UNIVERSITÄT BASEL

Christian Tschudin christian.tschudin@unibas.ch
Claudio Marxer claudio.marxer@unibas.ch
Christopher Scherb christopher.scherb@unibas.ch

Departement Mathematik & Informatik
Spiegelgasse 1
CH-4051 Basel

Introduction to Internet and Security
Frühjahrsemester 2018
Projekt

Projekt # 16: WPA2 Cracking

Kontaktperson: Claudio Marxer <claudio.marxer@unibas.ch>

1. Einführung

WPA2-PSK ist ein weit verbreiteter Standard zur Verschlüsselung von Datenverkehr in Drahtlosnetzwerken (WLANs). Werden genügend aufwändige Passwörter eingesetzt, gilt WPA2-PSK als “sicher”.

2. Einstiegspunkte

Ihr Projekt soll folgende Fragestellungen und Schritte enthalten, ist aber nicht darauf beschränkt:

- Konfigurieren Sie ein mit WPA2 gesichertes WLAN. Zeichnen Sie für unterschiedlich starke Passwörter einen WPA2-Handshake auf und versuchen Sie mit durchprobieren des Passwortraums (Brute Force), das Passwort zu finden. Vergleichen Sie die Performance bei der Verwendung CPU bzw. GPU.
- Welche Passworträume - abhängig von Länge und Zeichensätze - können als “sicher” bezeichnet werden?
- Untersuchen sie die Standardpassworte von WLAN-Geräten mit WPA2-Verschlüsselung auf ihre Sicherheit (z.b. WLAN-Router, Mobile Hotspots). Finden Sie im öffentichen Raum Hotspots, von denen Sie vermuten können, dass Passwort unsicher ist? Benutzen Sie SSIDs als Heuristik dafür, welches Produkt das Drahtlosnetwerk zur Verfügung stellt.

3. Material und Links

- `https://de.wikipedia.org/wiki/WPA2`
- `https://www.aircrack-ng.org`