Praktikum Aufgabe
Übung 1

Angriffszenarien und
Gegenmaßnahmen
SS2018
Hochschule Emden/Leer

Liang He und Yang Mao

3. April 2018

Inhaltsverzeichnis

1 WEP

a). Wie funktioniert Keystream-Reuse bei WEP?

b). Warum ist Keystream-Reuse möglich und so effizient?

c). Warum reicht es nicht aus den IV auf 32 bit zu verlängern? Begründen Sie ihre Antwort mit Hilfe des „Birthday-Paradox“.

d). Warum ist eine Modifikation von WEP-Nachrichten möglich? Welche Angriffe sind dadurch denkbar?

e). Wie könnte man diese Angriffe verhindern, wenn man trotzdem weiterhin RC4 bzw. eine Stromchiffre verwenden möchte?

f). Implementieren Sie (selber) den RC4. In der Datei IVKeystream.txt finden Sie Paare von IVs und ein byte große, abgefangene Chi- texte einer mit WEP-Verbindung. Bestimmen Sie daraus mittels einer geeigneten (eigenen) Implementierung des in der Vorle- sung beschriebenen Angriffs das erste Byte des WEP-Schlüssels. Beschreiben Sie dabei kurz ihre Vorgehensweise.

2 WPA/WPA2

a). In der Vorlesung wurden mehrere Angriffe auf Basis von Keystream-Reuse für WEP-Verkehre beschrieben (vgl. auch Aufgabe 1). Sind diese auch bei WPA-/WPA2-Verkehren möglich? Begründen sie kurz Ihre Antwort.

Ne, das geht nicht.

b). Unter welchen Bedingungen können WPA-Verkehre trotz des verbesserten Key-Managements immer noch entschlüsselt werden. Beschreiben Sie Ihren Angriff.

c). Kann WPA2 auch noch angegriffen werden? Begründen Sie Ihre Antwort.

d). Wie werden die Angriffe heutzutage, z.B. bei Eduroam, verhindert? Welche Rolle spielen dabei EAP und RADIUS bzw. DIAMETER?

e). Was ist die Grundidee des Key Reinstallation Angriffs. Wie kann dieser verhindert werden?

3 Aircrack & Co

a). Brechen Sie die im IT-Labor eingerichtete WLAN-Verbindung mit der für Sie vorgesehenen SSID (im Praktikum erfragen) mittels Aircrack unter zu Hilfenahme der Datei Password.txt. Beschreiben Sie kurz die einzelnen Schritte ihrer Vorgehensweise.

Wir haben folgende Schritte durchgeführt und die AP 'ITS-WEP' geknackt. Das Passwort ist

`ED:98:ED:38:DF:BB:C3:BB:B0:D2:8C:62:B3`

a. Mit Airmon-ng die Netzwerkkarte zu promiscuous versetzen

```
airmon-ng start wlan0
```

b. WLAN mit WEP identifizieren und Netzwerkverkehr mitschneiden.

```
airodump-ng wlan0mon --ivs -c {CH} --bssid {target_ssid} -w
```

c. Die Menge an Netzwerkverkehr(bzw. ARP-Verkehr) kann durch 2 Arten erhöht werden. Entweder durch Abmelden des zulässige Clients oder Versuch einer falschesten Authentifizierung am AP. Wir haben leider keine zulässige Geräte vorhanden, wir müssen auf 2. Weise gehen, also eine Aireplay-attacke durchzufuhren.

```
aireplay-ng wlan0 --deauth 0 -a {target_mac}
```

Da normalerweise soll viele Gerate nach einer abmedlung wieder dem AP zu verbinden, und damit können wir genug ARP Requests und ACKs sammeln.

d. Wenn c.a. 1500 Paket gesammelt wurden, können wir schon mit Aircrack-ng das Passwort zu knacken.

```
aircrack-ng {.ivs file} -b {target_ssid}
```

b). (Optional) Versuchen Sie, da Sie nun den PSK kennen, die Verkehre mittels eines geeigneten Tools (z.B.Wireshark) aufzuzeichnen und zu entschlüsseln.

c). (Optional) Machen Sie sich mit WPS-Pin-Verfahren vertraut. Versuchen Sie die WLAN-Verbindung mittels WPS anzugreifen.

Nicht gemacht.