Warum ist WEP unsicher?

© by Thomas Hackner, am 01.07.2006
http://www.defense.at
http://home.pages.at/inzider

Grundlagen

WEP heißt ausgeschrieben “Wired Equivalent Privacy” und wurde 1999 im Standard IEEE 802.11 implementiert. Dabei sollte eine Sicherheit in Funknetzwerken geschaffen werden, die der von klassischen Kabelnetzwerk gleicht. Obwohl man damals schon um einige Implementierungsfehler von WEP wusste, wurde der Standard trotdzem durchgesetzt und sofort von vielen Hardwareherstellern übernommen. Mit zunehmender Verbreitung wurde dieses Feld auch für Kryptografen und Hacker interessant und so kam es, dass schon 2001 WEP als definitiv unsicher und geknackt deklariert wurde. Die Hardware war jedoch schon verbreitet und fertige Implementierungen auf der Hardware fehlten. Erst dann folgten die Nachfolger WPA und IEEE 802.11i (WPA2), die das Genre nun endlich auf einen der Zeit angemessenen Sicherheitsstandard brachten.

Nun aber genauer zu WEP. Grundsätzlich versuchte man 3 Bereich abzudecken:
- Authentication (Authentifizierung)
- Privacy (Vertraulichkeit)
- Integrity (Integritätssicherung)

Welche Fehler man aber jetzt genau mit WEP begangen hat, wollen wir uns nun näher ansehen.

Authentication

Bei WEP gibt es die zwei Betriebsarten “Open Mode” und “WEP Authentication”. Im *Open Mode* sendet der Client dem Server lediglich einen Authentication request und erhält sofort einen Authentication response zurück. Es findet keinerlei nähere Überprüfung statt.

Bei der WEP Authentication hingegen handelt es sich um ein CHAP-Verfahren. Der AP sendet einen 128-Bit Zufallswert an den Client, dieser verschlüsselt den Wert mit einem privaten Schlüssel und sendet den erhaltenen Wert an den AP zurück. Nach kurzem Vergleich wird entschieden, ob der Client Zugriff zum WLAN hat oder nicht.

Wir haben hier den Fall, dass sich der Client gegenüber dem Access Point (AP) authentifiziert, jedoch umgekehrt ist dies nicht der fall. Das ermöglicht es einem Angreifer einen AP zu faken (Rogue AP) und somit an wichtige Informationen über den Client zu kommen bzw. eine MitM Attacke auszuführen, sollte sicher dieser bei dem gefälschten AP anmelden.

Zudem liefert der Client dem Angreifer die Möglichkeit auf eine Known-Plaintext-Attacke. Da WEP für die Authentifizierung und die Verschlüsselung ein und denselben Schlüssel verwendet hätte dies jedoch die Kompromittierung des gesamten Netzwerkverkehrs zu Folge.

Tipp: Wenn die Möglichkeit auf eine andere Verschlüsselung als WEP nicht gegeben ist - “Open Authentication!! (um Plaintext Attacken vorzubeugen) + WEP Verschlüsselung + ...” aktivieren.

Privacy

Zur Erzeugung des Schlüssels wird der RC4 Algorithmus verwendet. Als Input bekommt dieser einen 24 Bit langen IV (Initialisierungsvektor) und einen von 4 fixen WEP-Keys (40 / 104 Bit).

Da fixe Keys und ihre weitere Verwendung immer eine schlechte Idee ist, fügte man beim RC4-Input noch den IV hinzu, der sich bei jedem Frame um eins inkrmentiert.

Integrity

Zur Integritätssicherung verwendet WEP eine 4 Byte Prüfsumme. Diese wird vor der Verschlüsselung an die Daten angehängt.

WEP enthält außerdem kein Key Management. Es gibt grundsätzlich einen Default Key, den jeder besitzt und evt. Auch einen Key Mapping Key. Dieser ist bei jedem Client anders und der AP verwaltet diese intern in einer Tabelle, in der die MAC-Adresse als Schlüsselelement gilt. Ist kein Key-Mapping Key vorhanden wird auf den Default Key zurück gegriffen.

Schließlich sieht eine übertragene Nachricht folgendermaßen aus:

Welche Fehler hat nun WEP?

Grundsätzlich sind folgende Punkte für ein sicheres WLAN notwendig

- Authentifizierung
- Zugangskontrolle
- Replay-Schutz
- Integritätssicherung
- Vertraulichkeit
- Sicherung der Keys

Leider stellt WEP in keinem dieser Punkte wirkliche Sicherheiten zur Verfügung. Sehen wir und dies aber ein wenig genauer an.

Authentifizierung

Eine vernünftige Authentifizierung setzt voraus, dass sowohl AP als auch Client sich gegenseitig zu erkennen geben. Dabei sollten jedoch die Schlüssel zur Authentifizierung getrennt von denen der Verschlüsselung sein. Außerdem sollte darauf geachtet werden, dass eine Reauthentifizierung schnell, aber trotzdem nicht spoofbar vonstatten geht.

WEP erfüllt leider keinen einzigen dieser Punkte. Es werden gleiche Schlüssel für alle Operationen verwendet. Außerdem mus sich der AP, wie oben schon erwähnt, nicht authenfizieren und stellt somit ein weiteres Sicherheitsrisiko dar. Eine schnelle Reauthentifizierung wäre z.B. per Tokens möglich, ist aber ebenfalls nicht implementiert.

Ein Beispielangriff würde so aussehen, dass der Angreifer bei einer legitimen Authentifizierung Challenge-Wert, IV, Key-ID und auch den Response mitlesen kann. Dadurch, dass der Challenge-Wert nur mit XOR verschlüsselt wird, kann sich der Angreifer den Random Wert aus dem RC4-Cipher errechnen. Nun hat er genügend Informationen um sich auch anzumelden. Der AP sendet ihm einen Challenge-Wert zu, der Angreifer verschlüsselt diesen mit dem erhaltenen Random-Wert und sendet ein Paket mit bekannten IV, Key-ID und verschlüsselter Challenge zurück. Für den AP sieht alles legitim aus und somit lässt er ihn passieren.

=> keine Sicherheit

Zugriffskontrolle

Bezüglich Zugriffskontrolle gibt es keine genauen Spezifikationen im Standard. Meist wird diese per MAC-Adressfilter umgesetzt. Da MAC-Adressen Spoofing kein weiteres Problem darstellt ist dieser Punkt widerlegt.

=> keine Sicherheit

Replay Schutz

WEP überprüft AP-seitig die Nachrichten nicht weiter. Weder der Wert des IV's (ob der Wert des letzten Pakets höher oder niedriger war) noch andere Mechanismen verhindern, dass ein Angreifer von einem Client schon gesendete Daten wieder versendet. Zwar kann der Angreifer die Daten nicht direkt lesen, aber sie werden vom AP akzeptiert. Oft kann man durch Standarddialog im Netzwerk schon erraten welche Pakete gesendet werden und so sind Login-Prozesse leicht zu attackieren.

=> keine Sicherheit

Integritätssicherung

Zur Sicherung der Richtigkeit der Nachrichten wird an das Paket der ICV angehängt. Dieser wird jedoch durch eine lineare Funktion berechnet. D.h. mann kann voraussagen welche Bits sicher im ICV ändern, wenn ich im Datenteil ein Bit ändere und somit die Daten gezielt manipulieren Die Verschlüsselung für Daten und ICV wird mit dem exakt gleichen Schlüssel und mit XOR durchgeführt, d.h. es ändert sich auch nichts an der Bitverteilung im Paket.

Somit kann WEP keine Nachrichtenintegrität sicherstellen.

=> keine Sicherheit

Vertraulichkeit

Bisher wurde WEP zwar in allen Punkten bezwungen, jedoch direkten Zugriff auf den Plaintext hatten wir bis jetzt noch nicht. Grundsätzliche Fehler bei RC4 in WEP sind die

- IV Wiederverwendung
- schwache Keys für RC4
- direkte Schlüsselattacke

Zwar wird der IV jedes mal um eins erhöht, damit die gleiche Nachricht jedes mal anders verschlüsselt wird, jedoch ist der IV nur 24 Bit lang. Bei einer Station in einem WLAN in einem 802.11b Netzwerk würde es maximal 7 Stunden dauern, bis sich der erste IV wiederholt. Hat ein Angreifer zwei Nachrichten mit gleichem IV, so kann er mit ein wenig Glück gegenseitig den Aufbau der Pakete erraten (festegelte Header in zb IP-Pakete usw) und kann somit den Random zu dem IV berechnen. Somit ist es dem Angreifer möglich neue Pakete ohne Kenntnis des WEP-Keys zu generieren.

RC4 hat weiterhin das Problem, dass die ersten Zufallsbits nur von wenigen Key-Bits erzeugt werden. In WEP hat man leider verabsäumt die Empfehlung von RSA zu beachten. Hier wurde vorgeschlagen die ersten 256 Byte Zufallsfolge zu verwerfen. Durch Wissen des normalen Paketaufbaus kann bietet man Angreifern so die Chance die ersten Key-Bits attackieren.

Durch die Inkrementierung des IVs und ohne die Verwendung des IVs in Kombination mit dem Schlüssel unter näherer Begutachtung und Kontrolle werden automatisch schwache RC4-Keys erzeugt. Durch das Versenden des IVs im Klartext ist es nun möglich bei einem schwachen Random-Key Rückschlüsse zu ziehen. Es werden ca. 60 IV Werte benötigt, aum auf das erste Schlüsselbyte schließen zu können. Durch die Struktur von RC4 ist den anschließend auch möglich bytweise die restlichen Bytes unter Zuhilfenahme weiterer schwacher IVs zu berechnen. Das Verlängern der Schlüssel von 40 auf 104 Bit stellt dabei lediglich einen linearen Aufwandsanstieg um den Faktor 2,5 dar. Wir wir sehen bietet WEP auch in dieser Hinsicht keine weitere Sicherheit.

Mit Programmen wie kismet, wepcrack, airsnort, usw lässt sich WEP sehr einfach aushebeln und man hat innerhabl weniger Minuten Zugang zu einem vermeintlich gesicherten WLAN. Wer sein WLAN halbwegs sicher wissen will, dem bleibt also nur der Umstieg auf WPA bzw. wenn möglich WPA2.