

Technische

Fortgeschrittene Aspekte
VON
Software Security VU
183.082
SS2004

Lab 2A
„Dispel the myth of WLAN Security“

Haider Gerald (0125638)
Radl Christoph (0102799)
Schachinger Josef (0125692)
Scheichenstein Thomas (0103825)

Inhaltsverzeichnis

1	BEGRIFFSVERZEICHNIS	3
2	HINTERGRUND ZUM CRACKEN DES WEP-KEYS	5
3	VERWENDETE HARDWARE	7
4	VERWENDETE SOFTWARE	7
4.1	Sniffing	7
4.2	Cracking	7
5	TESTBEDINGUNGEN	7
5.1	Testumgebung Exp1	9
5.2	Testumgebung Exp2	10
5.3	Testumgebung Exp3	10
6	TESTERGEBNISSE	11
6.1	Zu Exp 1	11
6.2	Zu EXP 2 und Exp 3	11
6.3	Zu Dictionary Attack	12
7	RISIKOEINSCHÄTZUNG	13
8	ABBILDUNGSVERZEICHNIS	13

Einleitung

Drahtlose Netze erfreuen sich aufgrund ihrer guten Ergonomie und ihres leichten Aufbaus sehr großer Beliebtheit. Kein Stemmen und Kabelverlegen ist mehr notwendig das Heim oder Firmennetzwerk ist mit geringem Investitionsaufwand sofort einsatzbereit. Doch genau in dieser vermeintlichen Einfachheit liegen die Tücken von WLAN (Wireless LAN). Bei vielen Netzen wird die Verschlüsselung erst gar nicht aktiviert und so sind diese für jeden der mit der entsprechenden Ausstattung in Reichweite ist. Doch auch mit aktivierter Verschlüsselung sollte man sich nicht in allzu großer Sicherheit wiegen.

Mit dieser Arbeit wollen wir deshalb versuchen zu demonstrieren wie die Verschlüsselung bei WLAN ausgehebelt werden kann. Nach dem Arbeitsprotokoll findet sich eine Risikoeinschätzung die helfen soll WLANs so zu betreiben dass die von uns vorgeführte Vorgehensweise so schwer wie möglich zu realisieren ist.

1 Begriffsverzeichnis

WEP

Wireless Equivalent Privacy

Derzeitige Standardverschlüsselungstechnik im Wlan. Dieses Verschlüsselungsverfahren basiert auf RC4 (Verschlüsselungsverfahren von der RSA Data Security Inc.). Umgesetzt als ein symmetrisches Verschlüsselungsverfahren mit einem 40/64 (WEP) oder 128 bit (WEP) langen Schlüssel (siehe WEP-Key). Aus der symmetrischen Verschlüsselungstechnik leitet sich auch gleichzeitig ein Teil des Problems ab, da auf beiden Seiten derselbe Schlüssel verwendet wird. WEP ist im IEEE 802.11 Standard definiert, wird aber auch laufen erweitert.

WEP-Key

Schlüssel der für die WEP Verschlüsselungstechnik eingesetzt wird. Typische Standardlänge ist derzeit 128 bit (WEP2).

Access Point

Der Access Point dient als eine Art Koordinator und Manager im seinem abgedeckten Funkbereich auf. Er ist verantwortlich dafür, dass die richtigen Clients miteinander kommunizieren und natürlich liegt auch die Schlüsselüberprüfung teilweise in seinem Bereich. Dazu muss aber noch unterschieden werden in

- Open System Authentisierung, Beliebige Bezeichnung die ein einzelnen Wlan identifiziert. Dabei kann es unter Umständen nicht sehr sinnvoll sein, wenn diese Bezeichnung eine Beschreibung der Organisation oder den Zweck des Netzes wiedergibt, da sich Hacker leichter ein Bild von diesem Netzwerk machen können und somit mehr Anhaltspunkt für einen Angriff feststellen können.
- Shared Key Authentisierung, Ist auch gleichzeitig Teil des WEP Protokolls. Clients können sich nur in die Netzwerkkomponente einwählen, wenn diese über den verein-

barten Schlüssel verfügen. Folgender Ablauf kann als typisch bezeichnet werden für ein einwählen in eine Netzwerkkomponente mit AP.

- Der neue Client sendet eine Authentisierungsanforderung an den AP.
- Der AP sendet eine Zeichenkette zurück, wird auch Challenge genannt.
- Der Client verschlüsselt die Challenge mit dem WEP-Key (siehe oben).
- Der Client sendet die verschlüsselte Challenge (Response) an den AP.
- Der AP entschlüsselt die Response mit dem gleichen WEP-Key.

Bei gelungener Einwahl teilt der AP dem Client seinen gewünschten Partner zu, dieser muss auch ein bereits authentifizierter Client sein, oder der AP selbst der die Anfrage zum Beispiel an ein Kabelgebundenes Netzwerk weiterleitet oder ähnliches.

SSID

Shared System ID Wird auch als Shared Key bezeichnet. Ermöglicht den gemeinsamen Zugriff auf ein definiertes WLAN. Nur Clients und AP's mit gleicher SSID dürfen kommunizieren.

Ad-Hoc Netzwerk

Mindestens 2 Clients bauen ein Netzwerk auf, dabei definiert der erste den Standard in diesem Netz, Verschlüsselung, Sichtbarkeit,...
Vorteil und Gefahr liegt in der Individualität.

WLAN

Wireless Local Area Network, Ziel und Gefahr in einem. Der Vorteil in dieser Technik liegt darin, dass die Basis und nur diese, sehr einfach umgesetzt werden kann. WLAN AP sind heute günstige Alternativen zum Switch und ersparen lästige Kabelleitungen quer durch die Wohnung oder Firma. Noch einfach und alternativ zu Bluetooth besteht auch die Möglichkeit zum Ad-Hoc Netzwerk (siehe oben).

Durch das Verlassen des physisch mehr oder weniger sicheren Kabels ist es aber auch jedem im Umkreis des AP's möglich mit diesem zu kommunizieren.

Wardriving

Bis vor einigen Jahren hätte man Wardriving als Sportart beschreiben können, die es verdient olympisch zu werden.

Grundsätzlich steht dahinter, dass man sich durch ein Gebiet bewegt und nach aktiven und auch möglichst wenig abgesicherten WLANs sucht. Um dies zu vereinfachen wird ein Netzwerkscanner eingesetzt, als bekanntestes Beispiel der Netstumbler [Nets]

Zusätzlich wird noch ein Notebook mit passender WLAN Karte benötigt, oder minimaler mittels PDA mit WLAN.

Als Einsatzgebiete kommen hier Messen (bekanntes Beispiel CeBIT), oder auch Wohn- und Gewerbegebiete. Diese werden mit aktiviertem Netzwerkscanner zu Fuß oder per Auto „durchforstet“.

Sniffing

Unter Sniffing versteht man das bewusste Absuchen der Packages die in einer definierten Netzwerkkomponente ausgetauscht werden.

Dazu können zwei verbreitete Tools eingesetzt werden.

Kismet [**Kism**] beschränkt sich auf das Sniffen und dementsprechende aufsuchen von so genannten „weak Packages“.

Als zweit bekannte alternative steht

AirSnort [**Airs**] zur Verfügung, wobei dieser zusätzlich zum Sniffen auch gleichzeitig das Cracken (siehe unten) ermöglicht.

Cracking

Als Cracken wird hier speziell das Ausarbeiten des WEP-Key bezeichnet, wobei man auf die oben beschriebenen weak Packages zurückgreift. Aus diesen lässt sich, falls in genügender Anzahl vorhanden (3000- 5000 bei 64 bit Key), der Key reproduzieren und somit den Datenverkehr zu entschlüsseln. Längere Schlüssel oder spezielle Firmwareupdates (Cisco WPA usw.) machen das Berechnen des Schlüssels ungleich schwerer.

Theoretisch wird bei einer simplen WEP Verschlüsselung (128 bit Key) ein Traffic von ca 800 – 2000MB benötigt um die Schlüsselreihe herauszufinden. Praktisch gesehen ist ein komplettes Entschlüsseln der aufgenommenen Daten nur schwer zu erreichen. Als Vergleich bleibt zu erwähnen das mit ähnlicher Datenmenge auch SSL entschlüsselt werden könnte!!

Dagegen sprechen.

- Geringe Abstrahlungsweite in „ungeschützten Privatnetzwerken“ (Heimnetz)
- Verbesserte Firmware und Updates in homogenen Firmennetzwerken
- Zusatzmethoden zur Verschlüsselung (SSL, VPN, PTPP...)
- Bei größeren Schlüssel schon sehr gute Hardware zum berechnen der Schlüssel notwendig (> 3 Tage)
- Passiv/Active WLAN Attack Tools benötigen meist spezielle Hardware um bestehendes WLAN zu infiltrieren (und zu funktionieren.)
- Mit Einführung der Quantencomputer ist ein RSA verwandter Sicherheitsalgorithmus hinfällig.

2 Hintergrund zum Cracken des WEP-Keys

Das Cracken des WEP Keys basiert auf einer eklatanten Schwäche des benutzten RC4 key scheduling Verfahrens, genauer beim Ausnutzen von Schwächen bei der Generierung von Initialisierungsvektoren. Mit genügend „abgehört“ Traffic ist ein Rückschluss auf die verwendeten Schlüssel möglich und das Dekodieren dieser realisierbar.

Der Nachteil von WEP, auf deren Basis bekannte Tools und Entschlüsselungsverfahren im WLAN operieren ist, das zu jeder versendeten Nachricht ein 24 bit großer Initialisierungsvektor (kurz IV) generiert wird. Diese IVs werden benötigt, da der verwendete RC4 Algorithmus darauf basiert, dass jede zu verschickende Nachricht/Fragment mit einem Shared Key (der vom Anwender definierte WEP Key) und eben diesem IV verschlüsselt wird. Der IV wird damit auch zum Entschlüsseln benötigt und muss dem zu übertragenden Paket beigefügt werden. Dieses Vorgehen soll das schnelle berechnen des WEP Keys durch ständige Verwendung bei der Cheffrierung ausschließen. Durch die Verwendung von ständig veränderten Zahlen ist ein schnelles Rückschließen auf den Secret Key ausgeschlossen. Dieser IV wird weiters im Klartext versendet. Das Datenpaket an sich, wird mit dem aus Shared Key und IV erzeugten

Schlüssel kodiert. Ein wechseln der IV innerhalb ihres Wertebereichs macht das Entschlüsseln mit statischen Methoden (z.B. raten aus zwei Nachrichten..) schwerer.

Implementierungsschwächen in diesem Verfahren machen es möglich, gewisse Fragmente einer Nachricht zu erraten und Rückschlüsse auf den Shared Key zu machen. Durch Erraten oder Erfassen von gleichen IV Folgen (Überlauf der IV Initialisierung, also gleich verschlüsselter Nachrichten mit verschiedenen Inhalten) wird nach einer mehr oder weniger langen Zeit ein Rückschließen auf den WEP Key möglich (ca. +1 GB).

D.h. ein Angreifer kann, wenn er lange genug „zuhört“ genügend Datenpakete sammeln um durch gleiche oder schwache IV einen Rückschluss auf den WEP Schlüssel zu erstellen. Das mathematische Verfahren hinter dieser Entschlüsselung ist jedoch weitaus komplexer als angenommen. So muss durch die gezielte Rekonstruktion von verschlüsselten Nachrichten durch die z.B. gleichen IV's, erst ein Dekodieren dieser gelingen um endgültig den WEP Key zu erhalten.

Dieser Prozess ist meist nur mit zweckorientierter und leistungsstarker Hardware möglich. Eine Abhilfe für diese Sicherheitsproblematik schaffen verschiedene Firmwares und Softwareerweiterungen.

So gibt es beispielsweise Tools die den IV nicht mehr benötigen und die Verschlüsselung via WEP anders realisieren. Das Problem hierbei ist jedoch immer die mangelnde Kompatibilität zu anderen Netzwerkkarten oder Netzwerken. Man sollte bei solchen Lösungen Wert auf ein homogenes WLAN legen.

Cisco bietet selbst für ihre Hardware die Erweiterung Aironet an, diese Erweiterung ist jedoch noch nicht standardisiert.

Generell werden mit der Einführung des 802.11i WLAN Standards einige Verbesserungen und Erweiterungen im Bereich WLAN Security spürbar sein.

Es bleibt aber trotzdem zu bemerken, das ein Entschlüsseln einer WLAN Sitzung via WEP theoretisch machbar ist, es ist jedoch fraglich inwiefern diese Sicherheitslücke auch praktisch ausgenutzt wird. Die Berechnungen zur Dekodierung sind sehr zeitaufwendiger Prozesse, die sich vor allem beim Ausnutzen von privaten Netzwerken nicht lohnen würden.

Firmen greifen meist auf teure Erweiterungen der Hard oder Software zurück, welche die Schwächen der WEP Verschlüsselung kompensieren oder diese ganz vernachlässigen lässt.

Es wurden auch bei intensiver Internetrecherche erstaunlich wenige Fakten über tatsächlich erfolgreiche WEP Attacken gefunden. Meist werden nur schwammige oder gänzlich kopierte Aussagen und Analysen präsentiert, die jedoch über ein exaktes Vorgehen nicht informieren.

Selbst die Autoren von Airsnort geben keine Details preis und geben sogar an das ihr Tool nur mit spezieller Hardware funktionstüchtig bleibt und auf sehr viele Faktoren, die in der Praxis nicht auftreten werden, angewiesen sind (IV Einsatz, keine neue Firmware..).

Diese Behauptung der möglichen und „einfachen“ Dekodierung könnte man in weiterer Folge nun auf alle kryptographischen Verfahren projizieren und es spiegelt die Meinung der Autoren, dass diese Sicherheitslücke größer dargestellt wird als sie tatsächlich ist.

3 Verwendete Hardware

Für die unten beschriebenen Experimente wurden folgende Geräte verwendet. Hierbei wechselten wir aber zeitweise auch die Kombinationen Netzwerkkarte/Notebook.

Tabelle 1 HardwareSpezifikationen für die Versuchsanordnungen

Testname	System	Betriebssystem	PCMCIA Karte	Karten Chipsatz
Bob	IBM Thinkpad 600e	Windows 2000 SP4	Netgear MA521	RTL8180
Eve	Dell Inspiron 8200	Auditor security collection (Adaptiertes Knoppix)	Benq AWL 100	Prism II
Alice	Compaq Armada	Windows 2000 SP4	Benq AWL 100	Prism II
ALF	Dell ATX	Windows XP SP 1	Lan (wire)	
AP	Netgear WG 602 v2 Accesspoint			

4 Verwendete Software

Weiters wurde folgende Software für Sniffing und Cracking-Experimente verwendet.

4.1 Sniffing

Kismet [**Kism**]
Netstumbler [**Nets**]

4.2 Cracking

Airsnort [**Airs**]
WEPCrack [**Wepc**]
u.a.

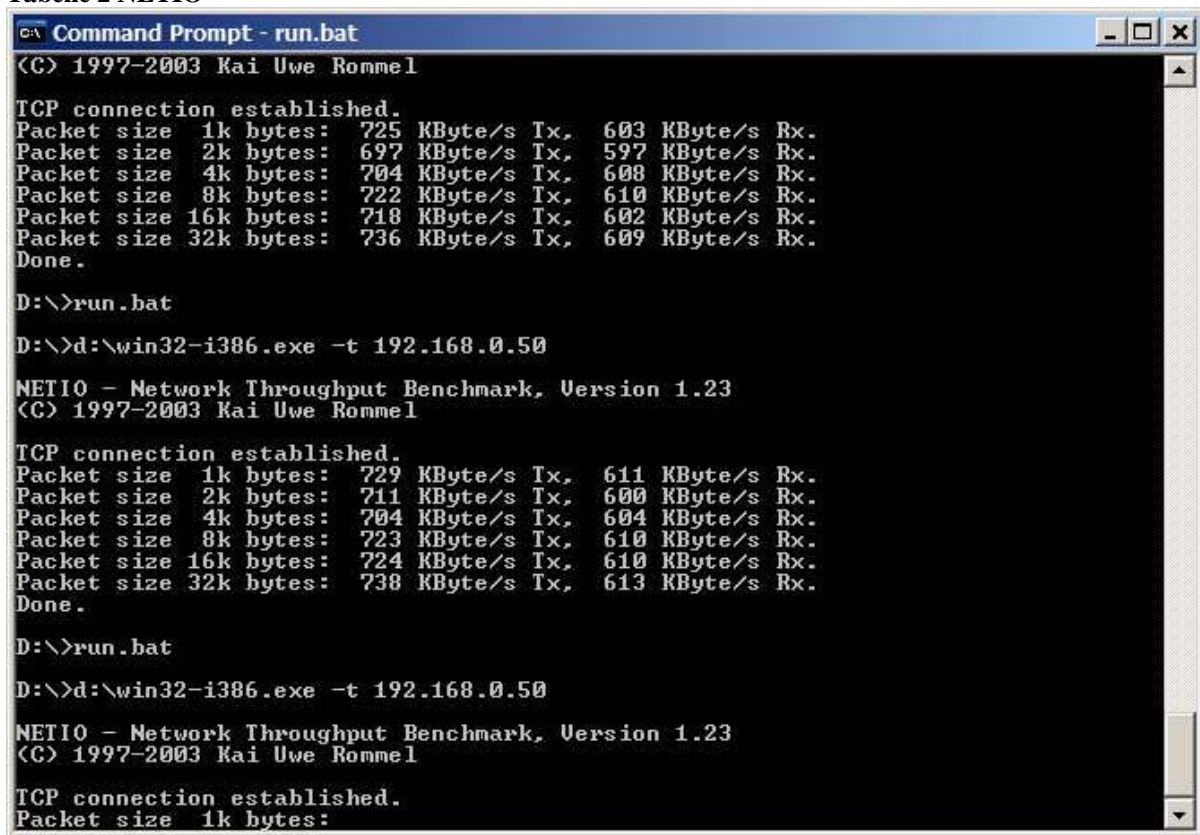
5 Testbedingungen

Die Versuchsanordnung 1 wurde eher aus Interesse für die private Anwendung zusammengesetzt, für den Officebereich hat diese nur bedingt Relevanz. Auf Exp 2 und Exp 3 wurden die meisten Untersuchungen durchgeführt.

Zur Generierung geeigneter Datenmengen wurde auf verschiedene Mittel zurückgegriffen. Zum einen wurden Windows Freigaben benutzt, zwischen denen größere Datenmengen transferiert wurden.

Als zweite Alternative wurde NETIO verwendet, dieses Tool generiert mehrere Packages unterschiedlicher Größe die zwischen zwei Rechnern hin und her transferiert werden und so den benötigten Netzwerkverkehr ohne lästiges Hin- und Herkopieren von Dateien erzeugen.

Tabelle 2 NETIO



```
Command Prompt - run.bat
(C) 1997-2003 Kai Uwe Rommel

TCP connection established.
Packet size 1k bytes: 725 KByte/s Tx, 603 KByte/s Rx.
Packet size 2k bytes: 697 KByte/s Tx, 597 KByte/s Rx.
Packet size 4k bytes: 704 KByte/s Tx, 608 KByte/s Rx.
Packet size 8k bytes: 722 KByte/s Tx, 610 KByte/s Rx.
Packet size 16k bytes: 719 KByte/s Tx, 602 KByte/s Rx.
Packet size 32k bytes: 736 KByte/s Tx, 609 KByte/s Rx.
Done.

D:\>run.bat

D:\>d:\win32-i386.exe -t 192.168.0.50

NETIO - Network Throughput Benchmark, Version 1.23
(C) 1997-2003 Kai Uwe Rommel

TCP connection established.
Packet size 1k bytes: 729 KByte/s Tx, 611 KByte/s Rx.
Packet size 2k bytes: 711 KByte/s Tx, 600 KByte/s Rx.
Packet size 4k bytes: 704 KByte/s Tx, 604 KByte/s Rx.
Packet size 8k bytes: 723 KByte/s Tx, 610 KByte/s Rx.
Packet size 16k bytes: 724 KByte/s Tx, 610 KByte/s Rx.
Packet size 32k bytes: 738 KByte/s Tx, 613 KByte/s Rx.
Done.

D:\>run.bat

D:\>d:\win32-i386.exe -t 192.168.0.50

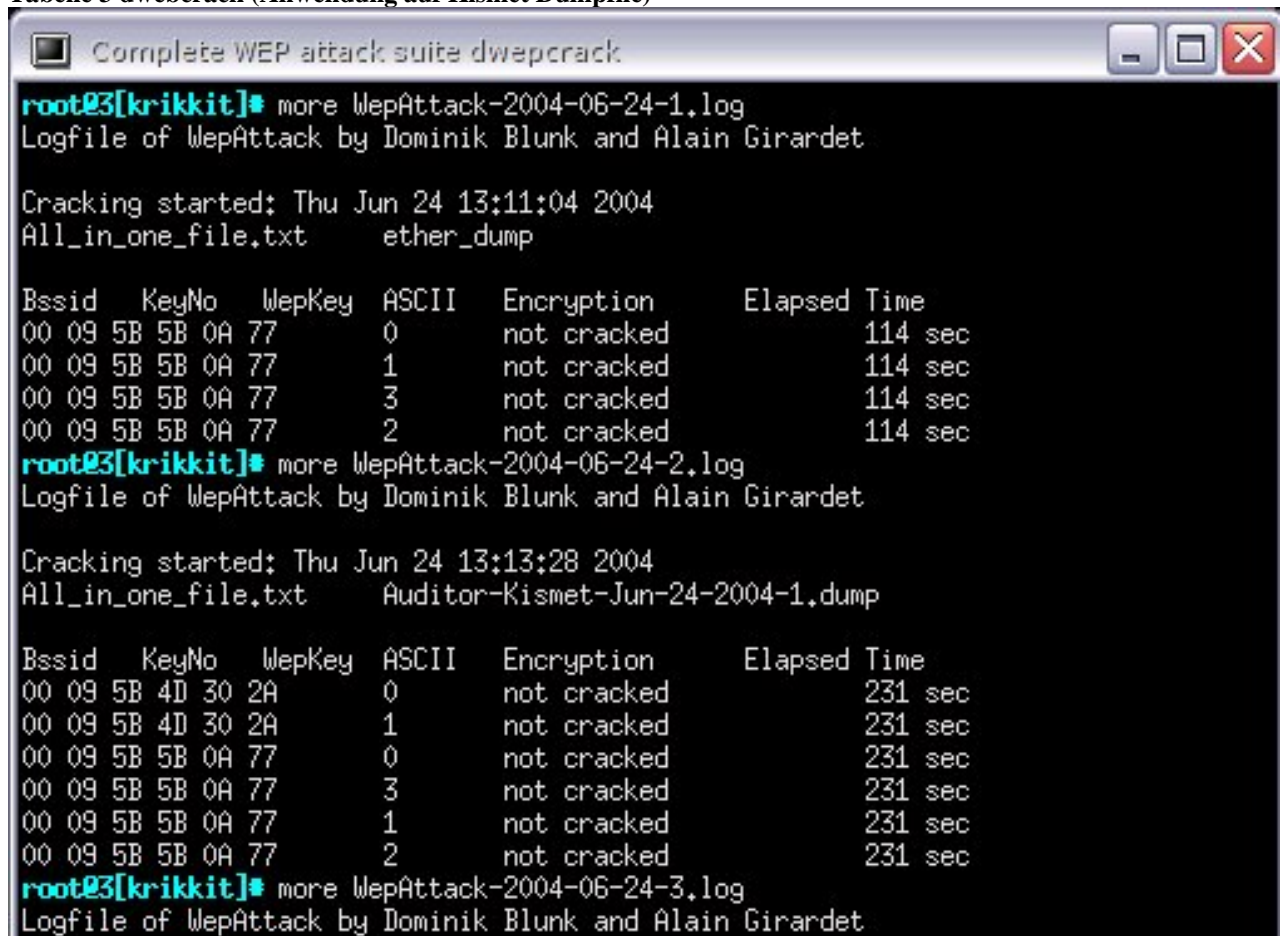
NETIO - Network Throughput Benchmark, Version 1.23
(C) 1997-2003 Kai Uwe Rommel

TCP connection established.
Packet size 1k bytes:
```

Da NETIO nur eine begrenzte Anzahl von Paketes generiert, wurde dieser mittels eines Batchfiles (siehe Anhang) immer wieder aufgerufen. So war es auch möglich Versuchsanordnungen während längerer Zeit, auch unbeaufsichtigt, ablaufen zu lassen.

Zum Berechnen des Key aus den weak Packages verwendeten wir dwebcrack, der ca 3000 bis 5000 dieser Packages benötigt.

Tabelle 3 dwebrack (Anwendung auf Kismet Dumpfile)



```

Complete WEP attack suite dwebrack
root@3[krikkit]# more WepAttack-2004-06-24-1.log
Logfile of WepAttack by Dominik Blunk and Alain Girardet

Cracking started: Thu Jun 24 13:11:04 2004
All_in_one_file.txt      ether_dump

Bssid  KeyNo  WepKey  ASCII  Encryption  Elapsed Time
00 09 5B 5B 0A 77    0    not cracked    114 sec
00 09 5B 5B 0A 77    1    not cracked    114 sec
00 09 5B 5B 0A 77    3    not cracked    114 sec
00 09 5B 5B 0A 77    2    not cracked    114 sec
root@3[krikkit]# more WepAttack-2004-06-24-2.log
Logfile of WepAttack by Dominik Blunk and Alain Girardet

Cracking started: Thu Jun 24 13:13:28 2004
All_in_one_file.txt      Auditor-Kismet-Jun-24-2004-1.dump

Bssid  KeyNo  WepKey  ASCII  Encryption  Elapsed Time
00 09 5B 4D 30 2A    0    not cracked    231 sec
00 09 5B 4D 30 2A    1    not cracked    231 sec
00 09 5B 5B 0A 77    0    not cracked    231 sec
00 09 5B 5B 0A 77    3    not cracked    231 sec
00 09 5B 5B 0A 77    1    not cracked    231 sec
00 09 5B 5B 0A 77    2    not cracked    231 sec
root@3[krikkit]# more WepAttack-2004-06-24-3.log
Logfile of WepAttack by Dominik Blunk and Alain Girardet

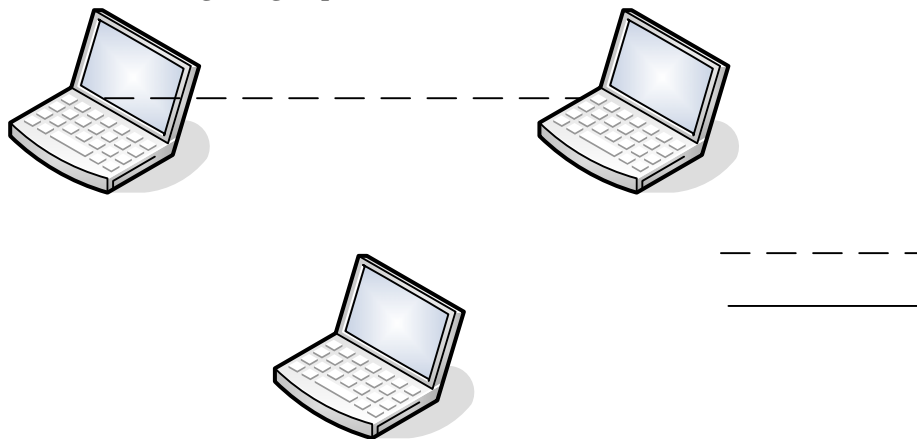
```

Um nicht zu hohe Ansprüche an die Datentransvermenge zu stellen, habe wir für die Web Verschlüsselung nur einen 64 bit Key verwendet, mit einem Hexwert von „AAAAAAAA-AA“.

Aus persönlichen Interesse wurde noch ein brute force Attack angewandt, in Form einer Dictionary Attack mit 9 Millionen Einträgen.

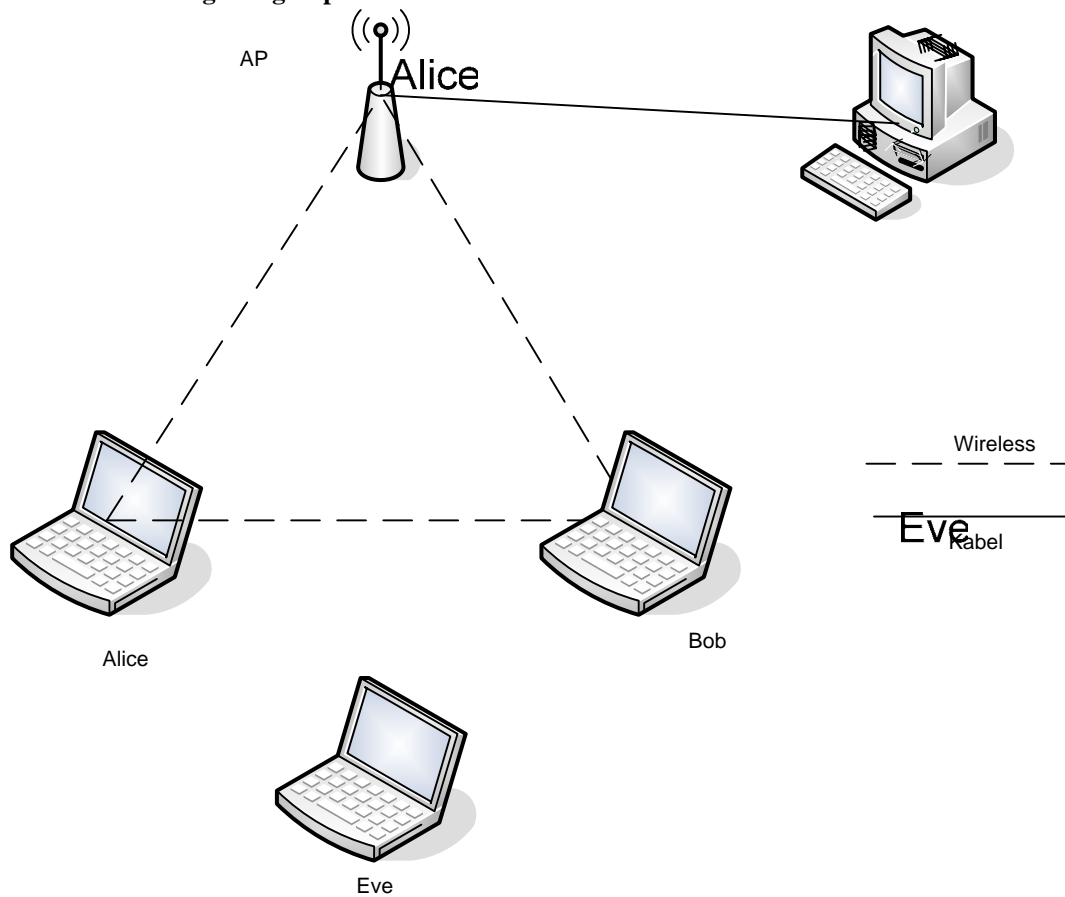
5.1 Testumgebung Exp1

Tabelle 4 Testumgebung Exp1



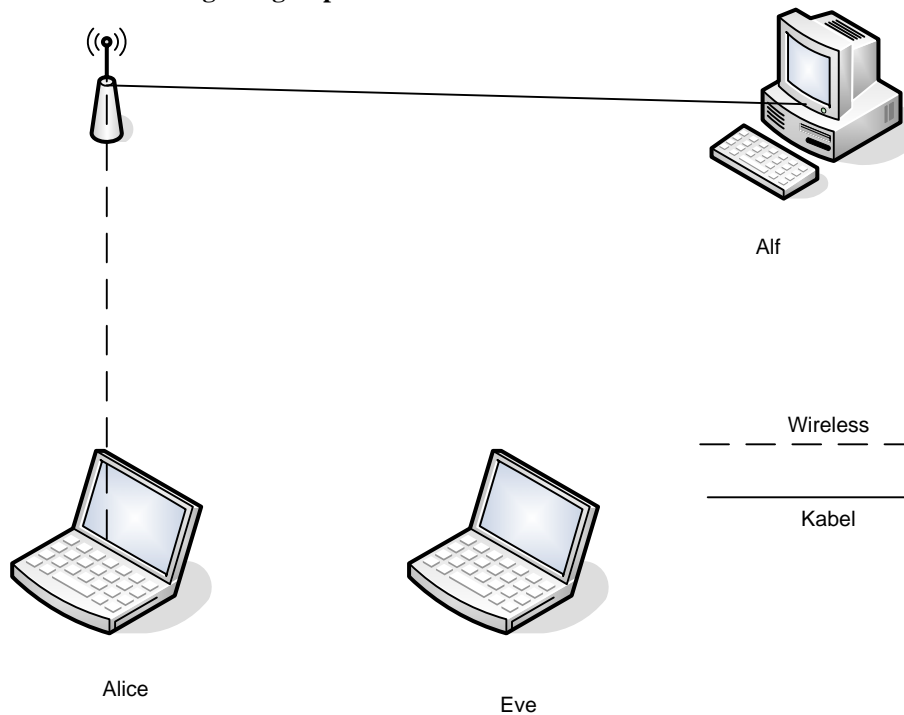
5.2 Testumgebung Exp2

Tabelle 5 Testumgebung Exp2



5.3 Testumgebung Exp3

Tabelle 6 Testumgebung Exp3



6 Testergebnisse

6.1 Zu Exp 1

Eigentlich war dieses Experiment nur zur Einstimmung gedacht. Zum einen zum Testen der verschiedenen Konfigurationen beziehungsweise um einige Erfahrungen mit WEP zu machen.

Nach relativ kurzer Zeit zeigte sich jedoch, dass Ad hoc Netze alles andere als einfach zu Erstellen sind.

Verbindungen ohne WEB Verschlüsselung konnten ohne größere Probleme etabliert werden, im Gegensatz dazu war eine Verbindung mit WEP eher ein Glücksspiel. Es konnten zwar teilweise Verbindungen aufgebaut werden, diese waren aber immer instabil und wenn überhaupt nur über einen begrenzten Zeitraum aktiv.

Nach Recherchen im Netz zeigte sich sehr schnell, dass dies durchaus üblich ist und maximal mit Karten des gleichen Herstellers bessere Ergebnisse erzielt werden konnten. Jedoch war auch dies keine Garantie für eine korrekte Verbindung.

Abschließend bleibt hier zu sagen, dass man, wenn ein verschlüsseltes Ad-hoc WLAN benötigt wird, in jedem Fall vor dem Kauf gründlich recherchieren sollte welcher Hersteller dieses Feature wirklich in seinen Geräten realisiert hat.

6.2 Zu EXP 2 und Exp 3

Um mögliche Einflüsse durch verschiedene Geräteanordnungen festzustellen haben wir den Standardangriff auf zwei verschiedene Anordnungen (Exp1 und Exp2) erstellt, es zeigte sich

jedoch, das dies keinerlei (messbaren) Einfluss hat und somit haben wir diese beiden Versuchsreihen zusammengefasst.

In dieser Versuchsanordnung haben wir unter anderem auch ausgetestet ob die Art der transferierten Files Einfluss auf die Anzahl der Weak Packages hat, weiter wurden auch versucht mittels häufiger Anmeldeversuche diese Anzahl zu erhöhen. Wir konnten dafür aber nur einen negativen Befund feststellen, beides hatte keinen merklichen Einfluss auf das Verhältnis von transferierten Packages zu Weak Packages.

Grundsätzlich sind wir bei unsern Versuchen davon ausgegangen, das innerhalb eines Volumens von 1 bis 5 GB sich ein 64 bit Schlüssel brechen lassen würde.

Jedoch zeigte sich sehr schnell, dass das Verhältnis von transferierten Packages zu Weak Packages sich anders als erwartet entwickelte. Bei einem Volumen von 5 GB konnten wir auf ca 50 weak's verweisen. Bei geschätzten 3000 bis 5000 geforderten die für ein Brechen eines 64 bit Keys mittels dwebcrack benötigt werden, zeigte sich sehr schnell die Komplexität der Aufgabenstellung.

Dementsprechend haben wird das Transfervolumen auf 50 GB erhöht, das bei Vollast bei unserer Konfiguration einen Zeitrahmen von 24 Stunden benötigte. Nach dem sich auch aus dieser Konstellation nur 536 Weak Packages ergaben, kamen wir zu folgenden Erkenntnissen:

- Das Cracken eines WEP Keys ist bei weitem nicht so einfach wie diverse Quellen im Internet vermitteln.
- Viele dieser Quellen beziehen sich auf sehr alte Hardware aus den Anfangszeiten von WLAN. Aktuelle Geräte produzieren schlicht und einfach nicht mehr so viele Weak Packages.
- Im Privatbereich kann WLAN bei angemessener Konfiguration und nicht datenintensiver Nutzung (z.B. lediglich Surftraffic) als sehr sicher betrachtet werden. Der WEP Schlüssel sollte dennoch von Zeit zu Zeit geändert werden.
- Es wird wesentlich mehr Datenverkehr benötigt als beispielsweise von den Entwicklern von Airsnort angegeben.
- Viele der oben erwähnten Cracking/Sniffing- Tools wurden seit geraumer Zeit nicht mehr weiterentwickelt funktionieren deshalb mit aktuellen Netzen nicht mehr einwandfrei.

Zu ähnlichem Urteil gelangte auch schon jemand auf den Seiten des Buchverlages O'Reilly siehe: [Orei]

6.2.1 Fazit:

Durch Upgrades der Firmware der Wlan Karten konnten die Hersteller erreichen, dass sich das Verhältnis von transferierten Packages zu weak Packages verbesserte. Dementsprechend wird wohl ein höherer Aufwand notwendig sein, um den Key zu brechen.

Unserer Einschätzung nach ist ein Transfervolumen von 300 bis 500 GB notwendig um in die Nähe eines Erfolgs zu kommen. Was in unserer Versuchsanordnung nicht getestet werden könnte, ist wie sich die Anzahl der aufgefingenen Weak Packages ändert wenn mehrere Clients sich in einem Wlan befinden bzw. sich oft an- und abmelden.

6.3 Zu Dictionary Attack

Eigentlich ist diese nur als Zugabe zur vorhandenen Versuchsanordnung gedacht. Dementsprechend wird das Ergebnis auch nur kurz abgefasst.

Dieser Angriff wurde auf das bereits vorhandene Dumpfile von Kismet angewandt. Nach ca 1 Stunde (abhängig von Rechnerleistung) war das gesamte Verzeichnis durchgelaufen. In dem Fall auch mit negativen Ergebnis, in dem Fall aber wegen des etwas ungünstig (oder auch gut-) gewählten Key.

Es zeigt sich jedoch auch, das mit sehr geringen Aufwand bei einem falsch gewählten Key („password“, ...) sehr schnell ein positiver Ergebnis erzielt werden kann.

7 Risikoeinschätzung

Mit derzeit vorhandenen Mitteln ist ein Angriff auf die WEP Verschlüsselung mittels Cracken nicht oder nur bedingt möglich.

Im Homeoffice Bereich würde es Monate oder Jahre dauern bis man an Volumen von 500 GB mitgeniff hat und in dieser Zeit ist es auch hoffentlich für einen Privatanwender möglich den Key zu ändern.

Für Unternehmen oder andere Heavy User sieht es schon anders aus. Bei optimalen Voraussetzungen kann(!) das geforderte Limit von 500GB Traffic in 3 bis 8 Wochen erzielt werden. Dieser Zeitraum ist schon eher ein realistischer Rahmen. Aber auch hier muss ergänzt werden, dass heutige Key üblicherweise 128 bit haben und weiters sollten oder haben größere Firmen meist zusätzliche Schutzmaßnahmen (Vpn, ..) um diesen geringen Risiko entgegenzuwirken. Auch deckte unsere Testreihe, wie bereits erwähnt nicht das Szenario ab, dass sich mehrere Clients in einem Wlan befinden bzw. anmelden, deshalb können über die Beziehung Zahl der Clients / (Un-)Sicherheit des Netzes keine Aussagen getroffen werden.

So sind als Risikogruppe noch Klein und Mittelbetriebe (v.a. Startups) zu nennen, die anfangs vollständig auf ein konventionelles LAN verzichten und sämtlichen Netzwerkverkehr über WLAN abwickeln. Z.B. Synchronisation oder Bewegen von sehr großen Dateien (beispielsweise in Graphikbüros u.ä.). Nach einiger Zeit wird in solchen Fällen auch aus rein ergonomischen Gründen ein LAN installiert werden (müssen), und so sollte sich das Sicherheitsproblem auch lösen. Unternehmen in der Anfangsphase können jedoch generell als Risikogruppe für Sicherheitsprobleme angesehen werden.

Nichts desto trotz soll man bei allen Wlan Anwendungen Vorsicht walten lassen und im Fall des Falles den Griff zum Netzwirkabel vorziehen. ☺

8 Abbildungsverzeichnis

Tabelle 1 HardwareSpezifikationen für die Versuchsanordnungen.....	7
Tabelle 2 NETIO.....	8
Tabelle 3 dwebcrack (Anwendung auf Kismet Dumpfile)	9
Tabelle 4 Testumgebung Exp1	10
Tabelle 5 Testumgebung Exp2.....	10
Tabelle 6 Testumgebung Exp3.....	11

9 Referenzen

[Nets] <http://www.stumbler.net>, Zugriff 6/2004

[Airs] <http://airsnort.shmoo.com/>, Zugriff 6/2004

[Kism] <http://www.kismetwireless.net>, Zugriff 6/2004

[Wepc] <http://sourceforge.net/projects/wepcrack>, Zugriff 6/2004

[Orei] http://www.oreillynet.com/cs/user/view/cs_msg/26023, Zugriff 24.6.2004