RFID TEKNOLOJİSİ ve GÜVENLİK TEHDİTLERİ

Zeydin PALA
Yüzüncü Yıl Üniversitesi, Özalp Meslek Yüksekokulu, Bilgisayar Programcılığı, Van
zeydinpala@yyu.edu.tr

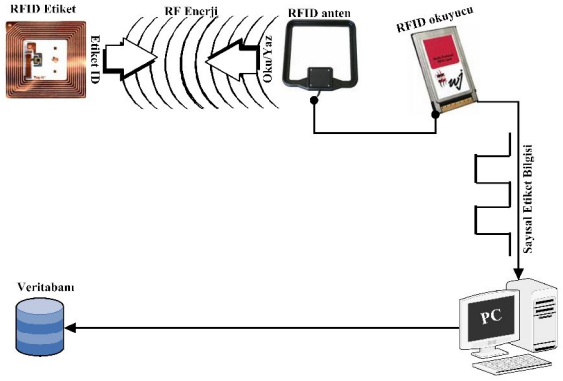
ABSTRACT

Radio Frequency Identification (RFID) is becoming a widely-used technology that makes life easier. Nonetheless, some issues concerning security and privacy discourages potential RFID technology users. To avoid these security issues, substantial amount of work is done by the academics environment. Thanks to EPCGlobal Class-1 Gen-2 protocol that is developed for UHF RFID passive labels, a certain amount of security can be achieved but this is not enough for security breaches of a higher level. The only side of this protocol that is considered as inadeqaute in terms of security is its using a one-sided reader-label validation scheme. Thus, there is an urgent need for protocols that prioritize security and individual privacy. In this research, RFID technology and the most common security issues of it have been examined.

Key words: RFID, security, privacy, threat

1. GİRİŞ

RFID (Radio Frequency Identification-Radyo frekanslı tanıma) genel olarak; canlıları yada nesneleri radyo dalgaları ile tanımlamak için kullanılan teknolojilere verilen isimdir [1]. Bu teknoloji, RFID okuyucu, RFID anten, RFID etiketler ve yazılımdan meydana gelmektedir. RFID okuyucu ile etiketler arasında veri alışverişi kablosuz olarak gerçekleşmektedir [2]. Bilgi alışverişi okuyucudan etiketlere gönderilen radyo dalgaları ile yapılmaktadır (Şekil 1).



Şekil 1. RFID teknolojisi çalışma prensibi

Bir RFID etiketi oldukça küçük bir elektronik aygıt olup kısa mesafede okuyucu ile kablosuz olarak haberleşir. Kablosuz olarak haberleşme süresi çok uzun olan etiketler olduğu gibi kısa olan etiketler de vardır. EPC (Electronic Product Code-Elektronik ürün kodu) etiketleri olarak adlandırılan pasif etiketlerin kapasitesi oldukça düşüktür. Bu etiketler okuyucuların elektromanyetik alanları ile güç tedariki yaparlar. Bu etiketleri besleyecek herhangi bir destek kaynağı olmaz. Dolayısıyla şarj edilemezler.

RFID EPC etiketler son kullanıcılar için oldukça farklı alanlarda kullanılabilmektedirler. Bu etiketler bir mağazada ödemesi yapılmayan ürünün dışarı çıkması halinde, mağaza sahibine haber vermede kullanılabileceği gibi bir çamaşır makinesinin içinde ne tür çamaşırlar olduğunu öğrenmede de kullanılabilir [3].

RFID teknolojisi, gerçek zamanlı ürün izleme ve ürün takibi yaparak ticari kuruluşlara stratejik faydalar sağlamaktadır. Üreticiler RFID teknolojisini kullanarak, pasif RFID etiketlerini kendi ürünlerine iliştirirler. Bu etiketlerin çoğu sadece ürünün EPC bilgisini içerirler. Daha gelişmiş olanları ise ürün hakkında daha fazla bilgi içerirler. Ürün tanımı, üretim tarihi, paketleme tarihi, taşıma biçimi gibi bilgiler bu gruba girer. Tüm bu bilgiler veritabanları ağına kaydedilir ve EPC-IS (Electronic Product Code-Information services-Elektronik ürün kodu bilgi servisleri) adını alır [4].

RFID teknolojisinin özellikle otomasyonda kullanılması ile elle yapılan işler minimuma indirgenmiştir [5]. RFID teknolojisi evrenseldir, yararlıdır ve elverişlidir [6]. RFID teknolojisi, şirketlerin verimliliğini artırır ve gerek müşteri, gerekse şirket için önemli faydalar sağlar [7].

Diğer bilişim sistemlerinde olduğu gibi RFID teknolojisi de sunduğu kolaylıklar yanında bir takım güvenlik riskleri ile de karşı karşıyadır. Bu riskleri en genel olarak; etiket içindeki bilgilere yetkisiz erişim, etiketteki bilgileri bozma yada değiştirme, etiketin sahte kopyasını çıkarma olarak ifade edebiliriz [8].

Tüm bunlarının önüne geçmek için okuyucular öncellikle kimlik doğrulama mekanizmasından geçmeli daha sonra etiket içindeki bilgilere erişmelidir.

RFID kullanımını desteklemek için sürekli olarak EPC için geliştirilecek standartlar üzerinde çalışan EPCGlobal Inc., adında bir organizasyon vardır. Bu

kurumun çıkardığı tek taraflı okuyucu etiket kimlik doğrulaması, Class-1 Gen-1 adını almaktadır [9].
RFID teknolojisine bağlanan en önemli standartlardan bir tanesi EPCGlobal Class-1 Gen-2 belirtimidir [10].
EPC Class-1 Gen-2 etiketleri pasif etiketler olup kendi enerjilerini okuyuculardan RF formundan alırlar.
Standardın takibinde pasif RFID etiketler, 16-bit PRNG (Pseudo-Random Number Generator) ve 16-bit CRC (Cyclic Redundancy Code) desteklediler. Etiket belleği 16-bitlik rastgele iki sayıyı saklayabilecek [11] kapasite de olup çevresindeki fiziksel ataklara karşı zayıf ve emniyetsizdir.
Sırasıyla etiketi kalıcı olarak devre dışı bırakma (kill) ve tetikleyicisini güvenli moda geçirmek için 2 tane 32-bitlik gizli erişim şifre kullanılır.

2. RFID TEKNOLOJİSİNE YÖNELİK GÜVENLİK TEHDİTLERİ

Otomatik tanıma sistemleri içinde sunduğu birçok avantajdan dolayı ön plana çıkan RFID teknolojisi, farklı noktalarda saldırılara maruz kalmaktadır. Maruz kalınan en temel güvenlik ve gizlilik saldırılarını şöyle ifade edebiliriz: Dinleme (sniffing), izleme (tracking), aldatma (spoofing), saldırıyı tekrarlama (Replay attack), hizmeti durdurma (Denial of service) [12].

1-Dinleme (Sniffing)

RFID etiketler, uyumlu tüm okuyucular tarafından okunacak şekilde tasarlanırlar. Etiketler üzerinde bulundukları canlı yada cansız maddenin onayını almadan menziline girdikleri okuyuculara cevap verirler. Bu durumu bilen bir saldırgan uzak menzilli bir RFID okuyucuyu kullanmak suretiyle etiketlerin bilgilerine erişebilir. Bu konuda en büyük sorunla karşı karşıya kalan nesneler RFID teknolojisini kullanan sayısal pasaportlardır [13].

2-İzleme (Tracking)

Stratejik noktalarda kullanılan RFID okuyucular orada çalışanların önemli bilgilerini kaydederler. Burada söz konusu problem bireyleri haberi olmadan uzaktan izlenebilme durumlarıdır. Bu yöntemle okul çocukları izlenebileceği gibi, bir şirketin çalışanları da izlenebilir.

3-Aldatma (Spoofing)

Saldırganlar boş yada okunur-yazılır özelliğine sahip etiketleri yazmak suretiyle gerçeği aratmayacak şekilde RFID etiketleri oluşturabilirler. Dikkate değer bu tür bir atağı Johns Hopkins University ve RSA Security araştırmacıları gerçekleştirdiler [14]. Araştırmacılar sinyal dinleme yöntemini kullanarak mevcut bir araba etiketinin bir kopyasını çıkardırlar. Kopyaladıkları bu etiketi kullanarak önce benzin aldılar ardında arabayı kilitlediler.

4-Takrarlanan Ataklar (Replay attacks)

Saldırganlar uygun RFID cihazları kullanarak, RFID okuyucudan gönderilen sorgu sinyallerini durdurup yeniden gönderebilirler [15]. Bu tür yeniden sinyal gönderim işlemleri; sayısal pasaport okuyucularını, temassız ödeme sitemlerini, bina erişim kontrol istasyonlarını aptal durumuna düşürür.

5-Hizmeti Durdurma (Denial of service)

Bu yöntem tamamen verilen hizmeti durdurmaya ve yavaşlatmaya yönelik olarak yapılan bir saldırı yöntemidir. Etiketlerin okunması Faraday kafesi (Faraday cage) [16] yada sinyal boğma yöntemiyle engellenir. Bu iki yöntem de radyo sinyallerinin RFID etiketlere erişmesini engeller.

6-İçeriden Saldırma (insider attack)

EPCGlobal tarafından onaylanmış olan Class-1 Gen-2 UHF RFID protokolü [17], sadece tek taraflı okuyucu-etiket kimlik doğrulama şemasını tanımlar. Bu standarda göre etiket üreticisi 32 bitlik erişim şifresini (Access password) etiket içine gömebilir. Sadece doğru şifreyi bilen bir okuyucu vasıtasıyla etiket ile iletişime geçilebilir. Bu şema güvenli değildir [4] ve etiketi üreticiden dağıtımcıya geçişinde de güvenli detayları sağlamaz. Erişim şifresi ürünün üretiminin başından, kullanım aşamasına geçene kadar hep aynıdır ve değişmez. Bu da ister istemez aynı etiketin bir kopyasını çıkarma riskini doğurur.

7-Ortadaki Adam Saldırısı (Man-in-the-Middle-Attack)

EPCglobal Class-1 Gen-2 UHF RFID etiketleri yakın alan performansı sergilerler. Okuyucular bu etiketler ile 10 metreden haberleşebilirler [4]. Bu özellik daha güçlü okuyucular kullanan kişilerin dikkatini çekmektedir. Bu durumda okuyucu ile etiket arasındaki iletişim biçimi dinlenmeye alınmak suretiyle hem erişim şifresi hem de etiket kimlik numarası ele geçirilebilir.

3. TEHDİTLERE KARŞI EPCGLOBAL CLASS-1 GEN-2 UHF RFID PROTOKOLÜNÜN GETİRDİKLERİ

EPCglobal Class-1 Gen-2 UHF RFID Protokolüne göre bir etiket çipi dört bellek bankına sahiptir:

Reserved (Ayrılmış), EPC, TID ve User (kullanıcı). Ayrılmış bellek 32-bit Access password (APwd) ve 32-bit Kill Password (KPwd) komutları için kullanılır. EPC bellek bankı EPC numarası için kullanılır. Ayrılmış bellek bankı kalıcı olarak üretici tarafından kilitlenmiştir. Bu yüzden APwd ve KPwd hiç bir RFID okuyucu tarafından değiştirilemez. RFID etiket bu şifreleri doğrulama yeteneğine sahiptir. Doğru APwd komutunu etikete gönderen bir okuyucu; okuma, yazma ve kilitleme işlemlerini yapabilir. Eğer okuyucu doğru KPwd komutunu etikete gönderirse, etiket kalıcı olarak ölü duruma geçer [4].

4. SONUÇLAR

RFID teknolojisi esnek ve kullanımı kolay bir teknolojidir. Bununla beraber güvenlik risklerini de göz ardı etmemek gerekir. EPCglobal Class-1 Gen-2 protokolü önceki protokol olan Gen-1'e göre daha güvenli, daha hızlı, daha uzak mesafede etiket okunmasını sağlamasına rağmen mevcut güvenlik risklerini tamamen ortadan kaldıracak özellikte değildir. Bu protokolün yetersiz görülen tarafı sadece tek taraflı okuyucu-etiket kimlik doğrulama şemasını tanımlamasıdır.
Bu nedenle daha güvenli ve kişisel gizliliğe daha fazla önem veren protokollere acilen ihtiyaç duyulmaktadır.

KAYNAKLAR

[1] Chen, J., W., 2005, A Ubiquitous Information Technology Framework Using RFID to Support Students' Learning,icalt, pp. 95-97, Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05), 2005

[2] Pala, Z., İnanç, N., 2007., Smart Parking Applications Using RFID Technology, The First International RFID Eurasia 2007 Conference, September 5-6, 2007, Istanbul, Turkey

[3] Castelluccia, C., Soos, M.,2007, Secret Shuffling: A Novel Approach to RFID Private Identification, Conference on RFID security 07, Malaga, Spain, July 11-13

[4] Konidala,D., M., Kim,Z., Kim, K.,2007, A Simple and Cost-effective RFID Tag-Reader Mutual Authentication Scheme, Conference on RFID security 07, Malaga, Spain, July 11-13

[5] Penttila, K., Keskilammi, M,. Sydanheimo, L., Kivikoski, M.,2006. Radio frequency technology for automated manufacturing and logistics control. International Journal Of Advanced Manufacturıng Technology, 31 (1-2): 116-124.

[6] Zhang, L., 2005. An Improved Approach to Security and Privacy of RFID application System. Wireless Communications, Networking and Mobile Computing. International Conference. (2): 1195- 1198.

[7] Higgins, N., L., Cairney, T., 2006., RFID opportunities and risks. Journal of Corporate Accounting & Finance, Vol, 17 (5):51-57.

[8] Lim, T., L., Li, T., 2007, Addressing the Weakness in a Lightweight RFID Tag-Reader Mutual Authentication Scheme, IEEE Global Telecommunications Conference 2007,Washington,USA.

[9] EPCglobal Inc., "EPC Radio-Frequency Identity Protocols Class- 1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.0.9", EPCglobal Standards, Jan 2005.

[10] Peris-Lopez,P., Hernandez-Castro, J., C., Estevez-Tapiador,J., Ribagorda, A., M.,2007, Cryptanalysis of a Novel Authentication Protocol Conforming to EPC-C1G2 Standard,Conference on RFID security 07, Malaga, Spain, July 11-13

[11] Konidala, D., M., Kim, K., 2007, RFID Tag-Reader Mutual Authentication Scheme Utilizing Tag's Access Password, Auto-ID Labs White Paper WP-HARDWARE-033, Jan 2007.

[12] Rieback, M., R., Crispo, B., Tanenbaum, A., S., 2006, Is Your Cat Infected with a Computer Virus?, Pervasive Computing and Communications, 2006.

[13] Monnerat, M., Vaudenay, S., Vuagnoux, M.,2007, About Machine-Readable Travel Documents, Journal of Physics: Conference Series, Volume 77, Issue 1, pp. 012006 (2007).

[14] Bono, S., Green, M., Stubble, A., Juels, A., Rubin, A., Szydlo, M., 2005, Security analysis of a cryptographically enabled RFID device, 14th USENIX Security Symposium, July 31-August 5, 2005, Baltimore, MD,USA.

[15] Kfir, Z., Wool, A., 2005, Picking virtual pockets using relay attacks on contactless smartcard systems, Cryptology ePrint Archive, citeseer.ist.psu.edu/kfir05picking.html

[16] http://en.wikipedia.org/wiki/Faraday_cage,2008

[17] EPCglobal Ratified Standard, "EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz Version 1.0.9", http://www.epcglobalinc.org/standards