serviu a essa empresa. Em julho de 2001, o portal de segurança da COPPE/UFRJ, o Lockabit, publicou um artigo sobre esse assunto, onde fala-se sobre a atenção especial que deve ser dado às informações que são dadas aos funcionários [Verissimo2001].

Footprint

Vão existir informações que o intruso não conseguirá coletar através de um telefonema ou um papo amigável com alguma secretária ou estagiário. Seja porque essas pessoas não detêm os conhecimentos necessários, seja porque ele não consegue ter acesso a essas pessoas ingênuas. Aí, então, surge a segunda técnica de intrusão, conhecida como footprint . Consiste em, através de softwares específicos, conseguir informações necessárias ao ataque. Footprint é um perfil completo da postura de segurança de uma organização que se pretende invadir. Usando uma combinação de ferramentas e técnicas, atacantes podem empregar um fator desconhecido e convertê-lo em um conjunto específico de nomes de domínio, blocos de rede e

endereços IP individuais de sistemas conectados diretamente à Internet. Embora haja diversas técnicas diferentes de footprint , seu objetivo primário é descobrir informações relacionadas a tecnologias de Internet, acesso remoto e extranet. A Tabela 2.2 mostra essas tecnologias e informações críticas que um atacante tentará identificar.

Tabela 2.2 – Tipos de informações procurados num footprint (McClure, 1999).

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).
	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 e grupos, faixa de sistemas, tabelas de roteamento, informações de SNMP).
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.

Personificação

Um dos problemas que o intruso encontra quando quer entrar sem permissão em um sistema é a falta de direitos de acesso, e a maneira mais fácil de resolver esse problema é se fazer passar por um outro elemento que tem direitos de acesso ao objeto que o intruso quer

invadir. Depois do footprint quase sempre o intruso consegue elementos que identifiquem as pessoas que têm acesso ao objeto alvo. Daí , basta configurar o computador dele com o login, nome, número IP que ele deseja personificar.

Replay

No replay o intruso intercepta um pacote que vem de um usuário autenticado e reenvia-o novamente mais tarde, visando confundir os sistemas, ou causando uma parada do sistema. O sistema que está recebendo os pacotes vai ingenuamente receber os pacotes reenviados pelo intruso, acreditando que ele fora enviado pelo dispositivo origem.

Recusa ou impedimento de serviço

Recusa ou impedimento de serviço, cujo nome em inglês é Deny of Service (DoS), é um ataque muito comum encontrado hoje. Esse ataque consiste no envio de muitos pacotes pelo intruso para um computador. Esse envio torna-se perigoso quando o número de pacotes é muito maior do que a quantidade que o computador atacado pode tratar. 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.

Armadilhas

Também conhecido como trapdoor ou backdoor. Ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando (emitido pelo intruso) ou a um evento predeterminado. Como exemplo, citamos a modificação de um processo para dispensar a verificação de senha na autenticação de um acesso, em resposta a uma combinação de teclas (Ctr l+Alt+U) ou a um evento do tipo “hora do sistema = 2:35:00” quando o acesso a qualquer usuário teria a necessidade de senha para autenticação dispensada.

Script Kiddies

Há um tipo de intruso que traz muito perigo. Perigo não por causa de seus conhecimentos avançados, mas por causa da sua aleatoriedade. Os usuários dos script kiddies quase todos são hackers iniciantes (algumas vezes, crianças, daí o nome), não tendo ainda conhecimento e experiência suficiente para fazer os seus próprios ataques, e por isso utilizam scripts feitos por outros hackers. O principal problema é que um hacker experiente escolhe as suas vítimas, normalmente são empresas grandes e importantes que estão mais expostos ao grande público, os scripts kiddies escolhem suas vítimas ao acaso.

2.2 Os requisitos de segurança para uma rede 802.11

Segundo Miyano (2004), os requisitos de segurança podem ser divididos em duas categorias:

Criptografia e Privacidade – O objetivo da criptografia no que se refere a redes sem fui é fornecer um mecanismo que permita que as informações não tenham sua privacidade atingida. Os dados cifrados não devem ser decifrados por pessoas não autorizadas. Todos os pacotes devem ser gerados pelas origens autenticas. Por fim, este mecanismo deve garantir sobre todas as circunstanciais a integridade das informações.

Autenticação e Controle de Acesso – Autenticação deve ser mutua, permitindo que os ativos autentiquem os Access Points e que estes autentiquem os ativos da mesma forma. Um framework deve ser desenvolvido com intuito de facilitar a troca de mensagens entre clientes, APs e servidores de autenticação. Do ponto de vista do APs, o mecanismo deve prover métodos para verificar as credenciais dos usuários com o objetivo de determinar o nível de acesso a rede em questão.

2.3 WEP – Wired Equivalency Privacy

WEP (Wired Equivalent Privacy - Privacidade equivalente à das redes com fios) é uma característica IEEE 802.11 opcional, utilizada para proporcionar segurança de dados

equivalente à de uma rede com fios sem técnicas de criptografia avançadas para privacidade. A WEP foi criada para permitir que os links de rede local sem fio sejam tão seguros quanto os links com fios. De acordo com o padrão 802.11, a criptografia de dados WEP é utilizada para impedir (i) acesso à rede por "intrusos" com equipamentos similares de rede local sem fio e (ii) captura do tráfego de redes sem fio por curiosos. A WEP permite ao administrador definir o conjunto das "chaves" respectivas de cada usuário da rede sem fio, de acordo com uma "seqüência de chaves" passada pelo algoritmo de criptografia WEP. É negado o acesso a quem não possui a chave necessária. Conforme especifica o padrão, a WEP usa o algoritmo RC4 com chave de 40 ou 104 bits, que somado ao vetor inicial de 24 bits temos chaves de 64 e 128 bits. Quando a WEP é ativada, cada estação (clientes e pontos de acesso) possui uma chave. A chave é utilizada para cifrar os dados antes de serem transmitidos pelas emissões de rádio. Quando uma estação recebe um pacote não criptografado com a chave adequada, o pacote é descartado e não é entregue ao host; isso impede o acesso à rede por curiosos e pessoas não autorizadas.

A transmissão de pacotes nas redes 802.11, com WEP ativado, ocorre da seguinte forma:

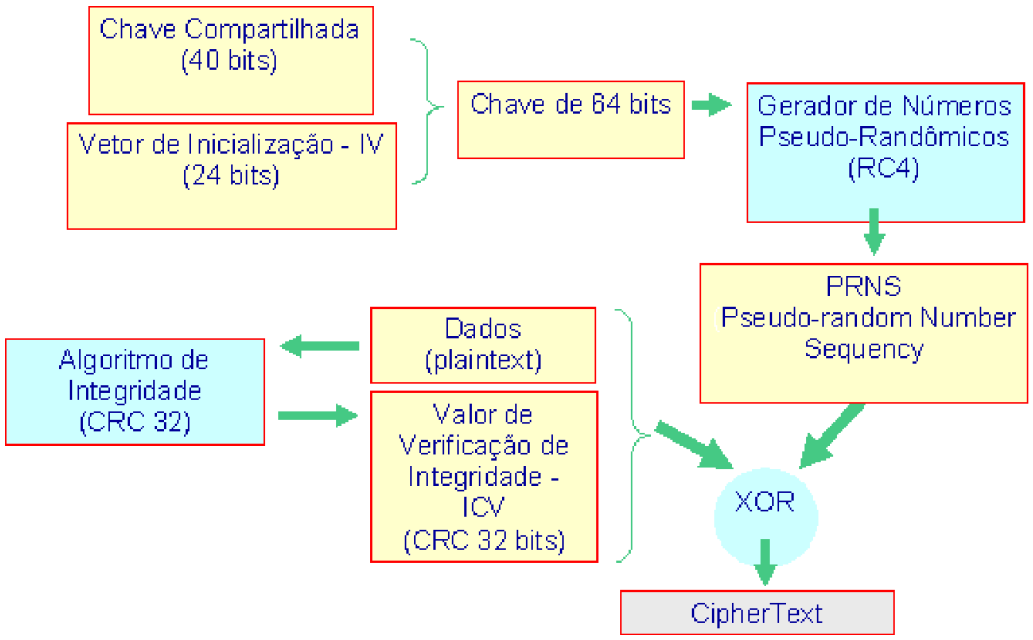


figura 2.2 – Transmissão do pacote usando WEP em rede 802.11

Como podemos observar a chave compartilhada, ajustada manualmente, pode ter 40 bits ou 104 bits (chave k), e a chave IV (vetor de inicialização) têm sempre 24 bits. As duas chaves são concatenadas para formar uma chave de 64 ou 128 bits. Esta chave concatenada de 64 ou 128 bits é inserida num algoritmo de criptografia RC4, que gera uma seqüência de números pseudo-randomica (PRNS), também chamada RC4(IV,k). Não existe especificação para a geração da chave IV, e normalmente, ela é gerada seqüencialmente sendo reinicializada toda vez que a placa de rede é conectada na estação de trabalho.

O texto a ser enviado passa por um "integrity check sum", no caso é computado o CRC-32, e então os dois são concatenados. Em seguida faz-se um XOR do texto+CRC-32 com o PRNS gerado pelo algoritmo e então se transmite o vetor de inicialização IV não criptografado e o texto+CRC-32 criptografado.

O receptor, por sua vez, concatena a chave IV transmitida com a chave compartilhada, e passa pelo algoritmo RC4 para gerar a mesma PRNS gerada para a transmissão. É feito então um XOR do texto+CRC-32 criptografado com o PRNS na transmissão. Então, para um texto transmitido C temos:

$$C = P \text{ o}(RC4(IV,k)$$

$$P' = C \text{ o}(RC4(v,k))$$

$$P' = (P \text{ o}(RC4(v,k)) \square\square RC4(v,k)$$

Como sabemos que (a oa = 0) e que (a o0 = a)

$$P' = P$$

O texto P original é então recuperado juntamente com o CRC-32, faz-se um novo calculo do CRC-32 para o texto recebido e então se compara este CRC-32 com o que foi recebido para verificar a integridade do texto. Caso o resultado obtido seja diferente, o pacote é desconsiderado. Caso contrário, o mesmo é passado ao host.

O processo acima descrito garante a integridade e a confidencialidade dos pacotes, mas ainda deve se garantir que apenas estações autorizadas tenham acesso aos pacotes. Há duas maneiras de autenticar um usuário no 802.11:

- Autenticação aberta – o protocolo autentica qualquer um que fizer a requisição de autenticação.
- Autenticação por chave compartilhada

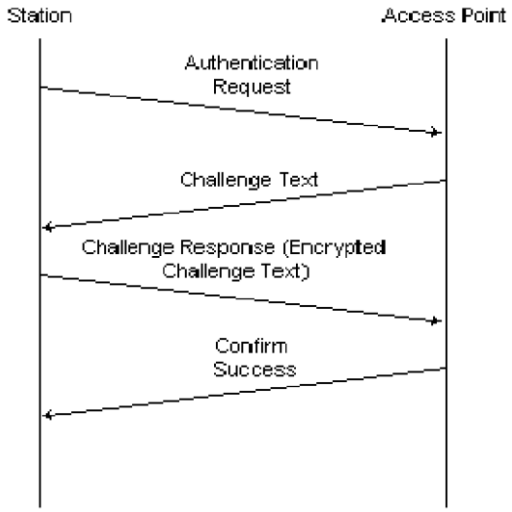


figura 2.3 – Processo de autenticação

O processo de autenticação (figura 2.3):

1. Desafio resposta rudimentar para saber se o usuário conhece a chave WEP. A estação envia um frame de autenticação para o Ponto de Acesso;

2. Quando o Ponto de Acesso recebe o frame de autenticação inicial, ele responde com um frame de autenticação contendo 128 bytes de texto randômico de desafio criptografados pelo WEP.

3. A estação deve então copiar o texto de desafio dentro de um frame de autenticação, encriptar com a chave compartilhada e um novo IV e devolver para o Ponto de Acesso.

4. O Ponto de Acesso vai decriptar o texto recebido com a chave compartilhada e comparar com o que foi enviado. Se estiver correto, ele responde com um frame indicande a autenticação teve sucesso. Senão, ele responde com uma autenticação negativa.

2.4 Problemas e Ataques ao WEP

O problema mais crítico do protocolo WEP é que sua idealização foi falha. A segurança não foi pensada fim-a-fim, visando apenas impedir ataques ao trecho wireless da transmissão. O fato de não usar algoritmos criptográficos complexos apenas impede que curiosos tenham acesso ao conteúdo trafegado, o que não ocorrerá quando o hacker desejar capturar informações desta rede. Uma simples análise do protocolo nos trás diversas falhas:

Algoritmos criptográficos simples permitem o ataque de freqüência para se obter uma informação aberta a partir de outra. No mundo real, textos contêm redundância (de linguagem) o suficiente para que mesmo sem saber os textos claros das mensagens pode-se obtê-los somente conhecendo uma parcela da informação. Por exemplo, cabeçalhos IP.

Reutilização da chave compartilhada - WEP utiliza a mesma chave compartilhada em todas as transmissões variando apenas o vetor inicial IV. Como o mesmo tem o tamanho limitado em 24 bits, teremos diversas transmissões onde o IV será reutilizado gerando uma colisão. Às vezes esse evento é acelerado já que diversos fabricantes utilizam o mesmo algoritmo para definir o IV (iniciando em zero cada vez que ativo for reconectado e incrementado um a um conforme utilização). Um pequeno conjunto de colisões já é o bastante para permitir que um hacker utilize um ataque de freqüência para obter a chave compartilhada.

Chave compartilhada precisa ser trocada manualmente – imaginemos uma empresa grande que demite um funcionário que conhecia a chave compartilhada. A troca desta chave em empresas menores é aplicável, mas numa empresa grande, este processo seria deveras demorado e inseguro já que um número maior de funcionários teria acesso a nova chave.

Access Points não autenticam NICs (Network Interface Card) – o protocolo WEP somente apresenta um método pelo qual os NICs podem autenticar os Access Points. O

processo contrário não está disponível o que permite que uma estação não autorizada escute as transmissões de uma rede livremente.

CRC-32 é linear e independente de k - O algoritmo utilizado para preencher o FCS (Frame Checking Sequence) do protocolo WEP é o CRC-32. Este algoritmo foi desenvolvido para encontrar erros randômicos, mas é ineficiente quanto a alterações maliciosas. Devido às vulnerabilidades apresentadas, o protocolo WEP é suscetível a diversos tipos de ataque:

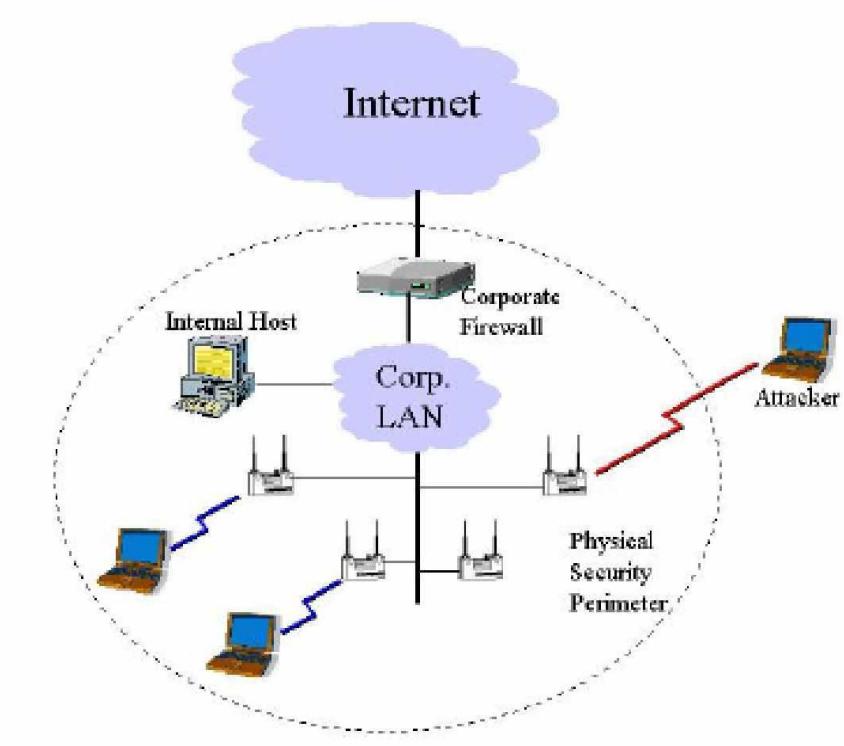


figura 2.4 – Acesso desautorizado

Todos os ataques clássicos de TCP/IP se aplicam normalmente:

- ARP spoofing: redirecionar tráfego para o impostor via falsificação/personificação do endereço MAC
- DNS spoofing: redirecionar tráfego para o impostor via adulteração dos pacotes DNS
- Smurf: sobrecarga de broadcasts para negação de serviço/saturação do canal

- DHCP spoofing: servidor DHCP impostor força configuração imprópria dos clientes

Man-in-the-middle – De posse da chave compartilhada, um hacker pode facilmente capturar um pacote, decifrar o seu conteúdo utilizando a chave. Alterar o conteúdo (inclusive o CRC32) e novamente cifrar para reenviar ao destinatário. Quando este receber o pacote alterado, irá tratá-lo como pacote normal já que a chave compartilhada confere.

Modificando Mensagens – Na última falha mencionada listada encontramos uma forma de alterar o conteúdo da mensagem sem que o destinatário possa verificar que tal modificação foi feita.

Inserindo Mensagens - Utilizando a propriedade do CRC de ser independente da chave k, desta maneira o adversário pode calcular campos de CRC válidos para suas mensagens. Se ele conhecer uma mensagem ele pode descobrir a seqüência chave relativa a um dado v e utilizá-la para injetar tráfego na rede.

A partir daí ele terá a seqüência chave e o vetor de inicialização correspondente, podendo validar qualquer mensagem que ele quiser.

Dicionários de decriptografia - Uma vez que um texto de uma mensagem interceptada é obtido, o adversário descobre o valor da seqüência chave e é capaz de decifrar qualquer outra mensagem com o mesmo vetor de inicialização. Depois de algum tempo o adversário pode armazenar em uma tabela a sequencia chave correspondente a cada vetor de inicialização. Uma tabela completa requer um espaço mínimo - talvez 1500 bytes para cada uma das 2^{24} possibilidades do vetor, ou aproximadamente 24 GB.

Decriptação de mensagens através do redirecionamento IP - Pode ser usado quando o ponto de acesso age como um roteador IP, o que é muito comum.Utilizando o procedimento descrito acima (modificação de mensagens) o campo IP pode ser alterado para enviar uma mensagem "escutada" através do roteador, que irá decriptar a mensagem e enviá-la à máquina

de destino, do adversário ou para alguma outra que ele controle, podendo assim ler o conteúdo.

Dupla encriptação - Sabemos que a técnica de encriptação é a mesma da decriptação. Então, adversário pode entrar na rede enganando a autenticação (Como foi dito anteriormente a mensagem de desafio e a sua versão encriptada podem ser copiadas e posteriormente utilizadas para se autenticar na rede). Utilizando uma segunda conexão à Internet pode enviar pacotes para seu laptop através da rede. A estação base irá, portanto, irá encriptar o pacote uma segunda vez. Se o adversário tentar na hora certa, a estação base utilizará o mesmo vetor de inicialização, e o resultado será o pacote decriptado.

2.5 Possíveis Soluções

Após verificar a existência de diversas falhas no protocolo WEP o grupo IEEE passou a focar seus esforços em propor soluções nas seguintes direções:

- Segurança em Camadas/em profundidade;
- Uso de vários recursos de segurança/contenção mutuamente independentes;
- Segmentação e contenção usando firewalls e configuração minuciosa dos APs, tentar impedir ao máximo ataques via TCP/IP;
- VPNs (Redes Virtuais Privadas) à existem vários protocolos de tunelamento disponíveis cada um com suas vantagens;
- Rotacionamento de chaves WEP à Firmwares mais novos mudam a chave de tempos em tempos melhorando assim a segurança e impedindo que o adversário possa fazer um dicionário com os keystreams (IV,k); e
- Monitoração para detectar APs impostores.

Seguindo essa linha diversos fabricantes de ativos para redes 802.11 implementaram suas próprias soluções com intuito de tratar as vulnerabilidades do protocolo WEP:

Aumentar o tamanho da chave WEP compartilhada – Em 1998, a Lucent passou a utilizar uma chave de 128 bits. Com isso, os hackers teriam que levar um tempo maior para quebrar as chaves. Entretanto, tal opção só postergava o problema. Seguindo esta mesma linha, a Agere criou a chave de 152 bits e a US Robotics a de 256 bits. A tendência de aumentar as chaves trás um novo problema que é a sobrecarga causada pelos mecanismos de segurança no tráfego das redes 802.11.

Troca Dinâmica de Chaves WEP – Mais tarde, diversos fabricantes incluindo Cisco e Microsoft, implementaram a troca dinâmica de chaves. Periodicamente, um pacote broadcast seria enviado para todos os NICs da rede com a nova chave. Desta forma, o hacker não teria informações suficientes para usar o ataque de freqüência e assim chegar a chave WEP.

Com intuito de resolver os problemas do protocolo WEP, o 802.11 working group adotou o padrão 802.1X para autenticação, autorização e gerencia de chaves. Já o IEEE formou o Task Group I com objetivo de desenvolver o padrão 802.11i (RSN – Robust Security Network) que tem como objetivo de criar mecanismos que realmente atendam os requisitos citados no início deste documento. Enquanto os trabalhos acima mencionados não são concluídos, a indústria corre por fora.

Representada pela Wi-Fi, em conjunto com o IEEE, desenvolveu o mecanismo Wi-Fi Protected Access (WPA – subset do padrão 802.11i) que se tornou um padrão altamente utilizado pelo mercado em 2003. Verificamos que os trabalhos caminham em paralelo. A indústria, representada pela Wi-Fi Alliance, busca novas soluções para resolver os problemas de segurança da rede 802.11.

Por outro lado, o IEEE busca padronizar as soluções. Devemos atentar para o fato que os trabalhos possuem sempre interseção e que o produto final dos mesmos será um mecanismo padronizado por um padrão IEEE implementado pelos fabricantes que compõe a Wi-Fi Alliance resultado em fim numa rede sem fio segura.

2.6 WPA – Wi-Fi Protected Access

O WPA é um padrão para um mecanismo de autenticação que possui a interoperabilidade como característica. Todos os ganhos com este novo padrão foram desenvolvidos no nível de software para que os hardwares legados possam utilizar o novo mecanismo.

Como dito anteriormente, o WPA é um subset do novo padrão 802.11i e possui as seguintes funcionalidades:

- Implementa o novo padrão de autenticação 802.1X que permite autenticação mutua
- Implementa o TKIP (Temporal Key Integrity Protocol) definido sobre o WEP com intuito de garantir a chave e com isso a integridade dos dados
- Usa Michel Message Integrity Check para garantir a integridade das mensagens WPA é uma solução interina que resolve todos problemas conhecidos do protocolo WEP e que será compatível como o novo padrão 802.11i. Este será a solução de segurança para redes sem fio e todos os produtos deverão ser compatíveis com este padrão.

  Passemos agora a discussão das funcionalidades disponibilizadas pelo WPA.

802.1X EAP based authentication

WPA adotou o padrão 802.1X para resolver o problema de autenticação do protocolo WEP. O padrão 802.1X foi desenvolvido inicialmente para redes com fio, mas hoje em dia é utilizado em redes sem fio. Este padrão define um serviço que escuta em uma determinada porta de um servidor que permite a autenticação mutua de clientes e APs.

O 802.1X é comprometido com 3 elementos:

- Um suplicante – um usuário que deseja se autenticar. Isto pode ser um software cliente instalado em um laptop, um PDA ou um outro ativo sem fio;
- Um servidor de autenticação – Um sistema de autenticação como o RADIUS que proceda as autenticações necessárias; e

- Um autenticador – Um ativo que permite a comunicação entre o suplicante e o servidor de autenticação. Normalmente, este autenticador é um Access Point.

A autenticação mutua definida no padrão 802.1X é constituída pelos seguintes passos:

- Um suplicante inicia uma conexão com um autenticador. O autenticador detecta a ocorrência e habilita uma porta para o suplicante. Entretanto, excluindo o trafego definido pelo 802.1X, todos os outros estão bloqueados;
- O autenticador requer a identificação do suplicante;
- O suplicante responde com a identificação que é imediatamente repassada para o servidor de autenticação;
- O servidor autentica a identidade do suplicante e envia uma mensagem do tipo ACCEPT para o autenticador. O autenticador muda o estado da porta para autorizado;
- O suplicante requisita a identificação do servidor. O servidor atende; e
- O suplicante valida a identificação do servidor e todo trafego é liberado.

O método de autenticação é definido no EAP – Extensible Authentication Protocol. Este protocolo fornece um framework para que o sistema de autenticação escolha método apropriado de autenticação. Este método pode ser: senhas, certificados digitais ou qualquer outro tipo de token.

Utilizando o EAP, o autenticador (APs) não precisa ser especifico quanto ao método de autenticação, basta operar como proxy das informações entre o suplicante e o servidor de autenticação.

Segue uma lista de métodos de autenticação:

- **EAP – LEAP** – desenvolvido pelo fabricante Cisco Systems; utiliza usuário e senha para identificar e autenticar o suplicante.

- **EAP – TLS** – este método obdece a RFC 2716; utiliza certificados digitais X.509 para identificar e autenticar o suplicante.
- **EAP – TTLS** – desenvolvido pelo fabricante Funk Software; semelhante ao EAP – TLS com a diferença que o suplicante é identificado com apenas uma senha.
- **EAP – PEAP** – Protected EAP – desenvolvido para sanar uma vulnerabilidade do EAP.
- **Pre-Shared Key** – utilizado em pequenas empresas ou em ambiente caseiros; lembra o antigo WEP só que opera sobre o protocolo EAP que é mais seguro.

TKIP

Temporal Key Integrity Protocol é o segunda funcionalidade derivada do 802.11i. Ele tem como objetivo tratar as vulnerabilidades no protocolo WEP no campo da criptografia de dados. Mas especificamente no momento em que o protocolo WEP reutiliza a chave compartilhada n vezes. O TKIP é também comprometido com 3 elementos:

- **Chave compartilhada de 128 bits** – chave compartilhada entre suplicantes e APs.
- **O endereço MAC de cada cliente**
- **Um vetor de inicialização de 48 bits** – descreve a seqüência de pacotes

Este comprometimento garante que os diversos clientes utilizem chaves diferentes ao longo da operação tornando a tarefa de capturar a chave compartilhada bem mais complexa. A troca das chaves é feita a cada 10.000 pacotes.

Com o objetivo de manter compatibilidade com hardwares legados, o TKIP utiliza o mesmo algoritmo RC4 que o WEP utiliza. Desta forma, apenas atualizações de software e firmware serão necessárias para que estes legados possam utilizar o TKIP. Todos os especialistas do assunto concordam que o TKIP trás um grande avanço em termo de segurança, mas todos concordam também que está solução é interina já que o RC4 é um algoritmo declaradamente “quebrado”.

Michael Message Integrity Check

A funcionalidade **Michael Message Integrity Check** é utilizada para garantir a integridade das mensagens que trafegam em uma rede 802.11. Um MIC (Message Integrity Code) é uma redundância de 64 bits calculada com o algoritmo "Michael". Este algoritmo é bem mais adequado e já é capaz de verificar qualquer modificação causada por erro na transmissão ou ainda por manipulação deliberada. O MIC faz parte do pacote TKIP mencionado acima.

Conclusões sobre o WPA

Verificamos que o WPA é uma solução que resolve diversos problemas conhecidos do WEP. Numa comparação podemos destacar os seguintes pontos:

- **Autenticação Mútua** – implementa um controle de acesso bem mais resistente do que o protocolo WEP já que os Aps também podem autenticar os NICs;
- **Novas tecnologia de segurança** – suporta o 802.1X, o EAP, o RADIUS e o Pre-Shared Key;
- **TKIP** – implementa um melhor gerenciamento de chaves;
- **Michael Message Integrity Check** – reforça a integridade das mensagens; e
- **Compatibilidade** – como dito anteriormente, o WPA pode ser visto como um subset do 802.11i e com isso a compatibilidade com soluções futuras parece estar garantida.

Entretanto, o WPA não é uma solução definitiva já que apresenta problemas:

- **Criptografia Fraca** – com intuito de manter compatibilidade com hardwares legados, o algoritmo RC4 foi mantido. Como já sabemos, o RC4 por si só já representa uma fraqueza. Tanto que existem alguns fabricantes que trocaram o RC4 pelo AES criando um novo padrão conhecido como WPA2.
- **Queda de Performance** – como os hardwares legados não foram projetados para suportar algoritmos pesados, a sobrecarga gerada pelo uso deles é relevante, tanto que

os novos ativos já apresentam processadores criptográficos potentes que tem a capacidade de processar algoritmos bem mais pesados como o AES.

2.7 802.11i – A última solução de segurança para redes Wi-Fi

O 802.11i é uma especificação criada pelo grupo IEEE Task Group "I" com intuito de sanar definitivamente todos os problemas conhecidos do protocolo WEP.

Esta especificação inclui diversas funcionalidades:

- **Novos Algoritmos de criptografia:**
  - **TKIP** – com intuito de manter compatibilidade com sistemas legados, o 802.11i suporta o TKIP implementado pelo WPA.
  - **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)** – o 802.11i inclui um novo padrão conhecido como AES – CCMP utilizando o modo CBC (Cipher Block Chaining). Entretanto um co-processador criptográfico é necessário.
  - **WRAP (Wireless Robust Authentication Protocol)** – similar ao CCMP só que utilizando um modo diferente, o OCB (Offset Codebook).
- **Integridade de Mensagens** – o 802.11i adota o algoritmo Michael Message Integrity Check com intuito de garantir a integridade das mensagens, assim como o WPA.
- **Autenticação Mutua** – o 802.11i utiliza o EAP, assim como o WPA.
- **Suporta Roaming**
- **Novos protocolos:**
  - **RSN – Robust Security Network Protocol**
  - **WRAP - Wireless Robust Authentication Protocol**
  - **EAP – Extensible Authentication Protocol**

Podemos verificar que a grande novidade do 802.11i é a substituição TKIP (RC4) pelo CCMP (AES). Desta forma, o novo padrão resolve o problema da criptografia fraca. O problema de performance é resolvido com a utilização de co-processadores criptográficos. Uma segunda novidade é a presença de tratamento para Roaming, mecanismo até então não presente nas soluções.

2.8 Wireless Intrusion Prevention System (WIPS)

O WIPS é um dispositivo de rede que monitora o rádio espectro procurando por acessos não autorizados (detecção de intruso), e pode, automaticamente, tomar as contramedidas necessárias para evitá-lo (prevenção de intrusão).

O propósito principal de um WIPS é a prevenção do acesso não autorizado a rede local por dispositivos sem fio. Este sistema é tipicamente implementado como uma extensão de uma infraestrutura de rede sem fio já existente, embora ele possa ser implementado em uma versão Stand Alone para reforçar uma política de “No Wireless” dentro de uma organização. Algumas infraestruturas de rede sem fio avançadas já possuem capacidade WIPS integrada.

Grandes organizações com muitos funcionários são particularmente vulneráveis a brechas de segurança causadas por Access Points externos. Se um funcionário (entidade confiável) trouxer para seu local de trabalho um roteador wireless, facilmente encontrado no mercado, toda a rede pode ficar exposta a qualquer um que esteja no raio do sinal do roteador.

Em julho de 2009, o PCI Security Standards Council publicou as Wireless Guidelines para PCI DSS recomendando o uso de WIPS para automatizar o monitoramento de redes wireless em grandes organizações.

Detecção de Intruso

Um Wireless Intrusion Detection System (WIDS) monitora o rádio espectro a procura de Access Points não autorizados e da presença de ferramentas de ataque. O sistema monitora o rádio espectro usado pelas redes wireless e imediatamente alerta o administrador do sistema quando um Access Point externo é detectado. Por convenção isto é conseguido comparando-se o MAC address dos dispositivos participantes.

Dispositivos externos podem fazer spoof de MAC address de um dispositivo de rede autorizado como se fosse deles. Novas pesquisas usam o método fingerprinting para eliminar os dispositivos com spoof de MAC address. A idéia é comparar a assinatura única dos sinais emitidos por cada dispositivo wireless com as assinaturas dos dispositivos wireless conhecidos e pré-autorizados.

Prevenção de Intruso

Em adição a detecção de intrusão, o WIPS também inclui medidas de prevenção contra a ameaça automaticamente. Para a prevenção automática é requerido que o WIPS seja capaz de detectar e automaticamente classificar a ameaça.

Os seguintes tipos de ameaça podem ser detectados por um bom WIPS:

- Rogue AP – O WIPS tem que entender a diferença entre um Rogue AP para um AP externo (vizinho);
- AP mal configurado;
- Cliente mal associado;
- Associação não autorizada;
- Ataque Man-in-the-middle;
- Redes Ad-hoc ;
- MAC-Spoofing;

- Honeypot /Ataque Evil Twin; e
- Ataque Denial of Service (DoS).

Implementação

A configuração do WIPS consiste de três componentes:

- Sensores — Estes dispositivos contém antenas e rádios que monitoram o espectro wireless atrás de pacotes e são instalados na área que se quer proteger.
- Servidor — O servidor WIPS analisa centralizadamente os pacotes capturados pelos sensores;
- Console — O console proporciona a interface do sistema com o usuário para a administração e a extração dos relatórios.

Um WIDS simples pode ser um simples computador, conectado a um dispositivo processador de sinais wireless, e antenas colocadas na área que se queira monitorar.

Em uma implementação WIPS, primeiro o usuário define as políticas da rede wireless no WIPS. Os sensores WIPS então analisam o tráfego no ar e enviam esta informação para o servidor WIPS. O servidor compara esta informação com as políticas definidas e define então se é ou não uma ameaça. O administrador do WIPS é então notificado da ameaça, ou, se a política foi bem definida, o WIPS toma as medidas de proteção automaticamente. O WIPS pode ser configurado como uma implementação de Rede ou de Host.

Implementação de Rede

Em uma implementação WIPS de rede o servidor, sensores e o console estão todos dentro de uma rede privada e não podem ser acessados pela internet. Os sensores se comunicam com o servidor por uma rede privada usando uma porta privada. Como o servidor reside dentro de uma rede privada, os usuários só podem acessar o console de dentro desta rede.

A implementação de rede é apropriada para as organizações onde todos os locais estejam dentro da mesma rede privada.

Implementação de Host

Em uma implementação WIPS de Host, sensores são instalados dentro da rede privada. Porém, o servidor fica em um Data Center seguro e é acessível pela intenet. Usuários podem acessar o console WIPS de qualquer lugar na internet. A implementação WIPS de Host é tão segura quanto a implementação da rede porque o fluxo de dados entre os sensores e o servidor é criptografada, assim como entre o servidor e o console. A implementação WIPS de Host requer muito pouca configuração porque os sensores são programados para automaticamente procurar pelo servidor na internet através de uma conexão SSL segura.

Para grandes organizações com locais que não fazem parte da mesma rede privada, uma implementação WIPS de Host simplifica o trabalho significativamente porque os sensores se conectam com o servidor pela internet sem requere configuração especial. Além da console poder ser acessado seguramente de qualquer lugar pela internet.

3 METODOLOGIA DE PESQUISA

3.1. Tipo de Pesquisa

Quanto aos meios, esta pesquisa é um Estudo de Caso que "é apenas uma das muitas maneiras de se fazer pesquisa em ciências sociais" (YIN, 1994). Por se tratar de um estudo profundo, visando obter o máximo de informações que permitam um amplo conhecimento, o que seria impossível em outras pesquisas (ALVES, 2003).

A característica principal da pesquisa por Estudo de Caso é o fato de que quanto maior quantidade de informação, melhor será a análise dos fatos.

3.2. Coleta e Análise da Dados

Segundo Gil (1996), a coleta de dados em um estudo de caso é baseada em diversas fontes de evidências. Para efeito de elaboração desta pesquisa foram utilizados os procedimentos de entrevista e observação participante.

As entrevistas focais, conforme classificação de Yin (2001) ou focalizadas, de acordo com Gil (1996), constituíram-se no principal meio de coleta de dados deste estudo. Ao mesmo tempo em que a entrevista concedida foi espontânea, ela também foi parcialmente estruturada, uma vez que precisou ser guiada por alguns pontos de interesse explorados pelo pesquisador. O roteiro utilizado durante a condução das entrevistas encontra-se disponível no Anexo I deste trabalho.

A coleta de dados ocorreu por meio de entrevista aboradando a implementação do projeto, seus problemas e seus benefícios. O roteiro da entrevista foi passado ao Encarregado da Divisão de Segurança das Informações da Diretoria de Comunicações e Tecnologia da Informação da Marinha do Brasil (DCTIM).

3.3. Limitações do Método

A primeira limitação encontrada refere-se ao tipo de pesquisa utilizada, especialmente, quanto aos meios. De acordo com Yin (2001), estudos de caso são generalizáveis a proposições teóricas e não a populações ou universos.

Já a segunda limitação relaciona-se com os procedimentos utilizados para a coleta de dados. As entrevistas focais (Yin, 2001) ou focalizadas (Gil, 1996), além de contarem com a presença de um entrevistador, que pode inibir o entrevistado levando-o a emitir uma opinião diferente do que realmente pensa sobre os fatos, que podem não corresponder à realidade das organizações e sim à visão prática, ou até mesmo ao anseio dos entrevistados, comprometendo assim a análise. Para tentar minimizar o constrangimento causado pela presença do entrevistador, o pesquisador buscou, logo no início da entrevista, garantir a confidencialidade das informações obtidas e deixar claro o caráter acadêmico da análise.

4. DESCRIÇÃO DO CASO – CRepSupEspFN

4.1. História

O Centro de Reparos e Suprimentos Especiais do Corpo de Fuzileiros Navais (CRepSupEspCFN) é uma Organização Militar Prestadora de Serviços (OMPS) e como tal possui autonomia de gestão e a necessidade de gerar lucros. Para tal, expande seus serviços para clientes externos à Marinha do Brasil (MB). Hoje, além de executar a manutenção de todos os meios de Fuzileiros Navais, o CRepSupEspCFN é representante autorizado da Toyota (Japão), da Land Rover (Inglaterra), da Mowag (Suíça) e Harley-Davidson (EUA). Estas representações devem-se ao fato de o Corpo de Fuzileiros Navais (CFN) se utilizar de viaturas desses fabricantes e no contrato firmado entre as partes ter uma cláusula de transferência de tecnologia.

Para que o CRepSupEspCFN atinja seus objetivos corporativos, cada vez mais necessita de uma administração ágil, segura e flexível. Por contar com uma gama enorme de sobressalentes oriundos de diversos fabricantes, necessita ter um controle ativo sobre seus estoques sob pena de aumentar os seus custos e perder competitividade no mercado.

Para isso foi decidido adotar um sistema de controle de inventário de sobressalentes baseado em coletores sem fio ligados por uma rede Wi-Fi que se conectasse com o Sistema Integrado de Gerenciamento do Abastecimento (SINGRA). Este projeto foi denominado SINGRA-Móvel.

Mas não podemos esquecer que o CRepSupEspCFN ainda é um Organização Militar e seus dados não podem ficar sujeitos a invasões e quebra de sigilo.

Este estudo visa entender como foi solucionado este problema.

4.2. Solução encontrada

De acordo com o Encarregado da Divisão de Segurança da Informação da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) a solução para redes sem fio na MB passa por um controle de acesso rigoroso utilizando o padrão WPA2 e pela monitoração do éter, através de um Wireless Intrusion Prevention System (WIPS) centralizado, ou seja, os sensores remotos ficam na área onde a rede está instalada mas a monitoração fica centralizada remotamente na DCTIM. Desta forma, todos os ataques feitos a qualquer rede sem fio na MB são detectados na central de segurança da DCTIM. A solução contratada pela MB suporta até 200 sensores e tem o controle (Servidor e Console) centralizado na DCTIM. O sistema WIPS, além de detectar as tentativas de invasão também "atacam" o invasor causando interferência na sua conexão, impossibilitando assim que continue tentando um ataque.

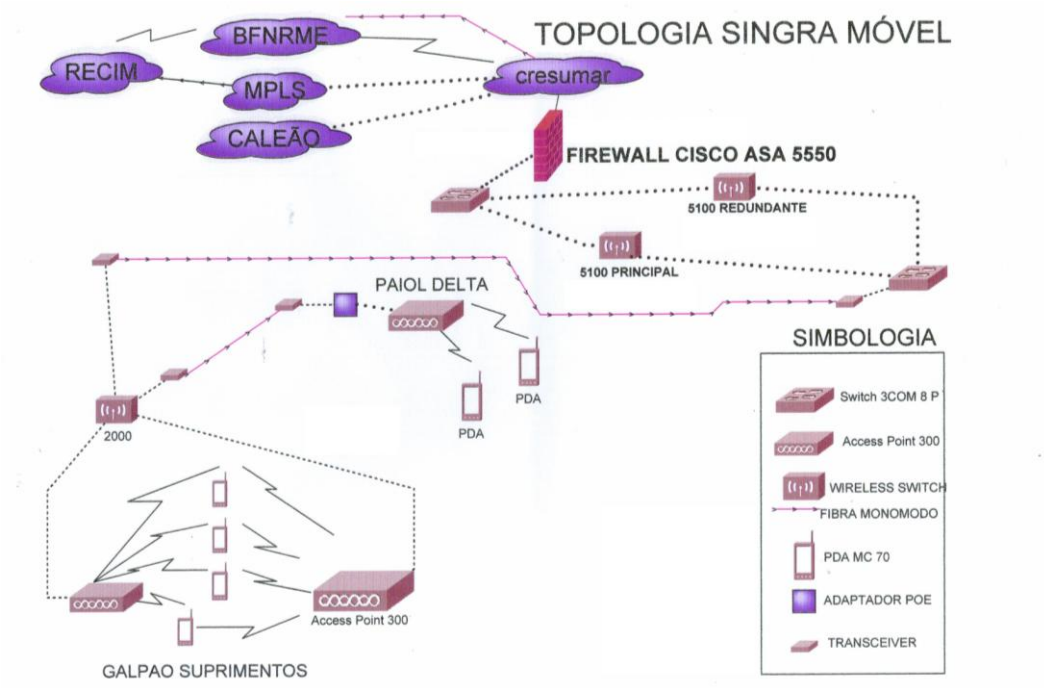


Figura 4.1 Estrutura da rede do CRepSupEspCFN

Quanto à infra-estrutura da rede, foi definida pela DCTIM que as redes sem fio da MB deveriam ter a administração dos Access Points (AP) centralizadas e deveriam ter redundância nos dispositivos de controle, além de um firewall dedicado e configurado pela

própria DCTIM, dando acesso somente aos servidores específicos do Sistema de Abastecimento da Marinha.

5 ANÁLISE DO CASO

A solução adotada pela MB, o WPA2, utiliza um protocolo denominado Advanced Encryption Standard (AES), que é muito seguro e eficiente, mas possui a desvantagem de exigir bastante processamento. Seu uso é recomendável para quem deseja alto grau de segurança, mas pode prejudicar o desempenho de equipamentos de redes não tão sofisticados (geralmente utilizados no ambiente doméstico). É necessário considerar também que equipamentos mais antigos podem não ser compatíveis com o WPA2, portanto, sua utilização deve ser testada antes da implementação definitiva.

O WPA2, como visto na seção 2.7, utiliza o AES junto com o TKIP com chave de 256 bits, um método mais poderoso que o WPA que utilizava o TKIP com o RC4. O AES permite ser utilizada chave de 128, 192 e 256 bits. O padrão no WPA2 é 256 bits, sendo assim, uma ferramenta muito poderosa de criptografia. Utilizando o AES surgiu a necessidade de novo hardware para processamento criptográfico, devido a isso, os dispositivos WPA2 tem um co-processamento para realizar os cálculos criptográficos (EARLE, 2006).

No caso específico da MB, a preocupação, pelo menos no estágio inicial, é maior com a segurança do que com a performance. Por isso foi decidido usar o WPA2 mesmo que isso implicasse em uma queda de performance devido ao já ultrapassado parque instalado. Não é novidade pra ninguém os seguidos cortes orçamentários que as Forças Armadas vem sofrendo nos últimos anos e os efeitos que estes cortes tem na área de tecnologia. O fundamental no momento é salvaguardar as informações de caráter militar e possibilitar a utilização da tecnologia sem fio sem restrições, mas com segurança.

A utilização do sistema WIPS complementa as medidas de segurança implementadas visto que, como exposto na seção 2.8, o WIPS cria uma barreira a mais para a tentativa de ataque a rede. A forma pró-ativa como atua este sistema vem ao encontro dos anseios de segurança da instituição, visto que a simples detecção poderia dar tempo ao dispositivo atacante de realizar

o seu intento. Como o WIPS atua de forma preventiva, interferindo ativamente e automaticamente na conexão do dispositivo atacante, este não tem meios de completar o seu ataque.

6 CONCLUSÃO

6.1. Principais contribuições

Como pudemos observar ao longo deste estudo, a tecnologia de segurança em redes de computadores avança na medida em que os tipos de ataque também evoluem. A solução encontrada pela MB passa não somente pelo controle do acesso a rede como também pela monitoração do éter, funcionando como um verdadeiro instrumento de "Guerra Eletrônica". Com certeza o sistema WIPS gera uma barreira praticamente intransponível, pelo menos por enquanto, gerando assim a segurança e a confidencialidade necessárias a atividade militar.

Durante muitos anos a tecnologia wireless não foi vista com bons olhos na MB, sendo considerada uma porta aberta para a invasão da rede corporativa, tornando-se portanto uma séria ameaça as informações confidenciais de caráter militar.

Até o momento não temos informação sobre tentativas de ataque à rede sem fio da MB, talvez fruto da natureza administrativa das informações. Mas o futuro das redes wireless na MB depende do sucesso da implementação feita no CRepSupEspCFN.

Com base neste estudo podemos concluir que a MB encontra-se no estado da arte da segurança em redes sem fio corporativas mesmo tendo que conviver com um parque tecnológico instalado já ultrapassado e mais todos os malefícios que os cortes orçamentários trazem em seu bojo.

6.2. Pesquisas futuras

Como a área de segurança de redes corporativas está sempre em evolução em decorrência do interminável duelo com os acessos não autorizados, ficam aqui algumas perguntas para estudos futuros:

Quais os aspectos legais que devem ser considerados ao se interferir na conexão de um dispositivo sem fio que não pertença à determinada rede?

Como fica a administração local no combate as ameaças de uma rede com a implementação centralizada (de Host) de um sistema WIPS?

Que tipos de ataque um sistema WIPS sofre e como se comporta em cada caso? Há casos de ataques não interrompidos? Seria o WIPS uma solução definitiva para o acesso não autorizado?

BIBLIOGRAFIA

BARNES, Douglas. “Network America: Wireless security? Read it and Wep”. June 27, 2002. Disponível em http://www.vnunet.com/Features/1133066. Acessado em 08 de março de 2010

BORISOV, Nikita. Goldberg, Ian. Wagner, David. “Security of the WEP algorithm”. February 02, 2001. Disponível em http://www.isaac.cs.berkeley.edu/issac/wep-faq.html Acessado em 10 de março de 2010.

DISMUKES, Trey “Azariah”, “Ars Technica: Wireless Security Blackpaper”. July 2002. Disponível em http://www.arstechnica.com/paedia/w/wireless/security-1.html. Acessado em 08 de março de 2010

"Fitting the WLAN Security pieces together". pcworld.com. Disponível em http://www.pcworld.com/businesscenter/article/144647/guide_to_wireless_lan_security.html. Acessado em 29 de agosto de 2010.

GAST, Matthew. “Wireless LAN Security: A Short History”. April 19, 2002. Disponível em http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html. Acessado em 08 de março de 2010

GEIER, Jim. “802.11 Security Beyond WEP”. June 26, 2002. Disponível em http:// www.80211-planet.com/tutorials/article.php/1377171. Acessado em 14 de março de 2010

JOHNSON, David. “Assorted 802.11 Related Crypto Algorithms”. Disponível em http://www.deadhat.com/wlancrypto. Acessado em 15 de março de 2010

MIYANO, R. N. A Evolução dos Mecanismos de Segurança para Redes sem fio 802.11. 2004. Monografia da disciplina Introdução a Computação Móvel. PUC-RJ.

"New Low-Cost Wireless PCI Scanning Services; New Offerings Satisfy PCI DSS Requirements". Disponível em http://newsblaze.com/story/20090722050115000038.mwir/topstory.html. Acessado em 19 de agosto de 2010.

"PCI DSS Wireless Guidelines". Disponível em https://www.pcisecuritystandards.org/ pdfs/PCI_DSS_Wireless_Guidelines.pdf. Acessado em 19 de agosto de 2010.

PINHEIRO , J.M.S. Programas de Segurança para Redes Corporativas. 2005. Disponível em http:// www.projetoderedes.com.br / artigos / artigo_programas_de_ seguranca_ redes_corporativas.php. Acessado em 07 de março de 2010.

"Security SaaS hits WLAN community". networkworld.com. Disponível em http://www.networkworld.com/newsletters/wireless/2008/040708wireless1.html. Acessado em 19 de agosto de 2010.

SOARES, L.F.G.; LEMOS, G.; COLCHER, S. Redes de Computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus. 1995.

TANEMBAUM, Andrew S. Redes de Computadores.1997.Tradução da Terceira Edição. Rio de Janeiro: Campus.

TECH FAQ. Disponível em http://www.tech-faq.com/wireless-networks. Acessado em 08 de março de 2010.

"University research aims at more secure Wi-Fi". eetimes.com. Disponível em http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=GPLEDVT0ZRBKUQSNDLPSKH0CJUNN2JVN?articleID=192501255. Acessado em 19 de agosto de 2010.

Wi-Fi Planet. Disponível em http://www.wi-fiplanet.com. Acessado em 10 de março de 2010

ANEXO I

QUESTIONÁRIO

1- Nome e Cargo do entrevistado e tempo de serviço na Marinha do Brasil (MB)?

2- Qual a sua formação na área de seurança de redes?

3- O que levou a MB a adotar redes sem fio no caso do Centro de Reparos e Suprimentos Especiais do Corpo de Fuzileiros Navais (CRepSupEspCFN)?

4- Como foi a instalação da estrutura física da rede?

5- Qual foi a solução de segurança implantada?

6- Quais os problemas encontrados na implantação?

7- Como são tratadas as tentativas de invasão?

8- Quais os benefícios trazidos pela implementação desta solução?

9- Qual o futuro das redes sem fio na MB?

10- Algum outro detalhe que ache interessante comentar?