RFID Sistemleri ve Veri Güvenliği

Ela Sibel Bayrak Meydanoğlu

(Almanca İşletme Enformatiği, Marmara Üniversitesi, İstanbul, Türkiye)
elasibelbayrak@yahoo.com

***Özet*—** Radyo Frekanslı Tanıma (Radio Frequency Identification, RFID) sistemleri radyo dalgalarını kullanarak etiketlenmiş objeleri tanımlayan ve takip edebilen kablosuz sistemlerdir. Potansiyel kullanıcıların ve etiketli objeleri tüketebilecek potansiyel tüketicilerin RFID sistemlerinde veri güvenliğinin temini ile ilgili endişeleri bu sistemlerin pratikte yayılmasının önündeki önemli engellerden biridir. Mevcut çalışma RFID sistemleri ile ilgili veri güvenliği risklerine, bu risklerin engellenmesi ya da azaltılması için alınabilecek karşı önlemlere ve uygun önlemin seçiminde dikkat edilmesi gereken hususlara temas eder.

***Anahtar kelimeler*—** Veri Güvenliği, RFID sistemleri

RFID Systems and Data Security

***Abstract*—** Radio Frequency Identification (RFID) Systems are the wireless systems that identify the labeled objects and track them by means of radio signals. One of the important barriers at the deployment of RFID systems is the anxiety of the potential RFID users and the potential consumers of the labeled objects in respect of ensuring the data security. The study deals with the data security risks related to RFID systems, the countermeasures that can be taken to prevent or mitigate these risks as well as the points that have to be taken into account when choosing the appropriate countermeasure.

***Keywords*—** Data security, RFID systems

1. GİRİŞ

Bir Auto-ID sistemi olan RFID etiket yapıştırılmış objeleri radyo dalgaları kullanarak otomatik olarak tanımlamayı sağlayan bir sistemdir. RFID sistemlerinin pek çok objeye ait etiketleri aynı anda okuyabilmeleri, toz, nem gibi dış etkilerin sistemin okuma ve veri kaydı fonksiyonlarını yerine getirmesinde engel teşkil etmemesi, sistem etiketlerinin veri kapasitesinin genişliği, okuma ya da kayıt fonksiyonun gerçekleştirilmesi için sistemin fiili görme zorunluluğunun bulunmaması yani sistemin etiketleri okuyabilmesi ya da veri kaydetmesi için okuyucunun etiketleri görme zorunluluğunun olmaması etiketlerin okuyucunun kapsama alanı içerisinde bulunmasının okuma ve kayıt işlemi için yeterli olması, sunulan önlemler ile veri taklidi ve tahrifinin zorlaştırılması, okuma ve kayıt mesafesinin uzunluğu RFID sistemlerinin pratikte yaygın olarak kullanılan bir başka Auto-ID sistemi olan barkod sistemlerine karşı üstünlükleridir [1]. Sayılan bu avantajlarına rağmen potansiyel kullanıcılar ve etiketli ürünleri tüketenler arasında sistemin veri güvenliği ile ilgili bazı risklere sahip olduğu düşüncesi sistemin kullanımı ile ilgili çekinceler oluşturmaktadır. Mevcut çalışmanın amacı söz konusu riskleri ve veri güvenliğinin temini için bu risklere karşı alınabilecek önlemleri izah etmek, uygun önlemlerin seçilmesinde hangi kriterlerin belirleyici olduğuna temas etmektir.

2. VERİ GÜVENLİĞİ

Veri güvenliği (*data security*) altında verilerin kötüye kullanımını, verilere yetkisiz kişilerin erişimini, verilerin tahrifini, veri kaybını, verilerin taklidini, tahribini, silinmesini önlemeye yönelik tüm organizasyonel ve teknik önlemler anlaşılır [2].

3. RFID SİSTEMİ

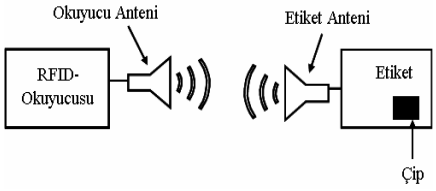
Bir RFID sistemi üç alt sistemden oluşabilir [3]:

- RF (radio frequency) alt sistemi (RF subsystem)
- Kurumsal alt sistem (enterprise subsystem)
- Kurumlar arası alt sistem (inter-enterprise subsystem).

RF alt sistemi etiket yapıştırılmış objeleri radyo dalgaları kullanarak otomatik olarak tanımlamayı sağlayan

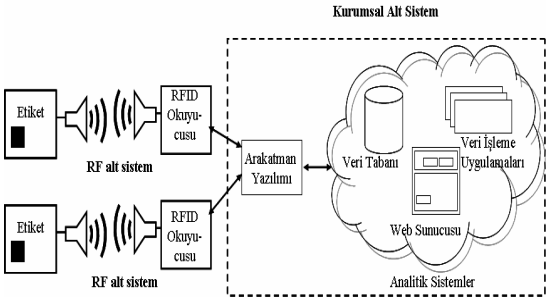
sistemdir. Bu sistemin bileşenleri etiketler (*tag*) ve okuyuculardır (*reader*) [3]. Etiket objelerin içine ya da üstüne monte edilen, bir anten ve mikroçipten oluşan veri taşıyıcısıdır [4]. Her etiket tek bir etiket tanımlayıcısına (*tag identifier*) sahiptir. Etiketlere veri güvenlik mekanizmaları, veri gizliliğini temin eden mekanizmalar, çevreden gelen verileri (örn. ısı, basınç vb.) kaydetmek için sensör, etiketler üzerine kaydedilen verilere daha sonra erişimi mümkün kılan uçucu olmayan bir bellek entegre edilebilir [3].

Okuyucu kullanılan teknolojiye göre anten ve okuyucu ya da anten ve yazıcı/okuyucudan oluşur. Okuyucu kapsama alanı içinde bulunan etiketler ile radyo dalgaları vasıtasıyla iletişim kurar, kullanım sistemlerinden aldığı komut ve verileri kodlayarak elektromanyetik dalgalara dönüştürür ve etiketlere gönderir, etiketten radyo dalgaları olarak aldığı komut ve verileri ilgili kullanım sistemi tarafından kullanılmak üzere dijital bilgiye dönüştürür [4].



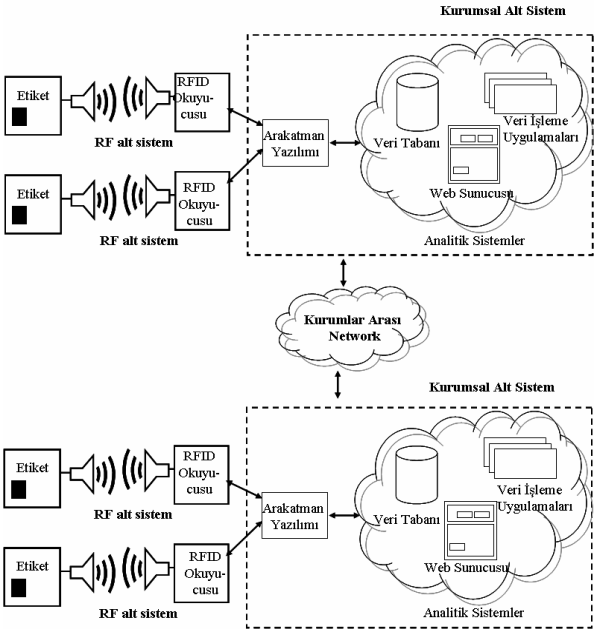
Şekil 1. RF alt sistemi [3]

Kurumsal alt sistem RF alt sisteminden elde edilen verileri işletme süreçlerinde kullanılabilir hale getirmek için saklayan, işleyen ve analiz eden özel yazılımları içeren bir sistemdir. Kurumsal alt sistemin üç bileşeni vardır: Ara katman yazılımı (*middleware*), analitik sistem (*analytic system*) ve ağ oluşturma servisleri (*networking services*). Ara katman yazılımı okuyucu ve kurumsal sistem arasındaki bağlantıyı sağlayan bir yazılımdır. Bu yazılım RFID okuyucularından elde edilen verileri filtreler, kümeler ve ilgili kullanım sistemine iletir. Bu yazılımın bir görevi de RFID aletlerini (okuyucu, anten, yazıcı vb.) kontrol ve idare etmektir. Analitik sistem işletme süreçlerinde kullanılmak üzere verileri işler ve saklar. Ağ oluşturma hizmetleri kurumsal alt sistem bileşenleri arasındaki ve kurumsal alt sistem ile RF alt sistemi arasındaki bağlantıları temin için kullanılır [3].



Şekil 2. Kurumsal alt sistem [3]

Kurumlar arası alt sistem tedarik zinciri uygulamalarında olduğu gibi verilerin kurumlar arası paylaşımının gerekli olduğu hallerde ilgili kurumsal sistemleri birbirine bağlayan sistemdir [3].



Şekil 3. Kurumlar arası alt sistemin mimarisi [3]

Tüm RFID sistemleri RF alt sistemi ihtiva eder. Çoğu RFID sistemi RF alt sistemi yanı sıra kurumsal alt sisteme de sahiptir. Bir RFID sistemi genelde kurumlar arası alt sistem içermez. Bu sistemler ancak gerekli durumlarda (örn. bir tedarik zinciri içerisinde ürünlerin takibi için RF sistemi kullanılması durumunda) RFID sistemin bir parçası olarak tanımlanır [3].

Çalışmada RF sistemi kullanımının doğurduğu RFID'ye özgü güvenlik sorunlarına ve bu sorunları önlemede kullanılabilecek metotlara temas edilir.

4. RF SİSTEMİNE İLİŞKİN VERİ GÜVENLİĞİNİ TEHDİT EDEN SALDIRILAR

Aşağıda RF sistemlerinde veri güvenliğini tehdit eden önemli saldırılar sıralanmıştır:

- İzinsiz okuma (unauthorised reading)
- Veri tahrifi (data tampering)
- Etiketin taklidi (tag spoofing)
- Etiketlerin çalışamaz duruma getirilmesi (*deactivation of tags*)
- Etiketlerin objelerden sökülmesi (removal of tags)
- Etiket ve okuyucu arasındaki frekansın bozulması (jamming)
- Blocker tag kullanımı ile okuyucunun bloke edilmesi (blocking)
- Okuyucuyu tanımlayan verilerin taklidi (reader spoofing)

- Etiket ve okuyucu arasındaki iletişimin izinsiz dinlenmesi (eavesdropping)
- İzleme (tracking)
- Yönlendirme saldırıları (relay attacks)
- RFID – kötücül yazılımları (RFID-Malware)

İzinsiz okuma altında RFID etiketlerini okuma yetkisi olmayan saldırganın etiketlere erişerek üzerindeki verileri okuması anlaşılır [5].

Veri tahrifi etiket tanımlayıcısının ve olası güvenlik verilerinin değil de etiket üzerindeki diğer verilerin etikete erişim yetkisi olmayan biri tarafından değiştirilmesi demektir. Bu tarz bir saldırı etiketin tanıtıcı ve güvenlik verileri dışında başka verilere de sahip olması durumunda söz konusudur [5, 6].

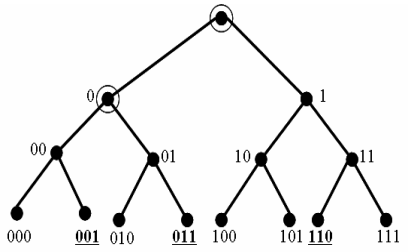
Etiketin taklidi durumunda saldırgan etiket tanımlayıcısı ve/veya etiketin güvenlik verilerini (örn. parola) ele geçirir ve etiketleri emüle eder ya da klonlar [5, 6].

Etiketlerin çalışamaz duruma getirilmesi etiketlerin ya fiziksel olarak tahribi ya da yetkisiz kişilerce "kill" komutu kullanımı ile kullanılamaz hale getirilmesi demektir [5].

Etiketlerin ait oldukları ve monte edildikleri bir objeden sökülerek ait olmadıkları yani tanımlamadıkları başka bir objeye monte edilmesi de veri güvenliğine zarar veren bir saldırıdır [5, 6].

Etiket ve okuyucu arasındaki frekansın bozulması radyo arayüzü (*radio interface*) üzerinden veri alış verişinin etiketlerin örtülmesi (*shielding*) (örn. etiketlerin üstlerinin metal folyolar ile örtülmesi) ya da parazit gönderme istasyonlarının (*jamming station*) radyo sinyallerini bozması yoluyla engellenmesidir [5].

Bir okuyucu sinyaline pek çok etiketin aynı anda sinyal göndermesi sinyallerin karışmasına ve başarısız bir iletişime neden olur. Bir okuyucu sinyalinin bir başka okuyucu sinyali ile karışması da söz konusu olabilir. İlgili literatürde sinyallerin karışması çarpışma (*collision*) olarak adlandırılır. Çarpışmaları önlemek için çarpışma önler protokoller (*anti-collision protocols*) kullanılır. Frekansların belirli bir süre ile belirli okuyucuların kullanımına ayrılması okuyucu sinyallerinin çarpışmasını önler. Örneğin zaman bölmeli çoklu erişim (*time division multiple access (TDMA)*) tekniği ile okuyucuların aynı zamanda değil belirlenmiş farklı zamanlarda ilgili frekansı kullanarak okuma işlemini gerçekleştirmeleri sağlanır [7]. Bir okuyucunun pek çok etiketten aynı anda gönderilen sinyaller ile teker teker iletişim kurmasını mümkün kılan protokollere seçme protokolü (*singulation protocol*) denir. RFID sistemleri çerçevesinde kullanılan önemli seçme protokolleri (ikili) ağaç dolaşma (*(binary) tree walking*) protokolü ve Aloha'dır [8]. Aloha protokolüne göre etiket sinyallerinin çarpışması söz konusu ise etiketler bir süre bekledikten sonra tekrar sinyal gönderirler. İkili ağaç dolaşma protokolüne göre olası tüm k bit uzunluğundaki etiket tanımlayıcıları/seri numaraları derinliği k olan standart bir ikili ağacın yaprakları olarak algılanır. Okuyucu ikili ağaçta özyineli derinlemesine aramaya benzer bir sorgulama ile etiketlerin seri numaralarını bit bit sorgulayarak etki alanındaki etiketler ile birer birer iletişim kurar. Protokole göre okuyucu etiketlerin ilk/bir sonraki bit değerini sorgular. Etiketlerden eğer iki farklı değer (0 ve 1) iletilirse bir çarpışma söz konusudur. Bu durumda okuyucu bir bit değeri (0 veya 1) göndererek bit değeri 0 mı yoksa 1 mi olan etiketin sorgulanmasına devam edeleceğini belirler. Bu şekilde ikili ağaçtan bir dal seçilmiş olur. Yapılan tercih ile ikili ağaçta bir seviye aşağı inilir. İkili ağaç içinde çarpışma noktası olarak tespit edilen her düğüme gidilerek yukarıda izah edilen sorgulama tekrarlanır. Böylece okuyucu etki alanındaki tüm etiketler ile birer birer iletişim kurar [7]. Uzunluğu 3 bit olan $2^3 = 8$ adet etiket seri numarası derinliği 3, kök seviyesi 0 olan bir ikili ağacın yapraklarında Şekil 4.'deki gibi gösterilir.



Şekil 4. İkili ağaç dolaşma protokolü örneği [8]

Örnekte okuyucunun etki alanında seri numaraları 001, 011 ve 110 olan etiketlerin mevcut olduğu varsayılır. Okuyucu etiketlerin ilk bit değerini sorgular bu sorguya 0 ve 1 değerlerini cevap olarak alır ki bu durumda bir çarpışma söz konusudur. Ağacın kökü ilk çarpışma noktasıdır. Şekilde daire içine alınmıştır. Okuyucu etiketlere cevap olarak 0 değerini gönderir. Bu gönderim ile seri numaralarının bit bit sorgulanmasına sol alt ağaçtan devam edileceği belirlenir. Okuyucu seri numarasının ikinci bit değerini sorgular, bu sorguya da hem 0 hem 1 değerini cevap olarak alır. Yine bir çarpışma söz konusudur. Bu çarpışma noktası da şekilde daire içine alınmıştır. Okuyucu 0 değerini gönderir bu durumda 0 olarak adlandırılan düğümün sol dalından sorgulamaya devam edilir ve üçüncü ve son bit değeri sorgulanır. Bu sorguya sadece 1 değeri cevap olarak alınır. Aynı zamanda ağaçta 001 olarak adlandırılan yaprağa ulaşılmıştır. Ulaşılan yaprak okuyucu tarafından okunacak etiketin seri numarasıdır. 011 ve 110 seri numaralı diğer iki etiketin seçilmesi ve okunması için şekilde daire içine alınmış olan çarpışma noktalarında yukarıda ilk etiket için izah edilen sorgulama tekrarlanır. Bu tekrarlamada ilk etiket için okuyucunun ağaçta hangi yönde devam edileceğini belirtmek üzere çarpışma noktalarında etiketlere gönderdiği bit değerlerinden farklı bit değerleri gönderilir. Örneğin kök çarpışma noktası olarak tanımlandığı için köke tekrar dönülür, etiket seri

numaralarının ilk bit değeri sorgulanır, gelen iki farklı bit değerine karşı okuyucu ilk bit değeri 1 olan etiket ile devam etmek istediğini belirtmek üzere 1 değerini etiketlere gönderir. Bu durumda kökün sağ alt ağacında sorgulama yürütülür. Seri numarasının ikinci bit değeri sorgulanır. Sorguya cevap olarak bit değeri 1 bildirilir. Çarpışma söz konusu değildir. Seri numarasının üçüncü bit değeri sorgulanır cevap olarak tekrar 1 değeri gönderilir. Bu sorgulama ile ikili ağaçta okuyucu tarafından okunacak ikinci etiketin seri numarasını içeren 110 olarak adlandırılmış yaprağa erişilmiş olur. Blocker tag'lar ağaç dolaşma protokolünü tamamen ya da kısmen bloke eden aletlerdir. Ağaç dolaşma protokolünün uygulandığı bir RFID sisteminde bir okuyucunun etki alanında bulunan ve seri numaralarının uzunluğu k bit olan etiketlerin ikili bir ağacın yaprakları olarak algılandığı yukarıda izah edilmişti. İkili ağaç yapraklarında maksimum 2^k adet seri numarası ifade edilebilir. Blocker tag kullanımı ile bir okuyucuya okuyucunun etki alanında gerçekte bulunan etiketten başka ikili ağaç yapraklarında olması mümkün 2^k adet etiketin simülasyonu ile 2^k adet etiketten sinyal gönderilmesi sağlanır. Bu tarz blocker tag'lara "full blocker tag" ya da "universal blocker tag" denir. Blocker tag okuyucunun yürüttüğü her sorgulamaya etiketlerden aynı anda 0 ve 1 sinyallerinin gönderilmesine ve çarpışma oluşmasına sebep olur. Yani ikili ağacın her düğümü bir çarpışma noktasına isabet eder. Eğer okuyucu yeterli belleğe, zamana ve işlem gücüne sahipse tüm ikili ağacı sorgular ve 2^k adet seri numarası dolaşma algoritmasının çıktısı olur. Seri numarasının k bit değeri artıkça sorgulanacak düğüm adedi de artar. Bu artış nedeni ile blocker tag kullanılması durumunda okuyucunun sadece birkaç yüz yaprağa eriştikten sonra durması beklenir. Sonuç olarak full blocker tag'lar tüm etiketlerin okunmasını bloke eder. Blocker tag'ların belirli etiketleri bloke edecek şekilde kullanılması da mümkündür. Bu tarz blocker tag'lara "selective blocker tag" ya da "partial blocker tag" denir. Örneğin bir selective blocker tag'ın kökün sol alt ağacı içinde ağaç dolaşma algoritmasının uygulanması sırasında okuyucuya çarpışmaya neden olur sinyal göndermesi ile sadece seri numaraları 0 ile başlayan etiketlerin okuyucular tarafından okunması engellenirken, seri numaraları 1 ile başlayan etiketler okunabilir. Blocker tag'lar kötü niyetle saldırı amaçlı kullanımları durumunda seçme protokolünün icrasına mani olurlar. Bu durumda okuyucu okuma işlemini gerçekleştiremez ve hizmetin kesilmesi söz konusu olur. Juels, Rivest ve Szydlo'ya göre bu tür saldırıları önlemek şu an için mümkün olmasa da bu saldırıların tespiti mümkündür. Örneğin bir RFID okuyucusunun algıladığı etiket sayısının makul eşiğin üzerine çıkması durumunda blocker tag saldırısı olması ihtimali üzerinde durulmalıdır [8].

Etiketlerin çalışamaz duruma getirilmesi, objelerden sökülmesi, blocker tag kullanımı ile okuyucunun bloke edilmesi, etiket ve okuyucu arasındaki frekansın bozulması ile iletişimin engellenmesi RFID sisteminin kullanımını engelleyen saldırılar olduğu için ilgili literatürde servis kullanımını engelleme saldırıları (*denial of service, DoS*) adı altında toplanır [9].
Etiketleri ancak yetkilendirilmiş okuyucular okuyabilir. Yetkilendirilmemiş bir okuyucunun etiketlerdeki bilgileri okumak amaçlı yetkilendirilmiş bir okuyucuyu tanımlayan verileri taklit etmesi de bir başka saldırı türüdür [5, 6].

Okuyucu ve anten arasındaki radyo arayüzü üzerinden gerçekleştirilen iletişimin radyo sinyallerinin deşifre edilmesi ile gizlice dinlenmesi de bir başka saldırı türüdür [5, 6].

RFID sistemlerinde izleme saldırıları saldırganların farklı noktalara yerleştirdikleri okuyucuların önlerinden geçen etiketli objelere ait verileri okumaları ve bu veriler arasında ilişki kurmak yoluyla hareket profilleri çıkarmaları, sosyal etkileşimleri tespit etmeleri, finansal işlemleri takip etmeleri şeklinde gerçekleştirilir [9].

Yönlendirme saldırısı saldırganın birbiri ile iletişim kurması gereken bir etiket ve okuyucunun birbirleri ile iletişim kurduklarını sanarken ayrı ayrı saldırgan ile iletişim kurmasını sağlaması ile gerçekleşir. Bu saldırı için saldırgan iki ek araca ihtiyaç duyar. Bunlardan ilki RFID okuyucusu ile iletişimi sağlayan, etiket gibi görünen ve "hayalet (*ghost*)" adı verilen araçtır. Diğeri ise etiket ile iletişimi mümkün kılan, okuyucu gibi görünen ve "sülük (*leech*)" olarak adlandırılan araçtır. Okuyucudan hayalete yapılan her talep sülüğe iletilir. Sülük bu talebi etikete iletilir. Gelen talebe karşı etiketten sülüğe bir cevap gönderilir. Sülük de bu cevabı hayalete iletir. Hayalet de cevabı okuyucuya gönderir. Hayaletten gelen cevap onaylanmış etiketten gelen doğru cevap olduğu için hayalet onaylanmış olur. Böylece hayaleti kullanan saldırgan erişimi sınırlı olan alana erişim hakkı elde eder [9, 10].

RFID kötücül yazılımları üç kategoride gruplanır: RFID korunmasızlık sömürücüleri (*RFID exploits*), RFID solucanları (*RFID worms*) ve RFID virüsleri (*RFID viruses*). RFID korunmasızlık sömürücüleri internette bulunan korsan saldırılara (örn. SQL enjeksiyonu (*SQL injection*), tampon bellek taşması (*buffer overflow*), araya kod sokma (*code insertion*)) benzer. RFID korunmasızlık sömürücülerinin bu saldırılardan farkı sömürücü saldırılarının kaydedildiği etiket belleğinin veri kapasitesinin küçük olabilmesidir. RFID solucanları ve virüsleri orijinal korunmasızlık sömürücüsü kodunu (*exploit code*) yeni RFID etiketlerine kopyalayan korunmasızlık sömürücüleridir. RFID solucanları ile virüsleri arasındaki fark solucanların yayılması için ağ bağlantılarına ihtiyaç duymaları virüslerin ise ağ bağlantısına gerek olmaksızın RFID sistemi aralığıyla kendi kendilerine yayılabilmeleridir. RFID kötücül yazılımları etiketler okunduklarında aktif hale gelir ve sisteminin ara katman yazılımına veya arka uçtaki veri bankasına geçerler. Sistemin güvenliği yeterince sağlanmamışsa sisteme bulaşan kötücül yazılım sistemin

zayıflığından yararlanır ve kendini diğer etiketlere kopyalar [9, 11].

5. GÜVENLİK ÖNLEMLERİ

Yukarıda izah edilmiş saldırıları engellemek ya da bu saldırıların etkilerini azaltmak amaçlı aşağıda sayılan önlemler uygulanabilir:

- Kimlik doğrulama (authentication)
- Kod saklama (cover-coding)
- Transfer edilen verinin şifrelenmesi (encryption of data in transit)
- Etikette kayıtlı verilerin şifrelenmesi (encryption of data stored on a tag)
- Kalkanlama (electromagnetic shielding)
- Press-to-activate anahtarının (press-to-activate switch) kullanımı
- "Kill" komutu kullanımı
- Kırılır etiketler (clipped tags) kullanımı
- Blocker tag kullanımı
- Aktif sinyal bozma yaklaşımı (active jamming)
- "Lock" komutu kullanımı
- Arka uçtaki veri bankasında (backend database) veri saklama
- Takma ad (pseudonym) kullanımı
- Dedektör kullanımı
- Frekans hoplaması (frequency hopping)
- Tekrar adlandırma yaklaşımı (renaming approach)
- RF sistemi kullanıcısı tarafından taşınan özel cihazlar
- Nizami önlemler (regulative countermeasures)

Kimlik doğrulama metodunda verilere erişim ancak başarılı bir kimlik doğrulama sonrası mümkündür. Etiket kimliği doğrulama, okuyucu kimliği doğrulama ya da çoklu simetrik kimlik doğrulama ile izinsiz okuma, veri tahrifi, etiket taklidi, "kill" komutunun kötüye kullanımı önlenebilir [5,6]. RF sistemlerinde kullanılan kimlik doğrulama metotlarına örnek olarak challenge-response metodu, parola kullanımı temelinde kimlik doğrulama (*password authentication*), hash temelli mesaj doğrulama kodu (*hash-based message authentication (HMAC)*), dijital imzalar (*digital signatures*) verilebilir.

Challenge-response metoduna göre metodu uygulayan taraflardan birinin onaylanması için metodu uygulayan diğer tarafca gönderilen soruya doğru cevap vermesi gerekir. RF sistemi içindeki bir etiketin sisteme ait olup olmadığının challenge-response metodu kullanımı ile kontrolünde öncelikle okuyucu etikete rastgele bir sayı (*random number*) gönderir. Bu işlem kimlik sorma (*challenge*) işlemi olarak adlandırılır. Etiket bu sayıyı şifreleyerek okuyucuya geri gönderir. Bu geri gönderim işlemi yanıtlama (*response*) olarak adlandırılır. Etiketin şifrelemede kullandığı anahtar etiketin kendi kimliğini ispat edebildiği ve okuyucu ve etiket tarafından bilinen ortak bir anahtardır. Okuyucu da etikete gönderdiği rastgele sayıyı ortak anahtarı kullanarak şifreler. Okuyucunun yaptığı şifreleme ile etiket tarafından gönderilen şifreleme uyumlu ise etiketin göz önüne alınan RF sistemine ait olduğu anlaşılır [5]. Okuyucular sadece yetkili etiketlerden gönderilen verileri doğru olarak kabul eder [6]. Bu metodun kullanımı ile etiket kimliğinin doğrulanması için etiketin kriptolojik fonksiyonları icra edebilmesi gerekir. Okuyucuların bu metot ile kimliklerinin doğrulanması için yukarıda etiketler için izah edilen gidiş yolunun tersten uygulanması gerekir. Bu metodun okuyucular tarafından kullanılması etiketlerin kriptolojik fonksiyonları icra edebilmesinin yanı sıra rastgele sayı üretebilme özelliğine de sahip olmaları durumunda söz konusudur [9]. Challenge-response metodunun etkinliği kullanılan anahtarın gizli tutulmasına ve her kimlik soruşta farklı bir rastgele sayının kullanılmasına bağlıdır [5].

Çoklu simetrik kimlik doğrulamada okuyucu etikete, etiket de okuyucuya kimliğini ispatlamak durumundadır. Okuyucudan gelen "get challenge" komutuna karşı ilgili etiket A rastgele sayısını üretir ve okuyucuya gönderir. Okuyucu da B rastgele sayısını üretir. Okuyucu A ve B rastgele sayıları ile bir şifreleme algoritması ve gizli bir anahtar K temelinde veri bloğu T'yi şifreler. Bu blok etikete geri gönderilir. Her iki tarafta aynı şifreleme algoritmasını kullandığı ve anahtar K etiket üzerinde kayıtlı olduğu için etiket veri bloğu T'yi çözebilir. Orijinal A rastgele sayısı ile deşifre edilmiş A' rastgele sayısı birbiri ile uyuşuyorsa okuyucunun yetkisi ispat edilmiş demektir. Bahsedilen süreç bir kez de etiketin yetkisini ispat için tekrarlanır. Bu amaçla etiket tarafından veri bloğu S üretilir ve okuyucuya iletilir. B rastgele sayısının deşifre edilmiş B' rastgele sayısı ile örtüşmesi durumunda etiketin okuyucu karşısında yetkisi ispat edilmiş demektir [5].

Etiket karşısında okuyucu kimliğinin ispatı için en basit çözüm parola kullanımıdır. Etiket okuyucudan alınan parolayı hafızasında kayıtlı parola ile karşılaştırır. Parolaların uyuşması durumunda etiket okuyucunun kayıtlı bilgilere erişimine izin verir [5]. Parola transferinin saldırganlar tarafından gizlice dinlenebilmesi ve öğrenilen parolanın daha sonra yetkisiz bir işlem yapmak üzere kullanılabilmesi [3,6] ihtimali nedeni ile bu metodun zayıf bir kimlik doğrulama metodu olduğu söylenebilir. Kısa parolaların kaba kuvvet atağı (*brute-force attack*) ile deneme yanılma usulüyle bulanabilmesi ihtimali de yüksektir. Bazı pasif etiketlerde güç analizi saldırılarıyla (*power analysis attacks*) parolalar kolayca açığa çıkarılabilir [3]. Bu önlem özellikle düşük maliyetli salt okunur etiketlerde uygulamaya uygun bir metottur. Pek çok etiket için aynı parolayı kullanmak yerine her etiket için ayrı parola kullanımı ile güvenlik artırılabilir [6].

HMAC bir mesaj doğrulama kodu (*message authentication code (MAC)*) türüdür. Bu metotta öncelikle gönderilecek olan mesaj N ve mesajı gönderen ve alan tarafından bilinen gizli bir anahtar (*secret key*) K'dan kriptolojik bir kıyım fonksiyonu (*cryptographic hash function*) kullanımıyla HMAC üretilir. Bu HMAC mesaj ile birlikte ilgili alıcıya gönderilir. Alıcı da gelen mesaj N'den ve elindeki gizli anahtar K'dan kıyım fonksiyonu

kullanımı ile bir HMAC hesaplar. Alıcının hesapladığı kod ile yani HMAC ile gönderenin kodunun aynı olması durumunda mesajın bütünlüğü ve doğruluğu teyit edilmiş olur. HMAC hesaplaması için MD5 (*message digest algorithm 5*), SHA-1 (*secure hash algorithm 1*) gibi bir kıyım fonksiyonu kullanılabilir. Bu metodun etkinliği anahtarın gizli kalmasına bağlıdır [3].

Asimetrik şifrelemeye dayanan dijital imza metodunda onay kurumu (*certification authority*) olarak tanımlanan okuyucu öncelikle bir özel (*private key*) bir de genel anahtar (*public key*) üretir ve uygun bir genel anahtar sertifikası temin eder. Bu okuyucu etiket tanımlayıcısının ve etiketteki olası diğer verilerin (örn. ürün üreticisini tanımlayan verinin) mesaj özünü (*message digest*) hesaplamak için özel bir kıyım algoritması kullanır, dijital imza oluşturmak amaçlı hesaplanmış mesaj özünü kendi özel anahtarı ile şifreler ve imzayı etikete kaydeder. Yetkili bir okuyucu ilgili etikete erişir, etiketteki dijital imzayı okur, dijital imzayı üreten okuyucunun genel anahtarını kullanarak imzayı deşifre eder ve bir mesaj özü elde eder. Söz konusu okuyucu ayrıca etiket tanımlayıcısından ve etiketteki olası diğer verilerden mesaj özünü kıyım algoritması kullanarak hesaplar. Hesaplanmış bu iki mesaj özünün birbiri ile aynı olmaması etiket verilerinin değiştirildiğini veya dijital imzanın yetkisiz bir okuyucu tarafından üretildiğini gösterir [3].

Kod saklama gizli dinleme saldırılarına karşı ileri yönde kanal (*forward channel*) üstünden transfer edilen verileri saklayan bir metottur. Bu metodun kullanıldığı EPCglobal birinci sınıf ikinci nesil etiketlerde okuyucu etikete etiketten bir anahtar istediğini bildirir bir mesaj gönderir, etiket anahtar olarak 16 bit'lik bir rastgele sayı üretir ve okuyucuya gönderir. Okuyucu bildirilen anahtar ile gönderilecek veriye özel veya (*exclusive-or, XOR*) operasyonunu uygulayarak şifreli veriyi üretir. Şifreli veri okuyucu tarafından etikete gönderilir. Etiket şifreli veri ve anahtara özel veya operasyonunu uygulayarak gönderilen veriyi deşifre eder [3].

Transfer edilen verilerin şifrelenmesi yaklaşımında etiketler üzerindeki veriler K isimli bir anahtar ile şifrelenerek taşınır. Verilerin işe yaraması için deşifre edilmesi gerekir. Veriler gönderildikleri yerde bir başka anahtar K' ile deşifre edilir. K ve K' aynı ise simetrik şifreleme kullanılmış demektir. K ve K' farklı ise asimetrik şifreleme yapılmış demektir. RFID sistemlerinde genelde simetrik şifreleme kullanılır. Gizli dinleme ile anahtarın öğrenilmesi ihtimaline karşı sözde rastgele sayı üreteci (*pseudo random number generator*) ile bulunan sözde rastgele sayılar (*pseudo random number*) anahtar olarak kullanılır. Bu sayılar ile orijinal veriye bir şifreleme fonksiyonu (örn. simetrik şifreleme fonksiyonu DES, 3DES) uygulanarak orijinal veri şifreli veriye dönüştürülür [12]. İzah edilen metot radyo arayüzü üzerinden gerçekleştirilen veri transferinin dinlenmesini önler bir metottur [3].

Etikete kaydedilecek verilerin kayıt işlemi öncesi şifrelenmesi ve şifrelenmiş verilerin etiketlere kaydedilmesi ile yetkisiz okuma saldırıları önlenebilir. Şifreli veriler etiket dışında ilgili okuyucu, ara katman yazılımı ya da kurumsal alt sistem tarafından deşifre edilir [3, 9].

Kalkanlama RF sisteminin bulunduğu mekanın ya da sistemin ilgili bileşenlerinin bir materyal ile korunması ve böylelikle radyo frekans sinyallerinin korunan alanın/bileşenin dışına yayılmasının sınırlandırılmasıdır. Bu metot ile gizli dinleme ya da izinsiz okuma işlemleri ile saldırganların RF sisteminden veri toplamaları engellenir [3].

Etiketlerde press-to-activate anahtarı kullanımı ile etiketler istendiğinde adı geçen anahtara basılarak aktif yani çalışır duruma getirilir. Anahtara basılmadığı sürece etiketler çalışamaz durumda bekler. Anahtara basılınca etiket radyo frekanslı iletişime katılabilir. Etiket aktif durumdayken anahtara basıldığında tekrar çalışamaz duruma geçer. Bu metot kullanıcıların etiketlerin okuyuculara ne zaman ve nerde cevap vereceğini kontrol etmelerini sağlar. Böylelikle izinsiz dinleme saldırıları ve izinsiz okuma/yazma işlemleri önlenir [3].

"Kill" komutu kullanımı ile etiketlerin etkinliğinin daimi olarak sonlandırılması mümkündür. Bu komut etiketler üzerindeki verilerin yetkisiz kişilerce okunmasını, izleme saldırılarını önler [13]. "Kill" komutunun yetkisiz kimselerce kullanımı etiketlerin istem dışı etkisiz hale getirilmesine neden olur. Komutun yetkisiz kişilerce saldırı amaçlı kullanımını önlemek adına komut bir kimlik doğrulama mekanizması ile kullanılmalıdır [6]. Örneğin EPC birinci sınıf ikinci nesil etiketlerde etiketi öldürmek için okuyucunun "kill" komutunu etikete spesifik 32 bit uzunluğundaki doğru PIN ile kullanması gerekir [14].

Kırılır etiketler kullanımı ile etiketlerin etkinliğini sonlandırmak ve yetkisiz kişilerce okunmasını, izlenmesini önlemek mümkündür. Bu tip etiketlerde kullanıcı etiketin antenini imha ederek etiketi çalışamaz duruma getirir [15].

Yukarıda DoS saldırısı amaçlı kullanılabileceği izah edilen blocker tag'lar aynı zamanda yetkisiz kişilerce etiketlerin okunmasını, izlenmesini önlemek amaçlı bir güvenlik önlemi olarak da kullanılabilir [9, 15].

Aktif sinyal bozma yönteminde rastgele radyo sinyalleri yayan bir radyo frekansı cihazı ile radyo kanalı rahatsız edilerek etiketlerin okunması, izlenmesi önlenir [8].

Parola korumalı kilitleme özelliğine sahip etiketlerde etiket belleklerinin okunması ve/veya bellekteki bilginin değiştirilmesi önlenebilmektedir. Bu tür etiketlerde kilitleme (*lock*) komutu kalıcı olarak ya da istendiği zaman devreye girecek şekilde etiketin tüm belleğine ya

da bellekte belirli bir bölgeye uygulanarak veri tahrifi, izinsiz okuma saldırıları önlenebilir [3].

Arka uçta bir veri bankasında veri saklama metoduna göre RFID etiketlerinde etiketleri tanımlayan veriler dışında herhangi bir veri saklanmaz. Etiketlenen objeyi ilgilendiren tüm veriler ekstern bir veri bankasında saklanır. Tanımlayıcı bir kod kullanımı ile ekstern veri bankasındaki verilere istenildiği zaman çok hızlı bir şekilde erişilebilir. Bu metot ile etiketlere yönelik olası fiziksel bir saldırıda verilerin zarar görmesi önlenmiş olur, bellek kapasitesi daha düşük ve dolayısıyla maliyeti daha uygun olan etiketler kullanılabilir, izinsiz okuma ve dinleme saldırıları önlenebilir [13].

Etiketlerin yetkisiz kişilerce okunmasını önlemek amaçlı takma ad kullanımı metodu da uygulanabilir. Takma ad kullanımı ile etiketlerin kimlikleri saklanır. Gerçek kimliği sadece yetkili okuyucular bilir. Hash-lock, randomized hash-lock, chained hashs takma ad kullanımına verilebilecek birkaç örnektir. Hash-lock metodunda etiket kilitlenir ve kilit çözülünceye kadar etiketin ID numarasına kimse erişemez. Geri döndürülemez bir hash fonksiyonu yardımı ile bir anahtardan etiket için takma ad olarak kullanılan Meta-ID üretilir ve etikete kaydedilir. Etiket bu işlemden sonra kilitlenir. Kilidi açmak için okuyucu etikete arka ucundaki bir veri bankasında sakladığı Meta-ID'ye ait bir anahtar veya PIN değeri gönderir. Etiket alınan anahtara hash fonksiyonunu uygular ve fonksiyon sonucunun kendi belleğinde kayıtlı Meta-ID ile aynı olup olmadığını kontrol eder. Meta-ID'lerin uyuşması durumunda etiketteki kilit çözülür ve okuyucunun etiketteki verilere erişimine izin verilir [5, 9]. Hash-lock metodunda Meta-ID etiketin kullanım ömrü boyunca aynı kaldığı için etiketlerin izlenmesi ihtimali mevcuttur. Bu nedenle ilgili literatürde hash-lock metodunun genişletilmesini öngören bazı metotlar geliştirilmiştir. Bunlardan biri randomized hash-lock metodudur. Bu metot her okuma işleminde yeni bir Meta-ID üretilmesi temeline dayanır. Bu amaçla etikete entegre edilen rastgele sayı üreteci (*random number generator*) etiketin ID numarası ile kıyılan rastgele sayıyı üretir. Rastgele sayı ve kıyım değeri (*hash value*) etiket tarafından okuyucuya gönderilir. İlgili etiketin ID numarasını hesaplamak için okuyucuyu kullananın göz önüne alınan RFID sistemine ait tüm etiketlerin ID numarasını bilmesi gerekir. Okuyucu ta ki gönderilen kıyım değeri ile örtüşen kıyım değerini bulana kadar etiket tarafından üretilmiş rastgele sayıyı kullanarak bilinen tüm ID numaralarının kıyım değerlerini hesaplar [5, 12, 13]. Bir başka metot chained hashs metodudur. Bu metotta etiket her aktive oluşunda iki farklı kıyım fonksiyonu ile yeni bir Meta-ID hesaplar. İlk Meta-ID yeni bir Meta-ID üretmek için kıyılır. Kıyılmış bu Meta-ID daha sonra ikinci kıyım fonksiyonu kullanılarak tekrar kıyılır. İkinci Meta-ID okuyucuya iletilir. Okuyucu kodu çözmek için etiket tarafından iletilen Meta-ID ile uyuşan kıyım değerini buluncaya kadar kıyım işlemini sürdürür [5].

İzinsiz okuma, veri tahrifi saldırıları yetkisiz okuyucuları tespit edebilen detektörler yardımı ile de önlenebilir [6].

Etiketlerin monte edildikleri objelerden sökülmesini önlemenin birkaç yolu vardır. Etiketler saldırganın kolayca bulamayacağı yerlere monte edilebilir. Etiketler etiketin sökülmesinin objeye zarar vereceği şekilde objelere monte edilir. Aktif etiket kullanılıyorsa bir sensör yardımı ile etikete müdahale edildiği bilgisi etikete kaydedilir ve bu bilgi bir okuyucunun kapsama alanına girilir girilmez okuyucuya alarm mesajı olarak gönderilebilir. Değerli objeler için etiketin yanı sıra barkod da kullanılabilir. Barkod ile etiket arasındaki ilişki verileri arka uçtaki bir veri bankasında kaydedilir. Manuel bir kontrol ile etiketin doğru objede bulunup bulunmadığı kontrol edilebilir [5].

Okuyucu ve etiket arasındaki frekansı bozmaya yönelik saldırılar parazit istasyonlarından gönderilen sinyalleri tespit edebilecek detektörler kullanımı ya da taşıyıcı frekansının kısa aralıklarla sürekli değiştirildiği bir yaylı spektrum yöntemi olan frekans hoplaması metodu ile önlenebilir [5].

Etiketlerin "kill" komutunun yetkisiz şekilde kullanımı ile çalışamaz duruma getirilmesini önlemek için yukarıda da izah edildiği gibi "kill" komutu uygun bir kimlik doğrulama mekanizması ile uygulanabilir. Etiketlerin çalışamaz durumu getirilmesini önlemek için etiketler saldırganın kolayca bulamayacağı yerlere monte edilebilir ya da etiketin sökülmesinin objeye zarar vereceği şekilde objelere monte edilir [6]. Etiketlerin elektromanyetik etki ile çalışamaz duruma getirilmesini önlemek için kırılma noktası (*predetermined breaking point*) yaklaşımı uygulanabilir [5]. Aşırı bir yüklemede bir sistemin daha büyük bir zarara uğramasını önlemek adına sistemin bir parçası tahrib edilebilir [16]. Kırılma noktası parçanın tahrib edileceği noktayı/zamanı gösterir.

Etiketlerin objelerden sökülmesi, etiketlerin çalışamaz duruma getirilmesi (örneğin "kill" komutu, kırılır etiketler kullanımı), tekrar adlandırma yaklaşımı ve bazı özel cihazların kullanımı ile de izleme saldırıları önlenebilir [5].

Etiket tanımlayıcılarının şifrelenmesi ile izleme saldırılarını önlemek mümkün değildir. Şifrelenmiş tanımlayıcılar statik verilerdir ve izleme saldırısını yapana bir mana ifade etmeseler de saldırıyı gerçekleştirmelerine herhangi bir engel teşkil etmezler. Yeniden adlandırma yaklaşımına göre tanımlayıcılar sık aralıklarla değiştirildiğinde ya da saklandığında izleme saldırıları engellenebilir. Yeniden adlandırma yaklaşımı çerçevesinde uygulanabilecek metotlar minimalist kriptoloji (*minimalist cryptography*), tekrar şifreleme (*re-encryption*), genel şifreleme (*universal re-encryption*) ve bozulmaz şifrelemedir (*insubvertible re-encryption*).

Minimalist kriptoloji metoduna göre her etiket belli sayıda takma ad içerir. Etiket her okuyucu sorgulaması

sonrası sırayla bu takma adlardan birini kullanır. Yetkili okuyucu etiketin tüm takma adlarını önceden kaydetmiş olduğu için erişmeye çalıştığı etikete erişim ile ilgili bir sorun yaşamaz [14].

Yeniden şifreleme metodu bir çift anahtar PK (genel ya da açık anahtar) ve SK'yı (gizli ya da özel anahtar) kullanır. SK uygun bir yürütme vekilliğinin (*law enforcement agency*) idaresindedir. Bu metoda göre bir etiket S olarak adlandırılan tek bir tanımlayıcıya sahiptir. S, PK'nın kullanımı ile şifreli metin (*cipher text*) C'ye dönüştürülür. Etiket okuyucu sorgulamasına C'yi cevap olarak gönderir. Sadece SK'ya sahip olan yürütme vekilliği C'yi deşifre edebilir ve etiket tanımlayıcısı S'yi öğrenebilir. Bu metot izleme saldırılarını önlemek için C'nin belirli aralıklarla yeniden şifrelenmesini öngörür. Bu işlem için PK ile programlanmış yeniden şifreleme okuyucuları kullanılır. Bu okuyucular düz metin (*plain text*) S'yi değiştirmeden PK'yı kullanarak şifreli metin C'yi şifreli metin C"ye dönüştürür. İstenmeyen bir yeniden şifreleme işlemini önlemek adına etiketlerin optik yazım-erişim anahtarı (*optical write-access key*) taşımaları öngörülür [14].

Genel yeniden şifreleme metodu da tıpkı yukarıda izah edilen yeniden şifreleme metodunda olduğu gibi düz metni değiştirmeden şifreli metin C'yi şifreli metin C"ye dönüştürür. Ancak yukarıdaki metottan farklı olarak yeniden şifreleme işlemi şifrelenecek olan şifreli metnin hangi genel anahtar ile şifrelendiğini bilmeksizin gerçekleştirilir. Tek bir genel anahtar kullanımı yerine yeniden şifrelenecek şifreli metni alan okuyucunun genel anahtarı yeniden şifreleme işlemi için kullanılır. Bu metodun uygulanması sonucu elde edilen şifreli metinleri deşifre etmek için metinlerin gönderildiği okuyucuların şifreli metinlerden kendilerine gönderilen metni bulmaları ve kendi özel anahtarlarıyla deşifre etmeleri gerekir [17]. Bir saldırgan genel yeniden şifreleme metodunda şifreli bir metni yeniden şifrelemek yerine düz metni değiştirerek yepyeni bir şifreli metin oluşturabilir. Yani veri bütünlüğünü bozabilir. Bunu önlemek adına genel yeniden şifreleme metodunda şifreli bir metnin bir onay kurumu (*certification authority*) tarafından dijital olarak imzalanabildiği ve ilgili düz metnin bütünlüğünün doğrulanmasının mümkün olduğu bozulamaz şifreleme metodu uygulanabilir [14].

Etiketlere erişim RF sistemi kullanıcıların taşıyacağı watchdog tag, RFID koruyucusu (*RFID guardian*) gibi özel cihazlar ile de temin edilebilir. Watchdog tag'ın amacı bu cihaza yakın olan okuyucu sinyallerinden okuyucular hakkında bilgi edinmektir (örn. okuyucu tanımlayıcısını (*reader identifier*) öğrenmek). RFID koruyucusu yakınındaki etiketlere sadece kimliği doğrulanmış okuyucuların erişimine izin verir. Yetkisiz bir okuyucunun etikete erişimi sinyal bozma ya da seçici bloklama (*selective blocking*) gibi metotların uygulanması ile engellenir [18].

Yönlendirme saldırıları okuyucu ve etiket arasındaki iletişimde gecikmeler oluşturur. Okuyucu ve etiket arasındaki sorgulama ve cevaplama işlemi sırasında icra edilen iletişimin zamanlama kısıtları sıkıştırılırsa yönlendirme saldırılarının icrası zorlaşır. Bunun için mesafe sınırlama protokolleri (*distance bounding protocol*) kullanılır [10]. Bu protokollere bir örnek Hancke ve Kuhn [19] tarafından verilmiştir. Tüm mesafe sınırlama protokolleri gibi bu protokol de hiçbir şeyin ışıktan daha hızlı hareket edemeyeceği prensibine dayanır. Sorgulama cevaplama işlemi için okuyucu ve etiket arasında sinyal gidiş geliş zamanının ölçümü ile okuyucu ve etiket arasındaki mesafenin üst limiti hesaplanabilir. Etiketler okuyuculara belirlenmiş mesafede bulundukları zaman belirlenmiş süre içinde cevap gönderebilirler ve ancak o zaman onaylanabilirler. Ancak sahte olmayan bir etiket gönderilen bir sorguya doğru cevap verebilir. Hayaletler sorguyu sülük üzerinden gerçek etiketlere iletmeden doğru cevabı okuyucuya iletemezler ve hakiki etiketleri taklit edemezler. Kullanılan protokol sayesinde hayalet ve sülük arasındaki radyo sinyali bağlantısının oluşturduğu erteleme okuyucunun hayaletin erişim çabasını reddetmesine neden olur. Böylelikle yönlendirme saldırısı önlenmiş olur [19]. Yönlendirme saldırıları etiketlerin kalkanlanması ile de önlenebilir. Etiketlerin örneğin mekanik ya da biyometrik bir uyarıcı (*activator*) kullanımı ile kullanıcılar tarafından aktif hale getirilmesi de bir başka önlemdir. Ayrıca iki faktörlü doğrulama (*two-factor-authentication*) yöntemi ile de yönlendirme saldırıları önlenebilir. Bu yöntemde erişime hak kazanmak için kullanıcının RFID etiketine sahip olduğunu ispatlamasının yanı sıra gizli bir bilgiyi (örn. PIN) bildiğini de ispatlaması gerekir [10].

RFID kötücül yazılımları herhangi bir IT sistemine uygulanabilecek kötücül yazılımlardan farklı olmadığı için RFID kötücül yazılımlarını önlemek için kötücül yazılımları önler bilindik metotlar uygulanır [10]. Örneğin SQL enjeksiyon saldırılarını önlemek için sisteme yapay zeka özellikleri içeren bir yazılım olarak geliştirilmiş bir onaylayıcı (*validator*) modülü eklenebilir. Bu onaylayıcının kontrolü ile SQL saldırıları önlenebilir [20]. Senaryo dilinde (*scripting language*) yazılmış verileri içeren RFID etiketlerle arka uçtaki RFID ara katman yazılımına kod araya sokma şeklinde yapabilecek saldırıları önlemek için örneğin arka uçta senorya dilinin şeçilemez kılınması mümkündür [10].

Veri gizliliğinin temini için bazı nizami önlemler de öngörülebilir. Bu tarz önlemlere önemli bir örnek Garfinkel'in "RFID Bill of Rights" adlı bildirisidir. Bu bildiriye göre RFID etiketli ürünleri satın alan tüketicilerin aşağıdaki haklara sahip olmaları gerekir [21]:

- Tüketiciler bir ürünün RFID etiketi olup olmadığını bilmek hakkına sahiptir.
- RFID etiketli ürünü satın alan tüketici etiketin sökülmesini veya etkisiz hale getirilmesini isteme hakkına sahiptir.

- Tüketici RFID etiketli ürünü almamayı tercih etse de ya da "kill" komutunun kullanımı ile etiketi etkisiz hale getirtse de ürün ile ilgili diğer haklarını (örn. ürünü iade etmek gibi) kaybetmemelidir.
- Tüketici aldığı ürünün etiketi üstünde hangi bilgilerin kaydedildiğini bilmek hakkına sahiptir.
- Tüketici RFID etiketinin ne zaman, nerde ve ne için okunduğunu bilmek hakkına sahiptir.

6. GÜVENLİK ÖNLEMİ SEÇİMİ

Yukarıdaki açıklamalardan da anlaşılacağı üzere bir saldırıyı önlemek için genelde birden fazla metot mevcuttur. RFID sistemi kullanıcısı sistemde kullanılan etiketin kriptolojik operasyonları icra edebilme kapasitesini, öngörülen operasyon süresini, metodun dezavantajlarını, sebep olacağı ek maliyetleri dikkate alarak kendisi için en uygun metodu seçmeli ve uygulamalıdır.

Bellek kapasiteleri, hesap güçleri düşük olan ve dolayısıyla bedelleri 1 US Dolar'dan az olan RFID etiketleri düşük maliyetli etiketler olarak adlandırılır [22]. Bu tür etiketlerde komplike kriptolojik fonksiyonların kullanımını gerektiren metotlar kullanılamaz. Buna karşın daha pahallı olan mikroişlemcili etiketler düşük maliyetli etiketlerden daha fazla belleğe ve özel güvenlik mekanizmalarına sahiptir. Bu tarz etiketleri kullanan kullanıcılar için kriptolojik fonksiyonların icrasını gerektiren güvenlik metotlarını kullanmak sorun olmaz [9].

Operasyon süresi ile anlatılmak istenen RFID sistemi tarafından gerçekleştirilen okuma/yazma işlemleri için öngörülen süredir ki bu süre sistemin adı geçen işlemleri gerçekleştirmedeki hızını gösterir. HMAC, dijital imzalar gibi kriptolojik fonksiyonların uygulanmasını gerektiren metotlar bu fonksiyonların icrası için gerekli süre nedeni ile okuma ve yazma işlemlerinde gecikmeye neden olur. Bu durum RFID sistemin hızını negatif etkiler [3].

Her metodun dezavantajları iyi bilinmeli ve bu dezavantajlar metot seçiminde mutlaka dikkate alınmalıdır. Örneğin "kill" komutu kullanarak etiketleri çalışamaz duruma getirmeyi ve izleme saldırılarını önlemeyi arzulayan kullanıcı bu komutun kullanımının etiketlerin daha sonra kullanımı ile sağlanabilecek avantajlardan (örn. bakım, değiştirme veya geri dönüşüm çerçevesinde ürün verilerine duyulan ihtiyaç ve verilerin kullanımı) yararlanılmasını engelleyeceğini bilmelidir. Yine bu komut ile etiketlerin üzerindeki verilere RFID sistemi ile ulaşmak imkansız hale gelse de etikete fiziksel olarak erişim sağlayan biri etiket hafızasındaki verileri okuyabilir [3]. RFID koruyucusunu izleme saldırılarına karşı kullanmayı arzulayan kullanıcı bu cihazların enerji kaynağının pil olduğunu, etiketlere sürekli sinyal gönderen bir saldırganın taleplerinin koruyucu tarafından bloke edileceğini ve sürekli olarak icra edilen bu işlemin koruyucunun enerjisini tüketebileceğini dolayısıyla bir süre sonra koruyucunun devre dışı kalması ile etiketlerin korumasız kalabileceğini unutmamalıdır [10].

Tercih edilen metodun kullanıcıya ne kadar bir ek maliyet getireceği de dikkate alınmalıdır. Örneğin blocker tag ya da RFID koruyucusu kullanmak isteyen kullanıcıların bu aletleri edinmenin maliyetini dikkate alması gerekir.

7. SONUÇLAR

RFID sisteminin veri güvenliğini tehdit edebileceği endişesini taşıyan ve bu sistemin kullanımına sıcak bakmayan tüketiciler ve şirketler vardır. Etiketlenmiş objeleri kullanan tüketiciler ya da kullanabilecek olan potansiyel tüketiciler sisteme yapılabilecek bir saldırının veri gizliliğine ve lokasyonel gizliliğe zarar vereceği endişesi ile RFID sistemi kullanımına karşı çıkarlar. Bunlar örneğin bir RFID sistemi içinde kaydedilmiş kişisel bilgilere istenmeyen kişilerin erişilebileceği, etiketlerin uzunca bir süre aynı kişinin kullanımında kalması durumunda etiketi tanımlayan ID numarasının pek çok kez okunması sonucu söz konusu kişi hakkında hareket profili çıkarılabileceği yani kişinin takip edilebileceği, pek çok kişinin takibi ile ilişki/bağlantı profillerinin çıkarılabileceği gibi endişelere sahiptir [5]. Bu tarz endişeler RFID etiketli objeleri tüketen, tüketme potansiyeli olan tüketicileri rahatsız etmekte ve RFID kullanımına karşı protestolar oluşmasına neden olmaktadır. Bu protestolardan etkilen şirketler RFID sistemi kullanımına sıcak bakmayabilir. Ayrıca sistemi kullanacak şirketler veri güvenliğinin saldırılar ile tehdit edilebileceği düşüncesi nedeniyle sistemi kurmakla ilgili endişeye sahip olabilir. Bunun yanı sıra şirketler RFID sistemin işlevselliğine zarar verecek yani çalışmasını engelleyecek bir saldırının sistemin desteklediği süreçleri kesintiye uğratabileceği endişesini taşıyabilir. Yukarıda izah edilmiş olan önlemler bahsedilen endişelerin ortadan kaldırılması ve RFID sistemi kullanımının yaygınlaşmasına katkı sağlayan önlemlerdir. Bu bağlamda RFID sistemlerini planlarken olası saldırılar tahmin edilmeli ve izah edilmiş olan önlemlerden uygun olanları seçilerek uygulanmalıdır.

KAYNAKLAR

[1] M. Strassner, **RFID im Supply Chain Management – Auswirkungen und Handlungsempfehlungen am Beispiel der Automobilindustrie**, Deutscher- Universitätsverlag, Wiesbaden, 2005.

[2] K. Pommerening, **Datenschutz und Datensicherheit**, Johannes-Gutenberg Universität Mainz, http://www.staff.uni-mainz.de/pommeren/Artikel/ds.pdf, Erişim Tarihi: 15.03.2008.

[3] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, **Guidelines for Securing Radio Frequency Identification (RFID) Systems – Recommendations of the National Institute of Standards and Technology (NIST)**, NIST Special Publication 800-98, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg 2007.

[4] D. Schmidt, **RFID im Mobile Supply Chain Event Management -Anwendungsszenarien, Verbreitung und Wirtschaftlichkeit**, Gabler Verlag, Wiesbaden, 2006.

[5] BSI (Bundesamt für Sicherheit in der Informationstechnik), Empa (Eidgenössische Materialprüfungs- und Forschungsanstalt), IZT (Institut für Zukunftsstudien und Technologiebewertung GmbH), **Risiken und Chancen des Einsatzes von RFID-Systemen**, http://www.bsi.de/fachthem/rfid/RIKCHA.pdf, Erişim Tarihi: 16.03.2008.

[6] S. Stadlober, **An Evaluation of Security Threats and Countermeasures in Distrubuted RFID Infrastructures**, Magisterarbeit, Institut für Informationssysteme und Computermedien, Technische Universität Graz, Juli 2005.

[7] B. Johansson, **An introduction to RFID – Information Security and Privacy Concerns**, http://www.ida.liu.se/~TDDC03/oldprojects/2004/final-projects/prj031.pdf, Erişim Tariki: 06.04.2008.

[8] A. Juels, R. L. Rivest, M. Szydlo, **The Blocker Tag – Selective Blocking of RFID Tags for Consumer Privacy**, http://interval.hu-berlin.de/downloads/rfid/prevention/JuelsRivestSzydlo-TheBlockerTag.pdf, Erişim Tarihi: 06.04.2008.

[9] Fraunhofer-Institut für Sichere Informationstechnologie, Fachgebiet Mikroelektronische Systeme der Technischen Universität Darmstadt, Technologie-Zentrum Informatik der Universität Bremen, **RFID-Studie 2007 – Technologieintegrierte Datensicherheit bei RFID-Systemen**, http://www.sit.fraunhofer.de/Images/RFID-Studie2007_tcm105-98165.pdf, Erişim Tarihi: 28.02. 2008.

[10] T. Haver, Security **and Privacy in RFID Applications**, Master Thesis, Norwegian University of Science and Technology, Department of Telematics, Trondheim, 2006.

[11] M. R. Riebeck, B. Crispo, A. S. Tanenbaum, **RFID Malware - Truth vs. Myth**, http://www.cs.vu.nl/~ast/publications/ieeesp-2006.pdf, Erişim Tarihi: 13.03.2008.

[12] Y.R.Michel, **RFID-Techologie**, http://page.mi.fu-berlin.de/ymichel/RFID_article.pdf, Erişim Tarihi: 10.04.2008.

[13] W. Franke, W. Dangelmaier, **RFID - Leitfaden für die Logistik - Anwendungsgebiete, Einsatzmöglichkeiten, Integration, Praxisbeispiele**, Gabler Verlag, Wiesbaden, 2006

[14] A. Juels, **RFID Security and Privacy: A Research Survey**, http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf, Erişim Tarihi: 17.04.2008.

[15] C. Balling, **RFID und Privatheit**, Seminarbeit, Universität Karlsruhe, Fakultät für Informatik, 2006.

[16] İnternet: http://de.wikipedia.org/wiki/Sollbruchstelle, Erişim Tarihi: 12.04.2008.

[17] P. Golle, M. Jakobsson, A. Juels, P. Syverson, **Universal Re-Encryption for Mixnets**, http://www.syverson.org/univrenc-ctrsa.pdf, Erişim Tarihi: 17.04.2008.

[18] J. A. Vilella, A. Martínez-Ballesté, A. Solanas, **A Brief Survey on RFID Privacy and Security**, http://crises-deim.urv.cat/~asolanas/Site/Publications_files/WCE2007_Solanas_CameraReady.pdf, Erişim tarihi: 23.04.2008.

[19] G. P. Hancke, M. G. Kuhn, "An RFID Distance Bounding Protocol", **Proceedings of IEEE / Create –Net SecureComm 2005**, Athens, Greece, 67-73, 5-9 September 2005.

[20] M. Kış, T. E. Kalaycı, **RFID Infrastructure and AI Approachs for Security**, http://yzgrafik.ege.edu.tr/~tekrei/dosyalar/yayinlar/RFIDEurasia2007.pdf, Erişim Tarihi: 14.04. 2008.

[21] E. Korkmaz, A. Üstündağ, M. Tanyaş, "Standards, Security & Privacy Issues about Radio Frequency Identification (RFID)", **4th International Logistics and Supply Chain Congress**, İzmir, 353-360, November 29-30 and December 1, 2006.

[22] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, **Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems**, http://www.eicar.org/taskforces/rfid/infomaterial/SecurPrivAspectsRFID.pdf, Erişim Tarihi: 17.04.2008.