

Kablosuz ağ güvenliği (3)



ÇETİN KAYA
KOÇ

Kablosuz ağ güvenliği konusundaki yazılarımıza devam ediyoruz.

Kablosuz ve mobil ağlarda son anlatacağımız konu, hizmet engelleme (denial-of-service) saldırıları. Prensipten saldırganlar, farklı metotlar kullanılarak abonelerinizin ağa ulaşmasına engel olabiliyorlar. Sizin yapabileceğiniz bir şey var mı? Ne yazık ki, pek yok.

İki farklı hizmet engelleme saldırısı görülüyor, birincisi düşük teknoloji saldırısı: Bütün yaptıkları kullandığınız frekanslarda yayın yaparak, sizin yayını zayıf (jamming). İkincisi daha ileri bir saldırı türü: 802.11 protokolunu manipüle ederek, sizin ağınızın paketleri göndermesine veya almasına engel olmak.

Bazen farkında olmadan da engelleme yapmak mümkün, mesela TV istasyonlarının gezici arabaların yaptıkları mikrodalga yayınları buna neden olabiliyor. Bunlar genellikle çok dar hüzmeleri uydura gönderdiği için sorun olmuyorlar, ancak bazen çatılarından yansıyan hüzmeler civarda ki kablosuz LAN'ları devre dışı bırakabiliyor. Az miktarda ev-yapımı veya ticari jammer cihazları bir LAN'ı engelleyecek güce sahip. Bir kaç yüz dolara satılan bazı cihazlar 100 metre içinde bir ağ

engelleyebiliyor. Daha ucuza satılanlar ise daha az alanı engelleyebiliyorlar. Diğer taraftan, laptop üzerine kurulmuş bir cihaz yardımıyla, seçilen bir ağın yayınlarına engel olup, baz istasyonuna tek başına sahip olmayı sağlayan bir teknolojiye var (wifi hog projesi). Ancak prensip olarak jamming pek kolay yapılacak bir iş değil ve saldırganlar da korkulacak kadar etkili olamıyorlar. Fakat bir problem daha var: hatların karışması (interference). Bu ise zaman içinde daha iyi haberleşme teknolojileri ile halledilebilecek bir soruna benziyor.

Önlemlere gelince: eğer maksatlı ve odaklı saldırı altında iseniz yapacağınız tek şey spektrum analiz cihazları ile yapını bulmak, sonra da oraya giderek yapınların jammer cihazını kırmak. Bunun hukuki bir çözüm olup olmadığını düşünmeden yapılmaması daha iyi tabii! En doğru davranış bu işi savcıya havale etmek olmalı. Ancak ileri tip saldırılarda (802.11 protokolunu manipüle eden saldırılarda) yapını bulmak çok daha zor. Burada ise beklentiler protokoldeki açıkların zamanla iteratif bir şekilde bulunup temizlenmesi.