Secure Roaming Wireless: Uma Abordagem de Segurança para Redes Locais 802.11 com Criptografia Forte

Marcos José Sarres de Almeida[1,2], **MAR Dantas**[3]

[1]Aker Security Solutions – Departamento de Tecnologia – Brasília – DF - Brasil

[2]Departamento da Ciência da Computação (CIC) - Universidade de Brasília (UnB) - 70910-900 – Brasília – DF – Brasil

sarres@aker.com.br

[3] Departamento de Informática e Estatística (INE) - Universidade Federal de Santa Catarina (UFSC) - Caixa Postal 476 - 88040-900 – Florianópolis-SC-Brasil

mario@inf.ufsc.br

Abstract - *In this article we present a proposal solution and an implementation for a more secure wireless LAN use based on the standard IEEE 802.11b.In the research project we have used the Aker Secure Roaming software package, which we have added the wireless feature. The environment originally helps clients to use some security facilities in a LAN such as authentication and cryptography. Our experimental results show more security level compared to the standard 802.11b, however with less network performance. In addition, we present some interfaces that we have developed that can be very friendly and efficient to users to configure the Aker Secure Roaming package in a more secure IEEE 802.11b environment.*

Resumo - *Neste artigo apresentamos uma proposta e uma implementação de solução para utilização com maior segurança de redes wireless baseadas no padrão IEEE 802.11b. Durante nosso trabalho de pesquisa, utilizamos um sistema de servidor de cliente de criptografia, o Aker Secure Roaming, com o objetivo de autenticar e cifrar todo o tráfego de dados de uma determinada rede. Nossos resultados experimentais indicam um grau de segurança muito superior ao padrão 802.11b, porém detectamos uma pequena perda de performance para a rede. Finalizamos o artigo apresentando algumas interfaces de nossa implementação que indicam a possibilidade de estabelecimento das abordagens de segurança e autenticação forte em uma rede 802.11b de maneira amigável e eficiente.*

1. Introdução

As redes *wireless* têm se apresentado como uma infra-estrutura interessante, que podem prover uma melhoria na conectividade dos dispositivos que com um determinado poder computacional desejam se conectar as redes convencionais. As facilidades de implementação e manutenção das redes *wireless* são diferenciais interessantes que motivam sua utilização. Todavia, apesar de alguns anos terem se passado após o desenvolvimento de inúmeras tecnologias *wireless* (exemplos são os padrões *Bluetooth*, 802.11a e 802.11b) (DANTAS, 2002), ainda não existe uma nítida sinalização no mercado de qual tecnologia será mais largamente utilizada. Este fato se deve principalmente aos problemas de segurança que sugiram junto com essas novas abordagens.

Quando um novo projeto de LAN *wireless* é desenvolvido, diversas vantagens aparecem de uma forma clara. Exemplos são: a colocação de novos pontos de rede com facilidade; a mudança de local de computadores com mais flexibilidade; ou ainda a manutenção dos pontos de rede de uma forma mais simples. Mas apesar de todas as vantagens expostas, as redes *wireless* ainda têm uma certa resistência de utilização por parte das empresas, pois os ambientes *wireless* não oferecem a segurança necessária para acesso a seu ambiente corporativo (PEIKARI et al., 2002).

O artigo é organizado da seguinte forma: na seção 2 fazemos uma breve apresentação do padrão IEEE 802.11 com especial ênfase aos aspectos de segurança; o ambiente de software Aker Secure Roaming e nossa extensão do pacote para redes *wireless 802.11b* são apresentados descritos na seção 3; finalizamos este artigo com nossas conclusões e sugestões para trabalhos futuros.

2. Segurança Padrão no IEEE 802.11

O padrão IEEE 802.11 é uma especificação que define um conjunto de protocolos baseados em Ethernet *wireless*. Todavia, dentro do padrão existem diversos conceitos que devem ser observados com bastante atenção para que se possa entender perfeitamente a especificação 802.11. O primeiro modelo do IEEE 802.11 foi criado em 1997 **(**IEEE Computer Society, 2003**)**, abrangendo as versões 802.11a, 802.11b e 802.11g, cada uma com a sua taxa de acesso. Desta forma, dependendo do protocolo utilizado (exemplos de protocolos são TCP, UDP, ICMP) e a forma como estes estão configurados para operar, é possível conseguir melhores (ou piores) taxas de acesso (ANJUM et al., 2003). Por esta razão, a industria temendo uma falta de interoperabilidade na área, criou uma aliança de empresas denominada de *Wi-Fi Alliance*, para tratar da compatibilidade de seus produtos. Os produtos Wi-Fi podem funcionar em dois modos: modos de infra-estrutura (*infrastructure mode*) ou modo ad-hoc (BUZKO et al., 2001). Neste artigo, apenas será analisado o modo de infra-estrutura.

Nos primeiros cinco anos de criação, o *Wi-Fi* possuía apenas um método de segurança conhecido como WEP (*Wired Equivalent Privacy*) **(**EDNEY et al., 2003**).** Em 2000 as redes *wireless* começaram a ganhar popularidade, o que chamou a atenção da sociedade da segurança da informação que rapidamente detectou falhas no método padrão. Diversos sistemas para atacar configurações *wireless* foram aparecendo, mostrando diversas vulnerabilidades das redes *wireless*. Desta forma, outras tecnologias

foram desenvolvidas para agregar valor à segurança das redes *wireless* (ALLEN et al.,2002). Todavia, ainda hoje não existe uma forma de segurança padrão atenda aos usuários dos ambientes *wireless* de forma satisfatória, visando evitar problemas contra elementos mal intencionados.

Alguns analistas **(**PARK et al., 2002**)** criticaram o projeto do modelo de segurança proposto pelo IEEE, pelo fato do mesmo apresentar inúmeras falhas. Assim, vamos a seguir apresentar algumas características e as vulnerabilidades na abordagem WEP.

Características e Vulnerabilidades do WEP

O WEP trabalha com chaves compartilhadas (*shared key*), fazendo com que tanto a STA (estação de trabalho) como o AP (Access Point) conheçam a chave de criptografia que é instalada em cada máquina e no AP pelos administradores. Quando a autenticação segura esta implementada em um ambiente *wireless* o processo de autenticação ocorre na forma *challenge/response*. O algoritmo de criptografia utilizado pelo WEP é conhecido como RC4 (SCHNEIER, 1997). A principal operação de criptografia executada pelo RC4 é uma operação binária conhecida como XOR (*Exclusive OR*).

O padrão WEP possui várias falhas muito sérias que o tornam um padrão extremamente fraco do ponto de vista da segurança da informação. As redes *wireless* do padrão IEEE têm sua vulnerabilidade expostas, uma vez que os sinais de rádio podem ser captados fora da empresa, fato preocupante para o 802.11b que possui uma área de alcance maior. Já foram demonstrados ataques a redes *wireless* a mais de 40 km de distância, com a utilização de antenas de alta intensidade (SHIPLEY, 2001).

Apesar do método RC4 ser extremamente rápido, este foi quebrado em 1994, existindo um processo de engenharia reversa através da qual é possível conseguir o valor das chaves diante de um conjunto de textos em claros e textos cifrados. Como Fluhrer comenta (FLUHRER, 2000), devido ao fato do início de toda mensagem 802.11 possui características próprias (tais como campos fixos), uma análise estatística pode ser feita e assim se quebrar uma chave WEP em poucas horas. Na tabela I identificamos os principais problemas de segurança relativos à abordagem WEP (SOUMENDRA, 2002). Alguns criptógrafos analisaram as características do WEP e encontraram formas de se descobrir a chave do sistema (Walker, 2001).

Tabela 1. Principais Vulnerabilidade do WEP

1	WEP e chaves de 104 bits são opcionais	6	Após a autenticação, existe a possibilidade de roubo da sessão da STA (*session hijacking*).
2	Chaves idênticas em todas as máquinas na abordagem *default.*	7	Método de autenticação fraco, facilitando a criptoanálise.
3	Troca de chaves não é segura.	8	Controle de acesso feito apenas pelo endereço MAC.
4	Mesma chave para autenticação e codificação dos dados.	9	Possibilidade de ataques de repetição.
5	Fragilidade do algoritmo criptografia RC4.	10	Pequeno tamanho dos vetores de inicialização.

3. Projeto de Secure Roaming Wireless

Nesta seção vamos apresentar nossa contribuição, visando aumentar a segurança para o tráfego de rede de um ambiente 802.11 com WEP implementado. Como todo o padrão 802.11 é definido sobre a camada de enlace de dados, a idéia é agregar todo um sistema

de criptografia e autenticação sobre a camada superior. Em outras palavras, nossa abordagem adiciona uma maior segurança na camada de rede.

Decidimos utilizar o pacote aplicativo comercial Aker Secure Roaming (Aker, 2004), da empresa Aker Security Solutions, visando que nossa contribuição pudesse ser testada em um ambiente real. Este software implementa a criação de um canal cifrado entre o cliente e o servidor, utilizando chaves de até 256 bits e autenticação de usuários..

O Aker Secure Roaming Server possui um certificado digital com um conjunto de chave pública e chave privada. Para cada tentativa de conexão de um cliente ao servidor, o servidor envia a sua chave pública ao cliente. O servidor então escolhe um algoritmo de criptografia (em geral, AES 256) e gera uma chave de criptografia simétrica para operar o túnel criptográfico. Uma vez validado os pacotes o túnel de VPN está estabelecido. Ilustramos na figura 1, um exemplo de estabelecimento de conexão segura.

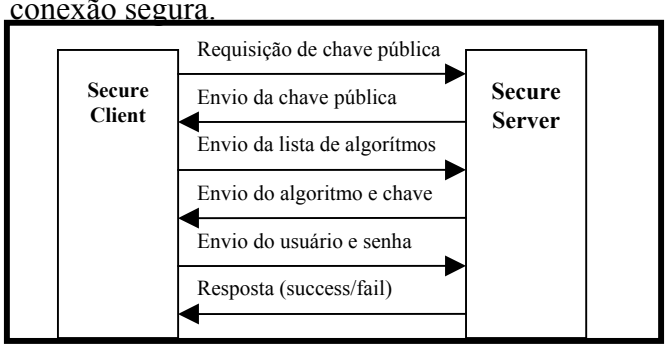

Figura 1: Estabelecimento de uma seção segura

3.1 Secure Roaming Wireless

Nesta seção apresentamos nossa contribuição de projeto que foi denominada de Secure Roaming Wireless (SRW). O ambiente utiliza as funcionalidades do Aker Secure Roaming para poder fornecer segurança forte para uma LAN *wireless* 802.11b. Conhecendo as falhas encontradas no WEP, foi importante definir alguns objetivos para a segurança da rede *wireless*, tais como privacidade e controle de acesso.

O modelo proposto para efetuar a segurança da rede necessita que a rede toda seja dividida em diversos departamentos, sendo cada um deles utilizando o Secure Roaming. Para poder acessar a rede local, o usuário precisa instalar um Secure Roaming Client na sua máquina e estabelecer uma conexão com o Secure Roaming Server.

Tabela 2 : Configuração IP do ambiente experimental

Roteador	192.168.200.254
Access Point	10.0.10.101 (para a rede interna *wireless*) e 10.0.20.101 (para a comunicação com o servidor)
Servidor	192.168.200.1 (para a comunicação com o roteador) e 10.0.20.1 (para comunicação com a AP)
Laptop	10.0.10.1 (para se comunicar com o AP através da placa *wireless*)

Configuração do sistema

O diagrama apresentado na figura 2 ilustra a comunicação da rede. Os endereços sobre as setas representam os IPs das placas de rede. Os endereços em itálico dentro das caixas representam os *gateways* padrão.

Um pacote que queria acessar a Internet, deve fazer o seguinte percurso: o pacote sai de STA (10.0.10.1) e vai através da rede *wireless* para o AP em 10.0.10.101 que envia para o servidor Windows 2000 Server, no IP 10.0.20.1, que repassa o pacote para o roteador ADSL no IP 192.168.200.254 (figura 2).

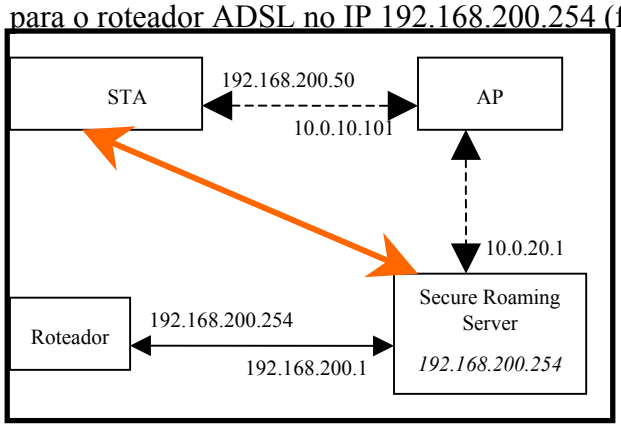

Figura 2: Diagrama da rede como Secure Roaming ativado

A configuração do Secure Roaming *Wireless* foi realizada para deixar a rede 10.0.20.0 uma rede segura. Tão logo o usuário faça acesso a uma máquina ele entra na tela de configuração do cliente e escolhe a opção de conectar. A partir deste momento ele está apto a trafegar na rede. Em adição, ainda existe a possibilidade de se estabelecer a sessão de criptografia de forma automática, agora evitando qualquer interação do usuário. Neste caso, tão logo o Windows realize o *logon,* o Aker Secure Roaming Client automaticamente se conecta com o Server e estabelece a sessão segura.

4. Conclusão e Propostas para Trabalhos Futuros

Com a crescente utilização das redes *wireless*, a necessidade de uma maior segurança do ambiente fica patente. Neste artigo, fizemos primeiramente uma pequena revisão da falta de segurança dentro do modelo padrão conhecido como WEP. Para resolver os problemas identificados utilizamos uma solução comercial. O pacote Aker Secure Roaming foi empregado e uma extensão *wireless* para o padrão IEEE 802.11b foi proposta e implementada.

Nossos resultados experimentais, após vários testes realizados, indicam que a proposta pode ser considerada uma abordagem bem sucedida, pois o ambiente pode contar com maior privacidade, melhor autenticação, controle de acesso por usuário, maior confiabilidade e integridade e proteção das chaves. Houve uma pequena perda de performance de 15% para o tráfego de rede, fato que tentaremos melhorar no futuro. Em adição, podemos dizer que a solução tem ainda como um diferencial a não requisição de nenhuma alteração de hardware ou atualização de *firmware*, sendo facilmente implementada em um ambiente de rede para suportar o padrão IEEE 802.11b.

5. Bibliografia

Aker, **Aker Secure Roaming,** http://www.aker.com.br, 2004.

ALLEN, J; WILSON, J; **Securing a Wireless Network,** Proceedings of the 30th annual ACM SIGUCCS conference on User services, 2002

ANJUM, F.; TASSIULAS, L.; **Comparative Study of Various TCP Versions Over a Wireless Link with Correlated Losses**, IEEE/ACM Transactions on Networking, Vol. 11, No. 3, 2003.

BUZKO, D.; LEE, W.; HELAL, A.; **Decentralized Ad-Hoc Groupware API and Framework for Mobile Collaboration.** ACM International Conference on Supporting Group, 2001.

DANTAS, M: **Tecnologias de Redes de Comunicação de Computadores**, Axcel Books, 2002.

EDNEY, J.; ARBAUGH, W.; **Real 802.11 Security – Wi-Fi Protected Access and 802.11i**, Addison-Wesley Pearson Education, 2003

FLUHRER, S.; MANTIN, I.; SHAMIR, A.; **Weakness in the Key Scheduling Algorithm of RC4.**, Cisco Corporation White Papers, 2000

PARK, J., DERRICK D.; **Wlan Security: Current and Future**, Syracuse University, 2002

PEIKARI, C., FOGIE, S., NEILSON, B., LANNERSTROM, S; **Wireless Maximum Security,** SAMS Publishing, 2002.

SCHNEIER, B.; **Applied Criptography**, Wiley, 1997.

SHIPLEY, M.; **Presentation on War Driving: Open WLANs**, 2001

SOUMENDRA N.; **Wireless Insecurity / How Johnny Can Hack Your WEP Protected 802.11b Network**, 2002

WALKER, J.; **Unsafe at any Key Size: An Analisys of the WEP encapsulation**, IEEE 802.11-00/362, 2001.

Wireless Lan Medium Access Control (MAC) and Phisical Layer (PHY) specifications, IEEE Computer Society, 2003