Krack Attack
An Study

Felipe A. C. Gemmal[1], **Leonardo A. Basilio**[1],
João Gabriel S. Fernandes[1], **Arthur C. Sousa**[1]

[1]Instituto de Informática – Universidade Federal do Goiás(UFG)
Alameda Palmeiras, Quadra D,Câmpus Samambaia –
74690-900 – Goiânia – GO – Brazil

{felipegemmal,leonardobasilio,joaofernandes,arthursousa}@inf.ufg.br

Abstract. *This paper references the study of Krack Attack and its correlated components with the objective of completing the networks 2 graduation course in UFG.*

Resumo. *Esse artigo referencia o estudo do Krack Attack e seus componentes correlatos com o objetivo de completar o curso de graduação da UFG de redes 2.*

Introdução

O Krack Attack é um ataque ao Wifi, mais precisamente no protocolo WPA2 (*Wi-Fi Protected Access*) responsável pela segurança. Mesmo com a prova formal da segurança de algumas partes no WPA2 não foi possível prever a falha ao se usar o Man In The Middle para bloquear a recepção de um pacote se confirmação no protocolo de conexão 4-Way Handshake do WPA2. Uma situação específica também pode ocorrer com os dispositivos Android e Linux que reseta a chave de autenticação para um valor fixo conhecido, assim facilitando ainda mais o acesso aos dados do dispositivo.

Tecnologias envolvidas

Wifi

Internet yay

WPA2

Substituiu o WPA a partir do IEE 802.11i que faz algumas mudanças no protocolo Wifi, nele o algoritmo de encriptação passa a ser o AES(*Advanced Encryption Standard*)

4-Way Handshake

Muitas mãos

Aircrack-NG

Viajem !!!

Conclusão