Kablosuz erişim teknolojilerinde uygulama hataları

ÇETİN KAYA
KOÇ

Wi-Fi uygulamalarında güven problemi kurumları daha çok ilgilendiriyor.

Birçok güvenlik açığının varlık nedeni, uygulama (implementasyon) da yapılan hatalar. Protokol ve alakalı güvenlik mimarisi ne kadar dikkatlice tasarımlanmış olursa olsun, uygulama da yapılan seçimler ve tercih edilen kısayollar, sistemin genel güvenliğini belirleyen faktörler olarak karşımıza çıkıyor. Bu yüzden "robustness test" denilen çalışmalar çok önemli. Bunların yardımıyla test ettiğimiz sistemin var olan protokol, algoritma ve mimariye ne kadar sadık kaldığına bakıyoruz.

Bir kaç hafta önce Codenomicon şirketinin bazı Bluetooth ve Wi-Fi uygulamalarına robustness testi uygulayarak sonuçları yayınladığını duyduk ve raporu merakla okuduk. Bluetooth kategorisinde 31 uygulamayı test eden Codenomicon, bunların sadece 3 tanesinin testleri tam manasıyla geçtiğini gözlemiş. Yarıdan fazla uygulama, daha test ederken resetlenerek "crash" olmuşlar. Bazı durumlarda, cihaz yeniden programlanmak durumunda kalmış.

Bluetooth mimarisinin güvenlik açısından uyumsuzluğu bir yana uygulamaların çoğunun testleri geçemiyor olması büyük bir talihsizlik. Cihazdan-cihaza bağlantı yaptığı ve bizi kablolardan kurtardığı için, Bluetooth gerçekten de çok faydalı bir teknoloji. Ancak piyasadaki uygulamaların yüzde 90'nın hem güvensiz (unreliable) ve hemde güvenliksiz (insecure) olması onu kurumsal olarak kullanılamayacak teknolojiler listesine sokuyor.

Diğer taraftan Wi-Fi uygulamalarında güven problemi kurumları daha çok ilgilendiriyor. Çünkü artık Wi-Fi kurumsal hayatın bir parçası haline geldi. Buradaki robustness problemlerinin Bluetooth kadar vahim olmaması iyi bir haber ama etkilerinin çok daha vahim olacağını biliyoruz. Sonuç olarak Bluetooth ile en çok yaptığımız şey, cep telefonundan cep telefonuna veya laptopa telefon listemizi göndermek; halbuki Wi-Fi kurumsal ağın en azından bir kısmını saldırıya açık hale getirebilir.

koc@krip.to