# K&K—oder Karma und Kismet

*Nachlese eines Clubabends vom 20.3.2014*

***Thomas Sulak***

## Die Ausgangssituation

Sie sitzen in ihrem Lieblings Café, verbinden sich mit einem kostenlosen Hotspot und jemand mit etwas technischem Wissen und einer guten Portion krimineller Energie liest all ihre persönlichen Daten aus. Zugegeben – man könnte jetzt sagen: *selbst schuld, wer sich mit einem kostenlosen WLAN verbindet!* Was aber, wenn ihr Smartphone das automatisch, ohne ihr Zutun, in der Hostentasche macht? Gibt's nicht?

## Das Szenario

Findet er ein kostenloses, offenes WLAN und stellt eine Verbindung her, denkt der gemeine User oft ein Schnäppchen gefunden zu haben. Tatsächlich surfen sie möglicherweise über einen Hotspot, den der Typ neben ihnen gerade eingerichtet hat, und der schaut ihnen vielleicht sogar noch über die Schulter bei Ihren Banküberweisungen.

Kostenlose Hotspots stellen in der Öffentlichkeit Internet zur Verfügung für Jedermann, jeder Orts. Diese stellen sich aber immer wieder als Mogelpackung heraus. Als Kostenfalle. Es ist unvorstellbar, wie viele Hotspots man auf öffentlichen Plätzen findet - offen! – unverschlüsselt - mit einem einzigen Ziel: Sie und Ihr Smartphone „abzuzocken". Nun ja – vielleicht ist es nicht ganz so schlimm, sie sollten jedoch davon ausgehen.

Ihnen passiert das nicht? Erlauben sie mir eine Frage: verbindet sich ihr Smartphone automatisch mit dem WLAN im Büro oder zu Hause? Ja? Praktisch und bequem! – Keine Frage. Aber damit haben Sie bereits den Opferstatus!

Es ist sehr einfach, einen eigenen Hotspot einzurichten und diesen z.B. „Café Free Web" zu benennen. Das kann heute jeder Smartphone User selbst. Will man sich etwas professioneller aufstellen, nimmt man einen dafür eigens konzipierten Router – einen sogenannten „Ja-Sager".

## Ja-Sager und KARMA

*„Karma attacks Radio machines automatically."* Radio machines sind einfach gesagt alle Geräte, die mit WiFi ausgerüstet sind. Das kann ein Desktop, Notebook, Smartphone, Tablet oder sogar eine Xbox oder Playstation sein.

Wie funktioniert KARMA? Jedes Mal, wenn sich Ihr Smartphone mit einem Hotspot verbindet, speichert es den Namen (SSID) und das Passwort. Somit verbindet es sich in Zukunft automatisch. Praktisch und bequem!

Was jedoch die wenigsten Benutzer wissen ist – egal wo sie sind, das Smartphone fragt ständig nach, ob eines der vertrauten Netzwerke in der Nähe ist; eine der Hauptursachen für einen erhöhten Stromverbrauch.

Dazu sendet das Gerät einen sogenannte Probe Request (Abb.1). Ein Probe Request ist die permanente Nachfrage, ob ein vertrautes Netzwerk in der Nähe ist, und falls ja, verbindet es sich.

KARMA analysiert diese Anfragen und extrahiert die Netzwerk Identifikationsdaten wie Netzwerkname und MAC Adresse und benutz diese Informationen um einen Klon dieses Netzwerkes zu kreieren. Es verhält sich an dieser Stelle wie ihr vertrautes Netzwerk und antwortet auf diese Probe Request mit *„Ja, ich bin Dein vertrautes WLAN „zuhause" – verbinde dich".*

Nachdem Ihr Smartphone nicht zwischen dem echten und dem geklonten Netzwerk unterscheiden kann, verbindet es sich (Abb.2).

Sobald die Verbindung hergestellt ist, beginnt das Smartphone auch schon zu kommunizieren und ruft E-Mails ab, verbindet sich mit Facebook, usw. – das alles, über den scheinbar kostenlosen Hotspot, in ihrer Tasche ohne ihr Wissen und ohne ihr Zutun.

So kann es schon mal vorkommen, dass sie am Stephansplatz mit dem WLAN zu Hause verbunden sind. Was technisch nicht möglich ist, sofern Ihre Adresse nicht 1010 Wien, Stephansplatz 1 lautet. Diese Verbindung kommt in jedem Fall zu Stande, auch wenn das eigentliche Netzwerk verschlüsselt ist. Das Smartphone fragt an dieser Stelle nicht nach.

Mit diversen Tools wie Wireshark kann nun der komplette Netzwerkverkehr mitgelesen werden. All ihre Passwörter, Login Daten, ihr komplettes Surfverhalten. Es werden manipulierte Login Seiten zur Verfügung gestellt—von diesen Fakes werden dann Benutzernamen und Passwörter abgegriffen.

## Tipp

Live Demos dieser Hacking Attacken finden immer wieder im Zuge diverser Veranstaltungen von Thomas Sulak statt. Infos und Anmeldung finden Sie unter *www.thomas-sulak.at*

## Conclusio

Noch immer gehen viele Smartphone User viel zu sorglos mit Ihren Datenverbindungen um! Im Inland wie im Ausland. Das Umdenken vom *„Handy"* zum *„Smartphone"* hat in vielen Köpfen noch nicht stattgefunden und wird viele Menschen noch sehr viel Geld kosten.

Ein Test in der Öffentlichkeit zeigt, dass sich zahlreiche Geräte bereits nach einigen Minuten erfolgreich mit dem Router verbunden haben (Abb. 3).

## In der Praxis

In der Praxis würde man vermutlich folgender Maßen vorgehen:

- Ja-Sager aktivieren und das vorhandene WLAN Klonen (Starbucks, McDonalds, usw.)
- Mittels einer DeAuth-Attacke, die man zum Beispiel über ein Smartphone ausführen kann, werden sämtliche Smartphones vom aktuellen WLAN getrennt und verbinden sich neu. Jetzt aber mit dem geklonten WLAN.
- Über einen manipulierten DNS Server, der am Router installiert ist, werden die ahnungslosen Benutzer nun auf falsche Webseiten umgeleitet, wie zum Beispiel: Facebook, wo sie ihre freundlicherweise protokolliert.

Nachdem nun der gesamte Netzwerkverkehr über den Ja-Sager läuft, kann dieser sehr leicht mittels Wireshark ausgelesen und protokolliert werden.

## Fazit

Der Datenaustausch über WLAN und Bluetooth ist sehr mangelhaft gesichert und lädt Spione ein. Darum schalten`s diese Funktionen nur dann ein, wenn Sie unmittelbar benötigt werden. Ein angenehmer Nebeneffekt - stark reduzierter Akku-Verbrauch!

Ich stelle mir ohnehin die ernstgemeinte Frage, wozu ich WLAN im Inland, in der Öffentlichkeit auf meinem Smartphone jemals aktivieren sollte? Der Schalter um diese Funktion zu deaktivieren ist mittlerweile sowohl bei iOS als auch bei Android sehr einfach über wischen zu erreichen. Selbiges gilt natürlich auch für Bluetooth – abdrehen!

Moderne Mobilfunk Verträge beinhalten mindesten 1-GB-Download-Volumen. Das ist bei weitem ausreichend für www, E-Mails, Facebook und Co. Wer, so wie ich, viel Musik online streamt, kann für ein paar Euro pro Monat das Downloadvolumen auf 4GB oder mehr erhöhen.

## Wie schützt man sich?

1. WLAN und Bluetooth abschalten, wenn diese nicht benötigt werden.
2. Kein automatisches Verbinden zulassen.
3. Login ausschließlich über „https" – Seiten.
4. kostenloses WLAN nur mit Registrierung. Stichwort: McDonalds oder Starbucks.
5. Steganos Online Shield® für ein paar Euro pro Jahr.

```
KARMA: Probe Request from f0:27:65:13:51:55 for SSID 'FreeWLan'
KARMA: Probe Request from ec:85:2f:99:21:85 for SSID 'Starbucks'
KARMA: Probe Request from 10:68:3f:ff:ca:44 for SSID 'Freewave'
KARMA: Probe Request from ec:85:2f:99:21:85 for SSID 'Freewave'
KARMA: Probe Request from 00:15:70:4b:b4:13 for SSID 'symbo_ap'
KARMA: Probe Request from 0c:3e:9f:5e:ff:68 for SSID 'Freewave'
```

Abbildung 1 – Der Probe Request wird von Karma abgefangen und analysiert

```
KARMA: Successful association of f0:27:65:13:51:55
KARMA: Checking SSID for start of association, pass through FreeWLan
```

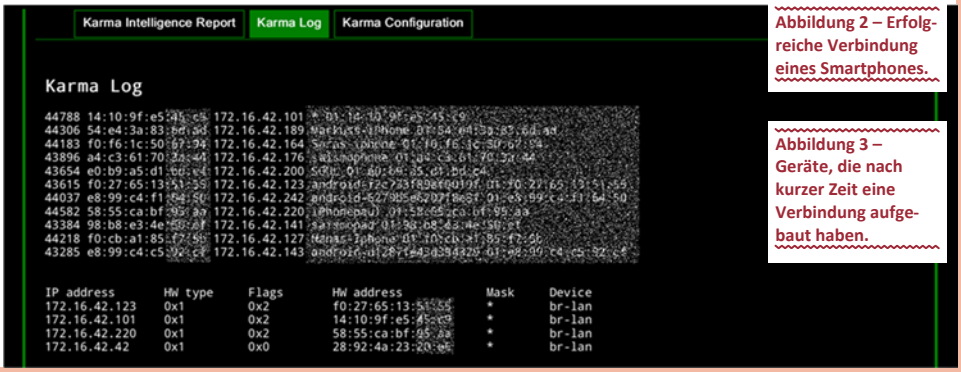


Abbildung 2 – Erfolgreiche Verbindung eines Smartphones.

Abbildung 3 – Geräte, die nach kurzer Zeit eine Verbindung aufgebaut haben.