A vezeték nélküli hálózatok és biztonsági rései

A WiFi (Wireless Fidelity) a WECA (Wireless Ethernet Compatibility Assocation) bejegyzett márkaneve, és a korábban IEEE 802.11b-nek nevezett szabvány könnyebben megjegyezhető márkaneve, valamint az ilyen eszközök kompatibilitásának is jelölése.

A WiFi-nek megfelelő eszközök olyan hálózati eszközök, amelyek segítségével rádiós adatátviteli összeköttetetést tudunk megvalósítani. Ezek az eszközök a 2400 Mhz-es frekvencia sávban, a 15 különböző csatorna egyikén működnek, néhányszor 10mW-os adóteljesítménnyel. A WiFi eszközök segítségével akár 11Mbps sebességet (a rendszer sebessége jelentősen függ a vételi viszonyoktól, ha nem megfelelő a rádió kapcsolat, a rendszer automatikusan visszakapcsol kisebb sebességre) is el tudunk érni, ami megfelel egy hagyományos 10 Mbps vezetékes hálózat sebességének.

Rádiós kapcsolatoknak két típusa van, az úgynevezett ad-hoc és a strukturált.

- Ad-hoc módban a hálózati kártyák közvetlenül egymással kommunikálnak.
  Az ad-hoc mód előnye, hogy kis gépszámnál (max 5-10 gép) nem szükséges a központ egység beszerzése.
- A strukturált módban egy központi egységen (Access point) keresztül tartják a kapcsolatot.
  Strukturált módban lényegesen több, akár 64-256 gép is kapcsolódhat egy központi egységhez. Ha több központi egységet összekapcsolunk lehetőségünk van roamingra is, tehát a kiépített hálózaton belül bárhol lehetünk, sőt akár mozoghatunk is, mindig on-line maradunk.

A 802.11b hálózati kártyák WLAN-ok után kutatva automatikusan lekérdezik ezeket a csatornákat, így az egyes klienseket nem kell bekonfigurálni a különböző csatornákra. (Az Acces Point-ot, ezzel ellentétben egy adott csatornára kell beállítani.)

Amint a NIC (Network Interface Card) talált egy csatornát, elkezdi a mögötte lévő elérési ponttal való kommunikációt. Amennyiben a kliens és az elérési pont biztonsági beállításai megegyeznek egymással a NIC felhasználója részt vehet a hálózatban.

A 802.11b-t nem tervezték különlegesen biztonságosra, így a rádiós hálózatnál mindig felmerül az adatbiztonság kérdése, habár rendelkezik néhány biztonsági jellemzővel.

Az SSID (Service Set Identifier) célja, hogy több hálózatot meg lehessen különböztetni egymástól. Az SSID-nél már található egy vékony biztonsági réteg. Egy könnyen kitalálható SSID teszi azonosíthatóvá a hálózatot mindenki számára, ezért az SSID-t egy jelszóval azonos módon kell használni. A legtöbb elérési pont néhány másodpercenként rendszeresen kisugározza az SSID-t, ami természetesen megkönnyíti a felhasználónak a megfelelő hálózat megtalálását. Ez egyben az elsődleges útja a támadóknak, hogy megszerezzék a hálózat nevét anélkül, hogy ismerték volna az SSID-t.

Mielőtt egy kliens az Access Point-tal kommunikálhat, mindkét készüléken elindul egy párbeszéd, amely során tisztázódik, hogy egyáltalán összetartoznak-e a készülékek. Ezt az eljárást associating-nek nevezzük. A 802.11b szabvány előírja, hogy a készüléknek közvetlenül ezután azonosítania kell magát. Ez az azonosítás a 802.11b keretén belül egy további biztonsági réteget hivatott létrehozni.

A hitelesség vizsgálaton belül két azonosítási módszer létezik.

- A Shared Key (közös, osztott kulcs)
  Itt a kliens először egy azonosításkéréssel fordul az Access Point-hoz, amely egy Challenge szöveget küld a kliensnek. A kliens WEP-pel rejtjelezi a szöveget és visszaküldi azt az Access Point-nak. Ha a szöveg hibátlanul rejtjelezve érkezik az Access Pointhoz, akkor a klienst átengedik és kommunikálhat az Access Point-tal. Korrekt rejtjelezés esetén az Access Point ki tud kódolni, vagyis a rejtjelezés megfejtését követően ismét az eredetileg kiküldött szövegét szeretné visszakapni. Az ehhez használt kulcs azonos a WEP-kódoláshoz használt kulccsal. Éppen ez jelenti a nagy biztonsági problémát, hiszen az Access Point először kódolatlanul küldi a klienshez a challenge-szöveget. Egy támadó, lehallgatva a rádióforgalmat, a rejtjelezés két eleméhez hozzájut. Egyszer elcsípi a kódolatlan challenge-szöveget, majd a kliens által visszaküldött rejtjelezett anyagot.
  Ezzel a két információval a támadó az RC4 algoritmust alkalmazva a rejtjelezéshez használt kulcs birtokába jut. Ha a kulcs ismert, akkor a WEP-kulcs is ismertté válik.
- Az Open Authentification (nyitott azonosítás)
  Ez egy egyszerűbb módszer, amely mindenki számára megengedi, hogy kommunikálni kezdjen az Access Pointtal.

A WiFi eszközök tartalmazzák a WEP-et (wireless equivalency protocol), ami egy 40 bites titkosítást jelent és a vezetékes hálózatoknál megszokott biztonságot nyújtja. Minden 40 bites kulcsot tartalmazó csomag RC4 algoritmus felhasználásával kódolódik az átvitel előtt. Az RC4 algoritmus rejtjelezi az adatokat. Átvitelre azután csak ezek a kódolt csomagok kerülnek. A címzett megkapja a kódolt adatokat és visszafelé alkalmazza rájuk az RC4 algoritmust. Ezzel használható, rejtjelezetlen adatokhoz jut, amelyekkel azután tovább tud dolgozni.

A WEP azért alkalmaz 40 bites kódolást, mert az RC4 eljárás az adatokat rejtjelezéséhez a 40 bites WEP-kulcson kívül egy 24 bit szélességű (40 + 24 = 64) véletlen számot is felhasznál. Ezt a számot IV-nek (Initialization Vector) nevezzük és a kódolt adatokkal együtt szintén átvitelre kerül.

A támadó a Shared Key azonosítási eljárástól eltérően, még semmit nem ismer a véletlen számból, mert az rejtjelezve kerül átvitelre, így a Shared Key azonosítástól eltérően, nem tudja azonnal meghatározni a WEP-kulcsot.

Az RC4 több gyenge és támadásra alkalmas ponttal rendelkezik. Az egyik támadási módszer esetén egy egyszerű számjegyes eljárást alkalmaznak a támadók. Az IV csak 24 bites, így csak fix számú olyan permutáció létezik, amit az RC4 az IV-hez fel tud használni.

Matematikailag 2^{24} lehetséges IV-kombináció létezik. Ebben az esetben a kliens aktivitásától függően néhány óra, esetleg néhány nap a kód feltörése. A lehetséges IV-k száma korlátos, ami oda vezet, hogy az RC4 kénytelen egy idő múlva mindig ugyanazokat a karaktereket alkalmazni egy adott IV-hez.

Tehát a támadó egy idő után felismerheti az ismétlődő IV-ket. Elég adat rendelkezésre állása esetén, meg tudja határozni az alkalmazott WEP-kulcsot. Ez egy úgynevezett Brute Force támadás, de ez a módszer időigényes más betörési módszerekhez képest. Ennek az az oka, hogy nemcsak 2^{24} csomagot kell jegyzőkönyvezni, hanem ennek többszörösét.

Egy másik támadási módszer azon alapszik, hogy léteznek ismert, gyenge IV-k. Ez az RC4 természetéből fakad. Az RC4 algoritmus egyes karakterekkel egyszerűen jobban működik, mint másokkal. Ebből származnak a gyenge 24 bites karakterek, de ezeket is felhasználja. Ha tehát ilyen gyenge karaktereket használnak, akkor a támadó néhány algoritmuson át tudja szűrni a lehallgatott adatokat és így képes meghatározni a WEP-kulcs részeit. Ez az eljárás egyik ismert implementációja 10-15 millió csomagot igényel a WEP-kulcs megtöréséhez. A kód megfejtése itt is hasonló módon néhány óra, esetleg néhány nap.

A rejtjelezést a WEP Plus eljárással javítják, amely nem része a 802.11b szabványnak. Ennél a módszernél a 40 bites helyett 104 bit széles kulcsot használnak. A probléma ezzel sem oldódik meg, de a hosszabb kulccsal elérhető, hogy a kulcs meghatározására kb. 5 hónapra emelkedik.

Ezen kívül van egy másik eljárás, amelyben a WEP kulcs automatikusan újra átvitelre kerül. A rendszergazda megad egy időtartamot (néhány perc), s ennek elteltével az Access Point egy új WEP kulcsot küld ki valamennyi kliensnek.

Egy kidolgozás alatt álló eljárásban 10000 csomagonként megújítva automatikusan szétküldik a WEP kulcsot. Ez a jövőben ésszerűen védetté teheti a WiFi hálózatok üzemeltetését.

Fái András István
informatikatanár II. évf.
FAAMACT.SZE