RFID SİSTEMLERDE GÜVENLİK AÇIKLARI ve ÇÖZÜM YOLLARI

Emre Çiftçibaşı
Sistem Mühendisi, STM A.Ş

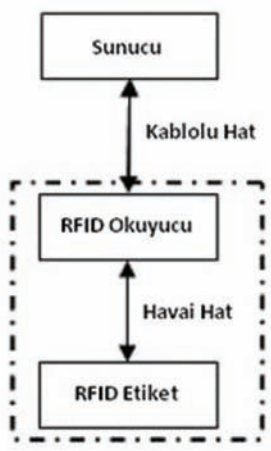
RFID (Radio Frequency Identification-Radyo Dalgası ile Tanımlama) sistemleri, elektronik etiketlerin malzemelere entegrasyonu sonucu, etiket belleklerinde kayıtlı bilgilerin belirli mesafelerden okunması esasıyla çalışır. İlk olarak 1940'larda uçaklarda dost-düşman (FoF-Friend or Foe) tanımlanması amacıyla kullanılan RFID teknolojisi, 2000'li yıllarla birlikte maliyetlerin düşmesi ile birlikte, tedarik zincirinde envanter görünürlüğü ve doğruluğu sağlaması sayesinde, barkod teknolojisinin yerini hızla almaya başlamıştır. Literatürde RFID teknolojisinin barkod sistemlerine olan üstünlüğünün detaylandırıldığı çok sayıda makale mevcuttur. Barkod teknolojisi fiziksel ortam koşullarından etkilenmekte, iyi planlanmış RFID sistemler ise çevresel şartlardan etkilenmemekle birlikte envanterdeki tüm malzemeleri aynı anda okuyup yazabilmektedir.

Otomatik Tanıma ve Veri Toplama (OT/VT) Sektöründe yaygınlaşan RFID envanter sistemleri, tedarik zincirinin tüm safhalarında malzeme bilgilerinin otomatik olarak okunması, kaydedilmesi ve bilgi görünürlüğünün sağlanmasını hedeflemektedir. Pasif RF etiket maliyetlerinin düşmesi ve malzemelerin üretici firmalar tarafından kendiliğinden pasif RF etiketli olarak üretilmeye başlanması sonucunda, RFID sistemler başta ABD olmak üzere tüm dünyada olduğu gibi ülkemizde de yaygın kullanım bulmuştur.

Yeni nesil pasif RFID (pRFID – bataryasız RFID etiketli) sistemlerde, maliyetin düşürülmesi sebebiyle, akıllı kartlar gibi gelişmiş bir kriptoğrafi (DES, 3DES, AES, ECC) teknolojisini barındıracak bellek ve enerji mevcut değildir. Güvenli bir pRFID sistem tasarımı için, mevcut sistem güvenlik açıkları ihtiyaca yönelik olarak incelenmelidir.

RFID sistemlerin güvenliği en zayıf bölgesi olan havai hattan maruz kalınan tehditler: Hattın Dinlenmesi, Hattaki Bilginin Değiştirilmesi, Bilgilerin Yetkisiz Okunması, Etiketin Kopyalanması, Havadan Gönderilen Bilgilerin Yetkisiz Tekrar Edilmesidir. Bu kapsamda maliyeti asgari seviyede sabitleyerek yapılabilecek en iyi havai hat güvenlik yöntemi okuyucu doğrulanması yöntemidir (Reader Authentication).

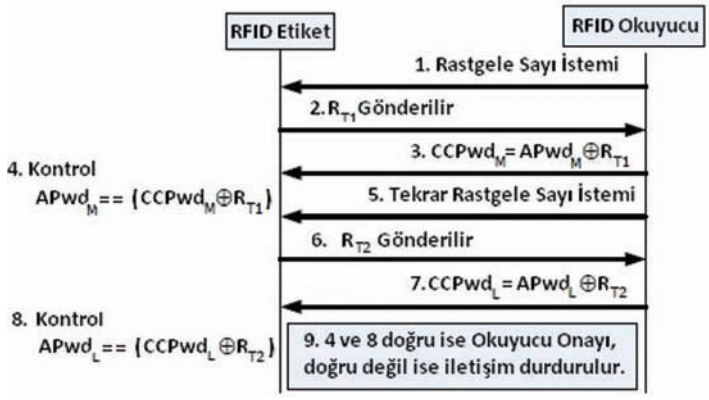
Okuyucu doğrulanması yöntemi, etiketin belleğindeki tüm bilgileri havai hat üzerinden göndermesi öncesinde okuyucunun bu bilgilere erişim yetkisinin olup olmadığının, okuyucu üzerinden güvenli ve kablolu bir hat üzerinden erişim sağlanan bir arka plan veritabanı sunucusundan sorgulanması ile sağlanır. (Şekil-1)



Şekil 1. RFID Güvenlik İhtiyacı

İkinci nesil pasif RFID sistemlerde temel güvenlik yetkilendirmesi amacıyla şifre sorgulama yeteneği mevcuttur. Fakat okuyucu-etiket iletişimi başlarken erişim şifresinin sorgulanması sırasında RFID etiketin kimlik ve şifre amacıyla havai hattan gönderdiği rastgele sayının (pseudo random number) kodlanmadan açık bir şekilde aktarılması sebebiyle pasif RFID sistemlerin esas güvenlik açığı oluşmaktadır. (Şekil-2)

Güvenlik açığının kapatılabilmesi amacıyla kullanılan ilk yöntem, 2 ve 6 nolu adımlardaki rastgele sayının xor işlemine tabi tutulacağı 16 bitlik ilk erişim şifresinin (APwd) okuyucuda değil, arka plan sunucusunda saklanması ve bilgilerin okuyucuda tekrar şifrelenerek kablolu



Şekil 2. EPC Sınıf 1 Nesil 2 Haberleşme Modeli

hat güvenliğinin havai hatta uygulanması yöntemleridir. Fakat standart olarak okuyucularda bu tür kabiliyetler mevcut olmaması sebebiyle, RFID etiket-okuyucu arası haberleşme sağlayan düşük seviye (low level) işlemler için, RFID okuyucu firmware yazılımının ihtiyaca göre güncellenmesi sonrası etiketlerle havai hat haberleşmesi için yeni algoritmalar geliştirilmesi gereklidir.

Güvenli kablolu hat için ise RFID Güvenlik Çerçevesi oluşturulmuştur. RFID Güvenlik Çerçevesi, okuyucu ile bilgi sunucusu arasında karşılıklı yetkilendirmeyi sağlayan ayrı bir yetkilendirme sunucusu kullanılması ve okuma/yazma işlemleri öncesinde yetkilendirme sunucusu tarafından izin verilmesi esasıyla çalışır. (Şekil-3)

RFID Güvenlik Çerçevesi çalışma esasları aşağıda listelenmiştir:

1- EPCVS (Electronik Product Code Veritabanı Sunucusu), yetkilendirme sunucusundan isim yetki sertifikası talep eder.

2- Yetkilendirme sunucusu EPCVS'nin isim yetki sertifikasını alır, kaydeder, yetkilendirme sunucusu anahtarını şifreler ve EPCYS'ye gönderir.

3- EPCVS aldığı verinin şifresini çözer ve EPCVS tarafından erişilebilecek yetki seviyelerine göre yetkilendirme sertifikasını yetkilendirme sunucusuna şifreli olarak gönderir.

4- Güvenlik Çerçevesi uygulama kullanıcıları her EPCVS'ye erişim istemlerinde, kendi isim sertifikalarını yetkilendirme sunucusuna gönderirler.

5- Yetkilendirme sunucusu kullanıcının isim sertifikasını kaydeder ve şifreleyerek kullanıcıya gönderir.

6- Yetkilendirme sunucusu kullanıcının yetkilerini isim sertifikasına ve sistem süreçlerine göre oluşturur, gerekli EPCVS yetki sertifikasını şifreler ve kullanıcıya gönderir.

7- Kullanıcı EPCVS yetki sertifikasını ve kendi isim sertifikasını şifreleyerek EPCVS'ye gönderir.

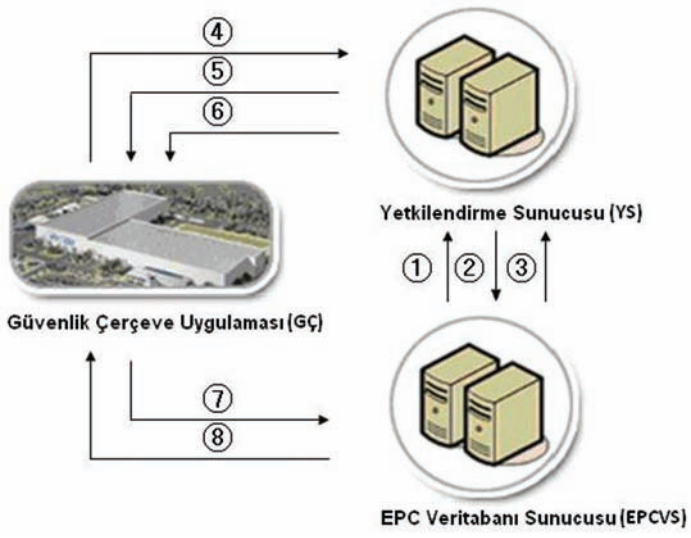
8- EPCVS aldığı verilerin şifrelerini çözerek yetkileri isimlerle kontrol eder, sonucu kullanıcıya gönderir.

Havai hat ve kablolu hatlarda güvenlik sağlanmasında özel mühendislik çalışmaları gereklidir. EPC Gen2 olarak bilinen pasif RFID etiketler üzerinde yalnızca rastgele sayı üreteci ve CRC kontrol işlemleri gerçekleşebilmekte ve 32 bitlik bir şifre koruması mevcuttur. Okuyucu doğrulama algoritması içermeyen bir sistemde, 32 bitlik erişim şifresinin standart bir RFID okuyucu ile azami 30 dakika gibi bir sürede kırılabildiği düşünüldüğünde, RFID sistemlerin güvenlik gerektiren durumlarda yüksek kriptoğrafi kullanılmış bir güvenlik çerçevesi üzerine entegre edilecek bir okuyucu doğrulanması algoritmasını içerecek şekilde tasarlanmalarının gerektiği değerlendirilmektedir.

Alternatif olarak EPCVS (EPC Veritabanı Sunucusu) üzerinde ve etiketlerde malzeme bilgilerinin hash edilerek saklanması değerlendirilmektedir. Hash edilmiş bilgilerin saklandığı bir RFID sistemde, erişim şifresi kırılsa dahi malzemelerin tanımlanması engellenebilecektir. Hash yöntemiyle uzun mesafeden malzeme bilgilerine erişim engellendiğinde, fiziksel güvenlik tedbirlerinin de uygulanması ile bilgiler değiştirilmeye ve kopyalanmaya karşı korunabilecektir. Sistem bütününde güvenlik sağlanması amacıyla, havai hat ve fiziksel güvenlik tedbirlerinin birlikte kullanılmasıyla, özel mühendislik çalışmalarının yapılmasının gerekliliği, RFID haberleşme standartlarını belirleyen EPCglobal kuruluşu tarafından vurgulanmıştır.

RFID sistemlerin güvenli hale getirilmesi için bilgi üreten ulusal kuruluşların, sanayinin ve akademinin birlikte çalışması gereklidir. Ülkemizde ve tüm dünyada güvenli RFID sistem geliştirme çalışmaları halen devam etmektedir. Bu geliştirme sürecinde en büyük aşama, pasif RFID teknolojisini kullanan güvenli bir pilot RFID sistem geliştirilmesi olacaktır. RF iletişimdeki güvenlik açıkları sebebiyle, envanter bilgilerine yalnızca yetkili kişiler tarafından erişim sağlanmalıdır.

RFID teknolojisinin savunma sanayiimizde kullanıma sunulması sonucu, gerçek dünyadaki malzemelerin sanal dünyada görünürlüğünün sağlanması ile envanter doğruluğu ve işgücü kazanımı sağlanacak, güvenlik açıklarının giderilmesi sonucunda ise RFID teknolojisi tüm OT/VT (Otomatik Tanıma/Veri Toplama) uygulamalarında kullanıma sunulmuş olacaktır.



Şekil 3. RFID Güvenlik Çerçeve Uygulaması

KAYNAKÇA

1. EPC Global Architecture Framework v1.3

2. EPC Global Class 1 Gen 2 UHF RFID Communications Protocol v1.2

3. A Simple and Cost-effective RFID Tag-Reader Mutual Authentication Scheme. Divyan M. Konidala, Zeen Kim, Kwangjo Kim

4. US Undersecretary of Defense, Acquisition Technology and Logistics, RFID Policy, 30 July 2004

5. United States Department of Defense Suppliers' Passive RFID Information Guide v11.0

6. RFID ve Tedarik Zinciri, Sistem Yayıncılık, Kitap No:615. Dr. Alp ÜSTÜNDAĞ

7. RFID Teknolojisi Gelişim Süreci ve Askeri Uygulamalar Açısından Değerlendirilmesi, TSK Dergisi Ocak 2008, sayfa 92-101. Dr. İkm. Kd. Bnb. Bülent ÖZDİL, Dr. Oğuz CAN.