

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE

ESTUDO DE SEGURANÇA DA
TECNOLOGIA VoIP EM REDES SEM FIO

Allan Rodrigo Cordeiro Leite

ESTUDO DE SEGURANÇA DA
TECNOLOGIA VoIP EM REDES SEM FIO

NATAL
2007

ALLAN RODRIGO CORDEIRO LEITE

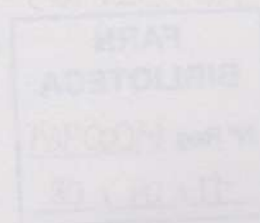
ESTUDO DE SEGURANÇA DA TECNOLOGIA VoIP EM REDES SEM FIO

Monografia apresentada ao curso de Graduação em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito obrigatório para a obtenção do grau de Bacharel em Sistema de Informação.

Orientador:

Aluizio Ferreira da Rocha Neto,
M.Sc.

NATAL/RN
2007



Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Leite, Allan Rodrigo Cordeiro

Estudo de segurança da tecnologia VoIP em redes sem fio / Allan Rodrigo Cordeiro Leite. – Natal: FARN, 2007.

31f.

Orientador: Aluízio Ferreira da Rocha Neto (M.Sc.)

Monografia (Bacharelado em Sistemas de Informação) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Segurança de Redes sem Fio – Monografia. 2. Tecnologia VoIP – Monografia. 3. Protocolo IEE 802.11 – Monografia I. Título.

RN/FARN/BC

CDU 004.72

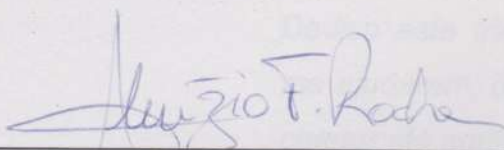


004.72
L55e
2007
ex.01

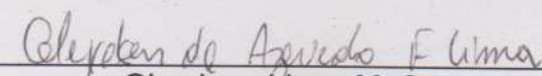
ALLAN RODRIGO CORDEIRO LEITE

ESTUDO DE SEGURANÇA DA
TECNOLOGIA VoIP EM REDES SEM FIO

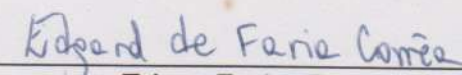
Trabalho de Conclusão de Curso apresentado em ____ de ____ de ____
pelo aluno ALLAN RODRIGO CORDEIRO LEITE, do Curso de Bacharelado em
Sistemas de informação, tendo obtido a média, _____, conforme a
apreciação da Banca Examinadora constituída pelos Professores:



Prof. Aluizio Rocha, M.SC.
Orientador



Gleydson Lima, M. Sc.
Membro Examinador



Edgar Faria, Dr.
Membro Examinado

AGRADECIMENTOS

Agradeço a Deus pela oportunidade de realizar este trabalho.

Agradeço aos meus pais, Euclides e Eufácia, por sempre apoiarem em mim e na minha jornada, sempre me apoiando e me fornecendo tudo o que eu precisava para concluir este trabalho.

Agradeço ao meu orientador, Prof. Alexandre Farias da Rocha Neto, pelas dicas, pelo seu conhecimento, pelas ideias que me motivaram a continuar desenvolvendo esta pesquisa, por ter sido tão paciente e sempre disponível para me ajudar e me apoiar em qualquer momento necessário.

Dedico a:

Dedico este trabalho a todos aqueles que me ajudaram, de uma forma ou de outra, a chegar até aqui.

AGRADECIMENTOS

Agradeço a Deus pela oportunidade de finalizar este trabalho.

Agradeço aos meus pais, Euclimar e Euridice, por sempre acreditarem em mim e no meu potencial, sempre me apoiando e me fornecendo tudo o que eu precisava para concluir este trabalho.

Agradeço ao meu orientador, Profº Aluizio Ferreira da Rocha Neto, pelas críticas, pois me ajudaram a melhorar, pelos elogios, que me motivaram a continuar trabalhando nesta pesquisa, por ter sido tão prestativo e atencioso, sempre estando pronto para me atender e me ajudar com qualquer que fosse minha dúvida e dificuldade.

Agradeço também a todos aqueles que participaram diretamente e indiretamente deste trabalho.

Um forte abraço a todos.

RESUMO

Este trabalho discute a evolução das redes de comunicação sem fio, desde os primeiros sistemas de rádio até as modernas redes de comunicação sem fio. O texto aborda os desafios técnicos e de segurança envolvidos na implementação de redes sem fio, bem como as soluções propostas para esses problemas. O trabalho também discute a importância da segurança em redes sem fio e as medidas necessárias para garantir a confidencialidade e a integridade das informações transmitidas.

Palavras-chave: redes sem fio, segurança, comunicação sem fio.

"Um telégrafo sem fio não é difícil de entender. O telégrafo normal é como um gato muito longo. Você puxa o rabo em New York e ele mia em Los Angeles. A tecnologia sem fio é a mesma coisa, só que sem o gato". (EINSTEIN, Albert)

RESUMO

Esta monografia descreve a evolução dos mecanismos de segurança disponíveis nas redes sem fio do padrão IEEE 802.11, como também na tecnologia VoIP. Seguindo uma ordem cronológica, esta inicia com uma análise da tecnologia de redes sem fio, demonstrando seus principais protocolos de segurança. Em seguida, é analisada a tecnologia VoIP, demonstrando suas principais falhas, em especial aquelas relacionadas a problemas de segurança. Por fim, soluções são propostas visando tornar as redes sem fio e serviços VoIP mais seguros.

Palavras-chave: *redes sem fio, IEEE 802.11, telefonia, VoIP*

ABSTRACT

This monograph describes the evolution of the available mechanisms of safety in the nets without thread of the pattern IEEE 802.11, as well as in the technology VoIP. Following a chronological order, this begins with an analysis of the technology of nets without thread, demonstrating their main protocols of safety. Soon afterwards, the technology is analyzed VoIP, demonstrating their main flaws, especially those related to problems of safety. Finally, solutions are proposed seeking to turn the nets without thread and services safer VoIP.

Keywords: *redes sem fio, IEEE 802.11, telefonia, VoIP*

IP Internet Protocol

LAN Local Area Network

MAC Media Access Control

Mbps Mega Bits por segundo

MHz MegaHertz

PA Ponto de Acesso

QoS Quality of Service

STA Stations

TKIP Temporal Key Integrity Protocol

VLAN Virtual Lan

VoIP Voice Over Internet Protocol

VPN Virtual Private Network

WEP Wired Equivalent Privacy

WFI Wireless Fidelity

WIMAX Worldwide Interoperability for Microwave Access

WLAN Wireless Local Area Network

WLL Wireless Local Loop

WMAN Wireless Metropolitan Area Network

WPA WPA Protected Access

WPAN Wireless Personal Area Network

WWAN Wireless Wide Area Network

SIGLAS

ADC	Analog to Digital Converter
AP	<i>Access Point</i>
BSS	<i>Basic Service Set</i>
DAC	Digital to Analog Converter
DHCP	<i>Dynamic Host Configuration Protocol</i>
ESS	<i>Extended Service Set</i>
FTP	File Transfer Protocol
GHz	Giga Hertz
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	<i>Media Access Control</i>
Mbps	Mega bits por segundo
MHz	MegaHertz
PA	Ponto de Acesso
QoS	Quality of Service
STA	<i>Stations</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
VLAN	Virtual Lan
VoIP	Voice over Internet Protocol
VPN	<i>Virtual Private Network</i>
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLL	<i>Wireless Local Loop</i>
WMAN	<i>Wireless Metropolitan Area Network</i>
WPA	Wi-Fi Protected Access
WPAN	<i>Wireless Personal Area Network</i>
WWAN	<i>Wireless Wide Area Network</i>

LISTA DE FIGURAS

Figura 1: Classificação Pela Abrangência das Redes Sem Fio.....	15
Figura 2: Rede sem fio no modo de infra-estrutura.....	18
Figura 3: Rede sem fio no modo <i>Ad Hoc</i>	18
Figura 4: Cenário clássico do uso da tecnologia VoIP.....	23

SUMÁRIO

1. INTRODUÇÃO	12
1.1 PROBLEMA DE PESQUISA	12
1.2 OBJETIVOS	13
1.2.1 Objetivos Específicos	13
1.3 JUSTIFICATIVA	13
2 REFERENCIAL TEÓRICO	14
2.1 REDES SEM FIO	14
2.2 PADRÃO 802.11	15
2.2.1 IEEE 802.11b/g	15
2.2.2 IEEE 802.11e	16
2.2.3 Outros padrões IEEE 802.11	16
2.2.4 Componentes	17
2.2.5 Modo infra-estrutura	17
2.2.6 Modo ad-hoc	18
2.3 SEGURANÇA EM REDE SEM FIO	18
2.3.1 WEP	19
2.3.2 WPA	20
2.3.3 WPA2	22
2.4 VOZ SOBRE IP	22
2.4.1 Compressão	23
2.4.2 Supressão de silêncio	24
2.4.3 Qualidade de serviço (QoS – <i>Quality Of Service</i>)	24
2.4.4 CODECs	24
2.4.5 G.711	24
2.4.6 G.729	25
3 SEGURANÇA DE VoIP EM REDE SEM FIO	25
3.1 Problemas de Segurança	25
3.2 Captura de chamadas	25
3.3 SPIT	26
3.4 Protocolos de suporte	26
3.5 Soluções	26
3.5.1 Implementações de VLANs (<i>Virtual Local Area Networks</i>)	27
3.5.2 Criptografia	27
3.5.3 VPN	28
4 CONCLUSÃO	29
REFERÊNCIAS	30

1. INTRODUÇÃO

A tecnologia VoIP permite a utilização das redes IP, como a própria Internet, para o transporte de voz. Uma das maiores vantagens de se adotar a tecnologia de Voz sobre IP é a redução nos custos de ligações de longa distância. Empresas ou pessoas que ligam freqüentemente para outros estados e principalmente outros países podem usufruir de uma redução muito significativa em suas contas telefônicas. Isto acontece, pois, como a ligação utiliza a Internet como meio de transporte, não é preciso pagar as altas taxas que as operadoras de telefonia cobram para efetuar estas ligações. A ligação pode sair totalmente sem custo, no caso de uma ligação de softphone para softphone, ou custar menos do que uma ligação local no caso de uma ligação através de um provedor VoIP. A característica da tecnologia VoIP explorada neste trabalho é relativa à falta de mecanismos segurança que evitem principalmente a captura da conversação nas ligações.

O padrão de rede sem fio para redes locais do IEEE (*Institute of Eletrical and Eletronic Engineers*) conhecido como 802.11 possui diversas variações que serão apresentadas nesse trabalho, como também seus protocolos de segurança.

Este estudo busca explorar os aspectos de segurança do uso da tecnologia VoIP em redes sem fio no padrão 802.11, assim como encontrar uma forma mais segura e confiável de transmissão de dados e voz em tais redes.

1.1 PROBLEMA DE PESQUISA

Devido à simplicidade de uso e de configuração, a segurança tem sido o elemento mais preocupante neste tipo de rede, pois uma pessoa mal intencionada pode obter acesso de modo fácil utilizando uma antena, por exemplo, feita com uma lata tubular com papel alumínio e *softwares* específicos para cada situação.

Para evitar que haja acessos indevidos, este trabalho descreve algumas das ferramentas utilizadas para conter as vulnerabilidades da rede sem fio baseada no padrão IEEE 802.11. Lembre-se que em redes sem fio com serviço de VoIP, uma segurança fraca significa que suas conversas telefônicas poderão ser facilmente interceptadas, e o pior é que isso poderá ser feito a uma distância razoável.

1.2 OBJETIVOS

Este trabalho tem por objetivo demonstrar como atua uma rede sem fio baseada no padrão IEEE 802.11, juntamente com a tecnologia de voz sobre IP, demonstrando suas vulnerabilidades e mostrando as suas principais defesas como também avaliando seus desempenhos ao trabalharem juntas.

1.2.1 Objetivos Específicos

O trabalho tem como objetivos específicos

- Estudar a tecnologia de redes sem fio WI-FI (IEEE802.11);
- Estudar a tecnologia voz sobre IP (VoIP);
- Estudar a segurança da tecnologia de rede sem fio (IEEE802.11);
- Estudar a segurança da tecnologia voz sobre IP (VoIP);

1.3 JUSTIFICATIVA

A natureza desta pesquisa é exploratória, onde este trabalho busca explorar os tipos de rede sem fio e descrever seus principais métodos de segurança em relação ao tráfego de voz sobre IP.

O método de pesquisa utilizado para este trabalho foi a pesquisa documental, fazendo-se através de referências bibliográficas disponíveis em livros, revistas, *sites* e artigos *online*.

Esta pesquisa é qualitativa, buscando adquirir conhecimento para se associar aos conceitos pesquisados.

2 REFERENCIAL TEÓRICO

2.1 REDES SEM FIO

São redes cujos cabos são substituídos por ondas de rádio. Sua utilização é muito simples, assim como sua instalação, o que ajuda a proporcionar seu crescente uso nos dias de hoje.

Existem vários tipos e padrões de redes *wireless*, como por exemplo, o *WiMax*, *Bluetooth*, *Wi-Fi*(*Wireless Fidelity*), *InfraRed*(*Infravermelho*). (ARTHAS, 2004)

Uma rede *wireless* é reconhecida por ser sem fio, pois o transmissor e o receptor estão se comunicando sem a presença de fios, no nosso caso, por ondas de rádio. (ENGST & FLEISHMAN, 2005)

Encaixam-se nessa categoria os seguintes tipos de rede: locais sem fio ou WLAN (*Wireless Local Area Network*), redes metropolitanas sem fio ou WMAN (*Wireless Metropolitan Area Network*), como por exemplo, o *WiMAX* (*Worldwide Interoperability for Microwave Access*), redes de longa distância sem fio ou WWAN (*Wireless Wide Area Network*), redes WLL (*Wireless Local Loop*) e o novo conceito de redes pessoais sem fio ou WPAN (*Wireless Personal Area Network*). (ARTHAS, 2004)

Global Wireless Standards

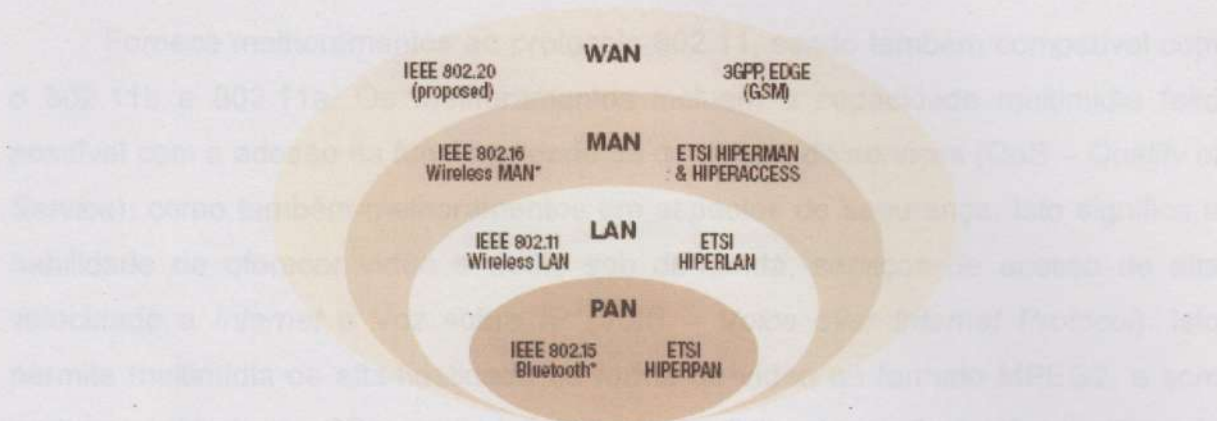


Figura 1: Classificação Pela Abrangência das Redes Sem Fio.
Fonte: TEIXEIRA (2005)

2.2 PADRÃO 802.11

É o padrão que descreve as especificações da camada de enlace e física para redes sem fio que atuam na frequência de 5GHz. Apesar de ter sido firmado em 1999 não existem muitos dispositivos que atuam nesta frequência.

Segundo ARTHAS (2004), quando se discute a configuração de uma WLAN existem alguns padrões, desenvolvidos ou em desenvolvimento pelo IEEE (*Institute of Electrical and Electronic Engineers*) que devem ser considerados.

2.2.1 IEEE 802.11b/g

Descrevem a implementação dos produtos WLAN mais comuns em uso atualmente. Este inclui aspectos da implementação do sistema de rádio e também inclui especificação de segurança. Esta descreve o uso do protocolo WEP (*Wired Equivalency Privacy*). Trabalha na ISM de 2.4 GHz e prove 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE.

O IEEE 802.11g descreve o mais recente padrão para redes sem fio. Atua na banda ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps.

2.2.2 IEEE 802.11e

Fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e 802.11a. Os melhoramentos incluem a capacidade multimídia feito possível com a adesão da funcionalidade de qualidade de serviços (QoS – *Quality of Service*), como também melhoramentos em aspectos de segurança. Isto significa a habilidade de oferecer vídeo e áudio sob demanda, serviços de acesso de alta velocidade a *Internet* e Voz sobre IP (VoIP – *Voice over Internet Protocol*). Isto permite multimídia de alta-fidelidade na forma de vídeo no formato MPEG2, e som com a qualidade de CD, e a redefinição do tradicional uso do telefone utilizando VoIP. QoS é a chave da funcionalidade do 802.11e. Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio.

Segundo Arthas (2004), os grupos do IEEE que estão desenvolvendo outros protocolos descritos nas próximas seções:

2.2.3 Outros padrões IEEE 802.11

O IEEE 802.11i trata-se de um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e 802.11g.

O IEEE 802.11d está concentrado no desenvolvimento de equipamentos para definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente (O corrente protocolo 802.11 só define operações WLAN em alguns países).

O IEEE 802.11f está desenvolvendo o *Inter-Access Point Protocol* (Protocolo de acesso entre pontos), por causa da corrente limitação de proibir *roaming* entre pontos de acesso de diferentes fabricantes. Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.

O IEEE 802.11h é a versão do protocolo 802.11a com regulamentações para a utilização de banda de 5 GHz.

2.2.4 Componentes

Segundo Arthas (2004), a topologia de uma rede IEEE 802.11 é composta pelos seguintes elementos:

- BSS: *Basic Service Set* - corresponde a uma célula de comunicação *wireless*.
- STA: *Stations* - são as estações de trabalho que comunicam entre si dentro da BSS.
- AP: *Access Point* - funciona como uma ponte entre a rede *wireless* e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS. Existem APs que também atuam como roteador, possibilitando o compartilhamento de *Internet* pelos outros micros da rede. Eles vêm de fábrica como servidores DHCP (*Dynamic Host Configuration Protocol*), facilitando a obtenção de um endereço IP na rede. Também conhecido como concentrador.
- Bridge: Faz a ligação entre diferentes redes, por exemplo, uma rede sem fio para uma rede cabeada convencional.
- ESS: *Extended Service Set* - consiste de várias células BSS vizinhas que se interceptam e cujos AP estão conectados a uma mesma rede tradicional. Nestas condições uma STA pode movimentar-se de um BSS para outro permanecendo conectada à rede. Este processo é denominado *Roaming*. Dois modos de operação são previstos: infra-estrutura e ad-hoc.

2.2.5 Modo infra-estrutura

Quando existe a presença de um AP coordenando a comunicação entre as estações de uma célula (BSS). (ARTHAS, 2004)

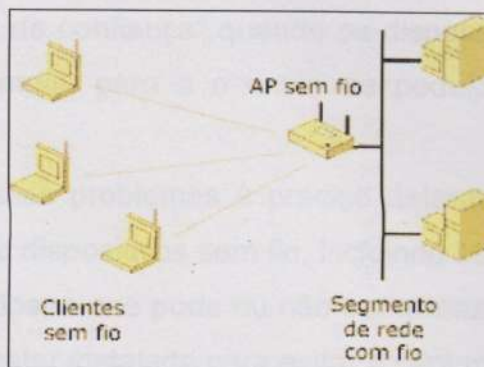


Figura 2: Rede sem fio no modo de infra-estrutura.
Fonte: Microsoft Brasil (2005)

2.2.6 Modo ad-hoc

Quando não existe AP e as estações se comunicam entre si diretamente. Este modo não é recomendado pelo padrão. (ARTHAS, 2004). Um exemplo deste modo pode ser visto na figura 3.

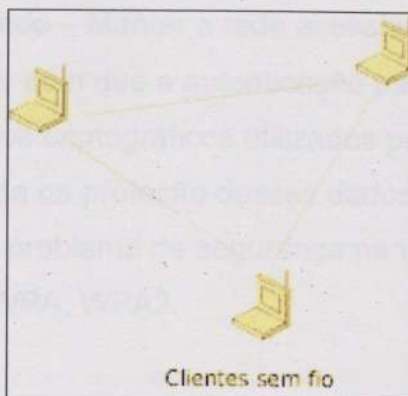


Figura 3: Rede sem fio no modo Ad Hoc.
Fonte: Microsoft Brasil (2005)

2.3 SEGURANÇA EM REDE SEM FIO

As redes sem fio vêm também acompanhadas de desvantagens significativas e talvez a segurança seja a principal delas.

Alguns dos os principais problemas de segurança com relação aos sistemas sem fio incluem:

- Intercessão de transmissão sem fio à medida que viaja via aérea.

- "Relacionamentos de confiança" quando os dispositivos sem fio são usados para comércio (por exemplo, para a o envio de pedidos ou compras, ligações confidenciais).

Para lidar com esses problemas é preciso determinar procedimentos muito específicos para o uso de dispositivos sem fio, incluindo as funções para as quais os mesmos podem ser usados, o que pode ou não ser armazenado e qual a tecnologia de segurança que deve estar instalada para evitar a captura destas informações.

A definição de políticas e padrões para os dispositivos sem fio é imprescindível. Por exemplo, sempre que uma LAN sem fio for ativada, a tecnologia VPN deve ser implementada.

Segundo Duarte (2003), a rede deve estar operante e garantir:

- Confiabilidade – O sinal transmitido pela rede pode ser captado por qualquer receptor atuante na área em que o sinal estiver ativo.
- Integridade da Informação – Garantir que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor.
- Disponibilidade da Rede – Manter a rede acessível.
- Autenticidade – Fazer com que a autenticação para o acesso à rede ocorra.

Temos alguns métodos criptográficos utilizados para a proteção de redes sem fio que iremos falar que ajuda na proteção desses dados trafegados nos ajudando na tentativa de solucionar o problema de segurança na transmissão da voz sobre IP.

Que são elas WEP, WPA, WPA2.

2.3.1 WEP

O *Wired Equivalency Privacy* (WEP) é o método criptográfico usado nas redes *wireless* 802.11. O WEP opera na camada de enlace de dados e fornece criptografia entre o cliente e o *Access Point*. O WEP é baseado no método criptográfico RC4 (*Route Coloniale 4*) da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 bits. O IV é concatenado com a chave secreta compartilhada para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Além disso, o WEP utiliza CRC-32 (*Cyclic Redundancy Check*) para calcular o *checksum* da mensagem, que é

incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o *checksum* para garantir que a mensagem não foi alterada.

O WEP 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 SSID e a lista de endereços físicos permitidos, também conhecidos por endereço MAC (*Media Access Control*).

O WEP se encarrega de encriptar os dados transmitidos através da rede. Existem dois padrões WEP, de 64 e de 128 bits. O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão *Wi-Fi*, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede. (MICROSOFT, 2004)

Segundo Rufino (2005), alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. Como disse o WEP não é perfeito, mas já garante um nível básico de proteção. Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possui falhas conhecidas e facilmente exploradas. Em resumo o problema consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados.

2.3.2 WPA

De acordo com Eduardo Prado (2004), com os problemas de segurança no WEP, a *Wi-Fi Alliance* adiantou a parte de autenticação e certificação elaboradas para o 802.11i e liberou o protocolo WPA (*Wi-Fi Protected Access*).

Apesar de avanços terem ocorridos nesse protocolo, a maioria deles requer novos elementos na infra-estrutura da rede e ainda deve trabalhar em conjunto com outros protocolos, como o 802.11.

Na versão 1 do WPA não há suporte a conexões *Ad-Hoc*, portanto, apenas as redes utilizando um concentrador podem fazer uso deste recurso.

O WPA atua em duas áreas. A primeira é a qual substitui o WEP, cifrando os dados e garantindo a privacidade do tráfego, e a segunda, autentica o usuário, utilizando para isso padrões 802.11 e EAP (*Extensible Authentication Protocol*).

O WPA (*Wi-Fi Protected Access*) possui diferentes modelos de segurança, adaptável ao tipo do uso em que ele será implementado, uma para aplicações pequenas, como redes domésticas e pequenos escritórios, utilizando uma chave previamente compartilhada (Pré-shared key ou WPA-PSK), sendo responsável pelo reconhecimento do aparelho. Outro método é conhecido como infra-estrutura, adicionando um servidor RADIUS (*Remote Authentication Dial-In User Server*) para autenticação, podendo ainda necessitar de uma infra - estrutura de chaves públicas (ICP), caso se utilize certificados digitais para autenticar usuários. (RUFINO, 2005)

O método de chave compartilhada é semelhante ao WEP, onde a troca de chaves é feita manualmente, fazendo com que seu uso se torne melhor adequado em redes pequenas onde os participantes estão acessíveis na maior parte do tempo. Não existem ainda problemas divulgados nos protocolos usados com WPA-PSK. TKIP, responsável pela troca dinâmica das chaves. (RUFINO, 2005)

O protocolo TKIP (*Temporal Key Integrity Protocol*) é o responsável pelo gerenciamento da troca de chaves, no WEP as chaves eram estáticas e seu vetor de inicialização era de apenas 24bits, passando agora para 48bits. (RUFINO, 2005)

O TKIP pode ser programado para alterar o vetor de inicialização a cada pacote, por sessão ou por período, tornando mais difícil a obtenção do mesmo via captura de tráfego.

"Com 802.11 e WEP, a integridade dos dados é fornecida por um valor de verificação de integridade, o ICV (*Integrity Check Value*) de 32-bit que aparece com a carga útil 802.11 e é criptografado com WEP. Embora o ICV esteja criptografado, pode-se alterar os bits na carga criptografada e atualizar o ICV criptografado sem ser detectado pelo receptor.

Com WPA, um método conhecido como *Michael*, especifica um novo algoritmo que calcula um código de integridade da mensagem, o MIC (*Message Integrity Code*) de 8 bytes usando os recursos de cálculo disponíveis nos dispositivos existentes. O MIC está localizado entre a parte de dados do quadro 802.11 do IEEE e o ICV de 4 bytes. O campo MIC é criptografado com os dados do

quadro e o ICV.

Michael também ajuda a fornecer proteção à reexecução. Para ajudar a evitar ataques de repetição, é usado um novo contador de quadros no IEEE 802.11.” (SUPPORT MICROSOFT)

No WPA também foi inserido um modelo para autenticação de usuários, conhecido como EAP (*Extensible Authentication Protocol*), que utiliza o padrão 802.11 e permite vários métodos de autenticação, incluindo a possibilidade de certificação digital. (SUPPORT MICROSOFT)

2.3.3 WPA2

De acordo com a publicação da Microsoft (2005), WPA2 é uma certificação de produto disponível por meio da *Wi-Fi Alliance* que certifica equipamentos sem fio como sendo compatíveis com o padrão 802.11i. O WPA2 oferece suporte aos recursos de segurança obrigatórios adicionais do padrão 802.11i que não estão incluídos em produtos que oferecem suporte ao WPA. Com o WPA2, a criptografia é realizada com o AES (*Advanced Encryption Standard*), que também substitui o WEP por um algoritmo de criptografia bem mais forte. Como o TKIP do WPA, o AES permite a descoberta de uma chave de criptografia de difusão ponto a ponto inicial exclusiva para cada autenticação, bem como a alteração sincronizada da chave de criptografia de difusão ponto a ponto para cada quadro. Como as chaves AES são descobertas automaticamente, não há necessidade de se configurar uma chave de criptografia para o WPA2. O WPA2 é a modalidade de segurança sem fio mais forte.

Como talvez não seja possível agregar suporte AES por meio de uma atualização de *firmware* ao equipamento existente, o suporte a AES é opcional e depende do suporte ao *driver* do fornecedor (MICROSOFT, 2005).

2.4.1 Comparação

2.4 VOZ SOBRE IP

A tecnologia voz sobre IP que tem como sigla VoIP, que vem do inglês e significa *Voice over Internet Protocol*, busca trafegar a voz (geralmente a voz humana) através de pacotes IP, em grande parte dos casos pela Internet.

Há tempos atrás foi descoberto que enviar um sinal para um destino remoto poderia ser feito através de um modelo digital: antes de enviar, precisamos digitalizar o sinal, usando um conversor analógico digital (ADC – Analog to Digital Converter), transmitir, e na outra ponta transformar novamente o sinal em um formato analógico (DAC – Digital to Analog Converter) para assim poder fazer isso do sinal transmitido.

VoIP funciona praticamente da mesma maneira, digitalizando a voz em pacotes de dados, trafegando pela rede e reconvertendo em voz novamente no destino. E no formato digital, o controle pode ser bem maior: podemos compactar e rotear, converter para outros formatos ainda melhores, etc.

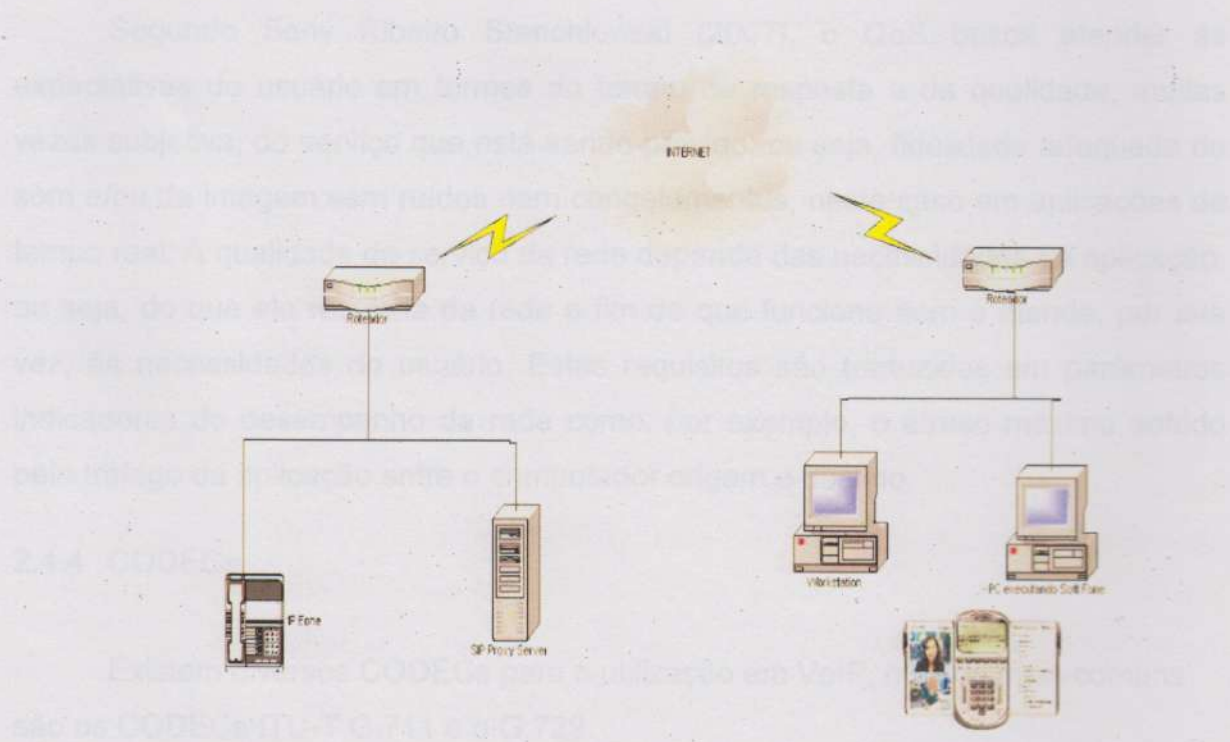


Figura 4: Cenário clássico do uso da tecnologia VoIP.
FONTE: Microsoft Brasil (2005)

2.4.1 Compressão

É o uso de algoritmos para reduzir o volume dos dados convertidos no processo de digitalização, que outrora era voz. O processo de compressão permite a diminuição do consumo de banda durante o tráfego. A relação que se deve buscar equalizar nesses algoritmos é a da “quantidade de banda vs. qualidade da voz”.

2.4.2 Supressão de silêncio

A maior parte do tempo de uma conversação é tomada pelo silêncio. Para tratar deste caso, temos algoritmos que buscam suprimir o envio de tráfego relativo a momentos de silêncio por parte do emissor, e compensar esses momentos por simulação no lado do receptor, reduzindo assim consideravelmente o volume de dados trafegados.

2.4.3 Qualidade de serviço (QoS – *Quality Of Service*)

Segundo Sony Ribeiro Stanchlewski (2007), o QoS busca atender às expectativas do usuário em termos do tempo de resposta e da qualidade, muitas vezes subjetiva, do serviço que está sendo provido, ou seja, fidelidade adequada do som e/ou da imagem sem ruídos nem congelamentos, neste caso em aplicações de tempo real. A qualidade de serviço da rede depende das necessidades da aplicação, ou seja, do que ela requisita da rede a fim de que funcione bem e atenda, por sua vez, às necessidades do usuário. Estes requisitos são traduzidos em parâmetros indicadores do desempenho da rede como, por exemplo, o atraso máximo sofrido pelo tráfego da aplicação entre o computador origem e destino.

2.4.4 CODECs

Existem diversos CODECs para a utilização em VoIP, mas os mais comuns são os CODECs ITU-T G.711 e o G.729.

2.4.5 G.711

Comprime a voz para ser transmitida em canais de 64 kbps, a mesma banda que as chamadas utilizam no sistema de telefonia tradicional. Este CODEC é o que oferece a melhor qualidade de voz atualmente, mas como utiliza uma quantidade razoável de banda, é utilizado em ambientes que disponibilizam uma grande quantidade de banda para as aplicações, como em redes locais corporativas, que

costumam ser formadas por equipamentos que fornecem 100 Mbps na porta de cada usuário.

2.4.6 G.729

Comprime a voz para ser transmitida em 8 kbps, o que otimiza bastante a utilização dos links de dados disponível, embora sacrifique um pouco a qualidade da voz. Este CODEC é o mais utilizado quando a quantidade de banda é baixa, como em links com a Internet.

3 SEGURANÇA DE VoIP EM REDE SEM FIO

A utilização da rede IP para o tráfego de voz faz com os riscos de segurança que já existem na rede IP afetem também o sistema de telefonia. Existem alguns riscos que devem ser considerados ao se implantar uma sistema VoIP.

3.1 Problemas de Segurança

3.1.1 Negação de Serviço

O ataque de explorar falhas nos equipamentos e sistemas ou simplesmente esgotar os recursos dos sistemas, como memória, processamento e banda de rede.

O ataque de negação de serviço a um sistema VoIP é fácil de ser realizado em redes que não são bem preparadas, pois por ser um tipo de aplicação em tempo real, o VoIP é particularmente sensível ao excesso de tráfego gerado por um vírus por exemplo.

3.2 Captura de chamadas

A captura de ligações telefônicas que carregam dados sensíveis e confidenciais pode acarretar grandes transtornos às empresas. Um ataque pode capturar os pacotes RTP e montá-los em um arquivo de áudio que pode ser ouvido posteriormente.

3.3 SPIT

O SPIT (SPAM na telefonia de Internet) traz para a telefonia um problema que todo usuário de e-mail conhece muito bem, o SPAM, ou seja, mensagens em massa não solicitadas

O SPAM é um problema sério para as empresas, pois consomem muitos recursos da infra-estrutura (servidores de e-mail, tráfego de rede, espaço de armazenamento nas caixas de email), Este problema se torna pior ainda quando é transferido para a telefonia onde também podem enviar mensagens de voz em massa pela rede VoIP. Este tipo de SPAM também consome muitos recursos, pois mensagens de voz costumam precisar de maior capacidade de armazenamento, e pior, consomem muito mais tempo dos usuários.

3.4 Protocolos de suporte

Um sistema de telefonia IP depende muito de outros serviços de rede para operar. Servidores DHCP são utilizados para enviar as configurações de rede para telefones IP, servidores de FTP e HTTP que guarda e envia configurações para os telefones IP, servidores DNS fornecem nomes para telefones e servidores.

Se um ataque tirar do ar o servidor de DHCP, novos telefones IP não conseguirão entrar na rede, causando assim uma negação de serviço.

Um ataque que consegue ter acesso à um servidor de FTP ou HTTP, pode modificar as configurações de todos os telefones IP, como causar o roubo de informações ou simplesmente causa uma negação de serviço em todos os telefones.

Um ataque no servidor DNS pode redirecionar as chamadas para onde quiser, ou simplesmente pode tirar o serviço de DNS do ar e causar uma negação de serviço aos usuários.

3.5 Soluções

Alguns procedimentos de segurança podem ser adotados para melhorar a confiabilidade da tecnologia VoIP.

3.5.1 Implementações de VLANs (*Virtual Local Area Networks*)

VLAN é uma rede virtual. A maioria dos switches atualmente é capaz de suportar a utilização de VLANs. Uma VLAN segrega um mesmo switch em diversas redes distintas, como se fossem redes físicas diferentes.

O tráfego de voz deve ser separado do tráfego de dados através de VLANs, e a comunicação entre as duas redes deve ser restrita e controlada. Esta abordagem evita que problemas na rede de dados afetem o tráfego de voz. Neste cenário, caso um vírus comece a se disseminar entre os computadores da rede, o alto tráfego gerado por ele não afetará muito o tráfego de voz que está em uma rede separada. A separação da rede através de VLANs também dificulta a captura do tráfego de áudio ou de sinalização.

Além de evitar que problemas na rede de dados afetem o tráfego de voz, a utilização de VLAN ajuda na implantação de mecanismos de qualidade de serviço, garantindo assim o desempenho necessário para as aplicações VoIP.

3.5.2 Criptografia

Ao criptografar o seu conteúdo, mesmo que um ataque consiga capturar os pacotes, o conteúdo dos pacotes continuará protegido.

Alguns equipamentos VoIP suportam a encriptação das mensagens utilizando o SRTP (*Secure Real-time Transport Protocol*) e o SRTCP (*Secure Realtime Transport Control Protocol*).

Para se evitar que o tráfego de voz seja capturado e utilizado por terceiros, é necessário utilizar a criptografia no tráfego de áudio, ou seja, nos pacotes RTP e RTCP. Já para evitar a manipulação dos protocolos de sinalização, a necessidade também de criptografar o tráfego de sinalização, impedindo assim a captura e modificação das mensagens de configuração de chamadas. Assim evitamos que um ataque engane os usuários enviando as chamadas feitas pelo mesmo para o lugar errado.

No caso dos equipamentos que não suportam o SRTP, pode-se encriptar o tráfego através da utilização do IPsec (*Internet Protocol Security*).

3.5.3 VPN

Virtual Private Network ou Rede Privada Virtual é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a *Internet*. (SANTOS, 2001)

O sigilo do tráfego da rede, a autenticação inicial dos usuários, a integridade das mensagens da rede sem fio serão garantidos através da implementação de uma VPN segura, para tanto se utiliza do protocolo IPSec a fim de garantir a privacidade virtual da rede e a segurança das eletrônicas que por ela passam. (CARRIÓN, 2003)

Nesta arquitetura todo o tráfego entre as estações e o AP é encriptado independente do destino dos pacotes enviados pelas estações. A VPN poderia ser configurada de forma que somente alguns pacotes com endereços de destino definidos fossem encriptados. (CARRIÓN, 2003)

"No estabelecimento de um túnel IPSec (*Internet Protocol Security*) todo o pacote IP é protegido e todas as mensagens provenientes das estações saem com o endereço do AP como endereço de destino. Garante-se com esta última característica uma privacidade maior para os usuários, dificultando a análise passiva do tráfego da rede." (CARRIÓN, 2003)

O servidor VPN pode se tornar um gargalo. Todo o acesso do cliente WLAN será canalizado pelo servidor. Os dispositivos VPN tradicionalmente atendem muitos clientes remotos de baixa velocidade. Ser solicitado a controlar a taxa de transferência de um grande número de clientes que funcionam na velocidade total da LAN significará que muitos dispositivos VPN não conseguirão atender mais de poucas dezenas ou centenas de clientes. (MICROSOFT, 2004)

4 CONCLUSÃO

A utilização das redes de pacotes comutados para o tráfego de áudio, conhecidas como VoIP, é uma tendência que está cada vez mais se firmando no mundo corporativo, bem como está sendo bastante empregado nas residências de usuários domésticos, seja através de simples programas de computador ou até equipamentos mais especializados para a telefonia, como a utilização de um telefone comum para as ligações via internet. É importante ressaltar a fundamental necessidade da aplicação da segurança para a utilização do VoIP, tendo em vista que a expansão freqüente desta tecnologia trás consigo ameaças, que devem ser combatidas com o máximo de eficácia.

Desta forma, conclui-se que a segurança sobre sistemas VoIP será cada vez mais requisitada conforme o seu crescimento e expansão, sejam elas corporativas ou domesticas.

REFERÊNCIAS

- ARTHAS, Kael. **Tutorial Wireless**. 2004. Disponível em:
<http://www.babooforum.com.br/idealbb/view.asp?topicID=269602> Acessado em: 24 Ago 2007
- DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Trabalho de Conclusão do Curso de Bacharel em Ciência da Computação. UNESP São José do Rio Preto. 2003. Disponível em:
<<http://www.apostilando.com/download.php?cod=230&categoria=Redes> > Acessado em: 18 Ago 2007.
- MICROSOFT. **Decisão sobre uma Estratégia de Rede sem Fio Protegida**. 2004. Disponível em:
<http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx>. Acessado em: 30 Set 2007.
- MICROSOFT. **Usando o 802.1X e a Criptografia Para Proteger WLANs**. Disponível em:
<http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod172.mspx> . Acessado em: 14 Set 2007
- PRADO, Eduardo. **Segurança em WLAN**. 2004. Disponível em:
http://www.wirelessbrasil.org/eduardo_prado/wifi_bible/seguranca.html . Acessado em: 30 Mai 2007
- Wireless VoIP. Disponível em:
www.planetarium.com.br/planetarium/noticias/2006/6/1151324096 Acessado em 10 Mai 2007
- Wireless. Disponível em: www.iweb.com.br/iweb/artigos.php3 acessado em 05 Mar 2007.
- Saldanha, Rodrigo de Menezes. **IEEE 802.11 – Wireless**, Disponível em:
www.gta.ufrrj.br/grad/98_2/rodrigo/trabalho.html> acessado em 15 Abr 2007.
- IEEE. Disponível em: www.ieee.org acessado em 10 Mai 2007.

Serafim, Ana Paula; Land, Sabrina. **Redes Wireless Acesso via rádio padrão IEEE 802.11**, Disponível em:
anacarol.blog.br/old/aulas/artigos_uteis/wireless_radio.pdf> acessado em 05 Mar 2007.

Stanchlewski, Sony Ribeiro. **QoS (Quality of Service)**, Disponível em:
www.dimap.ufrn.br/~glaucia/RAV/QoS-Artigo.pdf acessado em 20 Out 2007.

TEIXEIRA, Edson Rodrigues Duffles. **Tutoriais: Banda larga e VOIP**. 2005.
Disponível em: <http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp>.
Acessado em: 04 Jul 2007.

VoIP. Disponível em: pt.wikipedia.org/wiki/Voip acessado em 10 Mai 2007.
Wireless. Disponível em: pt.wikipedia.org/wiki/rede_sem_fios acessado em 10 Mai 2007

Voz sobre IP. Disponível em www.cliconnect.com/br/Artigos/VozsobreIP_pt.html
Acessado em 10 Nov 2007