# UM ESTUDO DAS VULNERABILIDADES NAS REDES IEEE 802.11

ALUNO: ANTONIO NÓBREGA
ORIENTADOR: PAULO GONÇALVES

17 DE ABRIL DE 2016


# CONTEÚDO

1. CONTEXTO ..... 3

2. OBJETIVOS ..... 4

3. CRONOGRAMA ..... 5

4. REFERÊNCIAS ..... 6

5. POSSÍVEIS AVALIADORES ..... 7

6. ASSINATURAS ..... 8

# 1. Contexto

As redes sem fio IEEE 802.11, popularmente conhecidas como redes Wi-Fi são amplamente utilizadas em ambientes comerciais, empresariais e residenciais por todo o mundo. Por causa da sua facilidade, rápida configuração e praticidade, as redes Wi-Fi estão cada dia mais  presentes no dia a dia das pessoas.

As redes Wi-Fi possuem múltiplas vulnerabilidades desde as suas primeiras versões, a maioria delas causadas pelo fato de que os dados que trafegam em uma rede sem fio são transmitidos através de frequências de rádio, e podem ser facilmente capturados. Para se obter pacotes de uma rede cabeada, um atacante terá que ter acesso físico a uma conexão de rede, o que muitas vezes significa ter acesso ao roteador da rede, tarefa essa que pode ser bastante trabalhosa. Já com redes Wi-Fi, um atacante poderá ter acessos a todas as informações que trafegam nessa rede muito mais facilmente, bastando estar nas proximidades do ponto de acesso da rede sem fio.

Este trabalho apresenta uma análise aprofundada dos mecanismos de segurança de redes Wi-Fi. Os protocolos WEP, WPA, WPA2, WPA-Enterprise e IEE 802.11w serão analisados em relação a critérios básicos de segurança: autenticidade, confidencialidade, integridade e disponibilidade. Também são analisadas as vulnerabilidades e ataques publicamente conhecidos aos protocolos mencionados, assim como os mecanismos de defesa, quando existentes, contra esses ataques. Por fim uma breve análise é feita dos protocolos e alterações que estão sendo desenvolvidos para redes IEEE 802.11 com o objetivo de melhorar a sua segurança.

# 2. OBJETIVOS

O objetivo deste trabalho é o de analisar os protocolos de segurança das redes IEE 802.11, comumente conhecidas como redes Wi-Fi, os ataques publicamente conhecidos contra essas redes e os mecanismos de defesa, quando existirem, contra esses ataques.

# 3. Cronograma

| ATIVIDADES | ABRIL | | MAIO | | JUNHO | | JULHO | |
|---|---|---|---|---|---|---|---|---|
| Estudo dos protocolos de Segurança das redes Wi-Fi | | | | | | | | |
| Estudo dos ataques e defesas as vulnerabilidades em redes Wi-Fi | | | | | | | | |
| Elaboração do documento final | | | | | | | | |
| Elaboração do Relatório e da Apresentação | | | | | | | | |

# 4. REFERÊNCIAS


[1]M. Eian and S. Mjølsnes, "A formal analysis of IEEE 802.11w deadlock vulnerabilities,"Proc. IEEE INFOCOM, pp. 918-926, 2012

[2]M. Kacic, P. Hanacek, M. Henzl, and P. Jurnecka, "Malware injection in wireless networks, " in Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013 IEEE 7th International Conference on, 2013.

[3] M. Agarwal, S. Biswas and S. Nandi, "Advanced Stealth Man in The Middle Attack in WPA2 Encrypted Wi-Fi Networks", IEEE Communications Letters, vol. PP, no. 99, pp. 1-4, 2015s

[4] Henning, Ronda R. "Vulnerability assessment in wireless networks."*Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*. IEEE, 2003.

[5] Guelzim, Tarik, and Mohammad S. Obaidat. "A new counter disassociation mechanism (CDM) for 802.11 b/g wireless local area networks." *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*. IEEE, 2009.

[6] Cache, J.; Wright, J.; Liu, V. Hacking exposed wireless. New York: McGraw-Hill, 2010.

[7] Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA."*Proceedings of the second ACM conference on Wireless network security*. ACM, 2009.

[8] Cassola, Aldo, et al. "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication." *NDSS*. 2013.

[9] Summers, Wayne C., and Anthony DeJoie. "Wireless security techniques: an overview." *Proceedings of the 1st annual conference on Information security curriculum development*. ACM, 2004.

[10] Yosuke, T. O. D. O., et al. "Falsification attacks against WPA-TKIP in a realistic environment." *IEICE TRANSACTIONS on Information and Systems*95.2 (2012): 588-595.

[11] Paterson, Kenneth G., Bertram Poettering, and Jacob CN Schuldt. "Plaintext recovery attacks against WPA/TKIP." *Fast Software Encryption*. Springer Berlin Heidelberg, 2014.

[12] Ahmad, Md Sohail, and Shashank Tadakamadla. "Short paper: security evaluation of IEEE 802.11 w specification." *Proceedings of the fourth ACM conference on Wireless network security*. ACM, 2011.

[15] Tsitroulis, Achilleas, Dimitris Lampoudis, and Emmanuel Tsekleves. "Exposing WPA2 security protocol vulnerabilities." *International Journal of Information and Computer Security* 6.1 (2014): 93-107.

[16] Wi-Fi and the Internet of Things: (Much) more than you think | Wi-Fi Alliance. Disponível em: <http://www.wi-fi.org/beacon/craig-mathias/wi-fi-and-the-internet-of-things-much-more-than-you-think>. Acesso em: 16 abr. 2016.

# 5. Possíveis Avaliadores

Carlos Ferraz – cagf@cin.ufpe.br

José Augusto Suruagy – suruagy@cin.ufpe.br

Ruy de Queiroz – ruy@cin.ufpe.br

# 6. ASSINATURAS

**Antonio Marino da Nóbrega Gomes**

Aluno

**Paulo André da Silva Gonçalves**

Orientador