AirStrike: Uma implementação de segurança para redes IEEE 802.11b

Demetrio S. D. Carrión
Luís Felipe M. de Moraes, Ph. D.
Laboratório de Redes de Alta Velocidade / Programa de Engenharia de Sistemas e Computação COPPE/UFRJ
Cidade Universitária – Ilha do Fundão
21.945-970 – Rio de Janeiro, RJ
{carrion,moraes}@ravel.ufrj.br

Palavras-chave: 802.11b, segurança, protocolos de autenticação

Novas propostas de segurança para redes 802.11b vêm tomando grande destaque pela grande aplicação deste protocolo nas redes locais sem fio e nas falhas do protocolo de segurança WEP (Wired Equivalent Privacy). Este artigo descreve uma implementação de segurança para as redes 802.11b utilizando o sistema operacional OpenBSD como base e o desenvolvimento de um protocolo seguro de detecção de desligamento de estação (Dead Peer Detection), fundamental no controle de acesso às redes sem fio.

Keywords: 802.11b, security, authentication protocols.

New security proposals for the 802.11b networks have been a major concern since this standard is the base for most wireless networks and the discovery of flaws in WEP (Wired Equivalent Privacy) protocol. This paper describes a security implementation for 802.11b networks based on OpenBSD operating system and the development of dead peer detection security protocol extremely important in the wireless networks access control.

1. INTRODUÇÃO

A segurança em redes sem fio, em particular as redes baseadas no padrão IEEE 802.11b, tem sido tema de intenso desenvolvimento e debate na comunidade acadêmica e na indústria.

As WLANs (*Wireless Local Area Networks*) transmitem os dados em meio não-confinado facilitando ataques contra a autenticidade, confiabilidade e disponibilidade das transações eletrônicas.

Com esta premissa em mente o padrão IEEE 802.11b definiu o protocolo WEP com o objetivo de garantir a segurança das WLANs. No entanto, diversas falhas de segurança foram reportadas com relação à implementação deste protocolo [Walker 2000].

Com a insegurança do WEP outras soluções de segurança foram propostas como o padrão 802.1X, WPA (*Wi-Fi Protected Access*) e soluções ad hoc como VPN/IPSec [Casole 2002].

O 802.1X contém falhas comprovadas por [Arbaugh 2002]; o WPA é um padrão a ser aprovado [Wi-Fi 2003]; as soluções ad hoc carecem de uma metodologia de implantação dificultando aspectos de integração e escalabilidade, por vezes esbarrando em padrões fechados definidos por algumas empresas.

2. AIRSTRIKE

2.1 OBJETIVOS

O sistema AirStrike tem como objetivo garantir a segurança das redes sem fio baseadas no padrão IEEE 802.11b através do desenvolvimento de protocolos, ferramentas e metodologias de segurança.

Sucintamente, o sistema AirStrike se baseia em uma implementação segura de um ponto de acesso (AP – *Access Point*) IEEE 802.11b utilizando o sistema operacional OpenBSD sobre uma plataforma i386.

2.2 PREMISSAS

O AirStrike foi desenvolvido com softwares livres permitindo o seu desenvolvimento contínuo pela indústria e pela comunidade acadêmica, facilitando sua integração nos mais variados ambientes de produção e evitando a definição de padrões fechados.

O sistema foi construído sobre bases sólidas, pois os softwares livres utilizados angariam grande reconhecimento pela comunidade quanto a segurança de suas implementações, podendo-se citar o sistema operacional OpenBSD, a biblioteca openssl e o servidor IPSec isakmpd. A rápida correção de falhas de

segurança garante também grandes vantagens para os administradores das WLANs.

Outras premissas do projeto dizem respeito à instalação simplificada e rápida de um sistema AirStrike a partir de um CD, a utilização de hardware com baixo poder de processamento, suporte a divesos sistemas operacionais nas estações clientes e a definição completa de mecanismos de segurança e seus protocolos em um ambiente integrado.

Um dos diferenciais do sistema AirStrike é a definição e implementação de um protocolo de detecção de desligamento de estação (DPD – *Dead Peer Detection*), denominado isAlive descrito em 2.7.

2.3 ARQUITETURA DE REDE

Os componentes de rede da arquitetura proposta pelo sistema isAlive está apresentada na Figura 1.

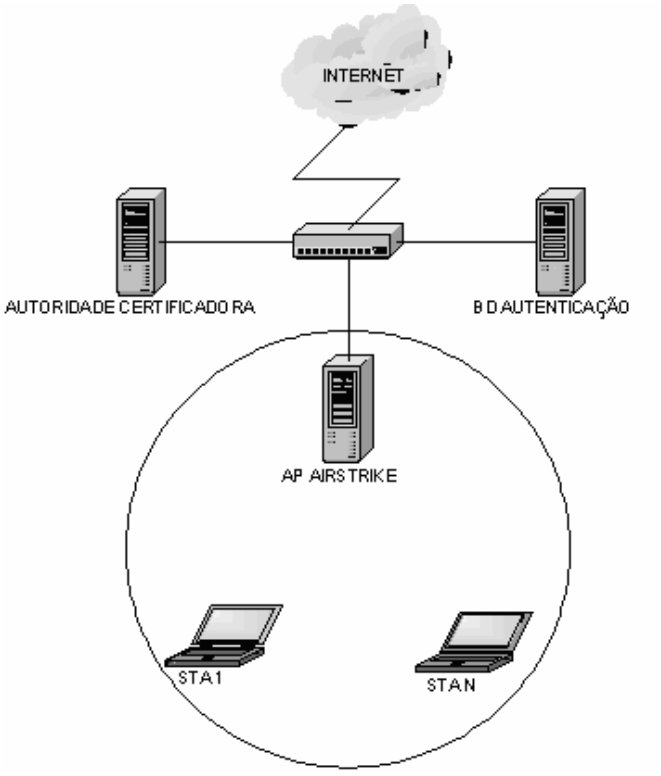

Figura 1 - Infraestrutura básica de uma WLAN AirStrike

Cada um destes componentes encerra os seguintes serviços e funcionalidades:

- AP AirStrike – dhcpd, firewall, NAT, Servidor WEB e isAliveDaemon
- Autoridade Certificadora – chave privada da CA (*Certification Authority*), certificados dos APs e lista de certificados revogados
- BD Autenticação – SGBD (Sistema Gerenciador de Banco de Dados) MySQL
- STA (estação cliente) – isAliveStation e cliente VPN (*Virtual Private Network*)

2.4 ORGANIZAÇÃO

O Sistema AirStrike está dividido nos seguintes módulos:

- AirStrikeAP – contém as funcionalidades do ponto de acesso IEEE 802.11b
- AirStrikeClient – contém as funcionalidades das estações clientes que se associarão a uma WLAN AirStrike
- AirStrikePKI – infraestrutura de chave pública utilizada no âmbito do sistema AirStrike
- AirStrikeDatabase – banco de dados de autenticação do sistema AirStrike
- isAlive – módulos relacionados à detecção automática de desligamento de uma estação (DPD)

2.5 PROCESSO DE INSTALAÇÃO

O pilar fundamental do AirStrike é o sistema operacional OpenBSD que conta com uma interface de instalação desenvolvida em [Strike 2002].

Todos os módulos apresentados na seção 2.4 possuem shell scripts UNIX de instalação que requisitam algumas informações do administrador como: faixa de endereços IP da WLAN, nome do domínio da rede sem fio (ESSID) etc. A instalação automática em sistemas Windows do AirStrikeClient encontra-se em desenvolvimento.

O módulo de instalação do cliente, descrito adiante com mais detalhes, lida com a interação do IPSec e o DHCP.

2.6 PROCEDIMENTOS DE AUTENTICAÇÃO

Abaixo, estão relacionados os mecanismos básicos que garantem a segurança e cumprimento do protocolo de autenticação e autorização de um SistemaAirStrike

- Autenticação - login/senha e certificado do ponto de acesso apresentados quando do acesso

à página de autenticação hospedada no próprio AP (Figura 2)

- Autorização – firewall, que através da mudança dinâmica de suas regras permite o acesso seletivo aos recursos da rede
- Privacidade e integridade – IPSec, implementação de uma VPN segura através do servidor isakmpd e dos clientes VPN (por exemplo: FreeS/Wan no Linux, SSH Sentinel no Windows XP etc)
- *Dead Peer Detection* (DPD) – isAlive, detectando automaticamente o desligamento de uma estação do ponto de acesso e reconfigurando as regras de firewall.

A princípio o firewall presente no ponto de acesso permite um conjunto limitado de serviços para uso das estações da WLAN, dentre eles: porta 67/udp DHCP e porta 500/udp para formação da VPN Segura.

O processo de conexão de um usuário ao sistema AirStrike está descrito pelos seguintes passos (Figura 3):

1. A estação requisita um IP ao AP
2. Um túnel VPN/IPSec é estabelecido entre STA-AP
3. O usuário acessa a página de autenticação contida no AP (Figura 2) obtendo o certificado digital do mesmo
4. Logo em seguida o usuário fornece o par login/senha
5. O AP valida o par login/senha no banco de dados de autenticação
6. Com as credenciais validadas o AP modifica as regras do firewall permitindo a utilização de outros recursos de rede pela STA
7. O AP inicia o processo de sondagem ativa da estação sem fio.

O processo de sondagem está definido pelo sistema AirStrike (AirStrikeDaemon e AirStrikeStation) onde mensagens criptografadas são trocadas entre o AP e a estação cliente, verificando assim se a mesma está ativa na rede. A partir do momento em que k-em-n mensagens de sondagem não são respondidas considera-se a estação desligada da WLAN, sendo portanto necessário redefinir as regras do firewall, retirando os privilégios dados a mesma.

Figura 2 - Página de autenticação

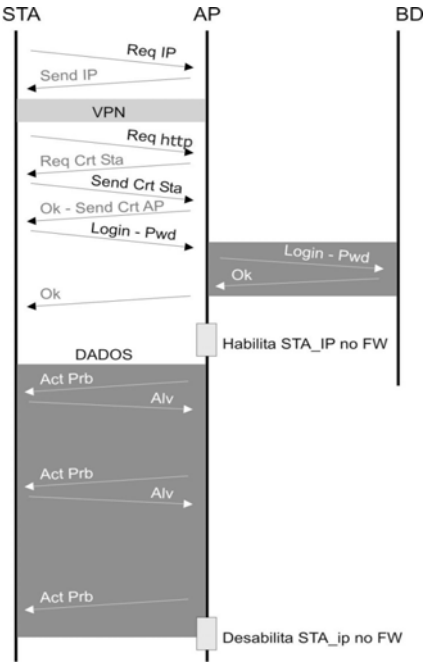

Figura 3 - Troca típica de mensagens entre uma estação sem fio e um Ap AirStrike

2.7 ISALIVE

O isAlive é fundamental na garantia de segurança do sistema AirStrike, pois garante de forma precisa que uma determinada estação utilize os recursos da rede até o momento de seu desligamento.

Outras propostas como [NetLogon 2003], [NoCatAuth 2003] e [Oasis 2003] verificam o desligamento de estações através de mensagens ICMP (ping) podendo ser facilmente forjadas ou através de timeout, oferencendo ao usuário um tempo limitado de utilização da rede.

O segundo método apresenta problemas de usabilidade pois requer a reautenticação do usuário de tempos em

tempos abrindo uma brecha de segurança quando uma determinada estação se desconecta antes do timeout, oferecendo assim uma janela de tempo para a atuação de crackers.

O isAlive utiliza técnicas de criptografia que permitem uma comunicação segura entre a estação e o AP. Um usuário mal intencionado é obrigado a descobrir qual a chave criptográfica utilizada na resposta à sondagem do ponto de acesso.

De acordo com a Figura 4 a estação (STA) e o ponto de acesso (AP) possuem uma senha em comum (PWD) que corresponde a mesma senha fornecida na página de autenticação (Figura 2).

O AP encripta uma nova chave gerada por um gerador de números pseudo-aleatórios, desenvolvido especificamente para o sistema AirStrike, com PWD e envia esta mensagem para STA.

A STA decripta esta mensagem de forma correta e responde um ACK encriptado com esta nova chave (PKT-KEY1), desta forma somente STA poderia gerar este ACK, pois a princípio, somente ela (além do AP) tinha acesso à chave inicial PWD. O processo de troca de mensagens e troca de chaves contínua até o momento em que k-em-n mensagens de sondagem (mensagens isAlive) enviadas pelo AP não são respondidas.

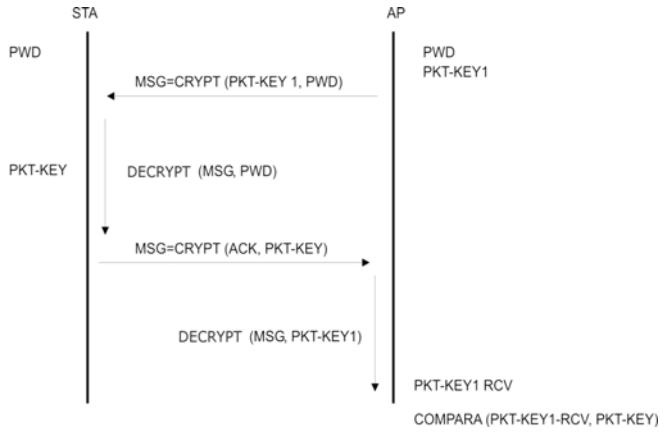

Figura 4 - Troca de mensagens isAlive

O isAlive é composto por dois programas: isAliveDaemon e isAliveStation, sendo que o primeiro reside no AP AirStrike e o segundo reside nas estações de rede sem fio.

O software foi escrito em C/C++ utilizando ambiente Cygwin, que emula Linux em plataformas Windows, garantindo a portabilidade entre os ambientes.

3. CONSIDERAÇÕES INICIAIS

3.1 USABILIDADE

O ponto a ser considerado é a usabilidade do sistema por parte do usuário. A fim de ter acesso a todos os recursos de rede oferecidos pelo AP AirStrike o usuário deve fornecer:

- Seu certificado digital ao acessar a página de autenticação
- Um par login/senha nesta mesma página
- O mesmo par login/senha para o isAliveStation

Nos primeiros testes ficou claro que a utilização de dois níveis de autenticação, representados por login/senha e a requisição de certificados digitais dos cliente, aumentaram a complexidade de gerência e usabilidade do sistema, optou-se, portanto, somente pela utilização de login/senha.

Mantém-se no entanto a apresentação do certificado digital do AP ao usuário como forma de garantir sua autenticidade.

Em seguida percebe-se o trabalho dobrado no fornecimento de uma mesma senha na página de autenticação e no isAliveStation. Por decisões de projeto optou-se por utilizar o Apache para a construção da página de autenticação aproveitando-se de suas características de segurança já implementadas em especial o SSL (Secure Socket Layer) que garante um túnel seguro de comunicação e a troca mútua de certificados digitais.

Esta escolha mostrou-se apropriada para uma prova de conceito, mas leva também aos detrimentos de usabilidade e no aumento da complexidade do sistema que por conseguinte pode ter implicações na segurança do sistema.

O desenvolvimento de um sistema de autenticação acoplado ao isAlive vem sendo foco de pesquisa e desenvolvimento pelos autores deste artigo.

Para melhor usabilidade do sistema estão sendo desenvolvidos mecanismos que facilitem ao usuário a verificação de seu status na conexão com o AP AirStrike.

Deve-se contar também com o desenvolvimento atual do gerenciamento do AP AirStrike e de toda a infraestrutura da WLAN.

3.2 DESEMPENHO

A utilização de mecanismos de criptografia acarreta em overhead na rede, diminuindo a vazão e aumentando o retardo das transmissões. Um estudo prático deste overhead pode ser visto em [Ditarso 2003] que apresenta os seguintes resultados: WEP 128 bits apresenta um overhead de 34% na vazão e a VPN/IPSec em modo túnel com protocolo ESP (3DES) autenticado (HMAC-SHA-1) apresenta overhead de 60% na vazão (Figura 5).

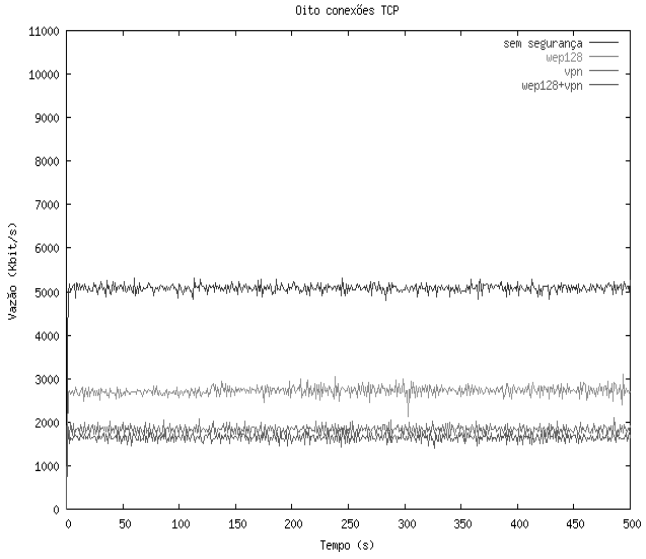

Figura 5 - Influência do WEP e IPSec na vazão das redes 802.11b [Ditarso 2003]

As imposições de desempenho de hardware do AirStrike estão apresentadas nas figuras abaixo, onde um ambiente com 2 estações WLAN, com IPSEC (Túnel-ESP-3DES-HMAC-MD5) estão em uso e o AP AirStrike é um Pentium II, 233 Mhz, 128 MB RAM e interface Wi-Fi 3 CRWE777A. Análises de desempenho mais precisas, contando com outros cenários serão desenvolvidos.

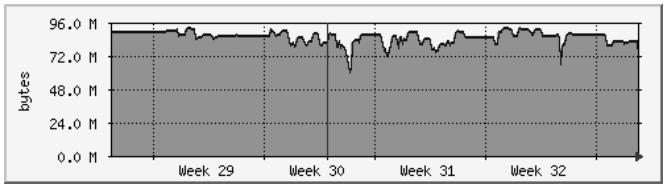

Figura 6 - Memória disponível no AP AirStrike de teste

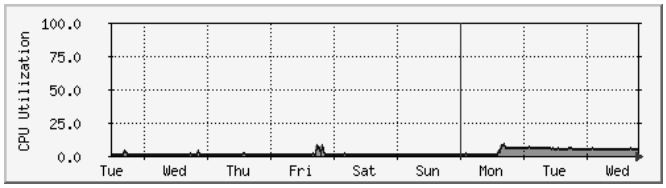

Figura 7 - Utilização de CPU no AP AirStrike de teste

Observa-se na Figura 6 que 85 MB de memória RAM estão livres, ou seja, cerca de 43 MB de memória estão sendo utilizados pelo AP AirStrike e na figura 7 a utilização de CPU teve uma taxa máxima de utilização de CPU de 10%, demonstrando um baixo requisito no poder de processamento do *hardware*.

3.3 SEGURANÇA

Os usuários autenticados na rede são identificados pelo firewall do AP AirStrike por uma tabela denominada de ipsValidos, isto proveniente em melhorias do filtro de pacotes do OpenBSD 3.3.

Com esta modificação simplificou-se a inserção de IPs autenticados pelos scripts da página de autenticação e também a sua remoção pelo isAliveDaemon, que deviam levar em conta uma escrita simultânea no arquivos de ipsValidos usados anteriormente.

3.4 COMPARATIVO

A tabela 1 apresenta um comparativo do AirStrike com outras soluções de autenticação e controle de acesso. Nota-se porém que nenhuma destas soluções garantem a privacidade das transações eletrônicas, sendo esta uma característica do AirStrike.

	Oasis	*NoCat*	*NetLogon*	*AirStrike*
Licença	**BSD**	**GPL**	**GPL**	**N.D.**
Software cliente	**Não**	**Não**	**Não**	**Sim**
Autent.	**PAM**	**Passwd MySQL**	**SSH POP3 IMAP NIS**	**MySQL**
S.O. AP	**Linux FreeBSD**	**UNIX**	**Linux**	**OpenBSD**
Controle Acesso	**IP/MAC**	**IP/MAC**	**IP**	**IP**
DPD	**Ping, Plug-in, Monitor tráfego**	**Timeout**	**ARP, Ping, SNMP**	**isAlive**

Tabela 1 – Comparativo com outras soluções de autenticação e controle de acesso

Outra solução de segurança semelhante ao AirStrike, também baseada no sistema operacional OpenBSD pode ser vista em [Godber 2002] onde se utiliza o VPN/IPSec e uma página de autenticação .

O AirStrike tem como vantagens a utilização do isAlive, que garante o controle de acesso, a metodologia de implantação, provida pela instalação integrada do sistema e o suporte à interação DHCP - IPSec.

3.5 DHCP – IPSec

Como mencionado, a existência de um túnel VPN (*Security Associtation*) depende dentre outras coisas, do IP da estação. Em um ambiente em que este IP muda (DHCP) pode ocorrer o término indesejado de uma *Security Association*.

Algumas medidas são tomadas na verificação automática da troca do IP das estações clientes, como a utilização do script dhclient-exit-hooks.

Esta solução possui alguns inconvenientes com relação à portabilidade para outras plataformas (Windows por exemplo) e intrinsicamente causa perda de pacotes devido à necessidade de reinicialização do túnel IPSec.

Uma nova proposta em desenvolvimento pelos autores é a implementação e ampliação do protocolo DHCP autenticado, definido em [RFC 3119], e sua integração com o IPSec.

Nesta proposta as mensagens DHCP serão autenticadas e criptografadas, servindo como controle de acesso às redes sem fio através da integração com o filtro de pacotes (*firewall*) e mensagens adicionais serão propostas de forma a lidar com configuração e reconfiguração das *Security Associations* (protocolo IPSec).

4. CONCLUSÕES

O sistema AirStrike foi submetido a testes iniciais pelos autores onde foi demonstrado o cumprimento de suas premissas iniciais de ter uma base sólida no provimento de segurança para redes 802.11b.

O desenvolvimento do isAlive é um ponto forte do sistema, pois assegura a validade do controle de acesso de todo o sistema.

Novas propostas estão sendo pesquisadas e desenvolvidas a partir das observações feitas na versão inicial denominada AirStrike 1.0. Dentre elas podem-se destacar o desenvolvimento de um sistema próprio de autenticação no lugar das páginas web, proposta de implementação do DHCP seguro conjunto com o IPSec e o Roaming entre APs AirStrike com especial atenção no controle de acesso e migração das *Security Associations*.

5. REFERÊNCIAS

Arbaugh, William 2002 “An Initial Security Analysis of the IEEE 802.1X protocol”

Carrión, Demetrio S. D. 2003, "Implementação de um ponto de acesso seguro para redes 802.11b baseado no sistema operacional OpenBSD", Projeto Final de Engenharia Eletrônica e de Computação, Departamento de Eletrônica da UFRJ

Carrión, Demetrio S.D. 2003, "Implementando uma PKI para uma WLAN baseada no WStrike", Monografia para o Curso de Redes Integradas de Faixa Larga e ATM do Mestrado em Redes de Computadores, COPPE/UFRJ

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

Ditarso, Paulo et al, "Avaliando a Sobrecarga Introduzida nas Redes 802.11 pelos Mecanismos de Segurança WEP e VPN/IPSec", WSeg 2003 - XXI Simpósio Brasileiro de Redes de Computadores (SBRC2003), maio de 2003.

Droms, R e Arbaugh William 2001, “Authentication for DHCP Messages”, RFC 3118

Godber, Austin e Dasgupta, Partha 2003, “Security Wireless Gateway”, WiSe 2002, Atlanta, Georgia, Estados Unidos

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/

Sarmento, André B. 2002, "Proposta e Implementação de um modelo de gerência de segurança de redes empregando CORBA", Tese de mestrado em Redes de Computadores, PESC/COPPE/UFRJ

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

Wi-Fi Alliance 2003, “Wi-Fi Protected Access Web Cast”, http://www.wi-fi.org/opensection/pdf/Wi-Fi_ProtectedAccessWebcast_2003.pdf