Angriffe auf WPA2

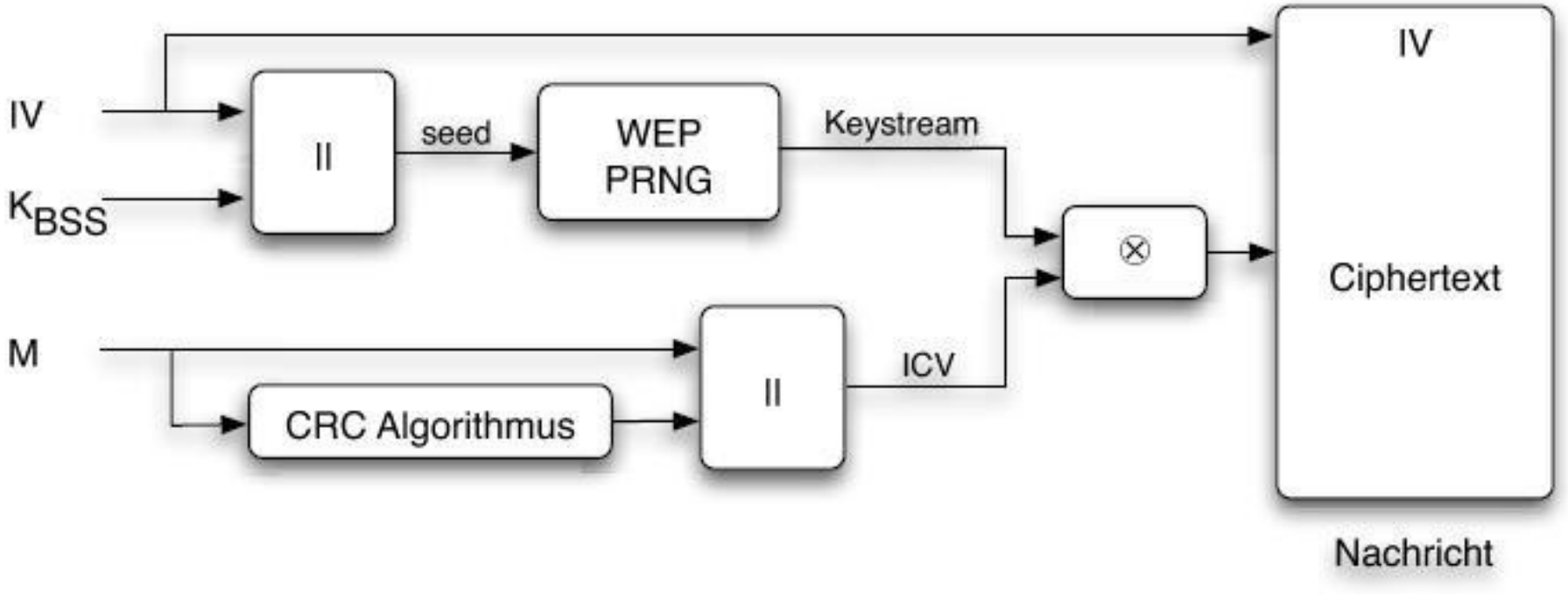
Von Michael Barfs

Gliederung

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

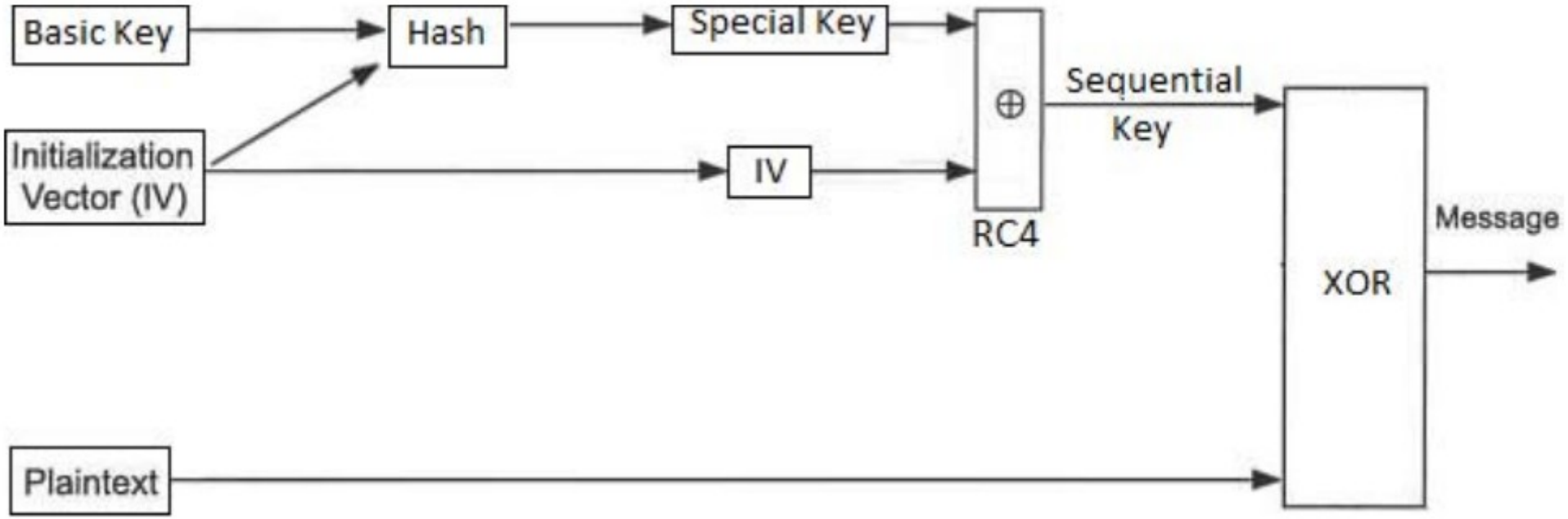
WEP-Wired Equivalent Privacy

- 1997 mit dem ersten IEEE 802.11 Standard
- RC4/CRC-32
- 2001 gehackt von Fluhrer, Martin und Shamir



WPA-Wifi-Protected-Access

- Erschien 2003
- Implementiert viele Standards der IEEE 802.11i
- TKIP



I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkia - Real-life paradigms of wireless network security attacks

WPA 2 -Wifi-Protected-Access 2

- Erschien 2004
- TKIP oder AES-CCMP
- Mehr Rechenleistung erforderlich
- Robust Secure Network (RSN)

Bruteforce

- Rainbow Table
- Wörterbuch
  - Online
  - Offline
- GPU

Hole 196

- Nutzt nicht signierten Broadcast-Traffic
- Angreifer muss angemeldet sein
- Schickt Packet an Broadcast Adresse
- Alle Klienten antworten mit PTK

Schlussfolgerung

- WPA2 ist zurzeit die beste Wahl
- Man sollte ein starkes Passwort wählen
- Das Passwort für Zuhause sollte aus um die 20 zufälligen Zeichen bestehen.

Ende, Fragen?

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