CENTRO UNIVERSITÁRIO FEEVALE

ISRAEL TIAGO FERRASSO

SEGURANÇA E VULNERABILIDADE EM REDES WIRELESS

título provisório

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo, outubro 2010.

ISRAEL TIAGO FERRASSO

israelferrasso@gmail.com

SEGURANÇA E VULNERABILIDADE EM REDES WIRELESS

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Sistemas de Informação
Anteprojeto de Trabalho de Conclusão

Professor orientador: Vandersilvio da Silva

Novo Hamburgo, outubro 2010.

RESUMO

Hoje em dia a crescente necessidade de estarmos conectados ao mundo virtual, compartilhando dados de forma cada vez mais rápida, em maior quantidade e onde quer que estejamos, torna o acesso às redes *wireless* (sem fio) um grande avanço para suprir tal necessidade. O crescimento destas redes, cada vez mais utilizadas pelas pessoas em suas residências e ainda mais pelas empresas, faz com que a necessidade de segurança das informações trafegadas seja cada vez melhor e de grande eficiência. Atualmente são utilizados os protocolos de segurança WEP, WPA e WPA II. Até que ponto eles provêm à segurança dos dados na rede sem fio? Hoje existem diversas técnicas para tentativas de quebra de senhas e criptografias utilizadas pelos protocolos de segurança *(Cracking)*. O presente trabalho busca estudar os protocolos WPA e WPA II em diferentes fornecedores, avaliando a eficiência e proteção oferecida de cada fornecedor e seu comportamento através de tentativas de quebra de segurança utilizando ferramentas desenvolvidas para este fim.

Palavras-chave: Segurança. *Wireless.* Criptografia. *Cracking*. WPA. *WPA II.*

SUMÁRIO

MOTIVAÇÃO

A necessidade de troca de informação cada vez mais rápida e eficiente, fez com que houvesse um grande avanço nas transmições de dados com computadores através da internet, tornando também o acesso a rede sem fio uma escolha que facilitasse a conexão de forma rápida e prática.

Esta facilidade e praticidade tornaram estas redes muito populares nas casas e empresas e até em locais de grande circulação com aeroportos, restaurantes e shoppings. Isso acaba fazendo com que poucas pessoas venham a se preocupar com a segurança da rede na qual estão conectadas, navegando de forma aparentemente sigilosa e segura.

Atualmente o autor atua profissionalmente em uma empresa de prestação de serviços em informática, onde instalações de rede *Wireless* são quase que diárias. Os equipamentos para estas instalações possuem grande facilidade de instalação. Esta facilidade acaba fazendo com que as configurações de segurança do equipamento não sejam adotadas corretamente, seja por receio ou mesmo desconhecimento de tais funções.

Estes equipamentos são facilmente encontrados e possuem diversos fabricantes e configurações diferenciadas. Suas criptografias são utilizadas para proteger os dados trafegados nesta rede. Entre o cliente e a base, é gerada uma chave de autenticação que é armazenada e transmitida no momento em que é feita a conexão. Em questão de segurança de redes *Wireless*, temos hoje os protocolos padrões WEP (*Wired Equivalent* Privacy), WPA (*Wi-fi Protected Access*) e WPA II (*Wi-fi Protected Access II*).

O protocolo WEP é destinando a servir três funções: evitar o acesso não autorizado à rede; proteger os dados de interceptadores; realizar uma verificação de integridade de cada pacote (ROSS, 2003). Este está presente em todos os aparelhos que utilizam o padrão wi-fi.

Este protocolo já teve muitas falhas divulgadas em sites, tornando a sua quebra facilitada e não sendo um protocolo confiável.

> "Existem problemas administrativos e técnicos em relação ao protocolo WEP. Em relação ao padrão original, os principais relacionam-se ao fato de usar uma chave única e estática, que deve ser compartilhada entre todos os dispositivos participantes de uma determinada rede. Portanto, caso seja necessária a troca da chave, o processo pode ser trabalhoso e, em alguns casos, inviável. Outro problema vincula-se ao fato de que, na época em que o padrão foi definido (1997), havia restrição dos Estados Unidos referentes à exportação de criptografia com chaves maiores que 40 bits. E finalmente, foram revelados outros problemas técnicos, que permitem ataques ao próprio algoritmo." (RUFINO, 2005, p.65).

Após o descrédito do protocolo WEP, foi desenvolvido o protocolo WPA. Este teve diversas mudanças e avanços incorporados além de possuir vários modelos que são moldáveis as necessidades do ambiente.

> Grande parte do problema de sigilo existente no WEP diz respeito aos mecanismos de criptografia utilizados. Para solucionar esses problemas, o WPA avança nos pontos mais vulneráveis, quais sejam a combinação de algoritmo e temporalidade da chave. Porém, dados a diversidade e os ambientes onde uma rede sem fio pode existir (ambientes domésticos, pequenos escritórios, pequenas e grandes indústrias etc.), pensou-se ser razoável que o WPA tivesse também diferentes modelos de segurança para ter melhor aderência às diferentes necessidades. (RUFINO, 2005 p.35).

Embora o WPA seja mais seguro que seu antecessor WEP, já é conhecido algumas vulnerabilidades deste protocolo que podem ser encontradas em diversos artigos e sites na internet. Tendo conhecimentos de tais vulnerabilidades, os usuários deste protocolo podem dessa forma se proteger de uma maneira mais eficiente contra tentativas de invasões minimizando danos.

Após este foi desenvolvido o WPA II. Mais seguro que o WPA, pois necessita de maior poder de processamento para sua criptografia. Neste é utilizado um protocolo denominado Advanced Encryption Standard (AES), que é muito seguro e eficiente, mas possui a desvantagem de exigir bastante processamento.

Hoje em dia, a grande facilidade na captura de sinas de *Wireless*, trouxe a tona diversos estudos e ferramentas de *Cracking*, buscando encontrar vulnerabilidades de segurança em redes *wireless*. Sendo isto executado por profissionais na área de segurança ou até hobbistas que querem divulgar falhas ou prover informações ao publico.

Sendo assim, este projeto visa o estudo dos protocolos de segurança WPA e WPA II, características e utilizações e também de ferramentas e técnicas de *Cracking* para tentar efetivar quebras de criptografias e protocolos de segurança, podendo assim avaliar fornecedores e sua segurança oferecida.

OBJETIVOS

Objetivo Geral

O presente projeto objetiva o estudo comparativo de técnicas de quebra de criptografia dos protocolos WPA e WPA II. Para isto, serão estudados os protocolos e ferramentas Cracking disponíveis para realizar quebras de criptografias. As ferramentas serão aplicadas em diferentes fornecedores para verificar seu funcionamento nestas diferentes implementações.

Objetivos Específicos

- Apresentar as características e descrever os protocolos WPA e WPA II;
- Fazer levantamento de ferramentas de quebra de protocolos WPA e WPA II;
- Desenvolver um ambiente de rede sem fio em laboratório, com equipamentos de diferentes fabricantes, para tentativa de quebra destes protocolos utilizando-se de ferramentas para este fim;
- Relatar os resultados dos testes de vulnerabilidade realizada em laboratório e analisá-los.

METODOLOGIA

O trabalho será desenvolvido do decorrer de dois semestres. A primeira etapa, denominada Trabalho de Conclusão I, ocorrerá no segundo semestre de 2010, e será focada no estudo bibliográfico dos protocolos em questão através de livros, artigos, periódicos, trabalhos acadêmicos e outras fontes disponíveis. Ainda na primeira parte do trabalho serão estudadas algumas técnicas e ferramentas disponíveis para análise de vulnerabilidade em redes *wireless*.

Durante o Trabalho de Conclusão II, partindo do estudo bibliográfico realizado na primeira etapa do trabalho, será desenvolvido um ambiente em laboratório para testes das ferramentas e técnicas para quebra de segurança dos protocolos WPA e WPA II.

Por fim, será apresentado um relatório com os resultados obtidos através dos testes práticos em laboratório, para dessa forma obter artefatos que demonstrem as vulnerabilidades das redes *wireless*, identificando os prós e contras de cada um dos protocolos estudados e seus fornecedores.

.

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses			
	Ago	Set	Out	Nov/Dez
Pesquisa bibliográficas e consultas na internet dos protocolos em questão através da leitura de livros, sites e outras fontes disponíveis.				
Desenvolvimento do anteprojeto.				
Entrega do anteprojeto.				
Estudo dos protocolos de criptografia WPA e WPA II				
Estudo das principais ferramentas de análise de vulnerabilidades.				
Redação do trabalho de conclusão I.				
Entrega do relatório final do trabalho de conclusão I.				

Trabalho de Conclusão II

Etapa	Meses				
	Jan	Fev	Mar	Abr	Mai
Análise das técnicas e ferramentas propostas.					
Definir equipamentos de fornecedores para testes em laboratórios.					
Realização dos testes utilizando as ferramentas.					
Redação do trabalho de conclusão II e geração do relatório sobre os testes em laboratório.					
Entrega do relatório final do trabalho de conclusão II.					
Apresentação final do trabalho de conclusão de curso para banca avaliadora.					

BIBLIOGRAFIA

LUCCHESE, Felipe. **Análise de Vulnerabilidade de Rede Sem Fio 802.11: Estudo de Caso em um Orgão Público Municipal** 2009. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Centro Universitário Feevale, Novo Hamburgo, RS, 2009.

ROSS, John. **WI-FI – Instale, configure e use redes wireless (sem fio).** Rio de Janeiro: Alta Books, 2003.

RUFINO, Nelson Murilo de Oliveira. **Segurança em redes sem fio.** 2.ed. São Paulo: Novatec, 2005.

WARCHALKING, **Wireless discussion fórum**. Disponível na Internet via <http://www.warchalking.com.br>.