

ANÁLISE DAS VULNERABILIDADES DE SEGURANÇA EXISTENTES NAS REDES LOCAIS SEM FIO: UM ESTUDO DE CASO DO PROJETO WLACA.

Lidiane Parente Andrade¹, Daniel Nelo Soares², Mauro Margalho Coutinho³,
Antônio Jorge Gomes Abelém²

¹SERPRO – Serviço de Processamento de Dados

²UFPA – Universidade Federal do Pará

³UNAMA – Universidade da Amazônia

lidiane.andrade@serpro.gov.br, danielnelo@amazon.com.br, margalho@superig.com.br, abelem@ufpa.br

Abstract. *The 802.11x standard for wireless network has been widely adopted by large corporations and institutions during its daily tasks, forasmuch the productivity increase produced by flexibility and mobility found in these new sorts of wireless equipments have provided great operational advantages. Nevertheless, there are some important security issues that should be take in consideration while using this new technology. Having the goal to provide another reference for researchers and technicians, this paper studies some security vulnerabilities, some methods and tools for wireless hacking used in today wireless networks.*

Resumo. *O padrão 802.11x para redes sem fio tem sido largamente adotado por corporações e instituições para suas tarefas cotidianas, haja vista que o ganho de produtividade, gerado pela mobilidade e flexibilidade encontradas nesses novos equipamentos sem fio, tem proporcionado grandes vantagens operacionais. No entanto, existem questões de segurança importantes que devem ser consideradas ao se utilizar essa nova tecnologia. Com o intuito de prover mais uma fonte de referência para técnicos e pesquisadores, este projeto estuda as vulnerabilidades de segurança, as formas e ferramentas de ataques existentes nas redes sem fio atuais.*

1. Introdução

No mundo moderno, em que os avanços tecnológicos proporcionam, a cada dia, alterações no modo de utilização das comunicações, as atenções estão voltadas para a mobilidade e flexibilidade de novas formas. Temos, hoje, que as barreiras a serem quebradas são as das transmissões de dados entre dispositivos que dispensem o uso de fios e cabos, surgem as chamadas Redes Sem Fio.

O termômetro do sucesso de qualquer tecnologia é representado pela sua aceitação no mundo corporativo-institucional. Se uma nova tecnologia consegue penetrar no mundo onde os negócios são feitos e os lucros são gerados, sua longevidade estará garantida até que uma nova descoberta científica se consolide em condições de substituí-la. O padrão 802.11x para redes sem fio alcançou este status de uso.

A mobilidade alcançada com a utilização dessa nova tecnologia gerou um aumento de produtividade em torno de 22% [Gaundêncio 2003] nos diversos setores da

economia mundial. Entretanto, apesar da euforia provocada nas corporações usuárias por esse novo paradigma de comunicação de dados, ainda existem restrições quanto ao seu uso para transmitir informações críticas ou sigilosas, devido às diversas vulnerabilidades detectadas no padrão 802.11x.

2. Redes sem fio

O desenvolvimento das redes locais sem fio se iniciou em meados da década de 80, com a utilização de diferentes tecnologias como infravermelho, rádio de microonda e rádio *spread spectrum* (espectro de dispersão), sendo este último um tipo de microonda com componentes adicionais de segurança [Tanenbaum 2003].

Em 1997, a IEEE (*Institute of Electrical and Electronics Engineers*) publicou um padrão específico para redes sem fio, denominado 802.11 [Tanenbaum 2003]. Na mesma época, foram criados outros padrões como a HiperLAN/2 e Bluetooth. Com estas padronizações, surgiu uma nova onda de interesse para este mercado, aumentando significativamente o número de sistemas implementados a partir de então. Obviamente que o estabelecimento do padrão IEEE trouxe grande melhoria da tecnologia, viabilizando a interoperabilidade entre os diversos fabricantes que o seguiram. Mais tarde, durante o processo de melhoramento deste padrão, houve uma divisão de opiniões que gerou a quebra do comitê e o prosseguimento de dois padrões independentes: o 802.11a e o 802.11b.

Com a evolução do protocolo para as versões 802.11a/b, tornou-se mais atrativo para o mercado investir em infra-estruturas deste tipo, já que as taxas de transmissão foram elevadas para 54 Mbps e 11 Mbps, respectivamente, ao invés dos 2 Mbps alcançados no 802.11 original. Além destes, foram criados outros padrões, como 802.11g e 802.11f, cada um com características específicas para diferentes aplicações.

3. Segurança em redes padrão 802.11x

Um dos grandes atrativos das redes sem fio reside no fato dos usuários ficarem livres para se moverem enquanto estão conectados à rede, considerando que os dados são transmitidos e recebidos sobre o ar, utilizando a tecnologia de transmissão via rádio.

É claro que nenhuma rede é totalmente segura, porém pode-se diminuir a vulnerabilidade em redes sem fio prevenindo os ataques mais conhecidos através de protocolos de segurança específicos e outros mecanismos utilizados também na rede cabeada. Entretanto, as redes sem fio apresentam problemas específicos além dos existentes nas redes cabeadas, já que a área de acesso ultrapassa a área física, quebrando um paradigma de controle de acesso à rede e tornando a proteção contra invasão bem mais complexa. Com isso, diversas falhas de segurança colocam em risco a confidencialidade, integridade, autenticidade e disponibilidade da comunicação destes tipos de rede.

3.1 Ataques às redes sem fio

Os ataques contras as redes sem fio decorrem da sua própria estrutura, uma vez que ponto de acesso precisa anunciar a existência da rede, de modo que os clientes possam se conectar e usufruir todos os serviços e recursos fornecidos. Para isso, *frames* especiais, conhecidos como *beacons* (balizas), são enviados periodicamente, facilitando a descoberta de uma rede sem fio, inclusive por pessoas mal-intencionadas.

Na realidade, o objetivo dos ataques não é apenas comprometer a rede sem fio, mas também ganhar acesso ou comprometer a rede cabeada, podendo levar à exploração de todos os recursos que a rede oferece.

3.1.1 MAC Spoofing

Para as redes onde os pontos de acesso utilizam o endereço MAC para o controle dos usuários autorizados, a conexão pode ser invadida por este tipo de ataque. Um atacante pode capturar um endereço MAC válido de um cliente e trocar seu endereço pelo do cliente, pois alguns dos dispositivos para redes sem fio possuem a particularidade de permitir a troca do endereço físico [Duarte 2003]. De posse de tal endereço, o atacante poderá utilizar a rede e todos os seus recursos.

3.1.2 Wardriving

Wardriving pode ser considerado uma forma de ataque de vigilância, tendo como objetivo encontrar fisicamente os dispositivos de redes sem fio para que estes dispositivos possam, posteriormente, ser invadidos. Para isto, algumas ferramentas fáceis de serem encontradas na Internet são usadas para encontrar redes sem fio que estão desprotegidas. A partir disso, pode-se fazer o *logon* ou conectar-se através dessa rede à Internet, podendo monitorar o tráfego da rede e até violar suas chaves de criptografia WEP.

3.1.3 Warchalking

A partir da utilização de técnicas de *wardriving*, o atacante identifica os sinais de redes acessíveis e as identifica através da pichação de muros e calçadas com símbolos próprios numa tentativa de mantê-las em segredo [Ross 2003].

3.2 Mecanismos de Segurança

3.2.1 WEP

O WEP (*Wired Equivalent Privacy*) é o protocolo de segurança padrão do 802.11x, atuando na camada de enlace entre as estações e o ponto de acesso. O WEP oferece três tipos de serviços que são: confidencialidade, integridade e autenticação.

Confidencialidade

A confidencialidade impede que pessoas não autorizadas tenham acesso à informação, e a implementação desta é opcional. Quando está ativada, cada estação tem uma chave secreta compartilhada com o ponto de acesso, e não há uma forma padrão de distribuição dessas senhas, sendo feita manualmente em cada estação.

Integridade

A integridade garante que o receptor obtenha os dados corretos, ou seja, que não haja alterações nos *frames* enviados pelo transmissor, nem dados indesejados incluídos na transmissão ou removidos no meio do caminho. A integridade é implementada no WEP através do polinômio CRC-32 (*Cyclic Redundancy Check*), onde é adicionado um ICV (*Integrity Check Value*) para cada carga útil [Maia 2004].

Autenticidade

A autenticidade identifica quem está executando uma determinada ação, podendo assim fazer um controle de acesso aos recursos disponíveis. A autenticação do

WEP é baseada na chave compartilhada, que utiliza a técnica de *challenge-response*. Nela, somente a estação é autenticada, solicitando ao ponto de acesso esta autenticação.

Vulnerabilidades

Apesar de o WEP ser bastante utilizado para tornar a comunicação de uma rede sem fio mais segura, muitas falhas são apontadas. Uma das vulnerabilidades desse protocolo está associada à reutilização do vetor de inicialização (IV).

Outra vulnerabilidade do WEP está relacionada ao CRC-32. Como seu algoritmo de garantia de integridade é linear, possibilita que modificações sejam feitas no pacote sem que sejam detectadas. Uma das grandes fraquezas do WEP é a falta de gerenciamento de chaves, pois o padrão WEP não especifica como deve ser a distribuição das chaves.

3.2.2. Controle do endereço MAC

Uma das maneiras utilizadas para garantir a autenticação do usuário é a partir do controle de endereços MAC. Esses endereços de 48 bits identificam uma placa de rede local de forma exclusiva, de modo que, a partir de uma lista contendo todos os endereços MAC válidos nos pontos de acesso, pode-se impedir que dispositivos que não possuam o endereço nesta listagem se associem ao ponto de acesso.

Vulnerabilidade

Esse mecanismo, entretanto, não é seguro, pois é possível falsificar os endereços MAC usados nas placas de redes. Com a observação do tráfego da rede, um atacante pode encontrar um usuário válido e clonar seu endereço MAC, obtendo assim acesso à rede.

3.2.3 FIREWALL

O *firewall* é um servidor de Proxy que filtra todo o tráfego que passa por ele, através da rede, nos dois sentidos, com base nas regras de sua configuração. O *firewall* pode estar localizado no *gateway* entre os pontos de acesso da rede sem fio com a rede com fio. Assim, o firewall isola as duas redes, com fio e sem fio, evitando assim que pessoas não autorizadas que consigam acesso a uma rede tenham acesso à outra.

Vulnerabilidade

Um *firewall* localizado no *gateway* protege a rede de invasores externos, porém não protege dos invasores que estão no mesmo lado da rede, pois os nós não são isolados uns dos outros. Um invasor pode ter acesso aos arquivos que estão na mesma rede e ler os arquivos que estão compartilhados.

4 ESTUDO DE CASO: PROJETO WLACA

4.1 DESCRIÇÃO DO CENÁRIO

O Projeto WLACA (Rede Wireless do Laboratório de Computação Aplicada) foi desenvolvido pela iniciativa do Departamento de Engenharia Elétrica e de Computação (DEEC) da Universidade Federal do Pará (UFPA), com o objetivo de realizar estudos na área de Redes de Sensores e TV digital (canal de retorno), utilizando o padrão rede 802.11b.

Neste estudo de caso foram submetidos a testes os seguintes mecanismos de segurança: controle de endereço MAC, WEP e RADIUS; realizados na própria UFPA,

tanto no LACA (Laboratório de Computação Aplicada), como no estacionamento do DEEC.

Os testes foram desenvolvidos em dois cenários diferentes e independentes:

4.1.1. CENÁRIO 1: uma rede outdoor com o SSID (*Service Set Identifier*) WLACAOUTDOOR.

O WLACAOUTDOOR funciona como um link entre o DEEC e o CT (Centro Tecnológico). Esta rede está configurada como um WDS (*Wireless Distribution System*) e possui dois pontos de acesso: um AP-2500 no DEEC e um AP-2000 no CT, cada um com duas antenas, sendo uma direcional e a outra omnidirecional.

A rede WLACAOUTDOOR provê acesso público à Internet através de um Proxy Transparente – sem autenticação – configurado no AP-2500, sendo que é neste ponto de acesso onde ocorre a gerência da rede WLACAOUTDOOR, configurada através da rede cabeada com a utilização de um cabo UTP (*Unshielded Twisted Pair*). Esta medida de segurança é adotada para que as configurações da rede não possam ser alteradas por usuários da rede sem fio.

4.1.2. CENÁRIO 2: uma rede indoor com o SSID WLACAINDOOR.

O WLACAINDOOR possui um ponto de acesso (AP-600) instalado dentro do LACA, funcionando como *bridge* entre a rede cabeada do LACA e a rede sem fio. Porém, a antena embutida no AP-600 emite sinal para algumas salas do prédio do DEEC.

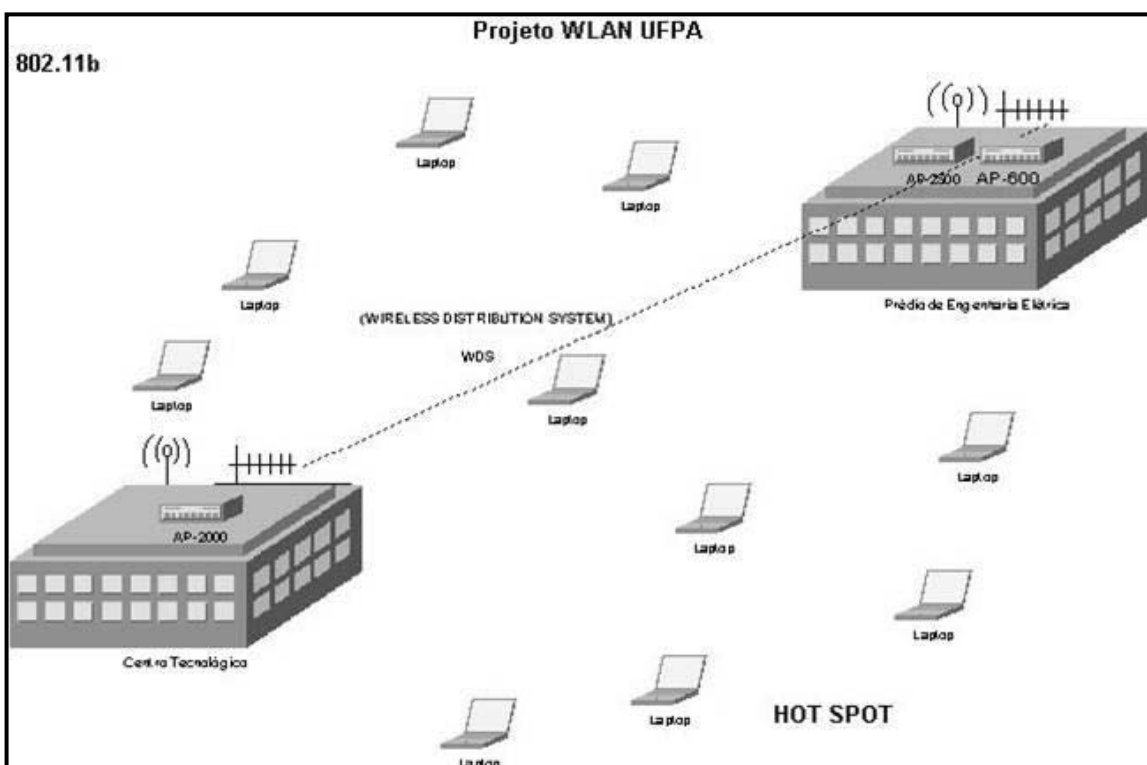


Figura 1. A Arquitetura do Projeto WLACA.

4.2. Especificação dos Equipamentos

Neste estudo de caso foram utilizados diversos equipamentos tanto para configuração da rede sem fio, quanto para a análise da rede, conforme a Tabela 1.

Tabela 1. Especificação dos equipamentos utilizados no estudo de caso.

Dispositivo	Especificação
<i>Desktop</i>	Windows XP utilizando adaptador de rede D-Link 802.11b
<i>Desknote</i>	Windows XP utilizando adaptador USB de rede Encore,
<i>Notebook</i>	Linux Knoppix-STD utilizando um cartão PCMCIA ORICONO GOLD.
AP-2500	Utilizando dois cartões PCMCIA ORICONO GOLD.
AP-2000	Utilizando dois cartões PCMCIA ORICONO GOLD.
AP-600	Utilizando um cartão ORINOCO GOLD e antena embutida.
Antenas omnidirecionais	Uma de 8 dBi e outra de 15 dBi.
Antenas direcionais	Tipo grade, as duas de 21 dBi.

4.3. Softwares

As redes sem fio apresentam novas necessidades, não só em tecnologia, mas também em monitoramento e visualização. Para supri-las, vários *softwares* com diversas finalidades são utilizados. Para este estudo de caso, foram necessários alguns *softwares*.

4.3.1. NetStumbler

O NetStumbler é a ferramenta para Windows mais conhecida para detectar redes sem fio, por ter a capacidade de encontrar os adaptadores de rede que estão emitindo sinais e reportar algumas de suas características, como: SSID, endereço MAC, nível de sinal, nível de ruído, canal de frequência e WEP. Este programa modificou significativamente o mundo da rede sem fio, pois além de ser utilizado para ações maliciosas, pode ser utilizado para monitorar a qualidade do sinal e quantos dispositivos estão instalados na rede.

4.3.2. AirSnort

O *software* Airsnort trata-se de um *sniffer* para redes sem fio capaz de monitorar o tráfego de toda a rede e, dependendo do tamanho da chave, quebrar a criptografia WEP.

4.3.3. MAC Changer

O *software* MAC Changer foi desenvolvido para linux, com o objetivo de manipular o endereço MAC de placas de rede. Esta ferramenta permite que seja alterado o endereço MAC de mais de 6000 interfaces de rede diferentes, inclusive para endereços de outros fabricantes.

4.3.4. WEPCrack

WEPCrack é um programa linux que explora as deficiências no algoritmo WEP, para extrair a chave criptografia. Pessoas mal intencionadas utilizam o WEPCrack para obter informações vitais à rede para gerar posteriores ataques.

4.4. Testes realizados nos mecanismos de segurança dos pontos de acesso.

Diversas medidas de segurança são suportadas na configuração dos seguintes pontos de acesso: AP-2500 para a rede WLACAOUTDOOR e AP-600 para a rede WLACAINDOOR.

O AP-2500 tem suporte para protocolos WEP, tanto de 64 bits quanto de 128 bits; controle pelos endereços MAC dos usuários autorizados; servidor de autenticação RADIUS, entre outros. Enquanto que o AP-600 possui suporte para criptografia WEP

de 64, 128 e 154 bits e, também, a criptografia 802.1x, podendo ser combinadas, além do controle pelo endereço MAC.

A implementação de mecanismos de segurança é extremamente importante para as redes sem fio devido à falta de segurança causada pelas particularidades do meio físico de transmissão. Entretanto, a escolha destes mecanismos deve ser bem analisada, devido à sua sobrecarga adicional inserida no tráfego da rede, comprometendo o desempenho em até 50% [Ribas 2001].

4.4.1. Controle do endereço MAC

Em princípio, o bloqueio por endereço MAC funciona perfeitamente, não permitindo que usuários não cadastrados entrassem na rede, porém este mecanismo de segurança possui dois problemas. O primeiro decorre da impossibilidade de ser utilizado em redes que provêem acesso ao público, como o WLACAOOTDOOR, uma vez que se torna impossível ter um controle de todos os endereços MAC.

O segundo problema está relacionado à fragilidade deste mecanismo. Devido ao fato de alguns adaptadores de rede suportarem que seus endereços MAC sejam alterados via *software*, podendo assim, através de um estudo da rede (*Sniffing* e *Mac Spoofing*), saber quais os endereços MAC cadastrados e adentrar na rede. Na simulação feita no ambiente real foi possível capturar pacotes da rede sem fio com o uso do *software* Airtsnort, identificar os MAC's capazes de comunicar com o Ponto de Acesso da rede e, através do *software* MAC Changer, alterar o endereço MAC do adaptador de rede ORINOCO GOLD pelo MAC do adaptador D-Link, modelo Air Plus DWL-520+ (válido para a rede) e assim conseguir acesso irrestrito a rede. Porém ao se tentar alterar o endereço MAC do mesmo adaptador ORINOCO pelo endereço do adaptador USB de rede Encore, modelo ENW1-USB-RE-CA não foi possível o ingresso na rede. Concluiu-se, portanto, que tal forma de ataque não apresenta sucesso garantido, devendo o usuário mal intencionado capturar vários endereços MAC's para ter a certeza de que pelo menos um irá funcionar.

4.4.2. RADIUS

Todos os três pontos de acesso utilizados neste estudo de caso têm suporte ao servidor RADIUS adicionando autenticação à rede. Nos testes realizados, foi possível, através do Airtsnort, capturar um login de usuário e uma senha quando a criptografia WEP estava desativada e as informações trafegavam pela rede em texto puro. No entanto, ao se habilitar o WEP tornou-se bem mais trabalhoso conseguir descriptografar um pacote de dados e obter o acesso à rede com autenticação.

4.4.3. WEP

A criptografia é uma camada adicional para evitar a escuta clandestina e acesso à rede, porém o WEP não é uma proteção forte, mas redes sem criptografia são, sem dúvida, muito mais vulneráveis. O AP-2500 suporta apenas criptografias de 64 e 128 bits, porém os *PC Cards* suportam também chaves de 256 bits. O WEP possui algumas vulnerabilidades devido à ausência de gerenciamento e ao compartilhamento da chave. Através do uso do *software* Airtsnort foi possível capturar poucas centenas de pacotes e assim quebrar chaves pequenas, até 64 bits, utilizando o *software* WEPCrack. Quanto maior o número de pacotes capturados, mais fácil quebrar a chave WEP, especialmente

as grandes, uma vez que com universo amostral mais vasto, torna-se mais fácil descobrir padrões entres os pacotes.

4.5. Avaliação dos Resultados

O estudo comprovou a insegurança existente nas redes sem fio baseadas no padrão 802.11b como as do Projeto WLACA. Diversas vulnerabilidades foram encontradas e quando aliadas às limitações de cada equipamento, demonstraram que tanto a rede interna (WLACAINDOOR) quanto a externa (WLACAOUTDOOR) são ambientes altamente suscetíveis à falhas e brechas de segurança que impedem seu uso para tráfego de dados importantes ou sigilosos.

5. Conclusão

Este projeto abordou aspectos referentes ao que hoje é considerada a maior preocupação existente ao se implantar redes locais sem fio: a falta de segurança. Verificou-se que os ganhos de mobilidade e produtividade gerados pelos aparelhos sem fio – que não deixam mais ninguém ocioso – são ainda insuficientes para roubar a hegemonia das redes cabeadas, mas já começam a ameaçá-las.

As vulnerabilidades demonstradas neste projeto têm suas origem em três pontos básicos: falha na especificação dos padrões 802.11x; limitações dos equipamentos utilizados e equívocos de configuração de técnicos ainda pouco familiarizados com o novo paradigma.

Os métodos de ataque são os mais freqüentemente utilizados por pessoas mal intencionadas para explorar as fragilidades de redes sem fio. Vale ressaltar que, apesar das vulnerabilidades serem de domínio público, exige-se um bom conhecimento técnico de várias áreas para poder explorá-las. O que, de certa forma, confere um certo grau de “proteção” – ou alívio – aos técnicos-administradores de qualquer rede sem fio.

Verificou-se que dados críticos e informações sigilosas ainda não devem ser transmitidos utilizando este meio, uma vez que não se consegue confiar na integridade de qualquer informação que trafega na rede.

6. Referências bibliográficas

- Duarte, Luiz Otavio. (2003) “Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.” www.acmesecurity.org/hp_ng/files/testes_monografias/acme-monografia-Wireless-2003-LOD.pdf, Agosto/2004.
- Gaudêncio, Maurício. (2003) “Quebrando barreiras”. <http://www.telecomweb.com.br/solutions/infra-estrutura/seguranca/artigo.asp?id=48566>, Agosto/2004.
- Maia, Roberto. (2003) “Segurança em Redes Wireless 802.11i”. http://www.gta.ufrj.br/~rmaia/802_11i.html, Agosto/2004.
- Ribas, Júlio C. da Costa. (2001) “Homologação de link, informações de desempenho e definição de acordo de nível de serviço para redes sem fio”.
- Ross, John. (2003) “O livro de WI-FI: Instale, configure e use Redes Wireless (sem-fio)”. Rio de Janeiro, Alta Books
- Tanenbaum, Andrew S. (2003) “Redes de Computadores”. 4. ed. Rio de Janeiro, Campus.