Abstrakt

Angriffe auf WPA2 von Michael Barfs

In diesem Vortrag geht es um Angriffe auf den Standard WPA2. Die in dieser Präsentation behandelten Sicherheitsprotokolle implementieren die Standards der IEEE 802.11 für WLAN. Zunächst wird eine kurzen Einleitung/Vorstellung des Präsentierenden stattfinden. Danach wird der Präsentierende etwas über WEP erzählen. WEP ist das erste Sicherheitsprotokoll der IEEE 802.11 und erschien 1997. Dieser Standard enthält große Sicherheitslücken und wurde 2003 offiziell gehackt.
Darauf wird der Präsentierende mit einer Vorstellung der 2003 erschienen Sicherheitsprotokolls WPA fortfahren. Dieses Sicherheitsprotokoll ermöglicht die Verwendung eines besseren Verschlüsselungsalgorithmus.
Ein Jahr nach WPA, im Jahre 2004 erschien die neue Verschlüsselungsmethoden WPA2. WPA2 verwendet einen stärkeren Algorithmus zur Verschlüsselung und ist das aktuellste Sicherheitsprotokoll der IEEE 802.11 Standards.
Daraufhin wird der Präsentierende über Brute-force-Angriffe sprechen. Die Brute-force-Angriffe werden in Wörterbuch-Angriffe und Raibowtable-Angriffe unterteilt, wobei es für Wörterbuch-Angriffe eine online und offline Variante gibt.
Darauf folgt dann noch eine kurze Erklärung des Man-In-The-Middle Angriffes Hole 196. Hole 196 ist ein Fehler in dem Standard, auf dem die Sicherheitsprotokolle WPA2/WPA basieren.
Am Ende wir der Präsentierende seine Schlussfolgerungen mitteilen.

Attacks on WPA2 by Michael Barfs

This presentation is about attacks on the security protocol WPA2. The in this presentation handled security protocols implement the standards of the IEEE 802.11 used for WLAN. First there will be a short introduction by and of the presenter.
Then the presenter will talk about WEP. The WEP security protocol holds bugs and was official hacked in 2001.
Then the presenter will introduce WPA which was released in 2003. This security protocol allows the use of a better encryption algorithm.
One Year later , in 2004, the new security protocol WPA 2 was released. WPA2 uses a better algorithm for encryption and is the newest security protocol based on the standarts of the IEEE 802.11.
After that the presenter will talk about brute-force-attacks . The brute-force-attacks are divided into rainbow-table-attacks and wordbook-attacks. Wordbook-attacks are divided into online and offline attacks.
The there will be a short introduce of the man-in-the-middle attack named Hole 196. Hole 196 is a mistake in the standards, on which WPA and WPA2 are based on.
At the end the presenter will talk about his conclousion.

Gliederung

- WEP - Wired Equivalent Privacy
- WPA - Wifi-Protected-Access
- WPA2 -Wifi-Protected-Access 2
- Bruteforce
- Hole 196
- Schlussfolgerung

Quellen

- Paper “Real-life paradigms of wireless network security attacks” von I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkias 2011
- Paper “Parallel Active Dictionary Attack on WPA2-PSK” von Omar Nakhila, Afraa Attiah, Yier Jin and Cliff Zou 2015
- “Network Hacks – Intensivkurs Angriff und Verteidigung mit Python” von Bastian Ballmann ISBN 978-3-642-24304-2
- Jörg Hedrich - "Seminar Net Security - Sicherheit im WLAN" http://www.uni-koblenz.de/~steigner/seminar-net-sec/sem8.pdf