

Aus aktuellem Anlass...

WPA2 ist geknackt, das ist das Ende der Welt!

(oder auch nicht.)

Erklärung des entdeckten Fehlers im WPA2-Protokoll (deutsch):

<https://www.heise.de/security/meldung/Details-zur-KRACK-Attacke-WPA2-ist-angeschlagen-aber-nicht-gaenzlich-geknackt-3862571.html>

<https://www.heise.de/security/artikel/KRACK-so-funktioniert-der-Angriff-auf-WPA2-3865019.html>

Paper des Entdeckers mit Details:

<https://www.krackattacks.com/>

Video mit Demonstration:

<https://www.youtube.com/watch?v=Oh4WURZoR98>

Erklärung 4-Wege-Handshake (nur Schritt 3 und 4 (Schlüsselaustausch) sind angegriffen worden, nicht die Authentifizierung!):

<http://www.kryptowissen.de/wpa2.php#4-wege-handshake>