Sicherheit in Wireless LANs

Bis vor kurzem galten Wireless LANs als sicher in Bezug auf unauthorsierten Zugriff und Abhören, vorausgesetzt, die standardmässig implementierten Features wurden fachgerecht konfiguriert. Obwohl schon länger bekannt war, dass es prinzipiell möglich ist, die für die Sicherheit relevanten Parameter aus den im Funk übertragenen Paketen zu ermitteln, standen die dazu notwendigen Mittel („Wireless Sniffer“) und die Kenntnis, wie aus den abgefangenen Paketen die relevanten Parameter extrahiert werden, nicht der Allgemeinheit zur Verfügung. Dies hat sich grundlegend verändert. Sniffer-Software für PCs mit Wireless LAN Karte ist kommerziell erhältlich, und die Verfahren zur Paket-Analyse sind in diversen Veröffentlichungen zugänglich.
Im folgenden werden die einzelnen Sicherheits-Features und ihre Schwächen, sowie Lösungen für eine bessere Sicherheit beschrieben.

WEP (Wired Equivalent Privacy):
WEP stellt ein Verfahren zur Verschlüsselung der im Funk übertragenen Datenpakete dar und wird im Wireless LAN Standard IEEE 802.11 als optionales Feature definiert. Je nach verwendeter Schlüssellänge spricht man von WEP64 oder WEP128. Dies entspricht Schlüssellängen von 64 bzw. 128 Bit, wobei jeweils 24 Bit den sogenannten Initialisierungsvektor darstellen (eine von der Hardware von Datenpaket zu Datenpaket veränderte zufällige Zahl) und der Rest (40 bzw. 104 Bit) vom Anwender definiert wird. Eine Kommunikation zwischen Client und Access Point kann nur stattfinden, wenn auf beiden Seiten der gleiche Schlüssel definiert wurde. Sind die Schlüssel nicht identisch, wird keine Verbindung aufgebaut.
Strenggenommen ist nur WEP64 im Standard definiert, das heute allgemein übliche WEP128 stellt einen erweiterten „Industrie-Standard“ dar.

Network Name:
Der Network Name wird ebenfalls im Wireless LAN Standard IEEE 802.11 definiert (dort **SSID**, System Set Identifier genannt) und diente ursprünglich der logischen Strukturierung von Funknetzen. Da sich nur ein Client mit passendem Network Name an einem Access Point anmelden kann, wird der Network Name oft auch unter dem Aspekt der Zugangskontrolle gesehen. Voraussetzung für diese Funktionalität ist jedoch das (nicht Standard-konforme) Abschalten der Funktion „Broadcast SSID“ im Access Point. Ist diese Funktion abgeschaltet, kann ein Datenverkehr zwischen Client und Access Point nur stattfinden, wenn beide Seiten den gleichen Network Name verwenden. Ist diese Funktion nicht abgeschaltet, kann sich jeder Client, dessen Network Name auf „ANY“ gesetzt wurde, am Access Point anmelden, egal welcher Network Name im Access Point gesetzt wurde.

ACL (Access Control List):
In der Konfiguration der Access Points können die MAC-Adressen der für eine Anmeldung freigegebenen Clients in einer Liste eingegeben werden. Versucht ein Client mit einer fremden MAC-Adresse sich anzumelden, wird er abgewiesen. ACL

ist nicht in einem Standard definiert, diese Funktionalität hat sich jedoch bereits in verkabelten Strukturen als „Industrie Standard“ etabliert und wurde in die Wireless LAN Welt übernommen.

Fazit:
Solange die Parameter WEP und Network Name sowie der ACL-Eintrag (MAC-Adresse des Clients) nicht explizit öffentlich bekannt sind, ist jedes korrekt konfigurierte Wireless LAN absolut sicher, da bereits die Unkenntnis eines der drei Parameter den Aufbau einer Kommunikation zwischen Client und Access Point und damit auch den Zugang zum Netzwerk verhindert.

Sicherheitslücken:
Aus den über Funk übertragenen Datenpaketen lassen sich die oben beschriebenen drei Parameter prinzipiell ermitteln. So werden die MAC-Adressen der aktiven Clients sowie der Network Name unverschlüsselt im Funk übertragen. Aus einer (allerdings grossen) Anzahl an Datenpaketen kann darüber hinaus auch der WEP-Schlüssel durch einen Algorithmus rekonstruiert werden, so dass alle für eine Kommunikation notwendigen Parameter in Erfahrung gebracht werden können, sobald ein physischer Zugang zur Funkzelle gegeben ist.

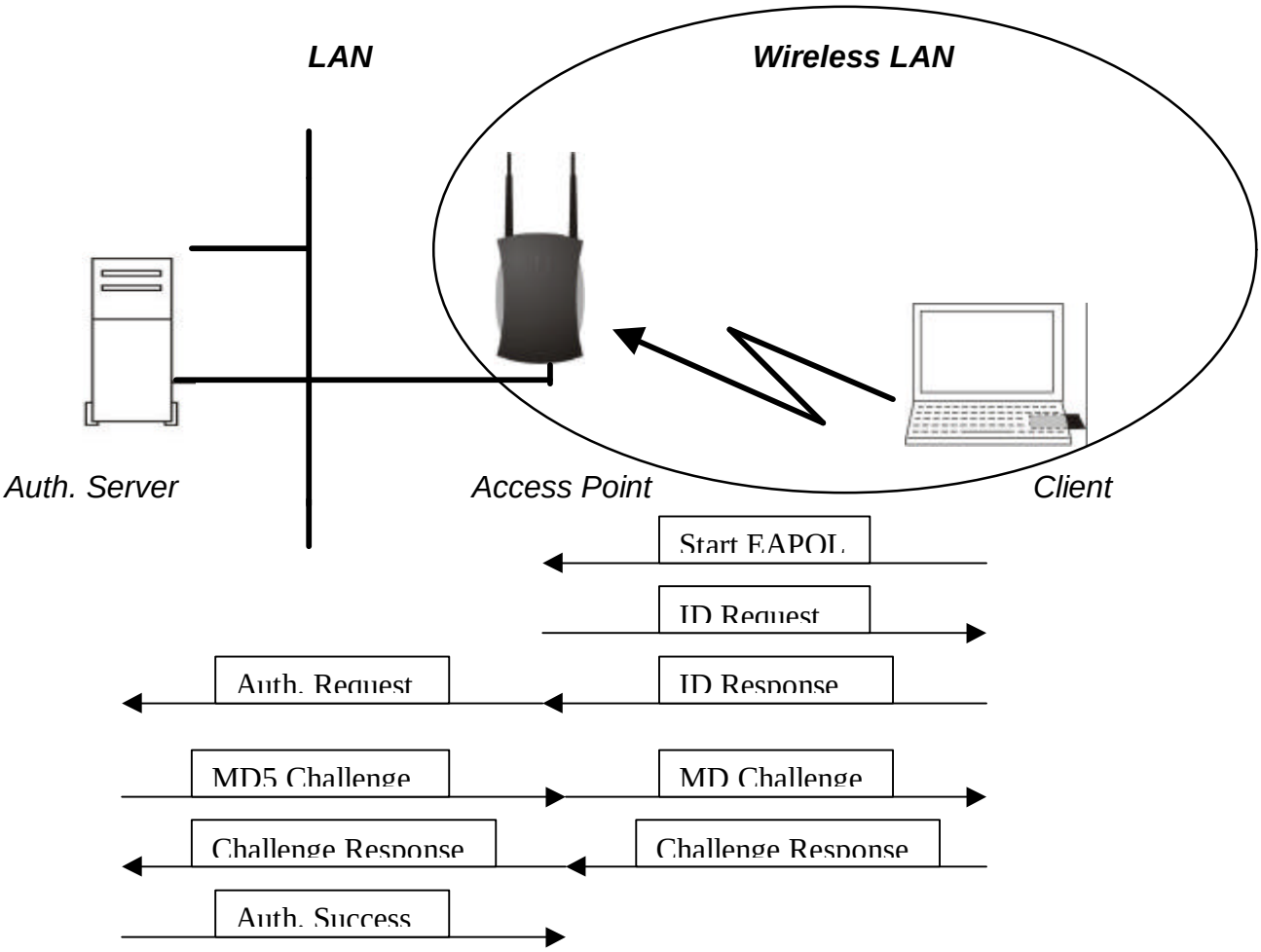
Die Analyse der Datenpakete kann mittels frei erhältlicher Software erfolgen, der Algorithmus zur Rekonstruktion des WEP-Schlüssels ist ebenfalls öffentlich bekannt. Es muss allerdings darauf hingewiesen werden, dass einschlägige Fachkenntnisse für ein erfolgreiches Abhören und Entschlüsseln notwendig sind. Ein Abhören und die Analyse der Daten „per Mausklick“ ist nicht möglich.

Problemlösung:
Diese seit Mitte letzten Jahres bekannten Sicherheitslücken in Wireless LANs können prinzipiell dadurch beseitigt werden, dass Verfahren eingesetzt werden, die einerseits die Rekonstruktion der Sicherheitsrelevanten Parameter aus dem Funkverkehr verhindern oder zumindest gravierend erschweren, und andererseits eine sichere Zugangskontrolle zum Netzwerk bieten.

Um aus dem Funkverkehr abgehörte Datenpakete erfolgreich entschlüsseln zu können, wird prinzipiell immer eine grosse Anzahl an Paketen benötigt. Die erforderliche Datenmenge hängt von der „Stärke“ des eingesetzten Verschlüsselungserfahrens ab. Die Sicherheit kann deshalb einerseits durch Verbesserungen im Verschlüsselungsverfahren selbst erreicht werden, oder dadurch, dass man die zur Entschlüsselung notwendige Datenmenge gar nicht „anbietet“. Letzteres kann durch entsprechend schnelles dynamisches Wechseln des Schlüssels erreicht werden.

„Weak Key Avoidance“
Bestimmte Werte für die unverschlüsselt über den Funk übertragenen Initialisierungsvektoren des WEP-Keys erlauben eine besonders einfache Rekonstruktion der Verschlüsselung. Dies sind die sogenannten „weak keys“. Aktuelle Wireless LAN Technologien sollten deshalb das Feature „Weak Key Avoidance“ oder auch **„WEPplus“** genannt implementieren, das sicherstellt, dass die schwachen Initialisierungsvektoren nicht verwendet werden.

IEEE 802.1x:
Der Standard 802.1x definiert ein vom Funk unabhängiges Authentifizierungsverfahren auf Port-Ebene. Dabei wird die Authentifizierung eines Users (nicht einer Client-Hardware) für den Zugang zum Netzwerk über die Einbindung eines Authentifizierungsservers (wie **RADIUS, Kerberos** oder auch propritäre Systeme) realisiert. Für die Verwendung von 802.1x in Wireless LANs bedeutet dies, dass der User eines Funkclients erst dann mit einem Access Point kommunizieren kann und Zugang zum Netzwerk erhält, wenn der Access Point diesen User an einem Authentifizierungsserver im Netzwerk verifiziert hat. Voraussetztung für das Verfahren ist, dass sowohl das Betriebssystem des Clients als auch der Authentifizierungsserver das in 802.1x definierte Protokoll **EAP** (Extensive Authentication Protocol) unterstützen. Von Seiten des Clients unterstützt derzeit nur das Betriebssystem WinXP dieses Protokoll. Für andere Betriebsysteme gibt es sogenannte „Supplicant"- Software, die EAP ermöglichen. Die folgende Darstellung erläutert den Authentifizierungsablauf.



1. Der Funkclient versucht, sich standardkonform (802.11b) am Access Point anzumelden.
   Anschliessend wird über das Protokoll **EAPOL** (EAP over LAN) die Authentifizierungssequenz gestartet.

2. Der Access Point verlangt eine Identifizierung des Users.

3. Der Client sendet diese Identifizierung (z.B.“UserName/Password“ nach Eingabe über das Betriebsystem des Clients) an den Access Point, der dies an einen ihm bekannten Authenifizierungsserver weiterleitet.

4. Der Athentifizierungsserver prüft, ob der User eingetragen ist, und sendet über den Access Point ein Datenpaket mit einer Zufallszahl an den Client.

5. Der Client verschlüsselt das empfangene Datenpaket mit seinem Password und schickt es über den Access Point zurück an den Authentifizierungsserver.

6. Wenn das vom Client zurückgesendete (verschlüsselte) Datenpaket mit dem vom Authenifizierungsserver selbst (mit dem ihm bekannten) Password verschlüsselten Datenpaket identisch ist, d.h. die Passwords übereinstimmen,

sendet der Authentifizierungsserver an den Access Point eine Success-Meldung. Der Access Point gibt daraufhin den Datenverkehr vom Client zum Netzwerk frei.

Anstelle des oben beschriebenen Verfahrens **EAP-MD5** kann auch das auf Zertifikaten basierende Verfahren **EAP-TLS** eingestzt werden.

Ausser dem Protokoll EAP zur Authentifizierung sieht der Standard **802.1x** auch ein Protokoll zum Austausch beliebiger Schlüssel (**Key Exchange**) vor. Dadurch wird die dynamische Schlüsselvergabe (WEP) zwischen Client und Access Point unter Verwendung des gleichen Standards wie für die Authentifizierung ermöglicht. Für die Implementierung der dynamischen WEP-Key Vergabe macht der Standard jedoch keinerlei Vorgaben. Dies bleibt allein den Herstellern überlassen.

802.11i:
Der Standard **802.11i** , der schon seit geraumer Zeit von der **TaskGroup i (TGi)** des IEEE bearbeitet wird, soll sowohl das Problem der per se schwachen Verschlüsselung in 802.11 beseitigen, als auch ein Verfahren für den dynamischen Schlüsseltausch zwischen Access Point und Clients definieren. Neben dem sich schon länger im Gespräch befindlichen Nachfolger **WEP2**, das die Sicherheit beträchtlch erhöhen sollte, tauchte vor kurzem eine Version **WEP2002** auf, die einen gänzlich neuen Verschlüsselungsalgorithus und ein Verfahren zum Schlüsseltausch verspricht.
Derzeit ist noch nicht in Aussicht, wann welche Lösung für eine Implementierung zur Verfügung stehen könnte.