UFSM

TRABALHO DE GRADUAÇÃO

SEGURANÇA EM REDES WIRELESS
PROPOSTA DE UM SERVIÇO DE AUTENTICAÇÃO BASEADO EM AGENTES – O CASO CRSPE

Aluno:

Érico Marcelo Hoff do Amaral

Orientador:

Raul Ceretta Nunes

Prof . Coorientador

Koiti Ozaki

Santa Maria, RS, Brasil

2006

SEGURANÇA EM REDES WIRELESS
UM SERVIÇO DE AUTENTICAÇÃO BASEADO EM AGENTES
O CASO CRSPE

Por

Érico Marcelo Hoff do Amaral

Trabalho de Graduação apresentado ao Curso de Graduação em Ciência da Computação – Bacharelado, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de

Bacharel em Ciência da Computação

Curso de Ciência da Computação

Trabalho de Graduação n° 200
Santa Maria, RS, Brasil
2006

Universidade Federal de Santa Maria

Centro de Tecnologia

Curso de Ciência da Computação

A Comissão Examinadora, abaixo assinada, aprova o

Trabalho de Graduação

SEGURANÇA EM REDES WIRELESS

UM SERVIÇO DE AUTENTICAÇÃO BASEADO EM AGENTES

O CASO CRSPE

Elaborado por

Érico Marcelo Hoff do Amaral

como requisito parcial para obtenção do grau de

Bacharel em Ciência da Computação

COMISSÃO EXAMINADORA

_____

Prof. Dr. Raul Ceretta Nunes
(Orientador)

_____

Profa. Dra. Roseclea Duarte Medina

_____

Profa. Dra. Iara Augustin

Santa Maria, 04 de janeiro de 2006

“Este trabalho é dedicado a toda a minha família”

Agradecimentos

Primeiro agradeço a Deus, aos meus pais pelo amor e dedicação, aos meus irmãos que sempre me apoiaram, à vó Pepa que sempre me incentivou e à Catilene por ter sido minha companheira em grande parte desse caminho. Também agradeço ao meu orientador Prof Raul Ceretta Nunes pelo voto de confiança e ao meu Co-orientador Koiti Ozaki que além de me apoiar e incentivar, me ensinou uma lição de vida. Sem esquecer de meus amigos e colegas que também contribuíram para a realização deste trabalho.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

AAA	*Authentication, Authorization and Accounting*
ACK	*Ackowledgment*
AES	*Advanced Encryption Standard*
AP	*Ponto de acesso*
ARP	*Address Resolution Protocol*
BPSK	*Binary Phase Shift Keying*
BSS	*Basic Service Set*
CCK	*Complementary Code Keying*
CCMP	*Counter Mode CBC MAC Protocol*
COFDM	*Coded OFDM*
CRC	*Cyclic Redundancy Check*
CSMA	*Carrier Sense Multiple Access*
CSMA/CA	*Carrier Sense Multiple Access/Collision Avoidance*
CSMA/CD	*Carrier Sense Multiple Access/Collision Detection*
DFS	*Dynamic Frequency Selection*
DHCP	*Dynamic Host Configuration Protocol*
DoS	*Denial of Service*
DQPSK	*Differential Bi Quadrature Phase Shift Keying*
DS	*Distribution System*
DSSS	*Direct Sequence Spread Spectrum*
EAP	*Extensible Authentication Protocol*
ESS	*Extended Service Set*
ETSI	*European Telecommunications Standards Institute*
FCC	*Federal Communication Commission*
FHSS	*Frequency Hopping Spread Spectrum*
GFSK	*Gaussian Frequency Shift Keying*
HR-DSSS	*High Rate Direct Sequence Spread Spectrum*
IBSS	*Independent Basic Service*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ISM	*Industrial Scientific and Medical*
LEAP	*Lightweight EAP*
MAC	*Media Access Control*
MIC	*Message Integrity Check*
OFDM	*Orthogonal Frequency Division Multiplexing*
PDA	*Personal Digital Assistant*
PEAP	*Protected Extensible Authentication Protocol*
PHY	*Physical Layer*
QoS	*Quality of Service*
QPSK	*Quadrature Phase Shift Keying*
RADIUS	*Remote Authentication Dial-In User Service*
RSN	*Robust Security Network*
RF	*Radio Frequency*

SSID	*Service Set Identifier*
TKIP	*Temporal Key Integrity Protocol*
TLS	*Transport Layer Security*
TTLS	*Tunneled Transport Layer Security*
VPN	*Virtual Private Network*
WDS	*Wireless Distribution System*
WECA	*Wireless Ethernet Compatibility Alliance*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	*WiFi Protected Access*

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Trabalho de Graduação
Curso de Ciência da Computação
Centro de Tecnologia
Universidade Federal de Santa Maria

SEGURANÇA EM REDES WIRELESS
UM SERVIÇO DE AUTENTICAÇÃO BASEADO EM AGENTES
O CASO CRSPE

Aluno:
Érico Marcelo Hoff do Amaral

Orientador:
Raul Ceretta Nunes

Co-orientador:

Koiti Ozaki

As redes sem fio (wireless) atualmente ocupam um lugar de destaque em termos de tecnologia de comunicação devido a aspectos como mobilidade e facilidade de implementação a um custo razoavelmente baixo. Em contra partida, a utilização de redes sem fios implica em alguns aspectos especiais em relação à segurança, tal como o controle de acesso de pessoas não autorizadas. Neste sentido, este trabalho propõe um serviço de autenticação baseado em agentes.

O laboratório do trabalho foi a rede do Centro Regional Sul de Pesquisas Espaciais (CRSPE), situada no campus da UFSM. O CRSPE já havia desenvolvido um estudo sobre os impactos na área de segurança que

a implantação de uma rede sem fio poderia causar em um ambiente de rede integrado, concluindo que os principais aspectos em relação a segurança que deveriam ser observados neste tipo de rede são: limites físicos definidos, meio controlável e controle de acesso.

O trabalho de implementação de um ambiente seguro para a rede sem fio do CRSPE teve como ponto de partida a elaboração de um adendo a política de segurança deste, onde foram incluídas regras especificas para a utilização da rede sem fio da instituição. Além disto, o padrão 802.11 foi estudado e analisado em relação às suas vulnerabilidades, riscos, segurança e alguns métodos de autenticação foram avaliados. Como conseqüência dos estudos e compreensão da rede do CRSPE, este trabalho descreve a modelagem e implementação de um serviço de autenticação de usuários que usa ferramentas úteis para o gerenciamento, monitoramento e controle do tráfego de informação na rede, tal como o servidor RADIUS que serve de meio de acesso à rede sem fio. Como resultado a solução proposta permite múltiplos acessos ao ambiente sem fio do CRSPE com um nível satisfatório de segurança.

1. INTRODUÇÃO

O CENTRO REGIONAL SUL DE PESQUISAS ESPACIAIS – CRSPE/MCT, que está localizado na cidade de Santa Maria - RS, têm por finalidade a pesquisa e desenvolvimento científico-tecnológico das atividades espaciais. O CRSPE promove as atividades de ciência e tecnologia espaciais através da formação de recursos humanos, realização de pesquisas, criação de novas tecnologias, execução de serviços de aplicações espaciais e ampliação da cooperação espacial com os países do MERCOSUL e países associados [1].

O projeto da rede fixa de computadores do CRSPE foi implementado com base em um sistema de cabeamento estruturado e na tecnologia Ethernet Gigabit, visando disponibilizar uma infra-estrutura única para o fluxo de informações. A rede suporta a evolução e flexibilidade de uma rede de telecomunicações agregando QoS (*Quality of service*), com o intuito de permitir aos integrantes deste centro terem acesso a uma ferramenta para o desenvolvimento de suas pesquisas.

Baseadas na sua importância e complexidade, a rede do CRSPE foi complementada com um método de transmissão de informações por radio freqüência que permite a mobilidade dos usuários deste sistema, garantindo um ambiente de alto desempenho com um nível adequado de consistência e satisfatório de segurança. A rede sem fio, apesar das conhecidas vulnerabilidades, está integrada à uma estrutura física de rede cabeada de alta capacidade e disponibilidade e viabiliza alterações, manutenções e implementações de forma rápida e controlada. O projeto da rede sem fio satisfaz os requisitos obrigatórios da rede cabeada já instalada.

Este trabalho se propõe a realizar um estudo detalhado sobre a utilização da tecnologia sem fio no CRSPE e sobre os aspectos relacionados à segurança deste padrão. Como resultado foi desenvolvido

uma política de segurança adequada para a rede wireless, a qual converge com a gestão de segurança do CRSPE, assim como foi especificado um serviço de autenticação baseado em agentes usado em sintonia como padrão IEEE 802.1x, que é um padrão definido para protocolos de autenticação em redes guiadas. Como resultado a solução proposta permite múltiplos acessos ao ambiente da rede sem fio do CRSPE com um nível satisfatório de segurança.

1.1. O SISTEMA DE CABEAMENTO ESTRUTURADO DO CRSPE

O conceito de cabeamento estruturado consiste de um conjunto de produtos de conectividade empregado de acordo com regras especificas de engenharia que visam obter uma arquitetura aberta, com meios de transmissão e disposição física padronizados, com projeto e instalação padronizados respeitando padrões internacionais. Este sistema integra diversos meios de transmissão, que suportam múltiplas aplicações, incluindo voz, vídeo, dados, sinalização e controle [2].

Com base em um conjunto de especificações que garantem uma implantação modular e com capacidade de expansão programada, os produtos utilizados na construção da rede do CRSPE asseguram a conectividade máxima para os dispositivos existentes hoje no mercado e tem a infra-estrutura preparada para conviver com outras tecnologias emergentes, como é o caso do tema deste estudo que são as redes sem fio.

O Sistema de Cabeamento Estruturado do prédio do CRSPE foi desenvolvido respeitando o padrão EIA/TIA 568A [03] e com facilidade de diagnóstico de problemas e gerência de mudanças na rede.

1.2. AS REDES SEM FIO E O CRSPE

As redes locais sem fio (Wireless LAN - WLAN) tem sido muito utilizadas em diversas áreas e aplicações. Através dos esforços do IEEE (*Institute of Electrical and Electronics Engineers*) e dos esforços de certificação da WECA (Wireless Ethernet Compatibility Alliance), as redes sem fio estão deixando de ser uma alternativa para se tornarem a principal opção visando a garantia de conectar todos os usuários da rede onde o cabeamento estruturado se torna inviável. Atualmente, pode-se encontrar WLAN em casas, escritórios, chãos de fábricas, hotéis e centros de convenção, além de aeroportos e lojas. Os pontos de acessos (pontos de conexão para as redes sem fio) tem sido utilizados na conexão de todos os tipos de equipamentos móveis, tais como: notebooks, computadores de mão e telefones.

As primeiras redes sem fio apresentavam um conjunto de problemas: eram muito caras e lentas, tinham uma série de problemas de interferências e eram baseadas em tecnologias proprietárias. Dois eventos caracterizam a difusão das redes sem fio. Os problemas técnicos de incompatibilidade e gerenciamento do espectro foram resolvidos e a utilização de notebooks e computadores de mão se multiplicou. Antes de 1998, instalar uma rede sem fio significava uso de uma ou mais soluções proprietárias. As conexões eram feitas através de redes pouco confiáveis, com baixas taxas de transmissão e a com um mínimo de segurança. O resultado do esforço de padronização levou a criação dos padrões HiperLAN/2, IEEE 802.11 [22] e Bluetooth [33]. Esse esforço de especificação assegurou que todos os equipamentos pudessem se comunicar utilizando os mesmos protocolos e interfaces de comunicação.

A rede do CRSPE é uma proposta de ambiente de alto desempenho, desenvolvido para a realização de suas atividades de pesquisa. A utilização da rede sem fio converge com esta proposta. Permite que todos seus

integrantes e pesquisadores que utilizem dispositivos móveis possam circular na área do prédio tendo acesso aos serviços da rede.

2. AS TECNOLOGIAS DE REDES SEM FIO

Neste capitulo são abordados alguns sistemas utilizados para transmissão de dados, utilizando a tecnologia sem fio, e também é descrito o padrão IEEE 802.11x, mostrando as principais características deste modelo.

2.1. PADRÕES DE REDES SEM FIO MAIS USADOS

Há várias tecnologias envolvidas nas redes locais sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens. A seguir, são apresentadas algumas das mais empregadas.

2.1.1. SISTEMAS NARROWBAND

Os sistemas narrowband [35] (banda estreita) operam numa freqüência de rádio específica mantendo o sinal de rádio o mais estreito possível, mas o suficiente para passar as informações. A interferência indesejável entre os vários canais de comunicação pode ser evitada coordenando cuidadosamente os diferentes usuários nos diferentes canais de freqüência.

2.1.2. SISTEMAS SPREAD SPECTRUM

Os sistemas Spread Spectrum [35] são os mais utilizados atualmente. Utilizam a técnica de espalhamento espectral com sinais de rádio freqüência de banda larga, provendo maior segurança, integridade e confiabilidade, em troca de um maior consumo de banda. Há dois tipos de tecnologias spread spectrum: a FHSS (*Frequency-Hopping Spreap Spectrum*) e a DSSS (*Direct-Sequence Spread Spectrum*).

? **A FHSS** usa uma portadora de faixa estreita que muda a freqüência em um código conhecido pelo transmissor e pelo receptor que, quando devidamente sincronizados, o efeito é a manutenção de um único canal lógico. Este modelo utiliza uma banda de 2,4 GHz, a qual é dividida em 75 canais por onde as informações são transmitidas em uma seqüência pseudo-aleatória, em que a freqüência de transmissão dentro da faixa vai sendo alterada em saltos. Com essa técnica limita-se a transmissão a uma taxa de 2 Mbits.

? **A DSSS**, utilizado no padrão 802.11b, o DSSS utiliza a técnica denominada *Code chips* que gera um bit-code (também chamado de *chipping code*) redundante para cada bit transmitido. Quanto maior o chip maior será a probabilidade de recuperação da informação original. Contudo, uma maior banda é requerida. Mesmo que um ou mais bits no chip sejam danificados durante a transmissão, técnicas estatísticas embutidas no rádio são capazes de recuperar os dados originais sem a necessidade de retransmissão. O DSSS trabalha em uma banda de 2,4 GHz, que é dividida em três canais, característica que o torna mais suscetível a ataques e a ruídos, o que pode diminuir a banda utilizada.

2.1.3. SISTEMAS INFRARED

Para transmitir dados, os sistemas infravermelhos utilizam freqüências muito altas, um pouco abaixo da luz visível no espectro eletromagnético. Igualmente a luz, o sinal infravermelho não pode penetrar em objetos opacos. Assim as transmissões por infravermelho ou são diretas ou difusas. Os sistemas infravermelho diretos de baixo custo fornecem uma distância muito limitada (em torno de 1,5 metros). São comumente utilizados em PAN (*Personal Area Network*) como, por exemplo, os palm pilots e ocasionalmente são utilizados em WLANs.

2.2. O PADRÃO IEEE 802.11x

O grupo de trabalho IEEE 802.11, do Instituto dos Engenheiros Elétricos e Eletrônicos, é responsável pela definição do padrão para as redes locais sem fio, as WLANs. O padrão proposto especifica três camadas físicas (PHY) e apenas uma subcamada MAC (*Medium Access Control*). Como apresentado abaixo, o *draft* provê duas especificações de camadas físicas com opção para rádio, operando na faixa de 2.400 a 2.483,5 MHz (dependendo da regulamentação de cada país), e uma especificação com opção para infravermelho.

- **Frequency Hopping Spread Spectrum Radio PHY:** esta camada fornece operação 1 Mbps, com 2 Mbps opcional. A versão de 1 Mbps utiliza 2 níveis da modulação GFSK (*Gaussian Frequency Shift Keying*), e a de 2 Mbps utiliza 4 níveis da mesma modulação;
- **Direct Sequence Spread Spectrum Radio PHY:** esta camada provê operação em ambas as velocidades (1 e 2 Mbps). A versão de 1 Mbps utiliza da modulação DBPSK (*Differential Binary Phase Shift Keying*), enquanto que a de 2 Mbps usa modulação DBPSK (*Differential Quadrature Phase Shift Keying*);
- **Infrared PHY:** esta camada fornece operação 1 Mbps, com 2 Mbps opcional. A versão de 1 Mbps usa modulação 16-PPM (*Pulse Position Modulation* com 16 posições), e a versão de 2 Mbps utiliza modulação 4-PPM.

A figura 2.3. demonstra o padrão proposto pelo IEEE para as camadas do modelo OSI, com a divisão em três camadas físicas.

Figura 2.3: Modelo OSI para comunicação Wireless. [17]

No lado da estação, a subcamada MAC fornece os seguintes serviços: autenticação, privacidade e transmissão da MADU (*MAC Sublayer Data Unit*), e no lado do sistema de distribuição: associação, dissociação, distribuição e integração. As estações podem operar em três situações distintas:

? Ad Hoc [6] [7], onde existem somente estações sem fio que se comunicam mutuamente, sem a presença de ponto de acessos. Todas as estações possuem o mesmo BSSID (*Basic Sevice Set Identifier*) que corresponde ao identificador da célula sem fio. O termo próprio do 802.11 para esta rede é IBSS (*Independent Basic Service Set*). Este tipo de configuração pode ser comparada às conexões ponto-a-ponto em redes cabeadas.

? Modo de infra-estrutura básica [7], onde as estações sem fio se comunicam com um simples AP. Este ponto de acesso pode funcionar como um bridge(ponte) entre a rede sem fio e a rede guiada. O termo utilizado para este tipo de rede é BSS (*Basic Service Set*).

? Modo infra-estruturado [6][7], onde redes distintas (com BSSIDs diferentes em cada uma) se comunicam através de APs criando uma única rede. Este modo tem como objetivo fazer com que o usuário possa mudar seu ponto de acesso e mesmo assim permanecer conectado. O termo mais utilizado para este modo de rede é ESS (*Extended Service Set*).

Os padrões e grupos são mantidos pelo IEEE relacionados com WLANs [4] e estão descritos no quadro abaixo:

Padrão	*Descrição*
IEEE 802.11	**O padrão original, 1 Mbit/s e 2 Mbit/s, 2.4 GHz RF and IR standard**
IEEE 802.11a	54 Mbit/s, 5 GHz padrão (*1999, shipping products in 2001*)
IEEE 802.11b	**Desenvolvido para suportar taxas de transmissão de 5.5 e 11 Mbit/s (1999)**
IEEE 802.11d	Internacional (inter paises) – para extensões em novo países
IEEE 802.11e	Implementando QoS
IEEE 802.11F	Inter-Access Point Protocol (IAPP)
IEEE 802.11g	**Opera a taxas de 54 Mbit/s, 2.4 GHz padrão (compatível com b) (2003)**
IEEE 802.11h	5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) e Transmit Power Protocol (TPC) para compatibilidade com padrão Europeu.
IEEE 802.11i	**Ratificado em junho de 2004 – Implementação de Segurança**
IEEE 802.11j	Extensões para o padrão japonês
IEEE 802.11k	Medidas de recursos de radio
IEEE 802.11n	Grande melhoria de throughput
IEEE 802.11p	WAVE - Wireless Access for the Vehicular Environment
IEEE 802.11r	Fast roaming
IEEE 802.11s	Wireless mesh networking
IEEE 802.11T	Wireless Performance Prediction (WPP) – Teste de métodos e métricas
IEEE 802.11u	Interoperabilidade com redes não 802 (ex. rede celular)
IEEE 802.11v	Gerenciamento de redes wireless

Descrição detalhada sobre os adendos ao padrão IEEE 802.11:

? IEEE 802.11a é o equivalente Fast-Ethernet do padrão IEEE 802.11b. Ela especifica uma rede cinco vezes mais rápida do que o 802.11b. É desenhada para operar numa banda de freqüência de 5-GHz-UNII (*Unlicensed National Information Infrastructure*). A potência máxima especificada é de 50mW para produtos operando em 5,15-GHz até 5,25-GHz, 250mW para produtos operando em 5,25-GHz até 5,35-GHz e de 800mW para 5,725-GHz até 5,82-GHz (tipicamente para aplicações em áreas abertas). Diferente dos padrões IEEE 802.11b/g, o 802.11a não usa o padrão DSSS. Ao contrário, utiliza o OFDM que opera mais facilmente em ambientes de escritórios.

? IEEE 802.11b é especificado para operar em 2,4-GHz utilizando a banda ISM (*Industrial, Scientific and Medical band*). Os canais de rádio freqüência usam a modulação permitido altas taxas de velocidade em

distâncias de até 50 metros em escritórios. O padrão permite taxas de transferência de até 11-Mbps, que são até cinco vezes maiores do que a especificação original do IEEE 802.11 e próxima ao padrão Ethernet. Tipicamente, o padrão IEEE 802.11b é utilizado em pequenos escritórios, em hospitais, em depósitos e em chãos de fábricas. É utilizado principalmente em grandes campi para prover conectividade em salas de conferências, áreas de trabalhos, e qualquer outro ambiente inconveniente ou perigoso para se instalar cabos, ou em qualquer ambiente onde exista a necessidade de mobilidade será aceitável a instalação de rede sem fios.

? IEEE 802.11g prevê a especificação do MAC (*Médium Access Control*) e da camada física (PHY). A camada física será uma extensão do IEEE 802.11b com uma taxa de transmissão de 54-Mbps usando a modulação OFDM (*Orthogonal Frequency Division Multiplexing*). A especificação IEEE 802.11g é compatível com a especificação IEEE 802.11b. Usando um protocolo estendido, o 802.11g permite o uso misto da rede. Esta característica de uso misto permite que equipamentos que usam o 802.11b operando em 11-Mbps possam compartilhar a mesma rede com os novos equipamentos operando em 54-Mbps. Isso permitirá a migração sem impacto das redes de 11-Mbps para as redes de 54-Mbps. Esta especificação para WLANs é a utilizada no prédio do CRSPE.

? IEEE 802.11d foi desenvolvido para áreas fora dos chamados cinco grandes domínios reguladores (EUA, Canadá, Europa, Japão e Austrália). O 802.11d têm um frame estendido que incluem campos com informações dos países, parâmetros de freqüência e tabelas com parâmetros.

? IEEE 802.11e o Task Group criado para desenvolver o padrão 802.11e inicialmente tinha o objetivo de desenvolver os aspectos de

segurança e QoS para a sub-camada MAC. Mais tarde as questões de segurança foram atribuídas ao Task Group 802.11i, ficando o 802.11e responsável por desenvolver os aspectos de QoS. O QoS deve ser adicionado as redes WLANs para me permitir o uso VoIP. Também será requerido para o ambiente doméstico, onde deverá suportar voz, vídeo e dados.

? IEEE 802.11f especifica a subcamada MAC e a camada física para as WLANs e define os princípios básicos da arquitetura da rede, incluído os conceitos de ponto de acessos e dos sistemas distribuídos. O IEEE 802.11f está definindo as recomendações práticas, mais que os padrões. Estas recomendações descrevem os serviços dos pontos de acessos (SAP), as primitivas, o conjunto de funções e os protocolos que deverão ser compartilhados pelos múltiplos fornecedores para operarem em rede.

? IEEE 802.11h: desenvolvido na Europa, os radares e satélites usam a banda de 5-GHz, a mesma utilizada pelo padrão IEEE 802.11a. Isto significa que podem existir interferências com radares e satélites. O padrão 802.11h adiciona uma função de seleção dinâmica de freqüência DFS (*Dynamic Frequency Selection*) e um controle de potência de transmissão TPC (*Transmit Power Control*) para o padrão 802.11a.

? IEEE 802.11i é o Task Group criado para melhorar as funções de segurança do protocolo 802.11 MAC, que agora é conhecido como ESN (*Enhanced Security Network*). O ESN tem por objetivo unificar todos os esforços para melhorar a segurança das WLANs. Sua visão consiste em desenvolver um modelo denominado RSN (*Robust Security Network*), que tem por finalidade garantir um meio mais seguro para as comunicações sem fio, para isto os seguintes protocolos foram avaliados: WEP (*Wired*

Equivalent Protocol), TKIP (*Temporal Key Integrity Protocol*), AES (*Advanced Encryption Standard*), IEEE 802.1x para autenticação e criptografia. Percebendo que o algoritmo RC4 não é robusto o suficiente para as futuras necessidades, o grupo de trabalho 802.11i está trabalhando na integração do algoritmo de criptografia AES dentro da subcamada MAC. O AES esta vinculado ao WPA2 (*Wi-Fi Protected Access*), e segue o padrão do DES (*Data Encryption Standard*). Tanto o DES como o AES usam criptografia por blocos. Diferente do DES, o AES pode exceder as chaves de 1024 bits, reduzindo as possibilidades de ataques.

Um modelo interessante e não descrito pelo IEEE é o HiperLAN/2, desenvolvido pelo Instituto Europeu de Padrões de Telecomunicações ETSI (*European Telecommunications Standards Institute*), o HiperLAN/2 é uma especificação de wireless LAN para operar até 54-Mbps, que pode ser utilizada em várias redes, incluindo as redes 3G, redes ATM e redes baseadas em IP. O padrão prevê o uso de dados, voz e vídeo. A especificação inclui o QoS, fundamental para o transporte em redes determinísticas. Similar ao 802.11a o HiperLAN/2 opera em 5-GHz utilizando a modulação OFDM. Sua subcamada MAC é diferente do padrão 802.11a.

2.2.1. A CAMADA MAC E SEUS SERVIÇOS

A camada MAC do protocolo para redes sem fio oferece três serviços básicos:

- Serviço de dados assíncronos, que permitem dispositivos na rede trocar chamados MSDUs (*MAC service data units*). Mas contudo não garantem a entrega deste chamado;

- **Serviço de segurança**, que implementa a segurança em um ambiente de rede sem fio por meio de métodos de criptografia dos MSDUs, com a utilização do WEP.

- **Serviço de ordenação**, quando verificado que a entrega em ordem dos MSDUs tem mais probabilidades de sucesso este serviço se encarrega de reordená-los.

2.2.2. FORMATO DOS FRAMES EM UMA TRANSMISSÃO SEM FIO

Em uma rede sem fio o frame é constituído por um cabeçalho, pelo corpo do frame e a seqüência de verificação do frame. O cabeçalho carrega informações como a duração, o endereço e controle de seqüência. O corpo do frame carrega as informações específicas sobre o que o frame transporta e por fim a seqüência de verificação que é um algoritmo de validação dos dados que formam o frame, este baseado no CRC (código de redundância cíclica).

3. SEGURANÇA DO PADRÃO 802.11x

A ratificação do padrão IEEE 802.11 deu-se em um período de grande desenvolvimento das redes sem fio devido às características de mobilidade e facilidade de migração das redes guiadas para esta tecnologia. A deficiência inerente a segurança identificada nestas redes não garantiram o aumento esperado de clientes em ambientes sem fio. As vulnerabilidades e riscos encontrados nestes ambientes de rede rapidamente difundiram-se, tornando-a pouco atrativa. A seguir serão descritas as vulnerabilidades e riscos de ataques atualmente identificados em redes sem fio, como também algumas soluções de segurança.

3.1. VULNERABILIDADES

As vulnerabilidades podem trazer grandes problemas à rede como um todo. As grandes vulnerabilidades em evidência hoje dizem respeito a criptografia WEP e as formas de autenticação permitidas (acesso e "beacon frame").

3.1.1. VULNERABILIDADE WEP

Diz respeito à implementação do protocolo WEP, que utiliza criptografia padrão RC4, que sabidamente possui algumas vulnerabilidades devido à forma de implementação utilizada. A criptografia RC4 é simétrica, ou seja, a mesma chave utilizada para a criptografia também é utilizada para a decriptografia, além de utilizar um vetor de iniciação fraco, de apenas 24 bits. Este padrão criptográfico também utiliza uma cifra conhecida como Stream Cipher que faz com que cada mensagem seja criptografada com uma chave diferente. Isto é possível, pois é inserido um

elemento adicional à chave criptográfica. Outra vulnerabilidade detectada neste protocolo diz respeito ao compartilhamento da chave de criptografia entre os equipamentos na rede, o que permite aplicações que capturam pacotes, identificar e se apossar desta chave.

3.1.2. VULNERABILIDADE DE ACESSO

As conexões em redes sem fio, realizam-se por meio dos pontos de acessos, que podem permitir a validação de usuários sem qualquer tipo de autenticação. Este tipo de acesso permite que qualquer dispositivo que tenha o identificador da rede chamado SSID, seja autorizado a utilizar a WLAN em questão. Apesar de garantir a facilidade de conexão entre um cliente e um ponto de acesso, esta forma de autenticação faz com que seja feito o broadcast na rede sem fio, ou seja, os pacotes chegam a todos os outros dispositivos. A forma de autenticação provida no caso de autenticação por chave compartilhada não suporta autenticação mútua, visto que, a autenticação no protocolo ocorre através das chaves WEP, que são chaves únicas para todos os clientes.

3.1.3. VULNERABILIDADE "BEACON FRAMES"

Devidamente especificado no protocolo 802.11, um beacon frame é um frame de sinalização e sincronismo, atuando como anúncios que transmitem informações importantes a respeito do funcionamento da rede sem fio a todos dispositivos que estejam no alcance da rede. Pontos de acessos a princípio são configurados de maneira a enviar beacon frames no canal em que atuam e nos canais subseqüente e antecessor. Estes "anúncios" geralmente contem o SSID da rede, o que caracteriza uma vulnerabilidade do ambiente, pois estes pacotes podem ser filtrados por

aplicações maliciosas, o que na maioria das vezes representa um grande risco de segurança as informações da instituição.

3.2. RISCOS E ATAQUES

São dois os tipos considerados de riscos inerentes às redes sem fio: os riscos internos e externos. Os riscos internos são relacionados usualmente à má configuração de dispositivos, configurações inseguras ou associação acidental. Os riscos externos são aqueles que expõe quase que diretamente as vulnerabilidades do ambiente de rede e serão citados são a seguir.

3.2.1. ASSOCIAÇÃO MALICIOSA

Tipo de ataque que ocorre quando um atacante configura algum equipamento simulando um ponto de acesso, dando a ilusão ao outro sistema de que está se conectando à uma rede sem fio real. Os passos a seguir demonstram as etapas da conexão de um dispositivo móvel a um ponto simulado:

1. O dispositivo faz uma solicitação Request à procura de um ponto para conexão;

2. O atacante responde à requisição utilizando um software do tipo “HostAp”;

3. O dispositivo associa-se ao falso ponto de acesso;

4. O falso ponto de acesso envia informações necessárias para a navegação na rede;

5. O ponto de acesso faz uma requisição de identificação, tipo login;

6. O cliente responde com seu login e senha;

Ao terminar esta seção, o falso ponto de acesso coletou informações suficientes para realizar um acesso à rede sem fio.

3.2.2. MAC SPOOFING

Em algumas redes sem fio são configuradas as permissões de conexão ao ambiente da rede por meio de listas de acesso. Um tipo de permissão pode ser através do endereço MAC da placa de comunicação do dispositivo, onde os dispositivos com endereços MAC que não estejam cadastrados, não teriam autorização de acesso à rede sem fio. Um dos possíveis ataques pode ocorrer através da utilização por um atacante, de um endereço MAC válido de um dispositivo de um usuário previamente autorizado. Geralmente técnicas como *Eavesdrooping & Espionage*, métodos de engenharia social, são utilizadas neste tipo de ataque.

3.2.3. ARP POISONING

É conhecido como envenenamento do protocolo de resolução de endereços ARP (*Address Resolution Protocol*), onde a violação ocorre quando o atacante está conectado na mesma rede local alvo. É um ataque direcionado à camada de enlace de dados que afeta apenas redes conectadas por switches, hubs e bridges. Este é um tipo de ataque utilizado não apenas em redes sem fio mas também em redes cabeadas. O atacante utiliza pacotes ARP replay, enviando estes pacotes a dois alvos distintos na rede. Os alvos acreditam que receberam pacotes de requisição do tipo *ARP request* verdadeiros, e a partir deste momento os pacotes enviados entre os

dois alvos necessariamente passam pelo dispositivo do atacante, onde são capturados e reenviados.

3.2.4. WARDRIVING

É o modo de ataque do tipo vigilância e utiliza uma técnica que fica monitorando dispositivos desprotegidos conectados à rede sem fio, descobrindo maneiras para posterior invasão. Utilizam softwares públicos, como o *ethereal,* que podem ser configurados para encontrarem todas as redes sem fio no perímetro coberto por seu dispositivo. Este ataque vislumbra mapear com a utilização de GPS *Global Position System,* todos os pontos de acesso dispostos na rede, para invadir e monitorar o tráfego da rede.

3.2.5. WARCHALKING

É o tipo de ataque que utiliza técnicas de *wardriving,* onde o objetivo é identificar redes vulneráveis através de pichação de muros e calçadas com símbolos pré-definidos. Como mostra a figura 3.2.5, os símbolos tem os seguintes significados:

- Semicírculos, um de costas para o outro: Uma rede acessível, “aberta”;
- Símbolo fechado: No local onde foi desenhado encontra-se uma rede fechada;
- Símbolo círculo com um W dentro: A rede utiliza criptografia WEP;
- SSID encontra-se na parte superior e a largura da banda é mostrada abaixo dele;

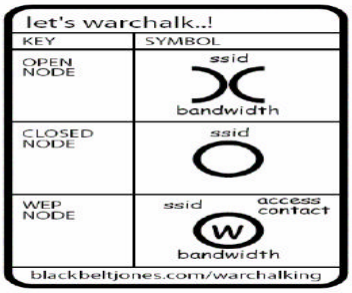

Figura 3.2.5. Símbolos de Ataque Warchalking [24].

3.2.6. D.o.S.

Ataques do tipo D.o.S. (*Denial of Service*) procuram indisponibilizar recursos ou serviços em uma rede. Geralmente utilizam técnicas de inundação de conexões da rede, com pedidos de dissociação, onde o atacante assume a identidade de um ponto de acesso, e solicita que os dispositivos desconectem e voltem a logar-se novamente na rede. A negação de serviços em redes sem fio também pode ser alcançada com a utilização de dispositivos que usem a mesma freqüência de comunicação destas, causando assim ruídos e a indisponibilidade na comunicação.

3.3. MECANISMOS DE SEGURANÇA

O padrão IEEE 802.11 inicialmente estabelece três mecanismos agregados para prover segurança em um ambiente móvel.

3.3.1. SSID

O SSID (*Service Set IDentifier*) é um método de autenticação. Configurado nos AP, funciona com uma senha simples. Para conectar-se com a rede sem fio os usuários precisam digitar uma senha. Permite segmentar uma rede em várias sub-redes, por meio das chaves de identificação.

3.3.2. FILTRAGEM DE ENDEREÇOS MAC

Outro método de autenticação de clientes é configurar cada AP com a lista dos endereços MAC dos dispositivos que podem associar-se ao AP. Esta prática necessita de uma gestão cuidadosa de cada AP. Este modelo de autenticação é considerado fraco, pois é praticável apenas para redes pequenas. Além disto apresenta o problema de que os endereços MAC de alguns dispositivos poderem ser simulados (*spoofed*).

3.3.3. WEP

O WEP (*Wired Equivalent Privacy*) é um mecanismo de confidencialidade, baseado em encriptação simétrica, que usa o RC4. Utilizando chaves estáticas de 40 e 104 bits, concatenadas com um vetor de inicialização de 24 bits, onde a chave de reconhecimento deve ser configurada no AP e no cliente. A norma 802.11 não define uma forma de distribuição especifica de chaves. Este método apresenta várias falhas já documentadas, tais como: chaves pequenas e estáticas que levam a uma relativa vulnerabilidade; não especifica mecanismo de distribuição e gestão de chaves; o vetor de inicialização é pequeno e transmitido em claro sem criptografia; e não garante a integridade da informação.

3.4. CONTROLE DE ACESSO E AUTENTICAÇÃO

A autenticação deve ser mútua, permitindo que os equipamentos que acessam a rede, autentiquem os pontos de acessos e sejam autenticados pelos mesmos. 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. Este modelo deve garantir que apenas estações autorizadas possam ter acesso à rede, dificultar que um interceptador casual compreenda o tráfego capturado e certificar que os dados que transitam na rede não serão adulterados.

3.4.1. AUTENTICAÇÃO ABERTA (*OPEN SYSTEM AUTHENTICATION*)

Neste mecanismo de autenticação, a estação pode associar-se com qualquer ponto de acesso e escutar todos os dados que estão circulando sem criptografia pela rede. O modelo de autenticação aberta se baseia na transmissão da identidade do dispositivo que quer se autenticar ao autenticador. Este é o método de autenticação padrão 802.11. O sistema autentica qualquer estação que solicite acesso a rede. Do ponto de vista de segurança este processo é muito ineficiente.

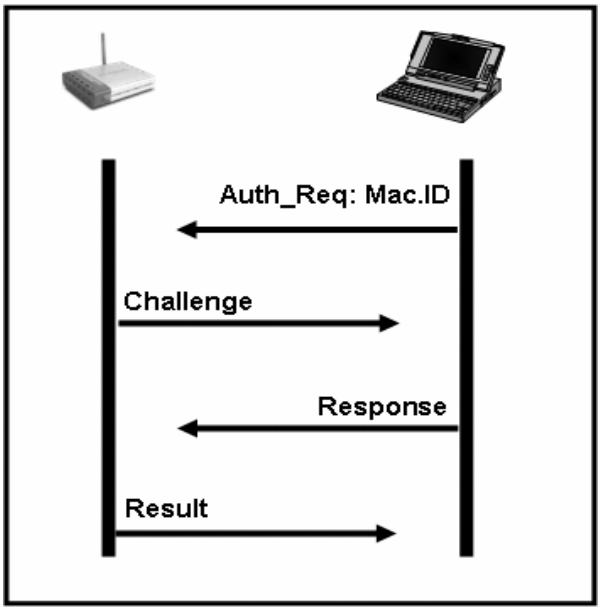

Figura 3.4.1. Requisição de autenticação no modelo aberto.

3.4.2. AUTENTICAÇÃO COMPARTILHADA (*SHARED AUTHENTICATION*)

Modelo de autenticação que utiliza uma chave secreta compartilhada e um método conhecido como desafio-resposta. O dispositivo que deseja autenticar-se envia um quadro contendo a requisição de autenticação, o ponto de acesso retorna um quadro com a resposta da autenticação, contendo um campo de 128 octetos de texto. Esse texto é o desafio gerado pelo PRNG (*pseudo random number generator*), juntamente com a chave compartilhada e o vetor de inicialização. O dispositivo de posse do desafio, copia este para um novo frame de gerenciamento. Este frame é encriptado e enviado novamente ao ponto de acesso. O ponto acesso decripta o conteúdo do frame e verifica a validade do texto, se é valido o processo é novamente repetido invertendo as posições, com o dispositivo validando o ponto de acesso. Após a validação mutua o dispositivo fica apto a acessar os recursos da rede.

3.4.3. LISTAS DE CONTROLE DE ACESSO

Autenticação baseada em listas de acesso, que são criadas com os endereços MAC dos dispositivos autorizados na rede, este modelo de segurança permite que apenas os equipamentos com seus MAC cadastrados na lista consigam se conectar ao ambiente sem fio. Este tipo de restrição é útil, mas existem inúmeras técnicas de MAC spoofing para burlar esse tipo de proteção.

3.5. O PADRÃO 802.11i

As últimas soluções integradas ao processo de normalização da tecnologia sem fio pelo IEEE estão incluídas no modelo 802.11i. As

medidas descritas nesta normalização solucionam alguns problemas detectados no modelo 802.11 e tornam as conexões sem fio mais robustas, método denominado RSN (*Robust Secure Network*). Este novo protocolo encapsula dois novos mecanismos para segurança baseado em criptografia, o TKIP e o CCMP, que devem ser utilizados em conjunto. A figura abaixo demonstra o padrão de segurança oferecido pelo padrão 802.11i. A seta ao lado direito demonstra os níveis de segurança alcançados com as alterações dos métodos de autenticação e criptografia.

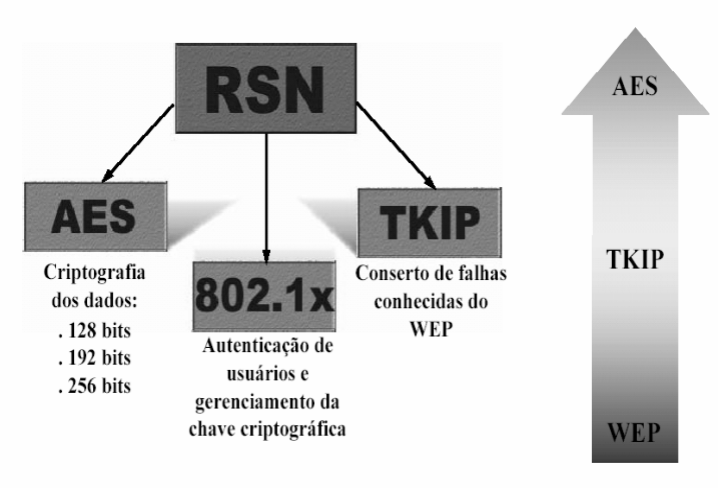

Figura 3.5. IEEE 802.11i – Segurança

3.5.1. TKIP

O *Temporal Key Interchange Protocol* (TKIP), protocolo que utiliza o RC4 como suporte de criptografia, permite que as mudanças de chaves ocorram frame a frame e sincronizadas automaticamente entre o ponto de acesso e o dispositivo. O chaveamento global trabalha anunciando as novas chaves aos usuários, e o TKIP determina que chaves de encriptação serão usadas e se responsabiliza em mudar a chave de cada frame. 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 – que descreve a seqüência de pacotes.

A integridade do conteúdo dos frames transmitidos através do TKIP é garantida por meio do MIC (*Message Integrity Check*), que é um campo próprio do frame, calculado utilizando criptografia chaveada a partir de uma função hash chaveada, que gera uma saída de 64 bits. O TKIP é uma solução desenvolvida de forma a permitir a atualização de sistemas baseados no WEP. Suporta simultaneamente equipamento baseado em WEP e em TKIP.

3.5.2. CCMP

O CCMP (*Counter Mode-CBC MAC Protocol*) protocolo que utiliza uma combinação de dois modos de operação, o CBCCTR (*Cipher Block Chaining Counter mode*) e o CBC-MAC (*Cipher Block Chaining Message*), além do AES (*Advanced Encryption Standard*) como suporte de criptografia. O AES trabalha em diferentes modos de operação que alteram a forma de como o processo de criptografia é realizado. Esta é denominada a solução final de segurança em redes sem fio do processo de normalização.

3.5.3. LEAP

Padrão proprietário da *Cisco Systems*, que se baseia principalmente em senhas para autenticar os usuários em um rede sem fio. Este modelo apenas autentica o cliente e não o dispositivo. Esta apresenta algumas restrições relacionadas a configuração, manutenção da própria identificação

do cliente, e vulnerabilidades a ataques. Além de ser uma solução proprietária que funciona apenas em hardwares da Cisco.

3.5.4. WPA e WPA2

O *Wi-Fi Protected Access* 2 (WPA2) é baseado na norma IEEE 802.11i; oferece um mecanismo de encriptação utilizando o Protocolo AES-CCMP (*Advanced Encryption Standard -Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*). O que garante o nível de privacidade de dados exigido por muitas instituições financeiras e governamentais. Por outro lado, o WPA2 oferece um conjunto de códigos e suporte para voz sem fios mais atualizado, prevenindo o tempo de espera e as interrupções no sinal de voz durante a navegação. O WPA2 pode funcionar em dois modos: *WPA2-enterrprise* e *WPA2-personal.* O modo *WPA2-enterprise* inclui todo o conjunto de requisitos WPA2 e suporte para autenticação 802.1 x/baseada em EAP; por seu lado, o modo *WPA2-personal* é essencialmente desenvolvido para utilização doméstica ou em pequenas empresas que requerem esquemas de gestão de chaves menos complexos. O WPA2 é totalmente compatível com o WPA (*Wi-Fi Protected Access*).

O WPA é, em muitos aspectos, semelhante ao WPA2. No entanto, a principal diferença entre o WPA e o WPA2 é o tipo de encriptação utilizada: RC4/TKIP para WPA e AES-CCMP para WPA2. Tanto o WPA como o WPA2 derivam da norma 802.11i, sendo que o WPA2 é a versão mais recente. O WPA utiliza a autenticação de rede 802.1x e as medidas de encriptação do Protocolo TKIP (Temporal Key Integrity Protocol) para criar uma chave 'de par' para a sessão informática do cliente em modo enterprise; para as sessões em modo home, o utilizador só tem de introduzir a chave mestra em cada um dos APs e PCs na rede sem fios. A chave de

par é, em seguida, distribuída para o cliente e AP. Após proceder à autenticação, o TKIP transforma a chave de segurança estática WEP única de 40 bits em várias chaves de segurança dinâmicas WEP de 128 bits. Em resumo,o TKIP substitui a chave WEP única repetidamente usada por cerca de 500 triliões de chaves alternativas.

3.6. FERRAMENTAS PARA REDES SEM FIO

Nesta seção serão descritas algumas ferramentas utilizadas por atacantes em redes sem fio. As mesmas ferramentas são instrumentos interessantes e poderosos para a proteção da própria rede, uma vez que bem utilizadas.

3.6.1. NETSTUMBLER [25]

Este é um software de varredura para redes sem fio, que utiliza um método de sondagem ativa da rede, identificando muitas funcionalidades desta, tais como potência do sinal e SSID. Também possui suporte a GPS. Esta aplicação quando bem utilizada pelo administrador da rede se torna uma valiosa ferramenta para gerência da rede. Permite o monitoramento da qualidade do sinal e quantos dispositivos estão conectados ou acessando o ambiente da rede.

3.6.2. KISMET [26]

Este é uma aplicação sniffer, que pode monitorar ambientes diferentes de redes e capturar vários pacotes diferentes criando um repositório para estes. O Kismet permite identificar a posição física do dispositivo móvel, através da utilização do sistema de GPS. A utilização de

bibliotecas específicas permitem que o Kismet forneça informações importantes para um ataque a rede, tais como: o número de WLANS no ambiente da rede, o número de pacotes que tramita, e a identificação dos métodos de criptografia estão sendo aplicados.

3.6.3. AIRSNORT [27]

Este aplicativo é um scanner da rede para quebra de chaves na rede. Após a captura de um número de pacotes, em torno de três a cinco milhões, consegue quebrar qualquer chave WEP. É um bom software para verificar o nível de criptografia aplicado as chaves trocadas pelos dispositivos na rede.

Além das ferramentas descritas acima, pode-se encontrar diversos outros softwares com a mesma finalidade na internet, as aplicações mais conhecidas e utilizadas para o monitoramento e segurança de redes estão relacionadas a seguir:

? AirTraf é uma ferramenta Linux que procura por Access Points 802.11b e exibe estatísticas de tráfego;

? Ethereal é um *sniffer* de rede disponível nas versões Windows/Linux/BSD/Mac dentre outros.

? BSD Airtools, WEPCrack são ferramentas que conseguem determinar as chaves WEP em uso e interceptar o tráfego de redes sem fio.

? WepAttack, WepLab estes são softwares para ataque a redes, baseados na fragilidade do vetor de inicialização, utilizando de força bruta.

? Wellenreiter, Airjack softwares de monitoramento de rede específicos, detectam e registram tentativas de invasão em um ambiente de rede.

? Hotspotter é um programa que redireciona o laptop da vítima para o equipamento do *hacker*.

? Airsnarf finge ser um access point para roubar *usernames* e senhas em hotspots públicos..

4. A REDE DO CRSPE E ASPECTOS GERAIS DE SEGURANÇA DA INFORMAÇÃO

Neste capítulo estão descritas as características físicas e lógicas da rede de computadores do CRSPE, os ativos que a compõem assim como o software de gerencia utilizado. São abordados também aspectos relacionados a Gestão de Segurança do CRSPE e por fim é descrita a Política de Segurança especifica para a rede sem fio, que foi desenvolvida durante a elaboração deste projeto.

4.1. DESCRIÇÃO DO CENÁRIO DO CRSPE

O prédio do CRSPE apresenta uma área construída de 10000 m² e sua estrutura é composta de quatro pisos, em formato de "L", onde a parte maior do “L” tem aproximadamente 90 metros e a outra parte mede 60 metros aproximadamente.

A rede sem fio que alcança toda a extensão do prédio, possui a seguinte estrutura de equipamentos instalados:

- 1 Ponto de Acesso no subsolo;
- 3 Pontos de Acesso no térreo;
- 3 Pontos de Acesso no primeiro andar;
- 1 Ponto de Acesso no terraço;
- 1 Switch para WLAN;

Esta distribuição dos pontos de acesso foi projetada de acordo com os padrões de difusão e alcance do sinal em redes sem fio. Os pontos de acesso alcançam a cobertura de um raio aproximado de 50 metros, permitindo assim disponibilizar o sinal de conexão em todos os pontos do prédio.

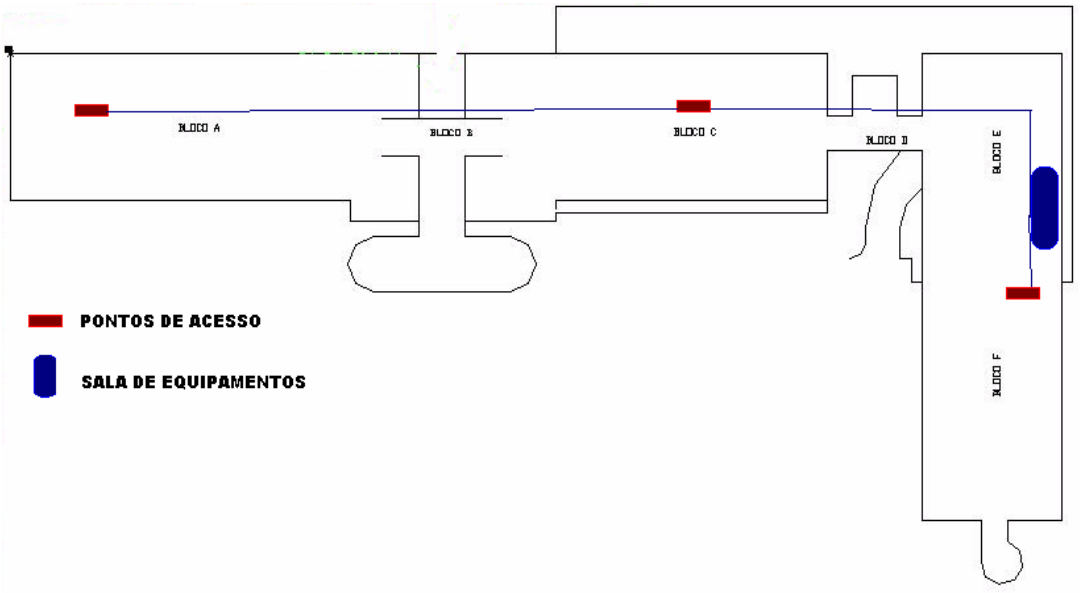

Figura 4.1. Estrutura do prédio do CRSPE

4.1.1. CARACTERÍSTICAS E FUNCIONALIDADES DOS EQUIPAMENTOS

Nesta seção são descritas as principais características dos dispositivos ativos da rede sem fio. As soluções adotadas são equipamentos da Extreme Networks [28].

4.1.2. SWITCH E PONTOS DE ACESSO

Os equipamentos utilizados na rede do CRSPE são um switch Summit 300 e os ponto de acessos são constituídos por equipamentos Altitude [28], conforme apresentado na figura 4.1.2b. O Summit 300, demonstrado na figura 4.1.2a possui a capacidade de disponibilizar aplicações sem fio e cabeada simultaneamente e fornece um elevado padrão de escalabilidade e flexibilidade para sua administração. Este realiza encriptação diretamente no hardware. A porta para rede sem fio implementa o AES (*government-endorsed Advanced Encryption Standard*) e WPA (*Wi-Fi Protected Access*) para assegurar maior segurança. Permite

a autenticação de usuários empregando IEEE 802.1x e também autenticação através de servidor RADIUS (*Remote Authentication Dial-In User Service*) como método de controle de acesso. Algumas características do Summit 300 serão listadas a seguir:

? Suporte simultâneo do IEEE 802.11, 802.11b e 802.11g;

? 48 portas Ethernet 10/100 auto-negotiating;

? 4 Portas Gigabit Ethernet 10/100/1000 (UTP e slot para SFP), formando 2 uplinks ativos e redundantes;

? Fontes de alimentação redundantes maximizam o uptime da rede e disponibilidade de rede;

? Gerenciamento por porta serial RS-232 no painel frontal;

? IEEE 802.3af PoE (Power over Ethernet) em todas as 48 portas 10/100, com alimentação de energia de 48V para os AP Altitude;

? Switching Wirespeed Nível 2/Nível 3 em todas as portas;

? Classificação de tráfego para QoS nas camadas 1-4 (*Policy-Based Mapping*), baseado em Mac, Source/Destination IP, TCP/UDP port, Diffserv, 802.1P;

? Link Agregation baseado no standard 802.3ad com suporte a sharing tanto em Fast Ethernet quanto em Gigabit Ethernet;

? Link Agregation com suporte a até 8 portas Fast Ethernet ou duas portas Gigabit Ethernet por Grupo;

? Suporte a Access Control Lists (ACLs) Baseadas em IP (origem/destino) e parâmetros TCP/UDP/ICMP;

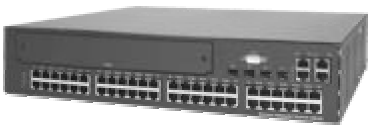

Figura 4.1.2a Foto Ilustrativa do Switch [28]

Figura 4.1.2b Foto Ilustrativa do Ponto de acesso [28]

4.1.3. SOFTWARE DE GERÊNCIA DE REDE

Está sendo utilizado o aplicativo EPICenter 5.0 [36] para gerência da rede. O aplicativo permite gerenciar e monitorar todos os elementos de rede instalada do CRSPE, tanto equipamentos Extreme Networks como de outros fabricantes, desde que sejam gerenciáveis através do protocolo SNMP. Permite uma administração centralizada, desde o cadastramento de usuários e dispositivos, assim como o acesso e configuração de quaisquer dos equipamentos cadastrados. As configurações de rede, incluindo as políticas de rede podem ser repassadas a todos os equipamentos da Extreme Networks automaticamente. Por exemplo, a aplicação de algumas regras de segurança, citados a seguir:

? *Rogue Access Point Detection*: detecção ponto-a-ponto com bloqueio seletivo de pontos de acesso não autorizados;

? *Access Intrusion Detection* com características de gerenciamento para prevenir acesso suspeito de usuário e *address spoofing*;

? Autenticação para dispositivos legados utilizando *Network Login* com SSL e para dispositivos 802.1x utilizando PEAP, EAP-TLS, EAP-TTLS e EAP-MD5;

? Encriptação utilizando WEP (*Wired Equivalent Privacy*), 802.11i draft, WPA (*Wi-Fi Protected Access*), AES (*Advanced Encryption Standard*) e TKIP (*Temporal Key Integrity Protocol*);

? Controle de acesso com ACLs (*Access Control Lists*), VLANs e proteção DoS.

Figura 4.1.3. Software de Gerenciamento da rede.

4.2. SEGURANÇA E GERENCIAMENTO DE INFORMAÇÕES

A segurança é um ativo que tem um valor para a organização e consequentemente necessita de uma proteção adequada. A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Confiabilidade, integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização [5].

4.2.1. GESTÃO DE SEGURANÇA DO CRSPE

Para entender como o aspecto segurança é implementado no CRSPE, deve-se conhecer as áreas-fim deste Centro, que são: ciência espacial, astrofísica, observação da terra, previsão de tempo e análise climática e controle de satélites.

A missão do CRSPE é a excelência em pesquisa, desenvolvimento na área espacial e formação de pessoal a nível de mestrado e doutorado nas áreas afins e tem a informática como a base de apoio, ou atividade meio, visando uma melhoria contínua nos processos envolvidos na instituição. Para que a melhoria seja continua, é preciso ter a preocupação com a qualidade dos produtos, com cumprimento dos prazos de entrega estipulados para qualquer projeto, no controle da documentação [9].

A implementação de regras de trabalho e procedimentos padronizados quais, usualmente são de responsabilidade de cada usuário, tudo isso é necessário para obtenção de um ambiente seguro.

O Modelo de Gerência da Tecnologia de Informação do Centro Regional Sul de Pesquisas Espaciais (CRSPE)[9], foi definido tendo como base um Grupo de Suporte, dividido de acordo com a função, atribuições e hierarquia a qual cada gerência é responsável, conforme descrito: Gerência; Gerência de Rede; Gerência de Desempenho; Gerência de Segurança.

A Gerência de Segurança é responsável pela elaboração, implementação e administração de mecanismos e regras que permitirão aos usuários de todo o CRSPE manipularem de maneira segura os documentos e dados. O Grupo de Segurança no CRSPE tem a estrutura hierarquicamente subordinada ao Grupo de Redes:

? **Grupo de Administração de Serviços e Sistemas:** implementa as regras de segurança, baseadas no Plano de Segurança do CRSPE;

? **Grupo de Administração de Qualidade:** verifica se os objetivos do Plano de segurança estão sendo atingidos;

? **Grupo de Operação:** ativa os procedimentos definidos no Plano de Segurança e Política de Segurança;

? **Grupo de Gerência de Segurança:** especifica procedimentos de segurança a serem operacionalizados, obedecendo ao Plano e Política de Segurança;

? **Grupo de Administração de Segurança:** valida o Plano e a Política de Segurança;

? **Grupo de Administração de Planejamento:** elabora o Plano de Segurança do CRSPE baseado na Política de Segurança em vigor.

4.2.2. POLÍTICA DE SEGURANÇA

Uma política de segurança é um conjunto de diretrizes, normas, procedimentos e instruções de trabalho que estabelecem os critérios de segurança a serem adotados em nível local ou intencional, visando o estabelecimento, padronização e normalização da segurança em âmbito humano e tecnológico. Com base na análise das principais características de segurança inerentes às redes sem fio como vulnerabilidade, riscos e tecnologias disponíveis, uma política de segurança específica para estas redes foi desenvolvida. Os aspectos de segurança física, corporativa, de usuários, de dados e também legais são considerados. A implementação desta política é a tentativa de desenvolver um modelo de gerência completo que permita a manutenção dos níveis de segurança já previamente alcançados pelo Grupo de Gerência de Segurança sobre a rede guiada. Seguindo as boas práticas de gestão definidas por este grupo, o resultado final almejado deste projeto é prover um ambiente integrado com um forte padrão de segurança agregado.

4.2.3. ESPECIFICAÇÃO DA POLÍTICA DE SEGURANÇA PARA A REDE SEM FIO

A seguir é descrito um adendo, que é a própria política de segurança implementada durante este projeto para rede sem fio. Este documento foi divido em aspectos gerais e aspectos técnicos. Esta política deve ser anexada aos documentos da gestão de segurança do CRSPE. Os aspectos mais importantes deste documento estão nos itens que descrevem regras para entrada de dispositivos móveis no prédio do CRSPE e os métodos de autenticação utilizados para isto. Estas duas descrições fundamentam o objetivo deste projeto, que é garantir uma forma dinâmica e segura de disponibilizar os recursos da rede sem fio aos visitantes do prédio.

ADENDO 1 - SEGURANÇA DA REDE SEM FIO

ASPECTOS GERAIS

INTRODUÇÃO

Esse documento tem caráter particular e confidencial, não podendo ou devendo ser redistribuído sem prévia autorização e supervisão dos responsáveis pela Gerência de Segurança do Centro Regional Sul de Pesquisas Espaciais (CRSPE), sendo a infração passível de punição pelas regras internas, bem como ações legais

A definição desta política de segurança para o uso da rede sem fio é de vital importância para a preservação da integridade e confiabilidade das informações que trafegam por dispositivos móveis. Esta política deve cobrir pelo menos os seguintes itens:

- Definir quem está autorizado a instalar *Ponto de acessos* (APs) nas dependências da instituição.
- Definir quem está autorizado a utilizar a rede sem fio da instituição;
- Prever as ações a serem tomadas em caso de roubo ou perda de equipamentos moveis;
- Definir que tipo de informação pode transitar pela rede;
- Descrever as configurações mínimas de segurança para APs, clientes, etc.

Confidencialidade, integridade e disponibilidade da informação estão diretamente ligados à segurança. Este documento descreve um conjunto de instruções que devem ser observadas para permitir a normalização e melhora da atuação deste centro em termos de segurança.

O CRSPE E A POLÍTICA DE SEGURANÇA

Todas as normas aqui estabelecidas serão seguidas à risca por todos os integrantes deste centro. Todos que receberem cópia deste adendo da Política de Segurança do CRSPE, comprometem a respeitar todos os tópicos aqui abordados e estabelecidos e que cada um está ciente de que seus e-mails e navegação na internet/intranet poderão estar sendo monitorados.

O NÃO CUMPRIMENTO DESSA POLÍTICA

O não comprimento dessa política acarretará a execução de normas restritivas e sansões descritas no modelo de gestão de segurança e clientes do CRSPE.

DA ENTRADA DE DISPOSITIVOS MÓVEIS NO PRÉDIO DO CRSPE

A entrada de todo e qualquer dispositivo móvel, PDAs, notebooks, etc, no ambiente do CRSPE deve ser registrado junto à recepção do prédio, relacionando o usuário e o dispositivo.

A recepção por sua vez, deverá encaminhar uma cópia desta relação à Gerencia de Segurança, para que providências sejam tomadas para o cadastramento de dados que permitam o monitoramento dos equipamentos, quando utilizados na rede interna do CRSPE.

Da mesma forma como foi registrada a entrada do equipamento, deverá ser registrada a saída dos equipamentos, afim de preservar a integridade física do equipamento e ter subsídios para o Grupo de Segurança, determinar quanto tempo cada equipamento permaneceu nas instalações do CRSPE.

AUTENTICAÇÃO

A autenticação será o método adotado pelo CRSPE para disponibilizar e permitir o uso da rede sem fio somente por pessoas autorizadas. A autenticação nos sistemas móveis será baseada na verificação do código de usuário, sua respectiva Senha e o endereço físico do dispositivo. Cada usuário poderá utilizar um ou mais dispositivos móveis, mas cada dispositivo poderá ser utilizado num dado instante por apenas um usuário.

Para conectar-se a rede, o usuário deverá obter junto à Gerencia de Segurança um ID, que servirá para configuração e reconhecimento do dispositivo no ambiente de rede.

POLÍTICA DE LOGIN E SENHAS

A senha deverá conter no mínimo 6 caracteres alfanuméricos intercalando letras e números.

Exemplo de senha:

> Senha com 8 caracteres: MsEt6D.

As senhas seguras garantem a integridade da instituição. Cada senha terá um tempo de validade pré-determinada pela Gerência de Segurança, devendo ser trocada quando o sistema de verificação de senhas emitir um aviso ao usuário. O usuário ficará sem acesso aos serviços da rede se tal procedimento não for executado.

O Grupo de Segurança estabelecerá execução de procedimentos com o intuito de identificar senhas fracas e fáceis de serem quebradas.

Alguns lembretes que devem ser de conhecimento de cada usuário:

- A senha não deve ser jamais passada a outro, mesmo que seja alguém do Grupo de Segurança. Providencie uma outra senha quando isto for necessário.
- Caso desconfie que sua senha não está mais segura, sinta-se à vontade para mudá-la, mesmo antes do prazo determinado de validade.
- Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para mantê-la secreta.
- Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, banco), datas (11092001) devem ser evitadas, pois são extremamente fáceis de descobrir. Existem ferramentas que conseguem quebrar senhas em alguns segundos.

PERFIL DE ACESSO A REDE

Todo usuário que tiver acesso a rede, deverá estar inserido em um perfil especifico. O perfis serão atribuídos pelo grupo de segurança, respeitando as atividades realizadas por cada cliente no âmbito da organização. Uma hierarquia bem definida e clara de níveis de acesso deve ser utilizada, para evitar que pessoas desautorizadas tenham acesso a áreas restritas as mesmas.

O USO DE MAILS E INTERNET

Hoje em dia grande parte da comunicação corporativa de uma instituição está sendo realizada por meio da internet e de e-mails.

Os servidores de e-mail de muitas instituições encontram-se protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são requeridas:

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com se não tver certeza absoluta de quem enviou esse e-mail.
- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc.
- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa , não pague alguma coisa, etc.
- Não utilize o e-mail para assuntos pessoais.
- Não mande e-mails para mais de 10 pessoas de uma única vez (to, cc, bcc)
- Evite anexos muito grandes.
- Utilize sempre sua assinatura criptográfica para troca interna de e-mails e quando necessário para os e-mails externos também

O uso e acesso a internet será restrito aos seguintes tópicos:

- Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização.
- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado.
- É proibido o uso de ferramentas P2P (kazaa, Morpheus, etc)

DISPOSITIVOS MÓVEIS

Cada dispositivo tem códigos internos que permitem sua identificação na rede. Isso significa que tudo que venha a ser executado por este equipamento acarretará em responsabilidade do usuário. Por isso sempre que sair da frente de seu equipamento, tenha certeza que efetuou logoff ou travou o console.

POLÍTICA DE USO DOS DISPOSITIVOS MÓVEIS

Lembramos que seu dispositivo é um importante componente de segurança para o ambiente de rede. Por isso observe as seguintes orientações:

- Não instale nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança.

- ? Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria.
- ? Mantenha o que é pessoal no equipamento móvel. Todos os dados relativos à ao CRSPE devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.

POLÍTICA DE USO DA INFORMAÇÃO

- ? Não fale sobre a política de segurança com terceiros ou em locais públicos.
- ? Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha.
- ? Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora do CRSPE.
- ? Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado.
- ? Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail.
- ? Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

VÍRUS E CÓDIGOS MALICIOSOS

Os vírus são um dos grandes vilões e geradores de problemas de segurança. Alguns procedimentos simples em seus dispositivos podem evitar grandes transtornos:

- ? Mantenha seu anti-vírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com a mesma para que a situação possa ser corrigida.
- ? Não traga disquetes ou CDs de fora da empresa. Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma descontaminação.
- ? Reporte atitudes suspeitas em seu sistema à gerência de segurança, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.
- ? Suspeite de softwares que "você clica e não acontece nada".

ASPECTOS TÉCNICOS

TOPOLOGIA DA REDE

Os fatores importantes a serem levados em consideração são a distribuição e posicionamento dos Ponto de acessos (AP) e a necessidade de se elaborar um perímetro de isolamento desta rede no interior do prédio do CRSPE. Para o posicionamento dos AP, devem ser considerados a potência de sua antena, para que o alcance destes não ultrapasse os limites do prédio, o que pode facilitar o uso e a escuta não autorizadas. Esse vazamento de sinal é extremamente comum o que deve fazer com que a gerência de segurança implemente medidas para amenizar esta situação. Ex. uso de autenticação e criptografia. É importante notar que esse procedimento deve ser encarado apenas como uma camada adicional de segurança, uma vez que um atacante pode fazer uso de uma antena amplificadora de sinal e ter acesso à sua rede sem fio mesmo a distâncias maiores.

Com relação ao isolamento, uma rede sem fio interna protegida por um firewall jamais deve ser conectada diretamente por uma rede externa, pois devem ser consideradas "untrusted". Colocar um AP de uma rede interna conectado diretamente não protegida seria equivalente à abrir uma porta de acesso a rede.

CRIPTOGRAFIA E AUTENTICAÇÃO

O padrão 802.11x originalmente suporta apenas dois tipos de autenticação do cliente: "*open authentication*" e "*shared-key authentication*".

No primeiro modo o cliente precisa apenas fornecer o SSID (*Service Set Identifier*) correto para juntar-se à rede.

No modo "*shared-key authentication*" é preciso o conhecimento de uma chave WEP (*Wired Equivalent Privacy*) para que isso ocorra. E importante notar que essa autenticação é do dispositivo *movel*, e não dos usuários da rede. Para aumentar a segurança de sua rede *wireless* deve-se escolher o maior tamanho de chave WEP possível, sendo essencial trocar as chaves WEP que venham nas configurações padrão dos equipamentos. O uso de criptografia nas aplicações, como SSH e SSL, também é recomendável para minimizar os riscos de escuta não autorizada. Existem várias iniciativas para a criação de novos padrões que aperfeiçoam a segurança das redes sem fio, sendo recomendada a utilização destas, assim que estiverem disponíveis.

O uso de um serviço de autenticação baseado em agentes proxy, pode permitir um nível mais adequado de segurança. Baseado na validação de usuários a partir de um login, senha e o endereço MAC de seus dispositivos. O cliente possuiu níveis de acessos aos serviços da rede e os logs das atividades realizadas por estes são armazenados em um repositório. O serviço agrega uma forma simples e eficaz de controle dos acessos a rede sem fio.

PONTOS DE ACESSO (*ACCESS POINT*)

A instalação dos AP deve ser realizada apenas por técnicos responsáveis pela rede, devidamente autorizados. Os AP devem ser configurados a partir de regras específicas e pré-determinadas, de maneira que nenhum um dispositivo móvel possa atuar como um AP dentro do ambiente de rede.

Existem várias questões importantes que devem ser consideradas para a configuração de um AP. Muitos modelos de APs vêm com configurações de fábrica que são de conhecimento público, incluindo senhas *default*. E extremamente importante que todas as configurações originais sejam mudadas, incluindo:

- Senhas de administração;
- SSID;
- Chaves WEP;
- SNMP *communities*.

Os AP possuem várias maneiras de serem configurados, é importantes que todas estas sejam desabilitadas, e que toda configuração seja feita por meio da rede cabeada, para evitar a captura por clientes indesejados dos pacotes de configuração. A localização dos AP também é de relevante importância, pois alguns dispositivos possuem botões que permitem restaurar as configurações originais de fábrica, o que permitiria um intruso reconfigurar um AP. Por fim é útil desabilitar o broadcast de SSID pelo AP, esta medida simples pode dificultar o uso de alguns programas, como por exemplo softwares para mapeamento de redes sem fio.

PROTEÇÃO AOS CLIENTES DA REDE SEM FIO

Todo usuário deve receber orientação sobre a utilização segura dos dispositivos móveis e da rede sem fio. E recomendável que os dispositivos móveis e clientes com receptores de sinal passem pelo seguinte processo :

- Aplicação de *patches*;
- Uso de *firewall* pessoal;
- Instalação e atualização de antivírus;
- Desligamento do compartilhamento de disco, impressora, etc.

MONITORAMENTO DA REDE SEM FIO

E recomendada a utilização de IDS (Serviços de Detecção de Intrusão), softwares desenvolvidos para o monitoramento de redes sem fio. A função dessas aplicações é detectar e registrar as seguintes ações no ambiente da rede :

- Instalação de APs não autorizados;
- Clientes conectados em um dado instante - fora do horário habitual
- Dispositivos que não estejam usando WEP;
- Ataques contra os clientes *moveis*;
- Acessos não autorizados;
- Mudanças de endereços MAC;
- Mudanças de canal;
- DoS (*Deny of Service*);

REQUISITOS PARA UTILIZAÇÃO DA REDE SEM FIO DO CRSPE

Para que um determinado dispositivo tenha acesso ao ambiente da rede do CRSPE o mesmo deve estar configurado da seguinte maneira:

- Deve possuir instalado um cliente SSH < download : http://www.ssh.com/ >;
- A porta de comunicação 3210 deve estar aberta;
- Aplicações do tipo firewall devem estar desativadas;
- O usuário deverá abrir um terminal e executar o seguinte comando:

  < scp anonimo@10.10.1.100:/install/acesso.sh > < Senha : anonimo >

- No mesmo terminal o usuário deve rodar o script acesso:

  < ./acesso.sh >

O script realizará a conexão deste cliente ao servidor, os dados solicitados durante esta conexão devem ser corretamente preenchidos, caso contrário o acesso à rede permanecerá bloqueado.

5. PROTOCOLOS DE AUTENTICAÇÃO E DESCRIÇÃO DO SERVIÇO DE AUTENTICAÇÃO BASEADO EM AGENTES

Neste capítulo é descrito o funcionamento dos padrões de autenticação para redes sem fio, baseados no IEEE 802.1x, com ênfase no servidor de autenticação RADIUS. O serviço de autenticação proposto neste trabalho, está definido também neste capítulo, com a sua descrição, apresentação da arquitetura utilizada, o modelo conceitual e por fim dados de implementação e testes.

5.1. O PADRÃO DE AUTENTICAÇÃO IEEE 802.1x

O IEEE 802.1x foi desenvolvido para redes guiadas com o proposto de inserir um padrão de autenticação mútua entre cliente e servidor. O WPA adotou essa tecnologia para redes sem fio, pelo fato da mesma atingir dois requisitos básicos de segurança, a autenticação e a privacidade, os quais não eram atendidos pelo protocolo WEP. O 802.1x define uma porta como sendo um ponto de conexão à rede; sendo uma porta física, em redes cabeadas, ou uma porta lógica, como no caso da autenticação entre dispositivo sem fio e AP. O modelo de autenticação é composto pelos seguintes elementos :

? Suplicante, dispositivo ou software que tenta se autenticar;

? Servidor de autenticação, um sistema com a função de realizar a autenticação de um suplicante;

? Autenticador, um dispositivo da rede que realiza a intermediação entre o suplicante e o servidor. Em redes sem fio esta é a função do ponto de acesso.

5.1.1. FUNCIONALIDADES DO 802.1X EM REDES SEM FIO

O padrão IEEE 802.1x surgiu como a solução para os problemas de autenticação encontrados no IEEE 802.11 fornecendo suporte à praticamente qualquer método de autenticação existente. O novo adendo do 802.1x inclui a técnica RSN (*Robust Security Network*) em sua descrição, que introduz a técnica de restrição de acesso para dispositivos autorizados na rede. Para manter um esquema de autenticação com um bom nível de segurança, o IEEE 802.1x utiliza certificados de clientes ou nomes de usuários e senhas. O autenticador difere a autenticação do usuário da do dispositivo. Este método de autenticação utiliza um ponto de acesso à rede, um servidor de autenticação e um um protocolo IETF (*Internet Engineering Task Force*). O EAP (*Extensible Authentication Protocol*) realiza a autenticação entre o usuário e o servidor. A utilização do 802.1x permite a compatibilidade entre o TKIP e o AES, que é o padrão de chave dinâmica para o WEP e o mecanismo de criptografia adotado pelo 802.11i. As funcionalidades do padrão se devem a utilização do EAP, é uma estrutura que define qual o método de autenticação será utilizado. Com 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.

O processo de autenticação que deve ser utilizado pelo 802.1x baseia-se no envio de mensagens EAP sobre redes locais (*EAP over LAN – EAPOL*). A descrição do funcionamento é a seguinte:

1. Um suplicante inicia uma conexão com um autenticador;
2. O autenticador detecta a ocorrência e habilita uma porta para o suplicante. Entretanto, excluindo o tráfego definido pelo 802.1x, todos os outros ficam bloqueados;
3. O replicante acessa o autenticador;

4. O autenticador requer a identificação do suplicante;
5. O suplicante responde com a identificação que é imediatamente repassada para o servidor de autenticação;
6. O servidor autentica a identidade do suplicante e envia uma mensagem do tipo *ACCEPT* para o autenticador;
7. O autenticador muda o estado da porta para autorizado;
8. O suplicante requisita a identificação do servidor, e atende o pedido;
9. O suplicante valida a identificação do servidor e o tráfego é liberado.

A figura 4.3.1 demonstra o processo de autenticação descrito acima :

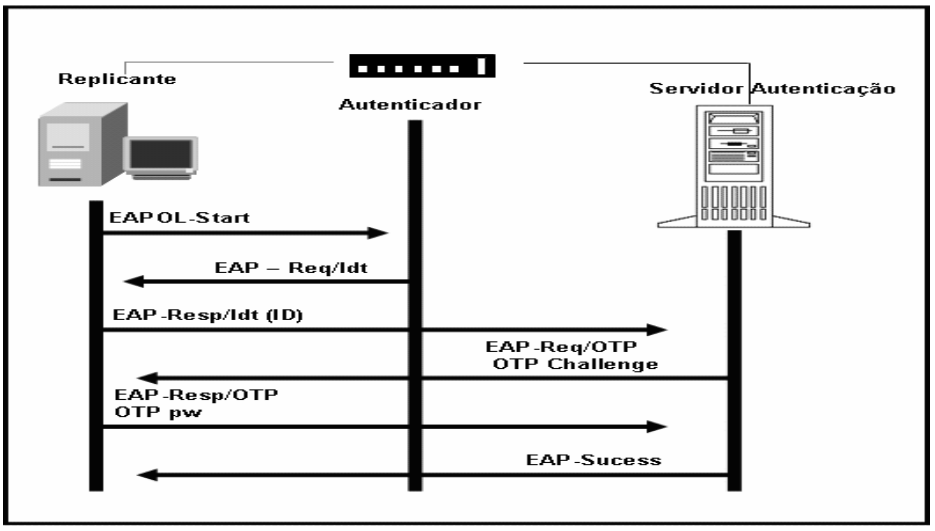

Figura 4.3.1. Descrição da Autenticação do padrão 802.1x

5.1.2. SERVIDOR DE AUTENTICAÇÃO RADIUS

O servidor RADIUS [34] não é o padrão aprovado para a utilização em processos de autenticação, mas é o método mais amplamente empregado para a geração e validação de dispositivos e usuários em um ambiente sem fio. Uma das vantagens deste servidor é que o mesmo pode ser usado para

gerar novas chaves de criptografia dinamicamente para o WEP, permitindo que os algoritmos de criptografia sejam usados de uma forma mais segura.

O protocolo do RADIUS disponibiliza o acesso baseado em três premissas: Autenticação, Autorização e Contabilização – AAA (*Authentication, Authorization, Accounting*). Em outras palavras, a função do RADIUS é centralizar as atividades de autenticação, autorização e contabilização permitindo assim uma gerência aglutinada de todos esses serviços.

O funcionamento do servidor RADIUS integrado ao padrão 802.11 é realizado utilizando o modelo de desafio, da seguinte maneira:

1. O suplicante deve se autenticar com o autenticador, usando o RADIUS sobre o EAP;
2. O suplicante deve começar uma associação 802.1x* ;
3. Mais de uma chave intermediária é negociada entre o autenticador e o suplicante, dificultando o processo de autenticação, mas aumentando a segurança;
4. A associação 802.1x toma lugar depois que a fase de associação da camada 802.11 está completa com o ponto de acesso;
5. Um ponto de acesso mantém um número considerável de informações depois da associação e antes que a 802.1x esteja completa;
6. Ao final da associação o suplicante têm uma chave para aquela sessão.

A figura 4.3.2 demonstra o processo de autenticação baseado em RADIUS em um ambiente de rede sem fio.

* Uma associação 802.1x mantém o estado de segurança relevante à conexão. O padrão 802.1x define explicitamente a associação dos dados que protege conexões de transporte entre uma estação base e uma ou mais estações clientes. [38]

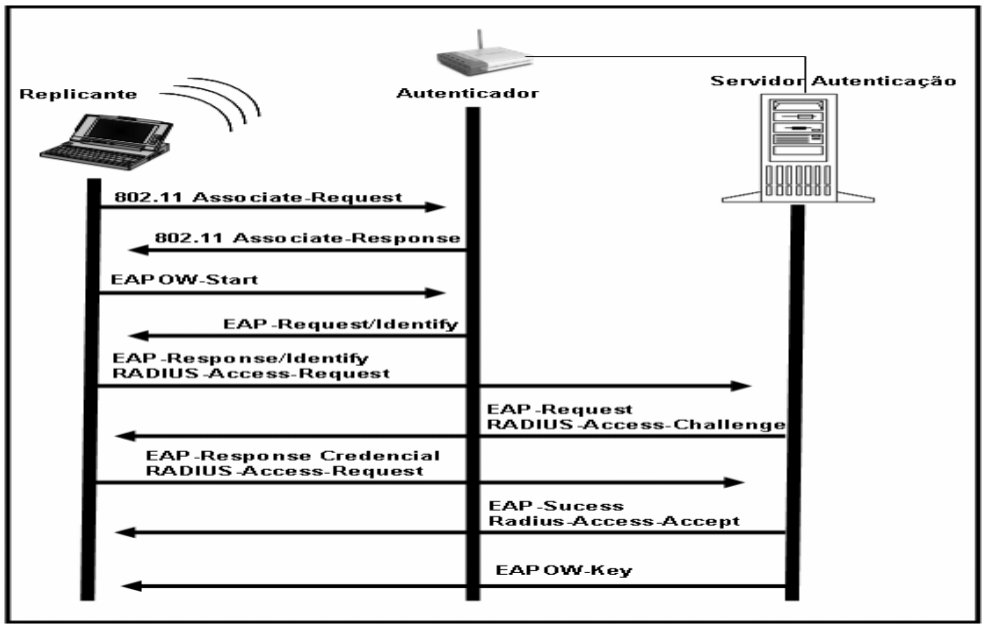

Figura 4.3.2. Descrição da Autenticação do padrão 802.1x em redes sem fio.

5.1.3. IMPLANTAÇÃO DO SERVIDOR RADIUS

Com os subsídios obtidos com o estudo detalhado dos padrões de redes sem fio, suas vulnerabilidades, riscos e brechas de segurança, nota-se o quanto são necessárias as especificações do modelo 802.11i, que implementam um modelo adequado de segurança para redes sem fio. A utilização de um serviço de autenticação converge com as necessidades de segurança identificadas no ambiente sem fio do CRSPE. A utilização do servidor de autenticação RADIUS foi o escolhido para integrar o padrão 802.1x na implementação do serviço de controle de acesso e autenticação no CRSPE. A escolha do RADIUS deu-se em virtude da compatibilidade dos ativos de rede e do software de gerência de rede instalado no prédio, além do fato deste serviço apresentar uma boa aceitação de mercado. Além do RADIUS, vários outros servidores de autenticação poderiam ser utilizados, como exemplo o KERBEROS [31] ou TACACS [32].

Duas versões de servidores RADIUS foram testados na rede sem fio do CRSPE, uma versão open source, o FreeRadius [34] que roda sob a

plataforma linux, e uma versão proprietária que esta encapsulada no próprio gerenciador da rede EPICenter. A escolha pelo FreeRadius foi motivada pelo fato desta aplicação usar uma licensa livre e possuir o código fonte aberto e disponível na Internet. Um dos objetivos deste trabalho é modelar um serviço de autorização baseado em agentes, o qual deve possuir um repositório de clientes, com informações para a autorização de acesso aos recursos da rede. O servidor RADIUS deve validar os dispositivos que fizerem requisições de acesso, a partir deste repositório. Para que isto seja possível, é necessário algumas modificações em seu código fonte.

O download da versão atualizada do FreeRadius encontra-se em : ftp://ftp.FreeRadius.org/pub/RADIUS/FreeRadius-1.0.1.tar.gz.

A configuração do servidor é realizada com a edição de três arquivos de configuração: *clients*, *naslist e users*. Os passos para ativar este serviço são os seguintes:

1. O arquivo `clients` encontra-se em `/etc/raddb/clients` e contém uma lista de clientes que possuem permissões de realizar requisições de autenticação, bem como sua chave de criptografia. Neste arquivo são incluídos os servidores de acesso e suas chaves. O formato do arquivo: tuplas <CLIENTE CHAVE>, onde CLIENTE é identificador de acesso do cliente que pode fazer uma requisição e a CHAVE é uma chave que deve ser utilizada para a desencriptação das requisições. O cliente pode ser designado pelo seu endereço IP e a senha deve ser a mesma no cliente e no servidor RADIUS.
2. O arquivo `naslist`, localizado em `/etc/rddb/naslist`, contém uma lista com os servidores de acesso conhecidos. Este arquivo carrega informações sobre o tipo do servidor e tem o seguinte formato: tuplas <SERVIDOR APELIDO TIPO>, onde

SERVIDOR identifica o servidor de acesso, APELIDO é o nome reduzido para identificar o servidor em arquivos de registro e TIPO descreve qual o modelo do servidor de acesso.

3. O arquivo `users` em `/etc/rddb/users`, descreve a forma e o local em que o servidor RADIUS irá autenticar os usuários. A lista de usuários pode ser a mesma de um servidor de nomes tipo NIS, ou ser a própria lista de usuários do sistema, neste caso encontra-se no arquivo `/etc/passwd`. Esta descrição utiliza o `/etc/passwd` como local de autenticação, bastando acessar o diretório de configuração `/usr/raddb` e editar o arquivo `users`. O conteúdo deste arquivo deverá permanecer da seguinte maneira :

```
DEFAULT     Auth-Type = System
            Framed-IP-Address = 255.255.255.254,
            Framed-MTU = 576,
            Service-Type = Framed-User,
            Framed-Protocol = PPP,
            Framed-Compression = Van-Jacobson-TCP-IP
```

4. O passo seguinte é inicializar o servidor RADIUS:

```
./RADIUSd start
```

Após ativar o servidor RADIUS é necessário configurar o software de gerenciamento de rede EPICenter :

? Logar no EPICenter.

? Acessar a opção Admin.

? Na paleta RADIUS, marcar a opção Client e identificar o endereço da maquina onde o serviço RADIUS esta rodando.

O passo seguinte é utilizar a opção TELNET do próprio software, acessar o switch e configurar as redes virtuais (*VLans*), que passarão a utilizar o servidor de autenticação. Os quadros abaixo demonstram o estado antes e após a autenticação.

(Antes da Autenticação)

```
Alpine3804:2 # sh netlogin ports 2:1 "Altitude"
Port: 2:1 Vlan: Altitude
Port State: Unauthenticated
DHCP: Enabled
_____________________________________________________
MAC IP address Auth Type User ReAuth-Timer
00:E0:18:01:32:1F 10.20.2.6 No 802.1x Unknown 79
```

(Após a Autenticação)

```
Alpine3804:5 # sh netlogin ports 2:1 "Altitude"
Port: 2:1 Vlan: Altitude
Port State: Authenticated
DHCP: Enabled
_____________________________________________________
MAC IP address Auth Type User ReAuth-Timer
00:E0:18:01:32:1F 10.20.2.6 Yes 802.1x admin 0
```

5.2. MODELAGEM DO SERVIÇO DE AUTENTICAÇÃO BASEADO EM AGENTES

5.2.1. DESCRIÇÃO DO SERVIÇO

Este serviço é um sistema de autenticação e controle de acesso de usuários que permite aos integrantes do CRSPE e visitantes terem acesso a

todos os serviços da rede, garantindo um satisfatório nível de segurança. Sua característica é limitar as ações que um usuário legítimo de um sistema de computação realiza, com base nas autorizações aplicáveis a este no momento de sua autenticação no ambiente.

O serviço caracteriza-se numa aplicação sintetizada, garantindo a Confidencialidade, Integridade e Disponibilidade de um sistema em uma situação real. Permite validar a entrada de um usuário no ambiente de rede, atendendo de forma rápida e eficiente as necessidades de um ambiente computacional conectado. O modelo desenvolvido utiliza um Agente conectado a um servidor de autenticação, que reporta as informações do usuário para um repositório de dados específico. Os usuários devem ser cadastrados de acordo com perfís pré-determinados pelo administrador da rede. O nível de acesso de cada cliente da rede é imposição do perfil ao qual o mesmo pertence.

Todas as regras definidas para utilização do serviço de autenticação, e por conseqüência a rede, respeitam a política de segurança descrita no capitulo 4.2.2. A figura 5.2.1. é um esboço do ambiente proposto, com o serviço de autenticação ativo hospedado em um servidor.

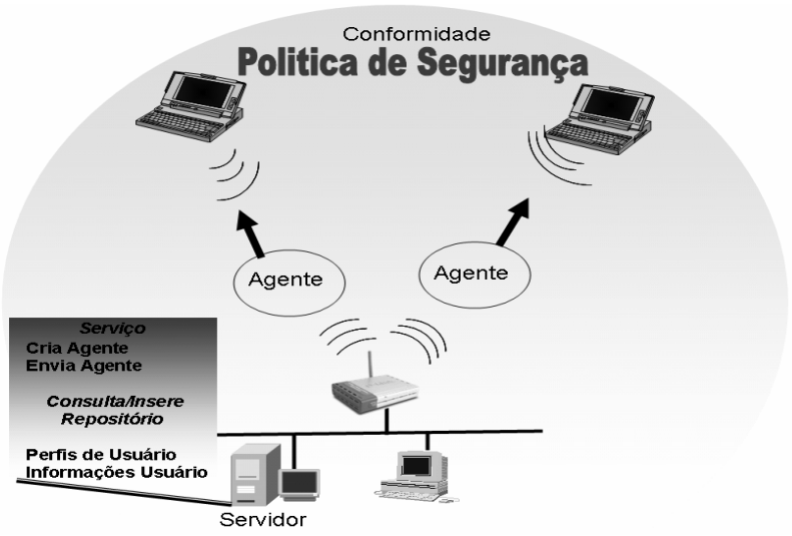

Figura 5.2.1. Serviço de Autenticação.

5.2.2. CARACTERÍSTICAS TÉCNICAS

5.2.2.1. ARQUITETURA DO SERVIÇO DE AUTENTICAÇÃO

Este serviço é um software que deverá rodar na camada de aplicação da rede e executa em sincronia com um servidor de autenticação RADIUS. A arquitetura deste serviço baseia-se em um modelo cliente-servidor, composto de um servidor de segurança, responsável pela autenticação de dispositivos que desejem se conectar a rede, e de um serviço de autenticação, baseado em agentes, com a finalidade de definir perfis e níveis de acesso dos dispositivos conectados a rede.

O agente possui três repositórios para armazenar informações especificas dos clientes que acessam a rede: arquivos de usuários, arquivo com informações dos clientes e arquivo de *log*. O arquivo de usuários lista os clientes autorizados a conectar-se a rede e contém o endereço MAC do dispositivo, o nome ou *login* do cliente e sua senha, sendo também utilizado pelo servidor RADIUS para autenticar o cliente na rede. O arquivo com as informações dos clientes é utilizado para determinar os perfis. Finalmente, o arquivo de log guarda o histórico dos clientes na rede. A figura 5.2.2 demonstra a arquitetura do serviço.

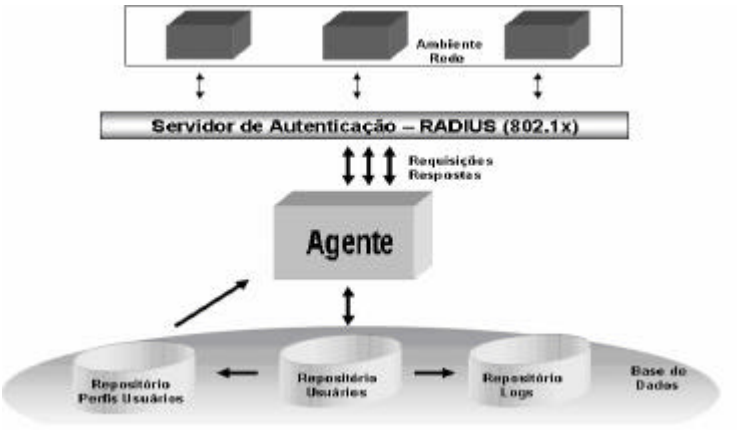

Figura 5.2.2. Arquitetura do Serviço de autenticação.

5.2.2.2. DESCRIÇÃO DO AGENTE

A lógica funcional que envolve o agente de autenticação é a seguinte:

1. Um novo dispositivo, ao solicitar uma conexão na rede, tem sua requisição tratada pelo RADIUS, que fará a consulta ao agente para identificar se este dispositivo é reconhecido pela rede;
2. O agente por sua vez consultará seu repositório de usuários. Se o usuário estiver cadastrado, o repositório de perfis é verificado para estabelecer o nível de acesso do dispositivo. Uma nova entrada é feita no repositório de logs com a identificação do dispositivo. O agente então informa ao servidor RADIUS a senha e o nível de acesso do dispositivo. Se a consulta ao repositório de usuários retornar falsa, ou seja, o dispositivo não estiver cadastrado, o agente realiza as seguintes atividades:
   - ? Informa ao servidor RADIUS que este dispositivo não é reconhecido pela rede, e por sua vez não autoriza o acesso;
   - ? Através de outra porta de comunicação, é enviado um novo agente ao dispositivo e estabelecida uma conexão direta com o serviço de autenticação, sem o conhecimento do servidor RADIUS. Neste momento, o agente solicita que o dispositivo preencha um formulário para poder garantir o acesso à rede. Após o dispositivo responder ao agente a conexão é encerrada. De posse das informações referentes ao cliente e ao dispositivo, o serviço atualiza seus repositórios e ativa o servidor RADIUS para reconhecer o dispositivo que agora está atualizado;
   - ? O usuário possui a opção de rejeitar a conexão com o agente, mas com a restrição de ter seu acesso à rede

bloqueado. Este bloqueio dos serviços da rede será implementado por meio da negação do endereço MAC do dispositivo.

A utilização de *sockets* para a comunicação com os dispositivos que acessam a rede é feita apenas no primeiro acesso de um cliente a rede, pois este meio de conexão consome muito recurso do sistema, além do fato que pode-se apenas manter uma conexão ativa por porta de comunicação. Para atender as diversas conexões simultâneas de clientes, é utilizado um método para controle de conexões. Este método deve ser implementado com o uso de *threads*, o que permite um ganho de desempenho para o serviço. Visando evitar problemas do tipo negação de serviço, um número limitado de conexões ao serviço dever ser estipulado.

Outros dois aspectos relacionados a segurança foram verificados durante a implementação do agente: (1) o primeiro é o fato de que o processo deve estar restrito e limitado apenas ao diretório onde o serviço esta rodando, com o acesso apenas aos arquivos necessários a este serviço; (2) o segundo aspécto esta relacionado a característica do agente, que é invocado durante a inicialização do sistema, por este fato é interessante que o mesmo possua apenas privilégios necessários para a execução do serviço.

5.3. MODELO CONCEITUAL

A análise e descrição do projeto para o desenvolvimento do agente é descrito nesta parte do trabalho. Algumas técnicas de engenharia de software são aplicadas para o desenvolvimento do modelo. O uso de UML [23] permite comunicar certos conceitos mais claramente do que certas linguagens alternativas. A utilização destes conceitos garante uma certa precisão, sem se deter em detalhes demorados .

O processo de modelagem é baseado em requisitos considerados relevantes e consistentes para o serviço de autenticação. O modelo é estruturado de maneira inteligível, procurando demonstrar as características mínimas que o serviço e o agente devem possuir para serem considerados úteis em uma organização.

Um diagrama de casos de uso é utilizado para demonstrar um cenário, composto por uma seqüência de passos onde o serviço pode interagir. A decomposição das etapas para a validação de um dispositivo na rede são descritas a seguir:

1. Um dispositivo móvel interage com a rede sem fio e solicita uma conexão.
2. A requisição é recebida pelo serviço, que verifica se este dispositivo já está cadastrado na base de dados de usuários do sistema.
3. O usuário não estando cadastrado, um agente é criado e enviado ao dispositivo.
4. O equipamento recebe o agente, o cliente aceita a instalação e emite um formulário, que deve ser preenchido pelo usuário, com alguns dados descritos pela política de segurança da empresa, dentre eles, o perfil de acesso desejado, logon e uma senha.
5. Os dados preenchidos no formulário são enviados ao servidor, que armazena os dados referentes ao cliente em uma base de dados.
6. O cliente passa a ter acesso ao ambiente da rede.

Alternativa: Falha no logon

O cliente não autoriza o usuário a utilizar a rede e rejeita a instalação do agente móvel, ou por algum tipo de restrição o dispositivo

não tem acesso permitido à rede. Este caso esta demonstrado no diagrama de casos de usos da figura 5.3a.

Alternativa: Cliente Cadastrado

Durante o primeiro acesso a rede o cliente aceita a instalação do agente móvel em seu dispositivo, ou este já é um cliente regular cadastrado. Este caso está demonstrado no diagrama de casos de usos da figura 5.3b.

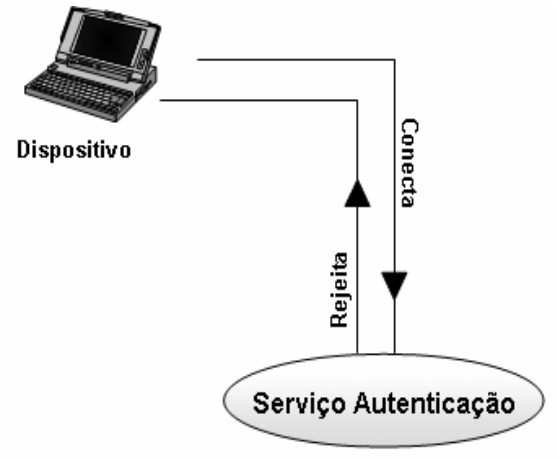

Figura 5.3a. Diagrama de Casos de Uso – Negação do Cliente.

Figura 5.3b. Diagrama de Casos de Uso – Validação do Cliente.

A figura 5.3c. demonstra o diagrama de classes, que é composto por objetos, que podem ser de negócios, interfaces ou de controle. A modelagem do diagrama descreve os relacionamentos, agregações e composições das instâncias que integram o serviço de autenticação.

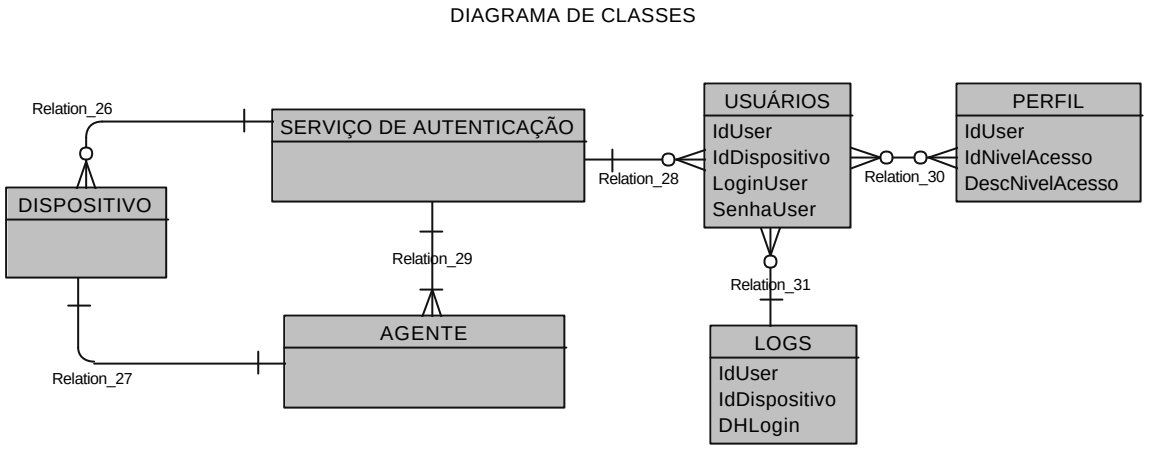

Figura 5.3c. Diagrama de Classes

O diagrama de seqüência descrito na figura 5.3d. demonstra os objetos na parte superior de uma linha tracejada. As linhas verticais são chamadas de linha de vida e representam o período de duração do objeto durante a interação. Este tipo de diagrama permite identificar de maneira simples e concisa as seqüências de atividades realizadas pelos objetos que constituem o serviço de autenticação.

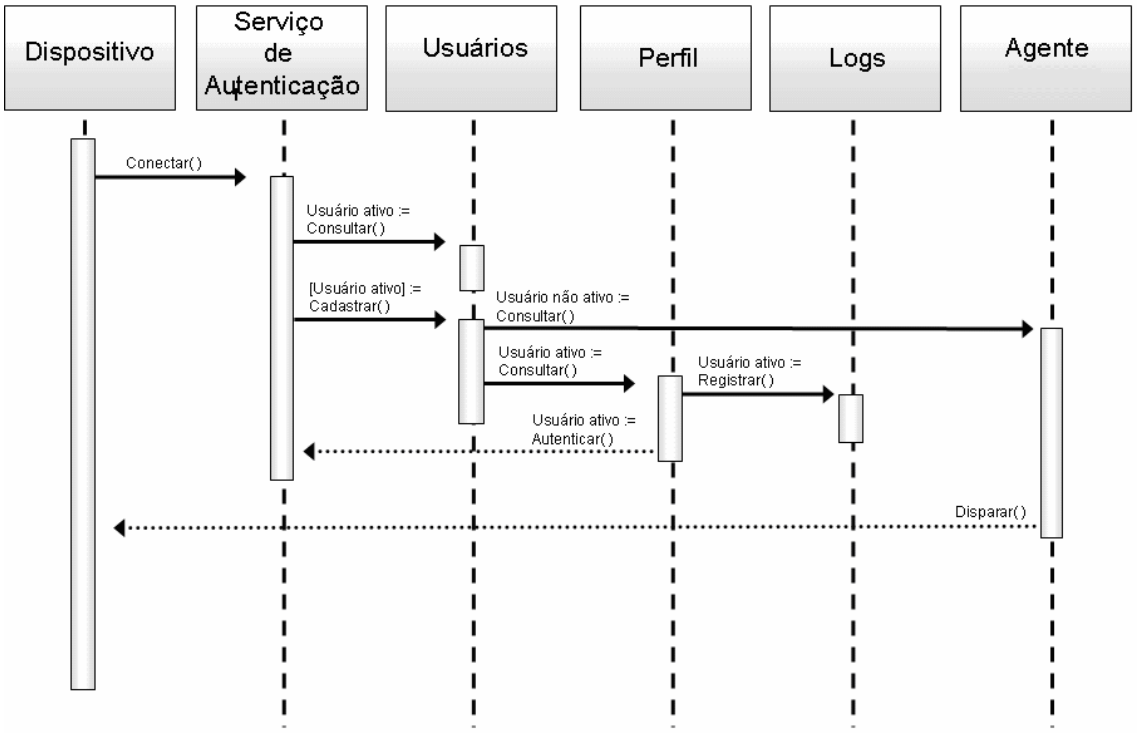

Figura 5.3d. Diagrama de Seqüência

5.4. IMPLEMENTAÇÃO E TESTES

O protótipo implementado para o serviço de autenticação foi desenvolvido com base na linguagem de programação Java e também com a utilização de Shell Script sob a plataforma linux. Para as funções de monitoramento de tráfego da rede e dos hosts as ferramentas *tcpdump, arp e iptables* [37] foram usadas. A seguir é apresentada a descrição das características do protótipo, com a descrição de suas funcionalidades.

Existem três módulos diferentes que formam o sistema:

1. O modulo desenvolvido com Shell Script, onde o tráfego da rede é analisado. Esta tarefa é realizada pelo *tcpdump*, que é uma ferramenta que gera um arquivo de saída, com os cabeçalhos dos pacotes que estão trafegando na rede, somente são monitorados os cabeçalhos dos pacotes IP, TCP, ICMP e UDP [29]. O arquivo de saída é filtrado, para a obtenção dos

equipamentos que solicitam acesso e tentam se sincronizar com a rede. Após a identificação destes, é usado o *ARP*, que é um protocolo usado para encontrar um endereço físico (MAC) a partir do IP de uma determinada máquina. O emissor difunde em *broadcast* um pacote *ARP* contendo o endereço IP de outro host e espera uma resposta com um endereço MAC respectivo [30]. Com a identificação do endereço MAC, o iptables que é um firewall, ferramenta utilizada para a proteção de uma rede, é configurado de forma dinâmica para bloquear todo e qualquer acesso deste host a rede, apenas um canal de comunicação com o computador onde o serviço de autenticação esta instalado é permitido.

2. O módulo servidor, desenvolvido em java, é um software que também analisa o arquivo de saída do *tcpdump*, identifica os equipamentos que acessam a rede e entra em estado de espera, aguardando a conexão do modulo cliente que deverá estar instalado na máquina que requer a utilização da rede. Ao receber a conexão o servidor verifica as informações recebidas, caso o cliente já esteja cadastrado no repositório de clientes, seu acesso a rede é liberado por meio de uma regra *iptables*. Se os dados não forem validados a máquina permanece bloqueada, e se for um primeiro acesso desta, os dados são armazenados no repositório e o acesso a rede é garantido. Um arquivo de *log* é gerado com um histórico de todas as conexões válidas e também das conexões perdidas na rede.

3. O módulo cliente, também desenvolvido em java, deve ser baixado da máquina onde o módulo servidor está instalado. Os procedimentos para o download estão descritos no adendo a política de segurança. O módulo cliente quando executado solicita a identificação do usuário e estabelece uma conexão com o servidor repassando essas informações. Ao término da autenticação do usuário e da máquina, a aplicação é removida do equipamento do cliente, onde permanece instalado apenas um script, que deve ser rodado quando o cliente desejar se conectar

novamente a rede. Este script fará o download e executará o módulo cliente automaticamente.

A fase de testes do protótipo foi realizada na rede sem fio do CRSPE, e os resultados mostraram que a utilização deste serviço pode ser aplicado em qualquer ambiente de rede, independente de ser guiada ou sem fio, desde que a rede utilize um mesmo conjunto de endereços (mesma faixa de IPs). Um trecho do script para monitoramento da rede, o arquivo com a análise dos pacotes que transitam na rede e o arquivo de log gerado pelo sistema são apresentados nas figuras 5.4a., 5.4b., 5.4c. e 5.4d.

```
while true
do
  kill -9 $PID_TCPDUMP
  # o cara !
  grep "arp reply" $ARQ_TMP \
  | sed "s/arp reply//;s/is-at//;
  s/ \+/|/g;s/^\([0-9:]\+\)\.[0-9]\+|\(.*\)$/\1|\2/" >> $LOG # OUTPUT

  # reinicia arqtmp
  tcpdump -i eth0 > $ARQ_TMP &
  PID_TCPDUMP=$!
      echo $PID_TCPDUMP >> ProcessoTcpDump.txt
  while read LINHA
 do
        hora=`echo $LINHA | cut -d "|" -f 1`
        ip=`echo $LINHA | cut -d "|" -f 2`
        mac=`echo $LINHA | cut -d "|" -f 3`
        echo "HORA: $hora"
        echo "IP: $ip"
        echo "MAC: $mac"
  done < $OUTPUT
sleep 5
done
```

Figura 5.4a. Trecho do script de monitoramento da rede

```
**** Saida TCPDUMP ****
19:02:52.017467 IP 192.168.1.7.1017 > 192.168.1.6.nfs: . ack 2503717163 win 49640
19:02:52.153261 IP baym-cs35.msgr.hotmail.com.1863 > 192.168.1.32.32771: P 1:9(8) ack 5 win 6529 <nop,nop,timestamp 23275747 544209>
19:02:52.153319 IP 192.168.1.32.32771 > baym-cs35.msgr.hotmail.com.1863: . ack 9 win 4110 <nop,nop,timestamp 544466 23275747>
19:02:52.454132 arp who-has 192.168.1.32 tell 192.168.1.1
19:02:52.454150 arp reply 192.168.1.32 is-at 00:0e:a6:3b:21:7f
19:02:53.052785 IP 192.168.1.5.netbios-ssn > 192.168.1.14.1588: P 2466484291:2466484295(4) ack 795317213 win 49640 NBT Packet
19:02:53.052988 IP 192.168.1.32.32778 > esfinge.ufsm.br.domain: 53676+ PTR? 5.1.168.192.in-addr.arpa. (42)
19:02:53.055114 IP esfinge.ufsm.br.domain > 192.168.1.32.32778: 53676 NXDomain* 0/1/0 (100)
19:02:53.163910 arp who-has 192.168.1.5 tell 192.168.1.14
19:02:53.164270 arp reply 192.168.1.5 is-at 00:03:ba:0c:b9:ba
19:02:53.164357 IP 192.168.1.14.1588 > 192.168.1.5.netbios-ssn: . ack 4 win 63893
19:02:55.242060 IP 192.168.1.14.2390 > outpostrr1.real.com.http: S 1866499821:1866499821(0) win 65535 <mss 1460,nop,wscale 2,nop,nop,sackOK>
19:02:56.661971 IP 192.168.1.7.3774037828 > 192.168.1.6.nfs: 140 lookup [|nfs]
19:02:56.674237 IP 192.168.1.6.nfs > 192.168.1.7.3774037828: reply ok 244 lookup [|nfs]
19:02:56.674599 IP 192.168.1.7.3774037829 > 192.168.1.6.nfs: 116 access [|nfs]
19:02:56.676266 IP 192.168.1.6.nfs > 192.168.1.7.3774037829: reply ok 124 access c 0000
19:02:56.676512 IP 192.168.1.7.3774037830 > 192.168.1.6.nfs: 112 getattr [|nfs]
19:02:56.677486 IP 192.168.1.6.nfs > 192.168.1.7.3774037830: reply ok 116 getattr [|nfs]
```

Figura 5.4b. Trecho do conteúdo do arquivo de saída do tcpdump

O quadro 5.4b. demonstra a saída gerada pelo script de monitoramento da rede, por meio do comando TCPDUMP, que rastreia e identifica os cabeçalhos dos pacotes que trafegam na rede. As linhas destacadas em negrito indicam a entrada ou sincronização de alguns dispositivos no ambiente. Por meio destas são extraídos os endereços IP e MAC ADDRESS destes dispositivos. As demais linhas do arquivo são descartadas e o arquivo de *log* é zerado, o que possibilita um grande número de usuários se conectem a rede sem que o arquivo de log se torne muito grande.

```
 ****  Arquivo  de  Log  ****

18:59:13|192.168.1.7|00:03:ba:92:99:a8
18:59:57|192.168.1.102|00:11:f5:57:ce:e3
18:59:59|192.168.1.9|00:e0:06:09:55:66
19:00:00|192.168.1.4|00:03:ba:0c:d5:61
19:00:10|192.168.1.1|00:40:f4:61:59:3e
19:00:15|192.168.1.6|00:03:ba:0c:e8:89
19:00:23|192.168.1.1|00:40:f4:61:59:3e
19:00:28|192.168.1.32|00:0e:a6:3b:21:7f
```

Figura 5.4c. Conteúdo do arquivo de log
(Hora/IP/MAC das máquinas que solicitam acesso a rede)

O quadro 5.4c. é o extrato do arquivo de Log criado pelo servidor de autenticação, este arquivo contém os dados de identificação das máquinas que acessaram a rede, assim como a hora especifica destes acessos.

```
#Tue  Nov  25  18:36:15  BRST  2005
920845658741=/192.168.1.31| ******
32165498728=/192.168.1.31| ******
98765432146=/192.168.1.31| ******
```

Figura 5.4d. Conteúdo do repositório de dados do usuário – arquivo properties
(CPF/IP/senha dos usuários conhecidos na rede)

O quadro acima (5.4d.) demonstra o conteúdo do arquivo *properties*, que é constituído pelos dados de identificação dos usuários que autenticaram seus dispositivos no ambiente de rede.

6. CONCLUSÃO

6.1. CONCLUSÕES GERAIS

A preocupação fundamental nos dias atuais, quando se fala em tecnologia de rede sem fio é a segurança. Este trabalho realizou uma analise geral sobre os padrões de redes sem fio disponíveis no mercado, levantou as principais características destas e apontou os aspectos falhos relacionados a segurança em ambientes sem fio. Nota-se que os principais riscos e vulnerabilidades destas redes, estão relacionadas as limitações do modelo IEEE 802.11, a inexperiência dos profissionais que realizam a configuração dos equipamentos e a usuários mal informados sobre os cuidados que devem ser tomados na utilização deste meio.

O resultado destes estudos, conciliado com a avaliação dos equipamentos e a topologia da rede sem fio instalada no CRSPE, permitiram avaliar os níveis de integridade e confiabilidade que a mesma apresenta. Essa avaliação serviu também de base para a elaboração de uma política de segurança específica para o uso da rede sem fio, com o objetivo de padronizar e alertar os usuários desta rede, sobre as regras e cuidados que devem ser tomados durante a utilização da mesma. Em relação a limitação do próprio padrão 802.11, as definições do modelo RSN foram aplicadas, através da implementação de servidor de autenticação RADIUS e da modelagem de um serviço de autenticação para múltiplos acessos a dados baseado em agentes.

Ao término deste trabalho conclui-se que as medidas de segurança agregadas a rede sem fio do CRSPE permitiram alcançar um nível de segurança. Além de disponibilizar ao grupo de segurança, ferramentas e métodos eficientes para o controle e gerenciamento da rede.

6.2. TRABALHOS FUTUROS

Uma proposta de trabalho futuro é a implementação de uma interface amigável para Serviço de Autenticação com Agentes, agregando funcionalidades do modelo de autorização baseado em hierarquia de papéis. O intuito da união desses métodos é disponibilizar uma maneira eficiente para a administração e também o gerenciamento da segurança de uma rede sem fio, agregando a formalidade imposta por este método de autorização.

REFERÊNCIA BIBLIOGRÁFICA

[1] MANIFESTO**,** Manifesto de apoio à Implantação do Centro Regional Sul de Pesquisas Espaciais (CRSPE), < http://www.crspe.net/>, 2004.

[2] FURUKAWA CERTIFIED PROFESSIONAL - MASTER MF 105 , Projeto de Sistemas de Cabeamento Estruturado, versão 2.01, Edição Revisada 10/06/00.

[3] TIA/EIA, (Telecommunications Industry Association/Eletronics Industry Association), "Comercial Build ing Telecommunications Cabling – Standard ANSI/TIA/EIA 568 A".

[4] WIKIPEDIA, The free encyclopedia, "IEEE 802.11 - Standard", <http://en.wikipedia.org/wiki/802.11>, 2005..

[5] NBR 17799 ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. "Código de pratica para gestão da segurança da informação" – NBR/ISSO/IEC 17799, 2001.

[6] Arcomano, R., "Wireless Howto", <http://tldp.org >, 2003.

[7] Volbrecht, J. e Moskovitz, R.; "Wireless LAN Access control and uthentication",
< http://www.interlinknetworks.com >, 2003.

[8] Cristina, Tereza Melo de B Carvalho, "Network Administration and
Management Model – A Proposal for Corporate Network: LARC, PSC, EPUSP", 2001.

[9] Mendonça, Evaldo Galvão, "Aplicação da norma NBR ISSO/IEC 17799 no desenvolvimento de um modelo de segurança para o CRSPE", Trabalho de Graduação, Curso Ciência da Computção, UFSM, 2004.

[10] AirDefense White Paper, "Wireless LAN Security – What Hackers Know That You Don't", < http://www.airdefense.net >, 2003.

[11] Murillo, N. M. de O., “Segurança Nacional”, Novatec Editora Ltda., 2002.

[12] M. Bernardes, P. Pinheiro, “Segurança em Redes IEEE 802.11”, Wireless Communication Symposium 2004 – 1st International Wireless Conference in Portugal, 2004

[13] W. Ye, J. Heidemann e D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks”, In Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies,< www.isi.edu/scadds/projects/smac >, 2001,

[14] Pereira R. Mariluce , “Tutorial sobre redes de Sensores”, Programa de Engenharia de Sistemas e Computação, UFRJ, 2002.

[15] ROSS, Keith W. KUROSE. James K. “Redes de Computadores e a Internet”. São Paulo: Addison Wesley, 2003.

[16] TANEMBAUM. Andrew S. “Redes de Computadores”, Rio de Janeiro: Campus, 2003.

[17] Garg, V.; Wilkes, J.; “Wireless and Personal Communication Systems”, Prentice Hall, 1996.

[18] Anastasi et alli; “MAC Protocols for Wideband Wireless Local Access: Evolution Toward Wireless ATM”, IEEE Personal Communications, Oct. 1998.

[19] LaMaire et alli; “Wireless LANs and Mobile Networking: Standards and Future Directions”, IEEE Communications Magazine, Aug. 1996.

[20] Peterson et Dave; “Computer Networks, A system approach”, Morgan Kaufmann, 2000.

[21] Walrand et Varaiya; “High-Performance Communication Networks”,Morgan Kaufmann, 2000.

[22] IEEE - Institute of Electrical and Electronics Engineers, http://www.ieee.org/

[23] Fowler, Martin et Scott, Kendall, “HUML Essencial – Um breve guia para a linguagem-padrão de modelagem de objetos”, 2° Ed., Bookman, 2000.

[24] http://www.warchalking.com.br/.

[25] InfoSecurity, Task Force , http://www.istf.com.br

[26] Kismet HomePage, www.kismetwireless.net/

[27] AirSnort HomePage, http://airsnort.shmoo.com/

[28] Extreme Networks HomePage, www.extremenetworks.com/

[29] TCPDUMP Public Repository, www.br.tcpdump.org/

[30] Wikipédia, Enciclopédia Livre,http://pt.wikipedia.org/wiki/ARP

[31] Kerberos: The Network Authentication Protocol, http://web.mit.edu/kerberos/www/

[32] Tacacs+ RPM Distribution Home Page, http://www.gazi.edu.tr/tacacs/index.php?page=documents

[33] The official Bluetooth Website, http://www.bluetooth.com/

[34] Radius, GNU Project, www.FreeRadius.org/

[35] RNP Rede Nacional de Pesquisa, http://www.rnp.br/newsgen/9805/wireless.html

[36] Extreme Networks, http://www.extremenetworks.com

[37] Source Forge, http://sourceforge.net/

[38] Christiane M. Schweitzer, Rony R. Sakuragui, Tereza Cristina Carvalho, Yeda Regina Venturini, “Tecnologias de Redes Sem Fio: Wpans, Wlans e Wmans Desafios de Segurança, Vulnerabilidades e Soluções”, http://www.linorg.cirp.usp.br/SSI/SSI2005/Microcursos/MC04.pdf