Levantamento e Análise das Redes Sem Fio IEEE 802.11 b/g/n em Campo Mourão

Eric Vinicius Lopes Costa Monte-Alto, Guilherme Brandão da Silva, Guilherme Lucas de Oliveira e Rodrigo Campiolo(Orientador)

Universidade Tecnológica Federal do Paraná (UTFPR)

Campo Mourão – PR – Brasil

{ericv2000, brandaogbs,guilherme9509, rcampiol}@gmail.com

Abstract. *This paper presents a study of local wireless networks based on the IEEE 802.11 b/g/n in Campo Mourão. The networks were analyzed considering the distribution and security to order to identify patterns of setting, use, security and interference.*

Resumo. *Este artigo descreve os resultados de um levantamento das redes sem fio locais baseadas no padrão IEEE 802.11 b/g/n na região central de Campo Mourão e de uma análise quanto a distribuição e segurança dessas redes, visando identificar padrões de configuração, uso, segurança e interferência.*

1. Introdução

O ato de coletar informações de redes sem fio é conhecido por *wardriving* (Vladimirov, 2004), nome que vem de coletar dados com uma antena em um veículo. Essa prática objetiva identificar a distribuição, segurança e localização das redes sem fio.

Baseado na prática de *wardriving* e na premissa da configuração inadequada dos pontos de acesso, este projeto tem como objetivo levantamento das redes sem fio locais na região central de Campo Mourão, com o intuito de realizar um estudo sobre a distribuição dessas redes e os padrões de segurança adotados.

A divulgação dos resultados para a comunidade poderá contribuir para uma melhoria na conduta do uso de dispositivos sem fio e para a correta configuração e manutenção das redes sem fio locais.

Vários trabalhos similares foram realizados em outros locais. Por exemplo, Valadon (2007) realizou uma coleta em Paris, porém, utilizando um celular equipado com GPS e constatou que havia um número elevado de pontos de acesso por metro quadrado.

2. Metodologia

Para a realização do levantamento utilizou-se um notebook com a distribuição Linux Backtrack 5 R2 e a ferramenta Kismet, que é um analisador de rede e sistema de detecção de intrusão para redes IEEE 802.11. O Kismet pode trabalhar com placas *wireless* no modo monitor, capturando pacotes em rede dos tipos 802.11a, 802.11b e 802.11g. O Kismet escuta as transmissões das redes de forma passiva, ou seja, não prejudica as redes alheias.

Primeiramente, realizamos alguns testes em laboratório de monitoramento e configuração de um ponto de acesso em diferentes modos de segurança. Avaliamos técnicas de coleta e de invasão de redes de computadores.

A coleta de dados reais foi realizada percorrendo as principais avenidas de Campo Mourão e mapeando as redes por georreferenciamento. Os dados foram armazenados para análise e para gerar algumas estatísticas.

3. Resultados

A partir dos dados coletados, as redes na região central de Campo Mourão foram mapeadas, analisadas e a localização dos pontos de acesso (APs) foram plotadas no Google Earth.

As análises mostraram que a grande maioria dos APs estão configurados nos canais 01, 06 e 11. Sendo que 70,3% das redes estão configurados em um desses canais. É possível afirmar que poucos se preocupam em ocultar o SSID do ponto de acesso, medida que torna a rede mais segura.

Aproximadamente 66,7% dos pontos de acesso utilizam como medida de segurança o protocolo WPA, 27,3% das redes utilizam o protocolo WEP, e cerca de 6% das pessoas utilizam suas redes sem nenhum tipo de criptografia.

Há uma grande variedade de fabricantes utilizados, entretanto os que aparecem em maior quantidade são TP-LINK (29,9%) e D-Link (13,6%).

4. Conclusão

Considerando a atual importância da comunicação e da informação, é necessário que as pessoas protejam suas redes e seus dados. Uma quantidade significativa de pessoas não utilizam nenhum tipo de meio de segurança, e isso pode trazer algumas consequências, já que um invasor pode facilmente interceptar dados.

Um dos principais problemas para as redes sem fio é a configuração feita por um usuário leigo, que muitas vezes acaba usando o ponto de acesso com a configuração de fábrica.

Apenas o protocolo de segurança não é o suficiente para que uma rede seja totalmente segura, medidas como ocultar o SSID e filtrar pelo endereço físico da placa de rede (MAC Address), são recomendadas para que a rede seja mais segura.

Referências

Souza, A.L. de & de A. Darwich, M. Análise sobre as Vulnerabilidades das Redes WiFi em Belém. Revista de Sistema de Informação, 2009.

Valadon, G., Le Goff, F. & Berger, C. Daily walks in Paris: a practical analysis of wi-fi access points. Proceedings of the 2007 ACM CoNEXT conference ACM, 2007, pp. 63:1-63:2.

Vladimirov, A.A., Gavrilenko, K.V. & Mikhailovsky, A.A. Wi-Foo: The Secrets of

Wireless Hacking. Pearson/Addison Wesley, 2004, pp. 592.