CENTRO UNIVERSITÁRIO FEEVALE

FELIPE LUCCHESE

SEGURANÇA EM REDES WIRELESS: WEP, WPA E WARDRIVING

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo, Abril de 2007.

FELIPE LUCCHESE

felipeinfo@terra.com.br

SEGURANÇA EM REDES WIRELESS: WEP, WPA E WARDRIVING

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Ciência da Computação
Anteprojeto de Trabalho de Conclusão

Professor orientador: Vandersilvio da Silva

Novo Hamburgo, Abril de 2007.

RESUMO

Os avanços tecnológicos, ao longo do tempo, permitiram a integração e o compartilhamento de informações através das redes. A crescente necessidade por mobilidade trouxe consigo uma rápida disseminação das redes *wireless* (sem fio). Esta praticidade no uso de dispositivos móveis e a ampla conectividade com outros dispositivos geram uma grande preocupação em torno da segurança dos dados trafegados. Embora os avanços nesta área sejam expressivos, uma rede *wireless* não é completamente segura. Protocolos de segurança e criptografia são utilizados para impedir que algum interceptador possa ler o conteúdo de pacotes trafegados ou até mesmo acessar a rede. Atualmente os protocolos WEP e WPA são utilizados para tal. Muitos problemas acerca destes protocolos são conhecidos, o que torna a segurança em redes *wireless* duvidosa. A facilidade na captação de sinais de redes *wireless*, em conjunto com diversos problemas de segurança destas, trouxe um termo conhecido como *Wardriving*. Este reúne conceitos e técnicas para captação de pacotes, quebra de protocolos de criptografia e acesso a redes *wireless*. Sendo assim, o presente projeto tem como objetivo descrever os protocolos de segurança e criptografia WEP e WPA, analisar suas vulnerabilidades e características e realizar um comparativo entre estes. Ainda neste, identificar e descrever ferramentas utilizadas para a interceptação de sinais de redes *wi-fi*, identificação e quebra de protocolos de criptografia. Por fim, utilizando de conceitos e técnicas de *wardriving*, realizar varreduras em busca de redes *wireless* com segurança ou sem, tentando sempre o acesso a estas (utilizando das ferramentas identificadas para tal propósito), relatando, então, os resultados obtidos em tal processo.

Palavras-chave: *Wireless*. Segurança. Criptografia. *Wardriving*.

SUMÁRIO

MOTIVAÇÃO

A grande difusão das redes de computadores e da internet possibilitaram um avanço sem precedentes no compartilhamento de informações e aplicações. As crescentes necessidades por informações em tempo real, conectividade e mobilidade trazem consigo um grande avanço tecnológico em sistemas de comunicação sem fio.

Redes *Wireless* (sem fio), em particular as redes *Wi-Fi* (*Wireless Fidelity*), tornam-se, sem dúvida, cada dia mais populares e imprescindíveis, sendo inegável a conveniência de sua utilização em lugares como aeroportos, hotéis e cafés. Redes *wireless* propiciam uma considerável praticidade e mobilidade em ambientes corporativos e/ou domésticos e pode mudar a maneira como as pessoas trabalham e permanecem on-line quando distantes de sua base habitual.

Segundo um estudo do IDG[1], o mercado de equipamentos de redes sem fio crescerá a uma taxa anual de 41%. Com toda esta comodidade e praticidade, surgem grandes preocupações quanto à segurança no uso e na transmissão dos dados por este tipo de rede. Diferentemente das redes cabeadas, que conhecem o ponto físico de conexão, as redes *wireless* transmitem sinais de rádio no ar, ou seja, dentro do espaço físico abrangente, qualquer dispositivo pode receber as informações (protegidas ou não). Normalmente este espaço excede os limites da empresa/escritório/casa, transmitindo assim os dados além do escopo necessário (ou não; esse é o fator determinante da mobilidade). Como se pode ter certeza que a rede está segura? Como se pode ter certeza que um interceptador não consiga visualizar os dados transmitidos ou acessar à rede?

[1] *International Data Group*, disponível em http://www.idg.com.

Seguindo neste escopo, pode-se constatar dois tipos de reação quanto à segurança de redes *wireless*, por parte dos administradores de rede ou por parte do usuário que instalara sua própria rede (em virtude da facilidade de instalação que estas possuem): a não-adoção da segurança por receio (ou desconhecimento) das implicações que tal possa ocasionar à rede; ou ainda a adoção da segurança por impulso, ou seja, sem conhecer os riscos, a tecnologia empregada e as medidas de segurança recomendadas. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são imprescindíveis.

Para resolver (ou reduzir) estes problemas de segurança, meios eficazes de autenticação e criptografia da transmissão de dados estão em constante desenvolvimento. Como a captura da informação pode ser feita de forma completamente passiva (basta ter um meio de receber o sinal), as redes *wi-fi* oferecem possibilidades de cifração de dados (criptografia). Atualmente, tem-se os seguintes protocolos de criptografia em redes *wi-fi*: WEP (*Wired Equivalent Privacy*) e WPA (*Wi-Fi Protected Access*). O uso destes protocolos está limitado às funções de cada dispositivo *wireless* (aplicável ou não).

O protocolo inicialmente sugerido para esta tarefa foi o WEP, cuja intenção original, como o nome sugere, era proporcionar um nível de segurança em redes *wi-fi* comparável à segurança de uma rede cabeada. A criptografia WEP é destinada 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 totalmente disseminado e presente em todos os equipamentos conformidados com o padrão *wi-fi*.

Diversos cientistas acadêmicos em computação publicaram relatórios sobre o protocolo WEP, questionando sua eficiência em proteger os dados. Todos indicam graves falhas na teoria e prática criptográfica que foram usadas para definir este padrão.

> "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).

Um grupo da Universidade da Califórnia, em Berkeley, identificou numerosas falhas neste protocolo, que o tornam mais vulnerável a pelo menos quatro tipos de ataque (ROSS, 2003):

- Ataques passivos que utilizam análises estatísticas para decifrar os dados;

- Ataques ativos que criam pacotes criptografados que enganam o ponto de acesso, fazendo-o aceitar comandos falsos;

- Ataques de análise de pacotes criptografados para construir dicionários que possam ser utilizados para decriptografar automaticamente os dados em tempo real;

- Ataques que alteram os cabeçalhos do pacote para desviar os dados para um destino controlado pelo atacante.

Tendo em vista os problemas de segurança encontrados no protocolo WEP, o *Wi-Fi Alliance* liberou o protocolo WPA. Diversas mudanças e avanços foram incorporados a este protocolo, porém a maior parte deles exige uma inclusão de novos elementos à infra-estrutura e ainda devem trabalhar combinados com outros protocolos, como o 802.11x.

> "Atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda, foca a autenticação do usuário (área não coberta efetivamente pelo padrão WEP)." (RUFINO, 2005, p.37).

Embora o WPA tenha características de segurança superiores às do WEP, ainda assim apresenta diversas vulnerabilidades já reportadas e que devem ser conhecidas para que o seu impacto possa ser minimizado.

A grande facilidade na captura de sinais de redes *wi-fi* trouxe consigo um termo muito conhecido como *Wardriving*. Uma vasta gama de ferramentas para identificação de redes *wireless*, interceptação e leitura de pacotes e ferramentas para quebra de protocolos de criptografia impulsionaram os ataques a esse tipo de rede.

> "WarDriving é o ato de mover-se ao redor de uma específica área e mapear a população de pontos de acesso *wireless* para um propósito estatístico. Estas estatísticas são então utilizadas para elevar a atenção sobre problemas de segurança associados a estes tipos de rede (tipicamente *wireless*)." [...] "WarDriving não utiliza os recursos de qualquer ponto de acesso ou rede *wireless* descobertas sem prévia autorização do proprietário." (HURLEY, Chris *et al*, 2004, p.12).

A realidade sobre *Wardriving* é simples. Profissionais em segurança, hobbistas e outros estão geralmente interessados em prover informações ao público sobre vulnerabilidades de segurança que estão presentes nas configurações de seus pontos de acesso. Porém a realidade vai além desta percepção. Usuários mal-intencionados interceptam sinais e varrem pacotes em busca de redes abertas, chaves de segurança e seus apensos, para um posterior ataque à rede (desde roubo de dados até uma simples conexão com a internet).

Pode-se considerar motivação o fato de que as redes necessitam, cada vez mais, de segurança na transmissão de seus dados. O presente projeto visa o estudo acerca dos

protocolos de segurança WEP e WPA, demonstrando suas características, diferenças e aplicações. Também utilizando as técnicas de *wardriving*, pretende-se realizar uma varredura por redes *wi-fi* que estejam abertas e acessíveis, ou do contrário, tentar a quebra dos protocolos de segurança e criptografia para um posterior acesso a estas. Um estudo sobre as ferramentas disponíveis atualmente para tais propósitos também se inclui neste projeto.

A importância deste eleva-se ao aprendizado sobre os protocolos de criptografia propostos, tendo como referencial a utilização das técnicas de *wardriving* para uma posterior incrementação de segurança nas redes descobertas e passíveis de ataques.

OBJETIVOS

Objetivo geral

O presente projeto objetiva o estudo aprofundado acerca das tecnologias de segurança e criptografia em redes *wireless* (notadamente *Wi-Fi*), sendo estes os protocolos WEP e WPA, descrevendo suas características específicas, suas principais vulnerabilidades e realizar um comparativo expressivo. Utilizando técnicas de *Wardriving*, realizar varreduras em busca de redes *wi-fi* abertas (sem segurança) e, quando do contrário, realizar uma minuciosa varredura em pacotes trafegados, efetuando assim a quebra (ou simplesmente uma tentativa de quebra) dos protocolos identificados na rede, criando, deste modo, relatórios de dados que possam identificar (ou não) as vulnerabilidades descritas neste projeto. Um estudo e detalhamento sobre as ferramentas disponíveis para tal propósito também se incluem no escopo deste projeto.

Objetivos específicos

- Descrever o funcionamento dos protocolos de criptografia WEP e WPA;
- Descrever as características e vulnerabilidades de tais protocolos;
- Realizar um estudo e descrição dos conceitos e técnicas de Wardriving;
- Identificar e analisar ferramentas de identificação de redes *Wi-Fi*;
- Identificar e analisar ferramentas de leitura de pacotes de dados para redes *Wi-Fi*;
- Identificar e analisar ferramentas para quebra dos protocolos de segurança e criptografia WEP e WPA;
- Descrever o cenário a ser utilizado para interceptação de sinais de redes *Wi-Fi* (ferramentas de software e hardware);

- Localizar redes *wireless* com ou sem segurança, tentando o acesso a estas (quando necessário, utilizar de ferramentas para a tentativa de quebra do protocolo utilizado), tendo sempre o empenho sigiloso e ético de tal processo;
- Descrever os resultados obtidos destas interceptações (trabalho de campo) em relatórios, dentro de um padrão a ser desenvolvido no decorrer do projeto, apresentando as variáveis mais pertinentes ao escopo do mesmo.

METODOLOGIA

O projeto em questão será dividido em duas partes. A primeira (TC1) apresentará toda a fundamentação teórica necessária acerca dos protocolos que se fazem objeto de estudo deste. Contará também com a conceituação do conjuntos de técnicas utilizadas para interceptação de pacotes de dados. Para isso utilizar-se-á pesquisas bibliográficas e/ou consultas na internet, tendo como base sites dos próprios mantenedores destes protocolos (utilizando *data sheets e/*ou *white pages*).

A segunda etapa do projeto (TC2) constituirá em realizar um levantamento das ferramentas disponíveis no mercado (proprietárias ou não) para a identificação de redes, interceptação de pacotes e quebra de protocolos de criptografia, montando assim um cenário real de ferramentas (software) + hardware para a parte final do projeto, que consiste em utilizar este cenário para localização e tentativa de acesso a redes *wi-fi*. O espaço geográfico em que se realizará este denominado trabalho de campo será definido no decorrer do projeto. Posteriormente, serão criados relatórios para identificação e situação dos objetivos propostos. Este, então, utilizando de referências bibliográficas, consultas a sites dos fabricantes das ferramentas propostas e equipamentos adequados para efetuar o trabalho de campo (varredura em busca de redes *wi-fi*).

Sendo assim, considera-se as seguintes etapas do projeto:

Etapa 1 –TC1

- Entregar aceite de orientação.
- Estudar problemas relacionados à segurança de redes *wireless*.
- Revisar bibliografia sobre WEP e WPA.
- Revisar bibliografia sobre *Wardriving*.

- Revisar o projeto junto ao orientador.
- Elaborar o anteprojeto.
- Estudar os protocolos WEP e WPA.
- Estudar o *Wardriving*.
- Elaborar o texto do trabalho de conclusão I.
- Entregar o relatório final do trabalho de conclusão I.

Etapa 2 –TC2

- Revisar bibliografia sobre WEP e WPA.
- Revisar bibliografia sobre *Wardriving*.
- Revisar o projeto junto ao orientador.
- Pesquisar e estudar ferramentas para *Wardriving*.
- Definir equipamento necessário para teste de campo.
- Realizar varredura em busca de redes e tentar o acesso.
- Gerar relatórios sobre o teste de campo.
- Analisar os resultados.
- Produzir o texto do trabalho de conclusão II.
- Entregar o relatório final do trabalho de conclusão II.
- Apresentar o trabalho de conclusão à banca avaliadora.

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses			
	MAR	**ABR**	**MAI**	**JUN**
Entregar aceite de orientação.				
Estudar problemas relacionados à segurança de redes *wireless*.				
Revisar bibliografia sobre WEP e WPA.				
Revisar bibliografia sobre *Wardriving*.				
Revisar o projeto junto ao orientador.				
Elaborar o anteprojeto.				
Estudar os protocolos WEP e WPA.				
Estudar o *Wardriving*.				
Elaborar o texto do trabalho de conclusão I.				
Entregar o relatório final do trabalho de conclusão I.				

Trabalho de Conclusão II

Etapa	Meses			
	AGO	**SET**	**OUT**	**NOV**
Revisar bibliografia sobre WEP e WPA.				
Revisar bibliografia sobre *Wardriving*.				
Revisar o projeto junto ao orientador.				
Pesquisar e estudar ferramentas para *Wardriving*.				
Definir equipamento necessário para teste de campo.				
Realizar varredura em busca de redes e tentar o acesso.				
Gerar relatórios sobre o teste de campo.				
Analisar os resultados.				
Produzir o texto do trabalho de conclusão 2.				
Entregar o relatório final do trabalho de conclusão 2.				
Apresentar o trabalho de conclusão à banca avaliadora.				

BIBLIOGRAFIA

EARLE, Aaron E. **Wireless Security Handbook**. United States of America: Auerbach Publications, 2006. 354p.

HURLEY, Chris et al. **WarDriving: Drive, Detect, Defend:** A Guide to Wireless Security**.** United States of America: Syngress Publishing, 2004. 524p.

ROSS, John. **Wi-Fi – Instale, configure e use redes wireless (sem fio)**. Rio de Janeiro: Alta Books, 2003. 246p.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio**. *2*.ed. São Paulo: Novatec, 2005. 224p.

WI-FI Alliance. **Wi-Fi standards**. Disponível em <http://www.wi-fi.org > Acesso em: março de 2007.