ANALISE DE DESEMPENHO DE PROTOCOLOS DE CRIPTOGRAFIA EM REDES SEM FIO

Camila Suzin [1], Walter Priesnitz Filho [1]

[1]Universidade de Caxias do Sul (UCS) - Campus de Vacaria
Av. Dom Frei Cândido Maria Bampi, 2800 - CEP 95200-000 – Vacaria
RS – Brasil

camilasuzin@yahoo.com.br, wpfilho@ucs.br

***Resumo**: À medida que o uso de redes sem fio e o desenvolvimento de novas tecnologias aumenta, aumenta também a necessidade de mais segurança, já que esta relação também se aplica às fraudes e espionagens na rede. Entretanto, a implementação de técnicas de segurança acabam por interferir, e muitas vezes degradar o desempenho da rede, uma vez que tais procedimentos requerem maior poder de processamento das máquinas, maior largura de banda, entre outros. Neste trabalho foi analisado o desempenho dos principais protocolos de criptografia para redes sem fio (WEP e WPA), no que diz respeito à sobrecarga introduzida na rede pela utilização de diferentes tamanhos de chaves criptográficas.*

1. Introdução

Atualmente, sabe-se que a implementação de técnicas de segurança acabam por interferir, e muitas vezes degradar o desempenho da rede, uma vez que tais procedimentos requerem maior poder de processamento das máquinas, maior largura de banda, entre outros. Desta forma, quantificar esta sobrecarga introduzida pelos mecanismos de segurança, bem como o desempenho obtido pelas redes, é essencial para a identificação das técnicas mais apropriadas, aumentando a qualidade dos serviços e a satisfação dos usuários.

Assim, neste trabalho realizou-se o estudo dos protocolos criptográficos específicos para implementação em redes sem fio, bem como a análise de desempenho dos mesmos, através de parâmetros que estabelecem relações entre segurança e desempenho.

Este artigo está organizado da seguinte forma: na sessão 2 são apresentados os padrões de criptografia utilizados nos testes (WEP e WPA). A sessão 3 é destinada às questões e avaliação de desempenho, bem como a descrição detalhada do andamento dos testes realizados. A sessão 4 é reservada às considerações finais.

2. Criptografia em Redes sem Fio

Em ambientes de rede que utilizam tecnologias sem fio, as questões relativas à segurança tornam-se críticas, uma vez que os dados e informações trafegam pelo ar, e não por um meio guiado. Assim, tais ambientes possuem uma necessidade maior de mecanismos que venham a prover segurança no acesso a rede propriamente dita, dentre os quais, destacam-se os mecanismos de criptografia.

Dentre os padrões de criptografia adotados pelo IEEE 802.11, tem-se o WEP (*Wired Equivalency Privacy*) e o WPA (*Wi-Fi Protected Acccess*), apresentados a seguir.

2.1 WEP (*Wired Equivalency Privacy*)

Atualmente, o WEP é o padrão de segurança desenvolvido para todos os padrões 802.11, e seu objetivo é prover o mesmo nível de segurança de uma rede cabeada a uma rede sem fio.

O WEP opera na camada de enlace de dados para autenticar e criptografar os dados entre o cliente e o *access point*. É baseado no método criptográfico RC4 da RSA *Security*, utilizando um vetor de inicialização (VI) de 24 *bits* e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 *bits*, a qual pode ser utilizada pelo *access point* para realizar a autenticação do cliente. (Park e Dicoi, 2003).

O VI, juntamente com a chave, servem de entrada para um gerador de números pseudo-aleatórios (PRNG – *Pseudorandom Number Generator*), utilizado para formar uma chave de 64 ou 128 *bits* que é usada para criptografar o texto plano através de uma operação XOR. Além disso, o texto a ser criptografado é concatenado com o resultado do processo de verificação de integridade dos dados (ICV – *Integrity Check Value*), realizado a partir do algoritmo de checagem de redundância CRC-32 (*Cyclic Redundancy Check*).

O resultado da operação XOR é concatenado com o VI e enviado ao receptor, sendo utilizado, juntamente com a chave secreta compartilhada, para gerar a mesma seqüência do PRNG e decriptografar o texto cifrado. Após, aplica-se o CRC-32, comparando-o com o ICV para checar a integridade da mensagem recebida. (Junior *et al*, 2003).

De acordo com Longjun *et al* (2003), atualmente o protocolo WEP não atinge seus objetivos, uma falha atribuída a seus desenvolvedores, que utilizaram incorretamente o algoritmo RC4. O autor enfatiza ainda que, desde o ano de 2000, pesquisadores e *hackers* já haviam descoberto várias falhas no protocolo, o que o torna muito limitado no que diz respeito à segurança.

Segundo Veríssimo (2001), o RC4 foi implementado de forma equivocada no WEP, uma vez que a cadeia de *bits* que é a chave para o RC4 é composta da cadeia de *bits* que é a chave para o WEP, mais um vetor de inicialização. Este é uma cadeia de 24 *bits* que o padrão WEP não especificou a forma como, se, ou qual a freqüência em que deveria ser alterada. Com isso, nas implementações, parte da chave do RC4 se repete de tempos em tempos. Para o autor, "o RC4 é um algoritmo para gerar cadeias de *bits* pseudo-aleatórias excepcionalmente simples e de extrema eficiência. Os ataques aconteceram graças a defeitos na arquitetura do WEP".

2.2 WPA (*Wi-Fi Protected Access*)

Em função das falhas de segurança encontradas no protocolo WEP, foi organizada uma comissão para tentar solucioná-las, dando início à elaboração do padrão IEEE 802.11i. Este grupo criou um padrão chamado RSN (*Robust Security Network*), incluindo duas partes: o AES (*Advanced Encryption Standard*) para criptografia do tráfego das WLANs; e o IEEE 802.1X (*Padrão de Autenticação baseado em Portas na Rede*) para autenticação de usuário e gerenciamento da chave criptográfica. (Amaral e Maestrelli, 2005).

Neste contexto, em 2003, foi lançada a primeira geração do WPA, produzido pela *Wi–Fi Alliance,* como estratégia para suprir as deficiências do protocolo WEP, seu antecessor, sendo desenvolvido para prover segurança a todas as versões do padrão 802.11.

De acordo com Heikkila (2005), o padrão utiliza um esquema de criptografia denominado TKIP (*Temporal Key Integrity Protocol*), o qual embaralha todos os *frames* utilizando um algoritmo de *hash*, onde, a cada 10.000 pacotes, a chave de criptografia é modificada. Ainda, provê autenticação através do uso do protocolo 802.1X, juntamente com um dos padrões EAP (*Extensible Authentication Protocol*), o qual identifica usuários através de certificados digitais. O padrão EAP é descrito na RFC 3748, de Junho de 2004.

Há um grande número de padrões com implementações EAP, entre eles destacam-se:

- EAP-TLS – EAP *Transport Layer Security*;
- EAP-TTLS – EAP *Tunneled Transport Layer Security*;
- PEAP – *Protected* EAP;

Segundo a *Wi-Fi Alliance*, (2005), utilizando o EAP, o 802.1X cria um *framework* onde as estações autenticam-se mutuamente com o servidor. Estas autenticações previnem que os usuários se conectem acidentalmente a *access points* proibidos, e ainda garantem que os usuários são quem dizem ser. Quando um usuário solicita acesso à rede, o cliente envia as credenciais do usuário ao servidor de autenticação, através do *access point*. Se o servidor aceitar tais credenciais, uma chave TKIP é enviada ao cliente e ao *access point*, completando o processo de autenticação.

A partir daí, o servidor de autenticação utiliza o protocolo 802.1X para gerar uma chave mestra para a sessão, a qual é distribuída ao cliente e ao *access point* pelo protocolo TKIP, senda utilizada para gerar dinamicamente chaves únicas de criptografia de pacotes.

A Figura 1 apresenta um comparativo, quanto ao nível de segurança, entre os algoritmos AES, TKIP e WEP, de acordo com Amaral e Maestrelli (2004).

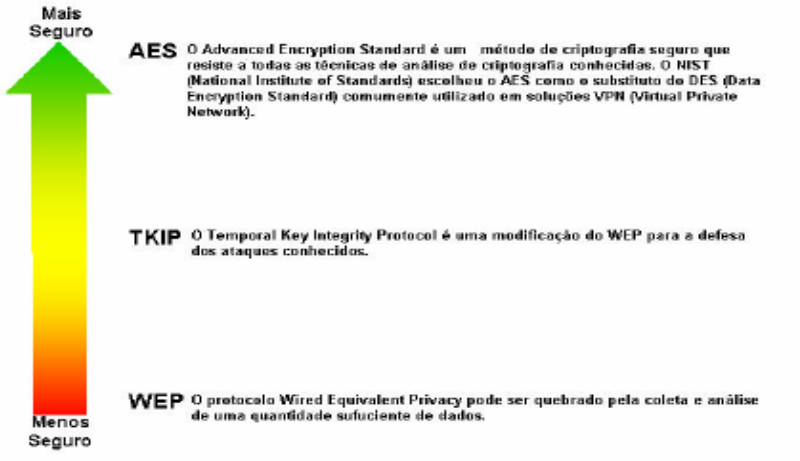

Figura 1. Comparativo entre algoritmos de criptografia

O WPA utiliza ainda o MIC (*Message Integrity Check*), também conhecido como "*Michael*", que previne contra a perda de pacotes, através de funções matemáticas que comparam os dados do emissor e receptor.

3. Avaliação de Desempenho

Apesar de algumas questões relativas a desempenho estarem relacionadas à camada de rede, a qual é responsável pelo roteamento dos pacotes e controle de congestionamento, é na camada de transporte que surgem os maiores problemas, uma vez que realiza a comunicação fim a fim entre os *hosts*.

Para realizar esta comunicação, a camada de transporte faz uso de alguns protocolos de transporte, sendo que os mais utilizados são o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*).

3.1 Metodologia

O método de pesquisa científica, utilizado do ponto de vista da natureza e da forma de abordagem do problema, foi o método Estatístico, o qual permite a redução de fenômenos a termos quantitativos e a manipulação estatística, permitindo comprovar as relações dos fenômenos entre si, e obter generalizações sobre sua natureza, ocorrência ou significado. (Lakatos e Marconi, 1991).

3.2 Métricas

As métricas, ou parâmetros, são critérios utilizados para analisar o desempenho do sistema ou componentes do mesmo, sob diferentes aspectos. Abaixo são apresentadas algumas delas, as quais foram utilizadas neste artigo:

- *Média de atraso*: é a média de tempo de retardo no envio dos pacotes;
- *Jittter* – é a variação de tempo entre a chegada dos pacotes;
- *Throughput* – também chamada de *vazão*, é o número (taxa) de itens processados por unidade de tempo (*bits* por segundo);

3.3 Equipamentos

Os equipamentos utilizados para a realização dos testes foram:

- 1 *access point*, padrão 802.11g, configurado como tal;
- 1 *access point,* padrão *802.11g,* configurado como *access point* cliente;
- 1 microcomputador *Pentium* IV, 2.4*GHz*, 256 MB RAM, Interface de Rede 10/100 *mbps*;
- 1 microcomputador *notebook* Centrino 1.8*GHz*, 1GB RAM, Interface de Rede 10/100 *mbps*.

3.4 *Softwares*

Foram utilizados os softwares *Rude e Crude* Versão 0.62 para a realização dos testes. Ambos pertencem ao mesmo pacote, sendo que o *Rude* é o responsável pela geração do tráfego UDP na rede; e o *Crude* é o responsável pela recepção do tráfego gerado, elaborando arquivos de *log*, onde constam informações acerca dos testes realizados, tais como número de pacotes recebidos e perdidos, número de *bytes* recebidos, número de pacotes fora de seqüência, entre outros.

A geração de tráfego pelo *Rude* é realizada de acordo com um arquivo de configuração (*script*), onde são informados parâmetros para a geração do tráfego, como

tempo de duração de cada teste, tamanho dos pacotes e taxa de transmissão, endereço de destino, e portas de origem e destino.

O sistema operacional utilizado em ambas as máquinas utilizadas, foi o *Linux,* distribuição *Fedora Core 6*.

3.5 Cenário dos Testes

Os equipamentos descritos anteriormente foram organizados da seguinte maneira: *Access point* conectado por rede cabeada *ethernet* a um microcomputador que recebe o fluxo de dados. Do outro lado, um *access point* cliente conectado por rede cabeada *ethernet* ao gerador do fluxo de dados. Este esquema pode ser visualizado na Figura 2.

Para que os testes obtivessem total precisão, as duas máquinas utilizadas na geração e coleta de dados foram conectadas a um servidor NTP (*Network Time Protocol*), sincronizando os relógios dos equipamentos, a partir de uma referência UTP (*Universal Time Coordinated*), conhecida como relógio de referência. Além disso, foi necessário desabilitar o *firewall* da rede, para que o *Crude* pudesse receber o tráfego gerado pelo *Rude*, do contrário, o mesmo seria bloqueado.

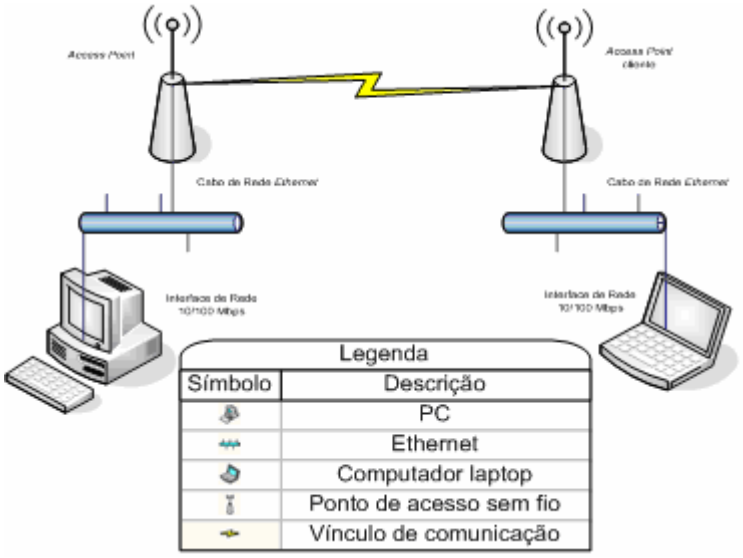

Figura 2. Cenário dos testes

No Quadro 1 é apresentado o arquivo de configuração para o *Rude*, onde são estabelecidos os parâmetros para a geração do tráfego.

```
START NOW
## Fluxo 1: (flow ID = 10)
## Inicia o fluxo imediatamente apos o START com os seguintes parâmetros:
## 256 pacotes/segundo, cada pacote com 108 bytes
## Onde:
## TI -> Tempo de início do fluxo
## IF -> Identificador do Fluxo
## Destino: Porta -> Endereço IP:Porta de destino do fluxo
## Pct -> Quantidade de pacotes por segundo
## Tam -> Tamanho dos pacotes gerados
#TI  IF       Destino:Porta                    Pct Tam
0000 0010 ON 3001 192.168.0.54:10001 CONSTANT 256 108 60000 0010 OFF
## Após 1 minuto, o fluxo é parado
```

Quadro 1. Arquivo de configuração do Rude, nomeado *script_rude.cfg*

A inicialização do *Rude* e do *Crude* é feita a partir do *prompt* de comando do Linux, através dos seguintes comandos:

```
# rude -s script_rude.cfg
# crude -p 10001 -s 10
```

Foram gerados fluxos de 256 pacotes por segundo, cada qual com 108 *bytes*, ou seja, um tráfego de 27648 *bytes* por segundo na rede. Além disso, os testes foram realizados com duração de 1, 2 e 4 minutos.

3.6 Resultados Obtidos

Para comparar, e analisar o desempenho, foram realizados testes com os seguintes algoritmos:

- Sem criptografia;
- WEP, com criptografia de 64 *bits*;
- WEP, com criptografia de 128 *bits*;
- WEP, com criptografia de 152 *bits*;
- WPA-PSK (*Pré-Shared Key*), com chave criptográfica padrão;

Uma vez que cada algoritmo foi testado três vezes (1, 2 e 4 min), foram gerados 15 arquivos de *logs*, os quais foram estudados a partir de análises estatísticas qualitativas, através do software *Statística 5*, avaliando-se as métricas: média de atraso, *jitter* médio, *jitter* máximo e *throughput*. As Tabela 1, 2 e 3 apresentam a Média, Desvio Padrão e Variância entre os protocolos para os três tempos, respectivamente.

Tabela 1. Média, Desvio Padrão e Variância entre os protocolos para 1 minuto

1 minuto			
	Média	**Desvio Padrão**	**Variância**
Média de Atraso	-0,32623940	0,11738666	0,01377963
***Jitter* Médio**	0,00027920	0,00019811	0,00000004
***Jitter* Máximo**	0,02304600	0,03948515	0,00155908
Throughput	27654,5000	0,12247449	0,01500

Tabela 2. Média, Desvio Padrão e variância entre os protocolos para 2 minutos

2 minutos			
	Média	**Desvio Padrão**	**Variância**
Média de Atraso	-0,33898080	0,11656913	0,01358836
***Jitter* Médio**	0,00022100	0,00001056	0,00000000
***Jitter* Máximo**	0,00588260	0,00248127	0,00000616
Throughput	27653,5400	0,05477226	0,003000

Tabela 3. Média, Desvio Padrão e variância entre os protocolos para 4 minutos

4 minutos			
	Média	**Desvio Padrão**	**Variância**
Média de Atraso	-0,35937080	0,11598259	0,01345196
***Jitter* Médio**	0,00022580	0,00000996	0,00000000
***Jitter* Máximo**	0,01417500	0,01923353	0,00036993
Throughput	27653,02000	0,04472136	0,00200000

Inicialmente, foi realizada a análise de variância não paramétrica de *Kruskal-Wallis* (Siegel, 1977), entre todos os algoritmos, nos três tempos de coleta, revelando que, ao nível de significância de 5%, não existe diferença significativa entre os tempos.

Também foi aplicada a análise de variância não paramétrica para verificar se havia diferença entre as médias das métricas utilizadas entre os algoritmos, encontrando-se diferenças significativas, ao nível de significância de 5%, para a *média de atraso* e para o *jitter médio*, o que descartou as demais métricas.

Assim, foi aplicado um teste para comparações múltiplas *Mann-Whitney* (Siegel, 1977), verificando-se, com nível de significância de 5%, que a maior diferença ocorre entre o fluxo gerado sem criptografia e o WPA-PSK.

A seguir, são apresentados os gráficos de desempenho para as métricas *média de atraso* (Figura 3) e *jitter médio* (Figura 4), em função do tempo.

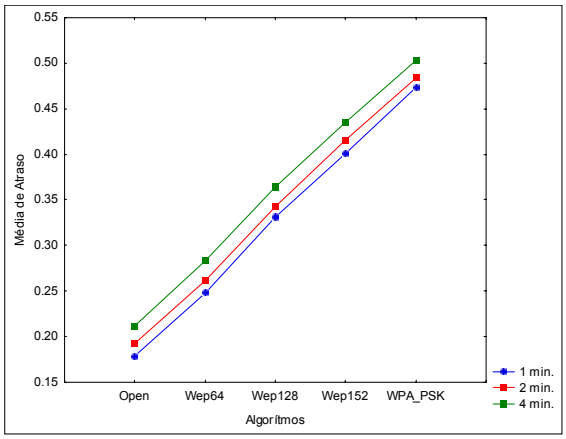

Figura 3. Média de atraso para os cinco algoritmos em função dos tempos de coleta

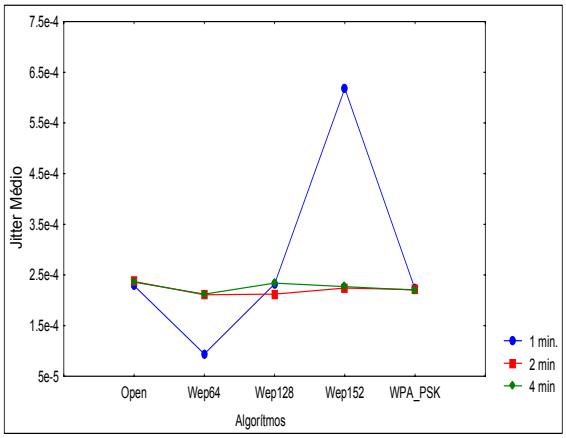

Figura 4. *Jitter* médio para os cinco algoritmos em função dos tempos de coleta

A Figura 5 representa a relação entre os níveis de insegurança da rede, determinados através de uma escala simbólica, (de 1 a 5, relacionando o menos inseguro ao mais inseguro, respectivamente) e os níveis de atraso, ilustrando o ponto onde começa a haver degradação do desempenho da rede em função do *overhead* gerado pelo algoritmo de criptografia utilizado. Desta forma, pode-se afirmar que o nível de segurança é inversamente proporcional ao nível de desempenho, uma vez que, quanto maior a média de atraso - encontrada em algoritmos mais seguros; menor o desempenho da rede.

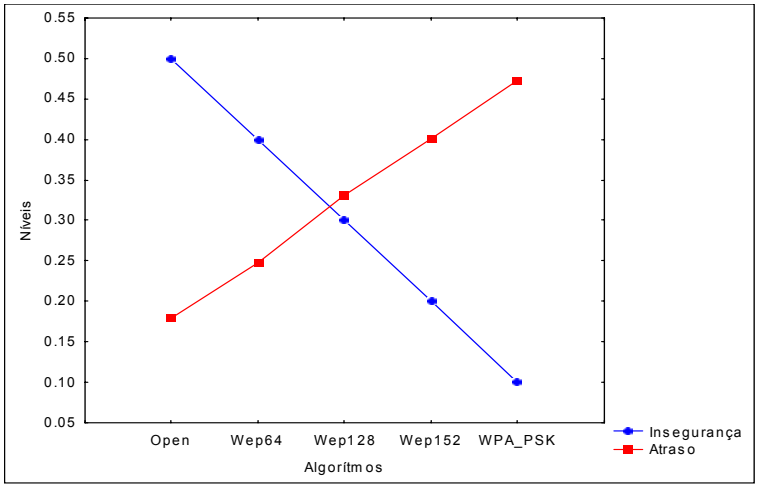

Figura 5. Representação da relação entre os níveis de insegurança e os níveis de atraso

4. Considerações Finais

Através dos testes realizados, constatou-se que a utilização de um protocolo de criptografia mais robusto, como o WPA, demanda um maior poder de processamento e largura de banda da rede, em função do nível de segurança requerido.

Desta forma, em qualquer situação, é preciso analisar com atenção os requisitos e especificações do ambiente em questão, tais como qualidade de serviço, proteção de ativos, confidencialidade de dados; avaliando a melhor relação custo X benefício.

Como sugestão para trabalhos futuros, pode-se ampliar o rol de algoritmos utilizados nos testes, bem como os ambientes de rede, diversificando os cenários de testes e aumentando a inserção de tráfego. Pode-se, ainda, avaliar outros mecanismos de segurança, abordados neste trabalho, como o WPA2 e 802.11X, e sistemas de autenticação RADIUS.

5. Referências Bibliográficas

AMARAL, Bruno Marques; MAESTRELLI, Marita. *Segurança em Redes Wireless 802.11*. 2004. Disponível em http://mesonpi.cat.cbpf.br/cbpfindex/publication_pdfs/nt00204.20060130225107.pdf . Acesso em 28/09/2006.

HEIKKILA, Faith M.. *SecureWorld Expo 2005*. IEEE Computer Society, 2005.

JUNIOR, Paulo D. M.; NUNES, Bruno A. A.; CAMPOS, Carlos A. V.; MORAES, Luis Felipe M. de. *Avaliando a sobrecarga introduzida nas Redes 802.11 pelos mecanismos de segurança WEP e VPN/IPSec*. Disponível http://www.ravel.ufrj.br/arquivosPublicacoes/WSeg2003_Sobrecarga_80211_WEP_VNIPSec.pdf . Acesso em 30/10/2006.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Metodologia Científica*. São Paulo: Atlas, 1991.

LOGJUN, Zhang; WEI, Han; DONG, Zheng; KEFEI, Chen. *A Security Solution of WLAN Based on Public Key Cryptosystem*. Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS´05) 0-7695-2281-5/05. IEEE Computer Society, 2005.

PARK, Joon S.; DICOI, Derrick. *WLAN Security:* Current and Future. Security Track. IEEE Computer Society, 2003.

SIEGEL, S. *Estatística não-paramétrica para as ciências do comportamento.* Mc Graw-Hill do Brasil, São Paulo, 1977.

VERISSIMO, Fernando. *Em defesa de Rivest*. Disponível em http://www.cos.ufrj.br/~ferver/defrivest.pdf. Acesso em 10/11/06.

Wi-Fi *Alliance*. *Deploying Wi-Fi Protected Access (WPA) and (WPA2) in the Enterprise*. Wi-Fi *Alliance*, 2005. Disponível em http://www.wi-fi.org/files/uploaded_files/wp_9__WPA-WPA2%20Implementation_2-27-05.pdf. Acesso em 15/11/2006.