



Falko Dressler Tobias Limmer Johannes Bauer

Netzwerksicherheit WS 2008/09

Hausaufgabe WEP-Verschlüsselung

26.1.2009

In dieser Aufgabe werden Sie versuchen, die Verschlüsselung einer WLAN-Verbindung zu brechen, die mit WEP verschlüsselt ist.

Zunächst einmal ist es wichtig, dass Sie sich damit vertraut machen, wie die Verschlüsselung von WEP-64 funktioniert. WEP-64 benutzt einen 24 Bit langen Initialisierungsvektor, der im Klartext übertragen wird. Daran wird zum Key-Setup ein 40 Bit langer Schlüssel (Shared Secret) konkateniert. Diese 64 Bit werden zur Initialisierung der Pseudozufallszahlengeneratorkfunktion RC4 verwendet. Der Keystream aus dem RC4-Algorithmus wird mit dem Plaintext durch einfaches XOR verknüpft um den Ciphertext zu bilden. Da XOR zum Einsatz kommt ist die Entschlüsselung gleich der Verschlüsselung. Die Passwörter werden bei WEP generell nicht gehashed, sondern direkt in Ihrer US-ASCII-Repräsentation eingesetzt, was den Suchraum erheblich reduziert.

Ihre Aufgabe ist, sich zunächst den PCAP-Dump von WPA-64 Netzwerktraffice herunterzuladen und mit Hilfe von **wireshark** zu analysieren. Hierfür stellen wir Ihnen zwei Dateien zur Verfügung: Eine, bei der Ihnen das Passwort bekannt ist (`mOR0n` bzw `6d 30 72 4f 6e`) und eine, deren Passwort Sie aufbrechen sollen. Sehen Sie sich die Dumps mit Wireshark genau an, um zu verstehen, welche Pakete Datenpakete darstellen und wie deren Header aufgebaut sind. Benutzen Sie die WEP-Entschlüsselungsfunktion von Wireshark, um auch den Inhalt der WEP-Pakete zu sehen (Edit - Preferences - Protocols - IEEE 802.11 - Enable decryption). Achten Sie darauf, dass in dem Dump noch andere, für die Übung nicht relevante, Netzwerke enthalten sind.

Finden Sie nun die Offsets folgender interessanter Werte aus der Protokollschicht IEEE 802.11 heraus, welche *unverschlüsselt* übertragen werden:

1. Die BSSID der assoziierten Station
2. Die Quell-MAC-Adresse des Pakets
3. Die Ziel-MAC-Adresse des Pakets
4. Der Initialisierungsvektor der WPA-Payload

Vervollständigen Sie die Datei `Packet.hpp` entsprechend um Ihre Ergebnisse zu reflektieren und testen Sie, ob die Daten stimmen.

Schreiben Sie dann ein Programm, das die Pakete aus einem verschlüsselten PCAP ausliest. Sie können bei Paketen der Länge 80 Bytes davon ausgehen, dass es sich um ARP-Pakete handelt. Hierbei sind 12 Bytes der BSD Radiotap-Header, 28 Bytes der IEEE 802.11 Frame-Header, 36 Bytes verschlüsselte Daten und 4 Bytes die Checksumme. Von diesen ARP-Paketen können Sie wiederum davon ausgehen, dass sie von einem Rechner im 192.168.0.0/16er Netzwerk gesandt wurden und die MAC-Adresse eines anderen Rechners im 192.168.0.0/16er Netz abfragen. Weiterhin beginnen die entschlüsselten WEP-Daten zunächst

mit einem LLC¹ Header in welcher die sogenannten SSAP und DSAP²-Felder enthalten sind. Diese zwei Felder haben bei WEP-Datenpaketen immer den Wert `0xaa`.

Finden Sie heraus an welchem Offset innerhalb der verschlüsselten Daten die Quell- und Ziel-IP-Adresse im ARP-Paket vorkommt. Zusammen mit dem SSAP und DSAP-Feld werden Sie diese Information benutzen um bei einem entschlüsselten Paket herauszufinden, ob der Key richtig war.

Schreiben Sie nun das Programm `WLANAttack`, welches mit folgender Syntax gestartet werden soll:

```
$ ./WLANAttack <PCAP-Datei> <BSSID> <Quell-MAC des ARP-Pakets>
```

also beispielsweise wie folgt gestartet wird:

```
$ ./WLANAttack output.pcap 1122ff00bbaa 000c0199ffab
```

Das Programm soll nach dem Aufruf folgendes machen:

- Die Dump-Datei öffnen
- So lange Pakete auslesen, bis ein Paket der Länge 80 Bytes gefunden wird, das die auf der Kommandozeile angegebene BSSID und Quell-MAC besitzt. Weiterhin soll die Ziel-MAC des Pakets die Broadcast-MAC-Adresse sein. Welche dies ist finden Sie am einfachsten mittels Wireshark heraus.
- Sobald ein passendes Paket gefunden wurde, starten Sie einen Passwort-Bruteforce-Angriff darauf. Als Passwörter kommen Groß- und Kleinbuchstaben sowie Ziffern vor. Das Passwort gilt als gefunden, wenn die SSAP und DSAP-Felder beide `0xaa` sind und sowohl die Quell-IP als auch die Ziel-IP des enthaltenen ARP-Pakets im `192.168.0.0/16`er Subnetz liegen.

Achten Sie darauf, dass Sie Ihr Angriffs-Programm hinreichend performant arbeitet. Ihr Programm sollte im langsamsten Fall 250000 Passwörter pro Sekunde testen können. Ein Richtwert für eine nicht weiter optimierte Musterlösung sind 600000 Passwörter pro Sekunde (beides gemessen an der `fau06a` auf einem Kern). Sobald Sie das Passwort gefunden haben, schreiben Sie es in die `passwd.txt` Datei.

Abgabe Legen Sie die Quellcodedateien `WLANAttack.cpp` und `Packet.hpp` sowie die Textdatei `passwd.txt` in unserem Abgabesystem in Verzeichnis `aufgabe08` ab. Treten Probleme auf, melden Sie sich bitte bei Tobias Limmer (`limmer@informatik.uni-erlangen.de`). Abgabeschluss ist der 2.2.2009.

¹Logical Link Control

²Source/Destination Service Access Point