Uma avaliação de vulnerabilidades em protocolos de autenticação para redes sem fio IEEE 802.11

Leonardo F. Soares[1], **Igor M. Moraes**[2]

[1]Laboratório MidiaCom, PGC - TCC
Instituto de Computação – Universidade Federal Fluminense
Niterói – RJ – Brasil

leonardofiorio@id.uff.br, igor@ic.uff.br

Abstract. *This paper evaluates security mechanisms of IEEE 802.11 networks. This standard, also called Wi-Fi, is widely used as a device connectivity infrastructure, providing Internet access and creating local area networks. For the evaluation of security mechanisms, dictionary and brute-force attacks are performed to obtain network passwords. The Krack Attack vulnerability is also exploited in order to verify vulnerabilities of Wi-Fi devices. Results show vulnerable devices and networks because of outdated security patches and the use of trivial passwords.*

Resumo. *Este trabalho avalia mecanismos de segurança implementados nas tecnologias de rede padrão IEEE 802.11. Este padrão, popularmente conhecido como Wi-Fi, é amplamente utilizado como infraestrutura de conectividade de dispositivos, fornecendo acesso à Internet e criando redes locais. Para avaliação dos mecanismos de segurança são efetuados experimentos de ataques de dicionário e força-bruta para obtenção das senhas das redes. A vulnerabilidade Krack Attack também é explorada com o objetivo de verificar se os dispositivos com Wi-Fi estão vulneráveis. Os resultados mostram dispositivos e redes vulneráveis a ataques devido à desatualização com relação a correções de segurança e à utilização de senhas triviais.*

1. Introdução

As redes sem fio se tornaram muito populares devido à sua facilidade de implantação, flexibilidade e robustez. Porém, essas redes exigem maior cuidado com a segurança. O fato de operar através do ar favorece a ação de agentes maliciosos que podem obter acesso e manipular os dados trafegados pela rede, uma vez que o ar é um meio de transmissão compartilhado. Para evitar ataques, mecanismos de segurança são implementados nos protocolos de comunicação para prover autenticidade, integridade, confidencialidade, disponibilidade e não-repúdio [Campos 2014]. As redes sem fio padrão IEEE 802.11 [Bianchi 2000], popularmente conhecidas como *Wireless Fidelity* (Wi-Fi), são exemplos da difusão das tecnologias sem fio. Este trabalho estuda métodos de segurança implementados em redes sem fio padrão IEEE 802.11 e os cuidados na sua configuração.

Para uma avaliação das vulnerabilidades em protocolos de autenticação de redes sem fio padrão IEEE 802.11 são realizados experimentos com diferentes métodos de ataque aos protocolos mais utilizados nos dispositivos: *Wired Equivalent Privacy*

(WEP), *Wi-Fi Protected Access* (WPA e WPA2) e *Wi-Fi Protected Setup* (WPS). O primeiro método consiste na utilização *softwares* que exploram as senhas utilizadas com ataques de dicionário e força bruta combinadas a métodos estatísticos como o FMS/Korek [Chaabouni 2006] e PTW (Pyshkin, Tews, Weinmann) [Tews 2007]. Este método é aplicado em redes sem fio encontradas na Universidade Federal Fluminense, *campi* Gragoatá e Praia Vermelha. Já o segundo método, denominado *Krack Attack* [M. Vanhoef e F. Piessens 2017] é uma vulnerabilidade específica contida nos métodos de autenticação da rede. Dessa forma, são testados dispositivos para verificar a incidencia da vulnerabilidade *Krack Attack*.

A Seção 2 apresenta as metodologias e resultados do primeiro experimento enquanto a Seção 3 aborda o segundo experimento. Por fim, a Seção 4 diz respeito as conclusões obtidas a partir dos experimentos e trabalhos futuros.

2. Experimento de Ataque de Dicionário e Força Bruta

O objetivo do ataque de dicionário e de força bruta é tentar obter as senhas utilizadas no processo de autenticação das redes sem fio. O ataque consiste em três etapas: a preparação das *wordlists*, a etapa de captura das redes e ataque WPS e, por último, a execução dos ataques de dicionário e força bruta com os arquivos de capturas obtidos na segunda etapa e as listas de palavras obtidas na primeira etapa. As *wordlists* geradas possuem palavras da língua portuguesa, inglesa e combinações de nomes de laboratórios e salas da universidade.

Para o experimento, é utilizado um notebook com processador Intel Core i5, 6 GB de memória RAM, um adaptador de rede Wireless TP-Link WN722N v1.3 e os *softwares* Aircrack 1:1.2-0 [Aircrack-ng], Reaver 1.4-2 e Crunch 3.6-2. Com o notebook é possível executar ataque de força bruta do Reaver ao WPS dos pontos de acesso e escutar o tráfego das redes no alcance do adaptador para armazenar mensagens de autenticação legítmas de dispositivos ao WEP, WPA e WPA2. Um *desktop* equipado com processador Intel Core i7, 16 GB de memória ram e Ubuntu 16.04.3 LTS é utilizado para a execução da força bruta do Aircrack sobre as mensagens de autenticação armazenadas no *notebook*.

Durante a execução dos experimentos reparou-se que a criptografia WEP não é mais usada. Isso se deve ao fato de poder ser explorada facilmente e em pouco tempo [J. F. Kurose e K. W. Ross 2006]. Além disso, mesmo com o WPS podendo sofrer um ataque de força bruta viável ao atacante, é encontrado habilitado em uma grande quantidade de roteadores. No entanto, os pontos de acessos já possuem um mecanismo de segurança que insere um intervalo de tempo entre as tentativas de autenticação do ataque de força bruta. Dessa forma, nenhuma rede é invadida pelo WEP e WPS dos pontos de acesso verificados no experimento.

A Figura 1 mostra o percentual do sucesso dos ataques e os tipos de senhas descobertas em redes com WPA2 configurado. Os resultados mostram que redes configuradas com senhas triviais favoreceram o sucesso do ataque. Em contrapartida, senhas não triviais tem menor probabilidade de estarem presentes nas *wordlists* e, por isso, diminuem a probabilidade de sucesso no ataque. Dentre as redes que participam do experimento, 15,8% do total são invadidas descobrindo-se as senhas numéricas, 15,8% são de senhas compostas por palavras de dicionário. Os 68,4% restantes das redes não são comprometidas. Através destes resultados percebe-se que mesmo com as recomendações de criação

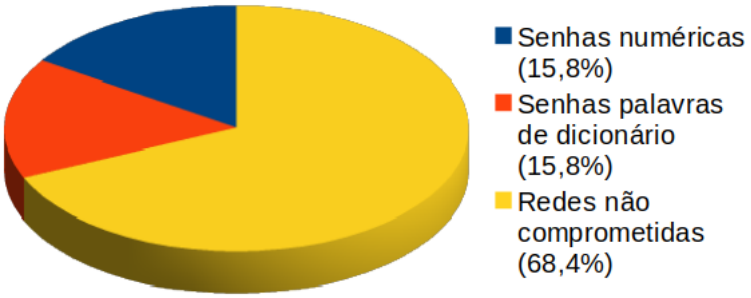

Figura 1. Percentual de sucesso de ataque de força bruta com listas de palavras contra redes sem fio WPA2.

de senhas complexas, administradores de rede configuram senhas frágeis que favorecem o ataque, como é o caso de 31,6% das redes analisadas.

3. Experimento Krack Attack

O objetivo do experimento é verificar se as medidas preventivas adotadas pelos fabricantes estão sendo eficientes e se os usuários estão atualizando seus dispositivos para a correção da falha após sua descoberta. Mathy Vanhoef, pesquisador que encontrou a falha, elaborou um *script* que está disponível em seu repositório do Github para identificação da vulnerabilidade em dispositivos padrão IEEE 802.11. Este *script* é utilizado para a verificação do funcionamento de protocolos de autenticação WPA2 em pontos de acesso e clientes.

O experimento consiste na execução do *script* em um notebook Lenovo Thinkpad T440 equipado com processador Intel Core i5, 4 GB de memória RAM e sistema operacional KaliLinux. Este *script* implementa a criação de uma rede na qual os dispositivos clientes devem se conectar para serem verificados. O módulo de testes de clientes Wi-Fi disponível no repositório possui a possibilidade de configurações do teste para alterar o tipo de ataque. No experimento desenvolvido as configurações padrões foram mantidas, os testes padrões verificam a possibilidade de reinstalação das chaves *Group Temporal Key* (GTK) e *Pairwise Transient Key* (PTK) nos clientes conectados [Paim 2014].

Para o experimento, alunos e professores da Universidade Federal Fluminense campus Praia Vermelha e da Moradia Estudantil da UFF (ME) são convidados a conectarem seus dispositivos com tecnologia Wi-Fi à rede criada. A saída da execução do *script* com os resultados dos testes é salva em arquivos para posterior análise e conclusão sobre os resultados. Isso possibilita que equipamentos de uso mais pessoais - menos usados em ambientes de trabalho - sejam testados pelo algoritmo.

A Figura 2 mostra o gráfico dos percentuais de dispositivos seguros e vulneráveis de acordo com o tipo e o uso. Observa-se no gráfico que dispositivos *Workstations* se destacam pela segurança pois estão atualizadas com as correções disponibilizadas pelo fabricante. Isso ocorre devido à política de atualização adotada nos equipamentos. Em contrapartida, os demais dispositivos caracterizados como uso pessoal tem uma porcentagem maior de dispositivos afetados. Quase 50% do total de dispositivos pessoais ainda estão susceptíveis ao ataque, o que demonstra a falta de preocupação de usuários finais

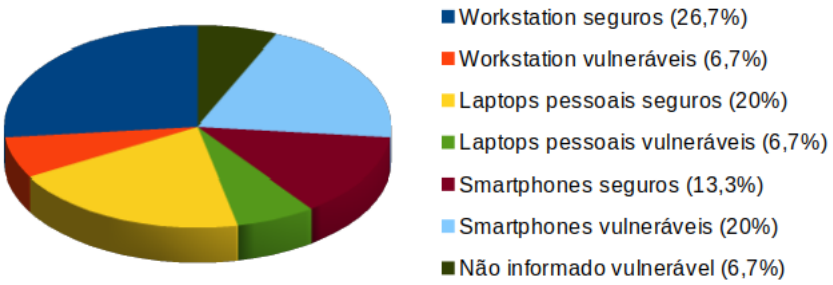

Figura 2. Percentual de aparelhos seguros e aparelhos vulneráveis observados nos testes do Krack Attack.

com atualizações corretivas ou o atraso na disponibilidade das correções por parte dos fabricantes.

4. Conclusão e Trabalhos Futuros

Após este trabalho é possível concluir que os métodos de invasão podem ser encontrados e aprendidos facilmente na Internet devido ao vasto material disponível. Outro fato importante e positivo é a preocupação dos fabricantes em disponibilizar correções para vulnerabilidades recentes, como foi o caso do Krack Attack. Porém, esse tipo de cuidado se mostra inútil se não for aliado a boas práticas dos usuários, como o de manter o sistema operacional dos dispositivos sempre atualizado e na criação de senhas elaboradas para que se evitem ataques como o do primeiro experimento. Como trabalho futuro, é possível aumentar a quantidade de dispositivos testados aumentando a área em que os experimentos são feitos e assim fazer uma análise estatística de maior precisão.

Referências

Aircrack-ng. Aircrack-ng documentation. `https://www.aircrack-ng.org/documentation.html`. Accessed: 2019-02-12.

Bianchi, G. (2000). Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547.

Campos, A. (2014). *Sistema de segurança da informação*. São Paulo: VisualBooks, 2 edition.

Chaabouni, R. (2006). Break WEP faster with statistical analysis. Technical report, EPFL, LASEC.

J. F. Kurose e K. W. Ross (2006). *Redes de Computadores e a Internet*. Pearson.

M. Vanhoef e F. Piessens (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer e Communications Security*, pages 1313–1328. ACM.

Paim, R. R. (2014). WEP, WPA e EAP. `https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/downloads/trabalho.pdf`.

Tews, E. (2007). Attacks on the WEP protocol. *IACR Cryptology ePrint Archive*, 2007:471.