Implementação de um ponto de acesso para redes 802.11b baseado no OpenBSD

Demetrio S. D. Carrión e Luís Felipe M. de Moraes

Laboratório de Redes de Alta Velocidade – RAVEL
COPPE/Programa de Engenharia de Sistemas e Computação
Universidade Federal do Rio de Janeiro – UFRJ
Caixa Postal: 68.511 - 21945-970 - Rio de Janeiro - RJ - Brasil
{carrion, moraes}@ravel.ufrj.br

Abstract. *The security of wireless local area networks represents a new challenge in the information security field. The flaws disclosed in WEP, the security protocol used by 802.11b networks, have driven the academic community and the industry in search for new security solutions. This paper describes the development and the implementation of an access point based on the OpenBSD operational system in conjunction with several open source softwares, as well as the construction of an infrastructure to support this secure implementation in a local area network based on 802.11b standard.*

Resumo. *A segurança de redes locais sem fio representa um novo desafio para segurança da informação. As falhas encontradas no WEP, o protocolo de segurança utilizado por redes 802.11b, mobilizaram a comunidade acadêmica e a indústria na procura de soluções de segurança. Este artigo descreve o desenvolvimento e implementação de um ponto de acesso baseado no sistema operacional OpenBSD em conjunto com diversos outros softwares de código aberto, assim como na construção de uma infraestrutura que suporte a implementação segura de uma rede local baseada no padrão 802.11b.*

1. Introdução

A implementação de uma WLAN infraestruturada requer a utilização de um ponto de acesso (*Access Point* – AP) que controle as comunicações na WLAN e que atue como *gateway* para uma LAN cabeada ou Internet.

Juntamente com a disseminação e utilização deste padrão surgiram diversas questões relacionadas à segurança das transações eletrônicas que notoriamente encontram novos desafios em uma interface aérea e não-delimitada por um meio condutor. Para endereçar estas questões e garantir a autenticação, autorização e sigilo do tráfego o próprio padrão 802.11b provê uma solução através do protocolo WEP (*Wired Equivalent Privacy*).

Diversas falhas de segurança foram encontradas no protocolo WEP como descritas em [Walker 2000], [Borisov 2001] e [Fluhrer 2001]. Neste contexto, foram

propostas a utilização do padrão 802.1x, de Redes Virtuais Privadas (*Virtual Private Networks* - VPN) e do DHCP seguro como alternativas à fragilidade do WEP [Casole 2001].

A arquitetura da WLAN é outro aspecto fundamental para a garantia de segurança dos usuários móveis, do AP e da própria infraestrutura da rede local cabeada de uma entidade, que tem na WLAN uma extensão de sua abrangência. A utilização de firewalls, endereços IPs não roteáveis, por exemplo, permitem que o tráfego da rede sem fio seja contido e controlado.

A entidade central na implementação de uma WLAN é o AP, portanto oferecer meios que permitam implementar um AP com baixo custo e com total controle sobre as características de segurança dos serviços e softwares configurados no AP é um dos objetivos deste trabalho. Para tanto, optou-se pela utilização de softwares de código aberto e gratuitos, contando assim com uma ampla documentação e suporte de diversos desenvolvedores na comunidade de código aberto.

Este artigo descreve a implementação de uma solução de segurança para WLAN baseada no sistema operacional OpenBSD [OpenBSD 2002]. Para tal, utilizou-se um microcomputador como AP onde realiza-se autenticação mútua, autorizando a comunicação entre as estações da rede sem fio e o AP através do fornecimento de credenciais como login, senha e certificados digitais. Além disso, criptografando-se toda a comunicação entre as estações da WLAN e o AP de forma a garantir a confidencialidade.

2. Oportunidades observadas

i. A necessidade de definição de métodos de interligação de uma rede sem fio a uma rede local cabeada, provendo uma estrutura de autenticação, certificação, distribuição de chaves, assim como da implementação de uma solução de forma rápida e segura

ii. O alto custo de um AP é um empecilho na configuração de uma WLAN, sendo vital implementar-se uma solução de baixo custo e que garanta um controle rígido sobre as características de segurança do AP e da rede como um todo

iii. Várias propostas com relação a autenticação dos usuários móveis e o sigilo das transações eletrônicas foram definidas nos últimos anos, inclusive utilizando softwares de código aberto, como o padrão 802.1x como visto em [Open1x 2002], DHCP seguro [Drach 1999], regras de firewall modificadas dinamicamente [Shaw 2002] e o próprio WEP. A implementação de um sistema de autenticação e criptografia eficiente é fundamental na segurança de redes sem fio

3. O WStrike

O WStrike é uma distribuição do sistema operacional OpenBSD que permite a configuração de um AP a partir de um microcomputador, de forma que sejam instalados por padrão um conjunto de ferramentas de segurança que garantam a autenticação dos usuários móveis da WLAN e o sigilo de todas as transações eletrônicas entre as estações da WLAN e o AP.

O OpenBSD é um sistema operacional UNIX gratuito, baseado no BSD 4.4, cujos principais esforços enfatizam a portabilidade, padronização, correção, segurança proativa e criptografia integrada. O sistema é reconhecido como um dos mais seguros [Vaughan-Nichols 2001] e [Dyck 2002].

O WStrike estabelece também uma arquitetura de segurança para utilização de uma WLAN como extensão da abrangência de uma LAN cabeada, permitindo o controle e gerência de vários APs a partir de uma estação de gerência.

Os objetivos do WStrike são:

i. Desenvolver uma distribuição do sistema operacional OpenBSD, denominada WStrike, que capacite um usuário a configurar de forma simples e rápida um computador como AP

ii. Gerar um conjunto de sugestões e práticas que contemple a segurança da interconexão de WLANs em ambientes com infraestrutura cabeada pré-existente

iii. Implementar um sistema de autenticação de usuários baseado em certificados digitais e credenciais fornecidas por login e senha

iv. Configurar uma VPN entre as estações WLAN e o AP

3.1 Arquitetura de segurança proposta:

Diversas medidas de segurança são adotadas na configuração do AP WStrike. Algumas considerações de segurança são relativas à própria configuração segura de um sistema operacional e outras são relativas aos mecanismos de autenticação, autorização, confidencialidade e integridade do fluxo de informações presentes na WLAN gerenciada pelo AP WStrike. Uma arquitetura proposta para a integração de uma WLAN a uma LAN cabeada está representado na figura 1.

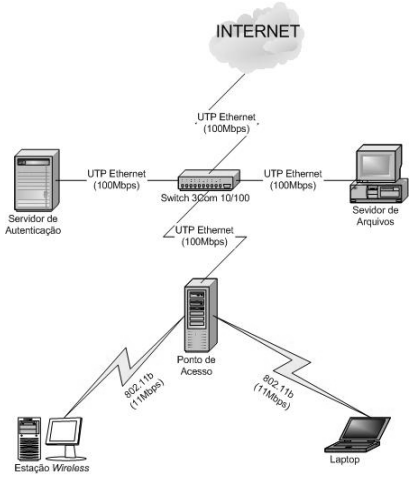

Figura 1 - Arquitetura WStrike

Esta descrito abaixo o processo pelo qual uma estação (STA) passa desde o momento em que deseja se associar ao AP até o fechamento da conexão.

i. STA procura uma rede no domínio definido pela SSID[1]
ii. STA e AP se sincronizam e a associação é estabelecida
iii. STA requisita um IP (cliente DHCP)
iv. AP fornece um IP à STA (servidor DHCP)
v. STA envia mensagens UDP para formação do túnel VPN
vi. AP verifica credenciais do usuário móvel, formando o túnel VPN
vii. Usuário da STA acessa página web a fim de se autenticar
viii. O AP requisita o certificado digital do usuário da STA
ix. O usuário da STA apresenta o seu certificado digital
x. O AP apresenta o seu certificado digital à STA
xi. O AP acrescenta o IP da STA no banco de dados de IPs autorizadas
xii. O AP reconfigura as regras de firewall
xiii. A STA está pronta para utilizar os recursos de rede oferecidos através do AP
xiv. Durante o período de conexão, o AP verifica se a STA continua ativa, a fim de que possa controlar de forma adequada as regras do firewall (implementado do sistema isAlive descrito no item 3.1.4)

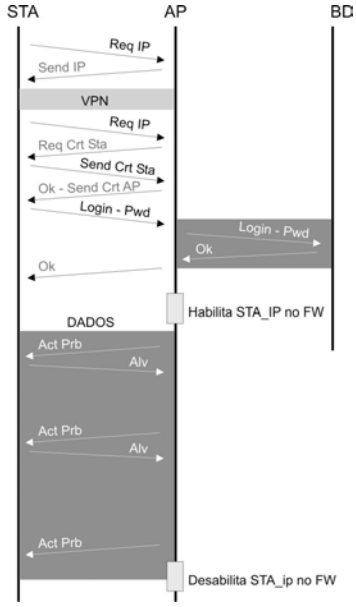

Figura 2 - Troca de mensagens no ambiente WStrike

A segurança do ambiente WStrike esta dividida em quatro partes fundamentais, sendo elas:

i. Regras de Firewall
ii. VPN

[1] Service Set Identification

iii. StrikeIN

iv. isAlive

3.1.1. Regras de firewall:

O OpenBSD possui um filtro de pacotes denominado pf (packet filter) que permite a configuração de um firewall no AP, assim como a utilização de endereços não-roteáveis através da aplicação de NAT (*Network Address Translation*) [Srisuresh 2001].

Desta forma pode-se controlar o tráfego presente na WLAN através da construção de regras de firewall específicas e dificulta-se, através do uso do NAT, o descobrimento das máquinas existentes em uma WLAN para um inimigo que se encontre fora do ambiente definido pela WLAN.

O uso do pf é vital para o funcionamento e controle de todo o ambiente WStrike pois, a mudança dinâmica destas regras permite que um usuário móvel tenha acesso seletivo aos recursos da rede na medida em que ele forneça as credenciais necessárias para passar para o próximo nível de acesso aos recursos da rede oferecidos pelo AP.

Inicialmente as regras de firewall só permitem que o tráfego destinado ao estabelecimento de uma VPN tráfegue entre a STA e o AP. Após o estabelecimento da VPN permite-se que deste tráfego critpografado, pelo protocolo ESP, somente uma página *web* de autenticação presente no AP possa ser acessada, onde credenciais como certificados digitais (autenticação mútua) e o par login/senha (autorização) são exigidos.

Após a verificação e validação do par login e senha em um banco de dados MySQL, implementado e hospedado em uma máquina específica da LAN cabeada, modificam-se mais uma vez as regras do firewall, permitindo que este usuário da WLAN acesse todos os recursos de rede oferecidos pelo AP através da VPN.

É fundamental verificar se a estação da WLAN continua ativa ao longo da utilização dos recursos do AP de forma a se previnir roubo de sessão e garantir a eficácia das regras do firewall. Isto é garantido pelo isAlive que sonda ativamente a presença de uma estação na rede, como será visto mais a frente.

3.1.2. VPN

O sigilo das transações eletrônicas no ambiente WStrike é garantido pela implementação de uma VPN entre o AP e as estações WLAN, sendo assim, todo o tráfego encontra-se critptografo no meio de transmissão.

A VPN foi implementada no modo túnel utilizando o ESP (Encapsulating Security Payload) encriptando e autenticando a parte interna do cabeçalho IP [Stalings 1999]. O gateway da VPN é representado pelo AP que executa o daemon ISAKMPD (Internet Security Association and Key Management Protocol Daemon), que efetua o gerenciamento automático das chaves e estabelecimento das SAs (Security Associations) .

Todas as estações da WLAN devem ter instalado um cliente VPN. Nesta implementação utilizou-se o SSH Sentinel [SSH 2003], que é um *software* proprietário para plataforma Windows utilizada no ambiente inicial de testes. A opção pelo SSH Sentinel se deve à farta documentação presente no site da empresa, a facilidade de

configuração do programa e ao um grande número de opções para o estabelecimento de VPN.

3.1.3 StrikeIN

O acesso à página WEB e o fornecimento das credenciais fazem parte do StrikeIN, um conjunto de procedimentos e regras que autenticam e autorizam os usuários das estações móveis. Existem algumas propostas semelhantes vistas em [NoCatAuth 2002], [OASIS 2002] e [NetLogon 2002]. No entato, nenhuma delas é baseada no OpenBSD e carecem de um mecanismo eficaz de sondagem das estações que estão ativas na rede.

Após formar a VPN o usuário da rede móvel deve acessar uma página *web* contida no AP, onde serão trocados certificados digitais entre o AP e o usuário. Em seguida este usuário fornecerá um par login/senha a fim de obter a autorização de acesso aos recursos de rede oferecidos pelo AP através da devida modificação das regras do firewall presentes nele.

A utilização de certificados digitais pressupõe a existência de uma infraestrutura de chave pública (*Public Key Infrastructure* - PKI) presente na arquitetura WStrike, onde uma autoridade certificadora deve ser implementada e os certificados devidamente assinados e distribuídos.

3.1.4. isAlive

A partir do momento em que um usuário se autentica através do sistema StrikeIN necessita-se de um mecanismo que possa verificar o momento em que ele se desligue da rede, pois a partir de então é preciso modificar as regras do firewall bloqueando seu acesso ao AP.

Dois mecanismos podem ser implementados, o primeiro baseado em um tempo determinado de conexão, após o qual o usuário deve se reautenticar e a segunda proposta que consiste em sondar a estação em intervalos de tempo determinados.

O isAlive é uma implementação do método de sondagem ativa para verificar o desligamento de um estação do AP que utiliza o Blowfish como método de criptografia.

A implementação conta com a existência de um daemon no servidor (isAliveDaemon) e um processo sendo executado nos clientes (isAliveStation), de forma que o AP e as estações possam se comunicar de acordo com um protocolo estabelecido.

Na figura 3 está apresentada uma troca típica de mensagens do sistema isAlive. Inicialmente a STA e o AP possuem uma senha em comum (PWD), a qual é utilizada pelo ponto de acesso para encriptar uma mensagem que conterá a próxima senha a ser utilizada (PKT-KEY1). A STA decripta a mensagem e desta forma obtém a PKT-KEY1, utilizada para encriptar um pacote ACK enviado para o AP. O AP verifica a identidade da estação através da decriptação desta mensagem ACK com a chave PKT-KEY1. O processo se repete utilizando-se outras chaves, até o momento em que a estação se desliga da rede e o AP não recebe um ACK como resposta, indicando o desligamento da STA para o AP.

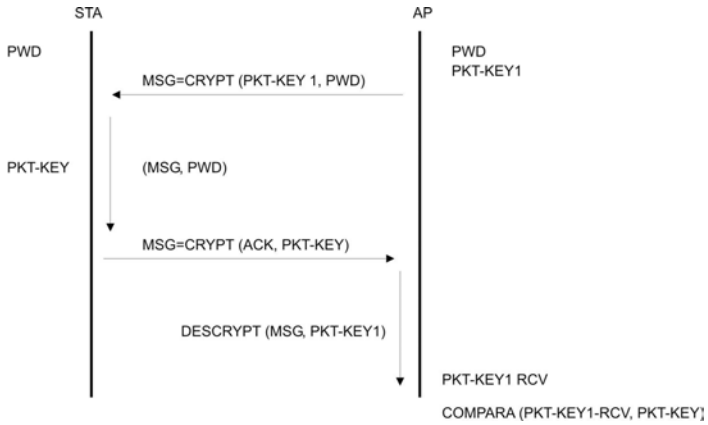

Figura 3 - Troca típica de mensagens do sistema isAlive

4. Conclusões e trabalhos futuros

A implementação de um AP para redes 802.11b utilizou-se de softwares gratuitos e de código aberto, sendo este um facilitador para a implantação WLANs. A farta documentação disponível na Internet foi fundamental para que o projeto tivesse esta abrangência, podendo-se implementar diversas características de segurança.

A arquitetura de segurança proposta, em conjunto com os métodos de autenticação, autorização e criptografia utilizados, permitem o uso em produção de uma WLAN em conjunto com uma rede local cabeada. O nível de segurança da rede sem fio através da utilização da VPN e do StrikeIN permitem um controle maior sobre as máquinas e usuários ativos na rede em comparação com uma LAN, além de se estar protegido contra ataques passivos como de sniffers.

Este trabalho possui alguns desdobramentos que são citados abaixo:

i. Implementação de uma PKI baseada em código aberto para dar suporte ao gerenciamento dos certificados digitais do AP e das STAs

ii. Teste de performance relacionado ao *overhead* introduzido devido aos processos criptográficos da VPN e do isAlive

iii. Projetar um novo gerador de números pseudoaleatórios para a geração das chaves utilizadas pelo isAlive

iv. Estudar a possibilidade de utilizar o SAMBA como um sistema autenticador de estações da WLAN

v. Implementar modificações no servidor DHCP de forma que este interaja com o firewall (pf) de forma que as regras de segurança sejam mais rígidas

vi. Submeter o isAlive a testes de avaliação de segurança

5. Referências

Borisov, N., Goldberg, I. e Wagner D. (2001) “Intercepting Mobile Communications: The Insecurity of 802.11”, 7th Annual International Conference on Mobile Computing and Networking.

Casole, M. (2002) “WLAN Security – Status, Problems and Perspective”, European Wireless 2002

Drach, S. (1999), “DHCP Option for The Open Group's User Authentication Protocol”, RFC 2485

Dyck, T. (2002) “OpenBSD 3.2 Gets It Right”, artigo publicado em

http://www.eweek.com/article2/0,3959,640713,00.asp

Fluhrer, S., Mantin, I. e Shamir, A. (2001) “Weaknesses in the key scheduling algorithm of RC4”, Eighth Annual Workshop on Selected Areas in Cryptography.

NetLogon, Ferramenta de autenticação centralizada, Páfina visitada em 2002, http://www.unit.liu.se/dokument/natverk/netlogon.html

NoCatAuth, Ferramenta de autenticação centralizada, Página visitada em 2002,

http://www.nocat.org

OASIS, Ferramenta de autenticação centralizada, Página visitada em 2002,

http://software.stockholmopen.net/

Open1X, Implementação de software aberto do padrão 802.1x, Página visitada em 2002, http://www.open1x.org

OpenBSD, Sistema operacional de código aberto e gratuito baseado no BSD 4.4, Página visitada em 2002, http://www.openbsd.org

Shaw, Derek G. e BOSCIA, Nichole K. (2002) “Wireless Firewall Gateway White Paper – Revision 3”, NASA Advanced Supercomputing Division

SSH Sentinel, Cliente VPN para a plataforma Windows, página web visitada em 2003

http://www.ssh.com/products/security/sentinel/

Srisuresh, P. e Egevang K. (2001) “Traditional IP Network Address Translator (Traditional NAT)”, RFC 3002

Stalings, William, “Cryptography and Network Security – Principles and Practice”, 2 ed, Prentice Hall, 1999, p. 399-440

Vaughan-Nichols, Steven J. (2001) “OpenBSD: The most secure OS around”, artigo publicado
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2822483,00.html

Walker, Jesse R. (2000) “Unsafe at any key size: An Analysis of the WEP encapsulation”, IEEE Document 802.11-00/362.