RFID Teknolojisinde İnsan Bilgisayar Etkileşimi

Human Computer Interraction In RFID Technology

Özgür Erkut ŞAHİN

erkut@bahcesehir.edu.tr

Bahçeşehir Üniversitesi Meslek Yüksek Okulu

ÖZET:

Çoğu güvenlik uygulamaları pahalı olduğundan tercih edilmez. Bu nedenle insanların kendi kişisel bilgilerini korumaları da güçleşir ve bilgi sızıntıları meydana gelir. RFID etiketleri eski bir teknoloji olmasına rağmen günümüzde yaygın olarak kullanılmaktadır. Bu teknoloji mikroçiplerin üzerine yüklenmiş kimlik tanımlama verilerinin radyo dalgaları kullanılarak okunup işlenmesi prensibine dayalı olarak çalışan bir veri işleme türüdür. Bugün bu teknoloji imalat sektöründen perakende sektörüne kadar geniş bir alanda ürün tanımlama aracı olarak kullanılmaktadır. Potansiyel kullanım şekillerinden pasaport üzerine RFID konularak kimlik belirleme işlemi de yaygınlaştırılmaya çalışılmaktadır. İnsan, teknoloji etkileşimin en son boyutu olan ve insana yapılan RFID implantasyonu yoluyla kimlik belirleme işlemi son aşamasına ulaşmıştır. Etkileşim boyutu ele alındığında güvenlik boyutu da maximum düzeye çıkmaktadır.

Bu çalışmada, RFID teknolojisine genel bir bakışla beraber, kullanıldığı alanlar, ürün etkileme yoluyla kimlik tanımlama, pasaportlar ve insanla direk temas konularında alınması gereken bilgi güvenliği önlemleri ve insanların özel hayatlarına müdahale konusunda dünyada AB' de ve Türkiye'de hangi aşamaya kadar hangi ölçüde korunduğu sorgulanmış ve yapılması gerekenler ile ilgili olarak görüş ve öneriler sunulmuştur.

KEYWORDS:RFID,Kimlik Tanımlama, Ürün Tanımlama, Pasaport, Etkileşim, RFID İmplantasyonu

1. GİRİŞ

Radyo Frekansı ile kimlik belirleme sistemi, dünyada kimlik belirleme ve nesne tanımlamaya ilişkin endüstriler içinde en hızlı büyüme gösteren otomatik veri toplama teknolojisi olarak gelişimini sürdürmektedir. Yeni bir teknoloji olmamasına rağmen, dünya çapında pek çok uygulama çerçevesinde kullanılmıştır. İlk defa II. Dünya savaşı sırasında dost uçakları düşman uçaklarından ayırabilmek ve tanımlayabilmek amacıyla müttefikler tarafından kullanılmaya başlanan bir otomatik veri toplama ve tanımlama sistemidir. Bugün de aynı amaçla dünyada çeşitli uygulamalarda kullanılmaktadır.

RFID'nin işletmelerde ve üretim sektöründe kullanımı artmaktadır. Burada amaç, üretimin standartlara uygun olması, tedarik zincirinde ürün

sahteciliğini önlemek ve hem üretici hem de tüketici güvenliğini sağlama ve işletmenin kârlılığını esas almaktır(Want, 2006).

RFID teknolojisi endüstride kullanılan diğer bazı teknolojilere, örneğin barkod teknolojisine, rakip değil onun tamamlayıcısıdır; örn, depolarda ürünlerin paletlenmesi sırasında, taşınmasında her ikisi de kullanılmaktadır. RFID ayrıca, barkodların kullanılmasından kaynaklanan bazı sorunların da üstesinden gelmiştir. RFID, barkodlar gibi optik okuyuculara sahip değildir, tamamen kablosuz data iletimi sağlayarak veri tabanında okuma ve yazma işlemini gerçekleştirir(Da, Ruan(Ed.),2006).

RFID teknolojisinin önündeki en büyük engellerden biri de standardizasyondur. Standardizasyonun amacı, işletmenin üretimde etkili olabilmesini sağlayacak olan en etkili platformlardan biridir (Asif, Z & Madviwalla, M, 2005)

Bu standartlar üzerinde firmalar çalışmakta; ancak şu anda herhangi bir sonuca ulaşılmamıştır.

2. RFID TEKNOLOJİSİNİN TEKNİK ÖZELLİKLERİ

RFID, bir verinin tanımlanabilmesi için veri değişimini gerçekleştiren ve bunun için de radyo sinyallerini kullanan bir teknolojik araçlar bütünüdür. Basit olarak bir nesneyi tanımlamak için bir etiket veya işaret içerir. İşleyiş şekli olarak radyo sinyallerinin alınması, verinin işlenmesi, ve sonuçta birçok belirleyici enformasyonun gönderilmesi şeklinde olmaktadır. Başka bir deyişle bu işlem kriptografik olarak kodlanmış, ardından bir veri tabanı tarafından yorumlanmış, küresel bir uydu sistemine yollanmış ve son olarak da gerideki ödeme sistemini etkileyen bir seri karmaşık işlemi gerçekleştirir (Parlikad,K,A&McFarlane,2007). RFID teknolojisinin mevcut kullanım alanları oldukça geniştir. POS sistemleri, otomatik araç tanımlama sistemleri, demirbaşların takibi, depo yönetimi ve lojistik, tedarik zincirinde ürün takibi, ürün güvenliği, kütüphaneler, hava limanlarında bagaj takibi, vb alanlarda kullanım gün geçtikçe yaygınlaşmaktadır. Daha pek çok alanda kullanımı yer alırken, özellikle tıp alanında ve insan vücuduna yerleştirilen RFID ler de geleceğe yönelik uygulamalar olarak yer almaktadır.

RFID sistem mimarisi etiketlerden ve okuyucudan oluşur. Okuyucu etiketi sorgular, gerekli enformasyonu alır ve enformasyona uygun yapılması gereken ne ise onu yapar. Enformasyon bir cihaz üzerinde görüntülenmesi gerekiyorsa görüntülenir veya bir POS noktası sistemine aktarılır ya da başka bir yerde veri tabanı üzerine girilen bir veri olur.

2.1. Temel Bileşenler:

Etiket, RFID üniteleri transponder denilen radyo aracı olarak sınıflandırılmış araçlardır. Transponder, alış işareti hatasız geldiğinde otomatik olarak tepki veren ve gönderme yapan alıcı verici düzeni olarak tanımlanır. En basit uygulaması, transponder dinler ve kendi cevabını gönderir. Daha karmaşık

uygulamalarda ise, tek harf ya da bir dizi sayı gönderilir veya seri olarak karakter yada sayılar gönderilir.

Sonuç olarak, daha gelişmiş sistemlerde elde edilen enformasyonun başkalarının eline geçmesini önleyecek şifreleme işleminden geçmiş radyo sinyalleri kullanılır. RFID'de kullanılan transponder genellikle tagler, chipler ve etiketlerdir. Chipler küçük üniteler için kullanılırken tagler büyük üniteler için kullanılır ve genelde değiştirilebilir niteliklerdir.

Genel olarak RFID tagleri,

- Kodlama/kod açma
- Hafıza
- Anten
- Güç ünitesi
- İletişim kontrolü

bileşenlerinden oluşur. RFID tagleri aktif ve pasif olmak üzere iki kategoride yer alır:

2.2 Pasif Tagler: RFID tagleri pil ya da başka bir güç kaynağı içermezler. Bu yüzden okuyucunun sinyalini bekler. Tag, okuyucunun anteninden gücü alabilecek rezonans devresini içerir. Okuyucudan gücü alma işlemini gerçekleştiren bu elektro manyetik özelliğe Near Field (yakın alan) adı verilir. Adından da anlaşılacağı gibi aracın çalışabilmesi için tag için yeterli enerji sağlar. Örneğin, 13,56 MHz dalga boyu olan bir RFID aracının çalışması için yaklaşık 3,5 metrelik bir Near Field (Yakın Alan) gereklidir.

2.3 Aktif Tagler: Aktif tagler pasif taglerin alternatifidir. Aktif taglerin kendi güç üniteleri vardır ve bunlar genellikle içlerinde bulunan pillerdir. Kendi güç üniteleri olduğundan Near Field ihtiyaçları bulunmaz. Bu sayede okuyucunun sorgulamasını ve göndermesini antenden daha uzak mesafelerde de gerçekleştirebilirler bu da alma ve gönderme işlemlerini uzak mesafelerde de yapabilmelerini sağlar. Yarı pasif tagler, radyo dalgalarını alırken ve gönderirken Near Field'a ihtiyaç duyarlar fakat hafızalarının çalışmasını sağlayacak kendi güç kaynaklarını barındırırlar.

2.4 Okuyucu (reader): RFID sistemlerinin en önemli ikinci bileşeni de okuyucu denilen araçtır. Buna genelde tranceiver (alıcı-verici) denir. Her ne kadar bunların görevi tagi sorgulamak ise de okuma işlemi yaparlar, okuyucular bünyelerinde anten barındırsalar da antenlerin ayrı olduğu cihazlar da mevcuttur. Küçük sistemlerde okuyucu ve anten bir arada bulunurken daha büyük sistemlerde anten ayrı tutulur. Okuyucunun öteki bileşenleri ise sistem arayüzü örneğin RS-232 seri port veya Ethernet jack, kriptografik kodlayıcı ve kod açıcı devreler, güç ünitesi veya pil ve iletişim kontrol üniteleridir. Okuma işlemi yaptıktan sonra enformasyon POS'lara, LAN'lere veya WAN'lere gönderilir.

2.5 Yazılım(Middleware): Özel yazılımlar, okuyucudan gelen enformasyonu koordine ederek veri tabanlarına aktarılmasını sağlar. Bu yazılımlar veri tabanlarıyla okuyucular arasında bulunur ve ikisi arasındaki enformasyon akışını düzenler. Bunlara ek olarak bu yazılımlar, okuyucunun sorgulama yapmasını ve gelen enformasyonun filtrelenmesini de

yaparlar. RFID teknolojisi geliştikçe bunların özellikleri de artış göstermektedir

(Krishna,P & Husak,D.2007).

3. RFID VE GÜVENLİK

Öncelikle güvenlikten bahsederken dışardan gelen bazı atakları analiz etmemiz gerekir. Bu ataklar, tüm sistemi hedef alan ataklar olabileceği gibi sistemin veri tabanı, envanter kontrolü gibi bölümlerini de hedef alan ataklar olabilir.

Bu daha çok veri güvenliği konusunda bilgi teknolojileri güvenliğini ilgilendirir. RFID güvenlik uygulamaları konusunda ise fiziksel öğenin güvenliği datanın güvenliğinden daha önemlidir. Çünki herhangi bir atak sırasında organizasyon zarara uğratılsa bile datanın kendisi bu ataktan etkilenmeyebilir. Atakların doğasına baktığımızda iki türlü olduğunu görmekteyiz. Birincisi RFID üzerindeki tek bir nesneyi çalmak veya tüm satış noktalarında satışı engellemek üzerine olabilir(Lindstrom,P.2005) . Bazı ataklar ise data ile ilgilenmeden doğrudan fiziksel erişim kontrollerine saldırmak biçiminde olabilir. Bu atakları, yayın sırasında sinyale atak, tag deki datayı değiştirmek, yazılım datasını değiştirmek ve veri tabanına ulaşmış dataya atak şeklinde gruplandırabiliriz.

4. RFID TEKNOLOJİSİNDE KİŞİSEL GÜVENLİK

RFID çipleri kimlik ya da ürün bilgilerini saklamak konusunda kolaylık ve maliyet uygunluğu sağlarken, diğer yandan da potansiyel ataklara açık hale gelmiştir.
Bu nedenle sadece bu teknoloji konusunda kullanıcıları bilgilendirmek ve organizasyonların da gerekli önlemleri almalarını beklemek yeterli görülmemektedir. Konuyla ilgili kapsamlı yasal düzenlemelere gidilmesi önem verilmelidir.

5. KİMLİK BİLGİLERİNİN KULLANILDIĞI ALANLAR

RFID çipli ilk pasaportlar ABD'de 2005 yılında basıldı. Bu çiplerde bütün kişisel bilgiler ve şahsın biyometrik fotoğrafları yer alır. Ancak bu çipler kimlik sahibinin bilgisi olmadan taranıp okunabilir. Kimlik hırsızları sahte pasaport yapmak için şahsa ait kişisel bilgileri kolayca elde edebilir. Bu çiplerdeki bilgilerse kötü amaçlara yönelik olarak kopyalanıp saklanabilir (http://www.riscure.com/news/passport.html).

6. İNSANA YAPILAN İMPLANT UYGULAMALARI

2001 yılında Applied Digital Solutions, kişisel bilgileri depolamak için Verichip'i piyasaya çıkardı. Verichip şahsın ön kol kasının altında yer alan yağ dokusuna yerleştirilerek uygulanmaktadır. Verichip halihazırda ABD'deki bazı klüplerin VIP üyeleri tarafından kullanılmaktadır. Bu uygulama kimlik sahteciliği ile ilgili pek çok sorun yaratabilir. Verichipler insan vücudunda hep aynı bölgeye uygulandığı için, şahıs kaçırıldığında ya da saldırıya uğradığında, kimlik

bilgilerini içeren Verichipler çıkartılıp çalınabilir ve başka bir kişiye uygulanabilir. Aynı şekilde, çıkartılmış olan Verichip başka bir çipe kopyalanabilir ve sahte kimlik yapımında kullanılabilir ya da en azından Verichip içindeki veriler saklanabilir ve kötü amaçlarla kullanılabilir. Kişiler Verichip'in kendilerine uygulanması için onay verdiklerinde, bu seçimlerinin sorumluluğunu aktif olarak üstlenmiş olurlar. Ancak güvenlik sorunları nedeniyle Meksika gibi bazı ülkelerde farklı senaryolar da yaşanabilir. Ebeveynleri daha kişi bebekken Verichip'i kendisine taktırabilir ve kişi reşit olana kadar böylesi bir implantı taşıdığından haberdar olmayabilir (Locton, V & Rosenberg, S, R.2005).

7. DÜNYADA VE TÜRKİYEDE MAHREMİYET VE ÖZEL HAYATA MÜDAHELE KONUSUNDA RFID'NİN KULLANILMASI

Avrupa Parlamentosu'ndan ilk kez 1988'de geçen ve halen Avrupa Veri Koruma Yönetmeliği (EUDPG 1995)olarak bilinen yönetmelik, kişisel bilgilerin kullanımıyla ilgili olarak güvenlik sağlamayı hedeflemektedir. Buna göre kişisel bilgiler ancak şu şartlar altında toplanabilir: Kullanıcının buna rıza göstermesi, sözleşme yapılırken, gerekli olduğunda, yasalarca gerekli görülürse ya da kişinin yaşamsal çıkarları gözetilecekse ya da yasaları uygulamak gerekiyorsa bu veriler toplanabilir (Peslak, R, A,2005). Bu hususlar, ilgili yönetmeliğin 13. maddesinde yer almaktadır.. Avrupa Birliği içerisinde veri güvenliğinin yasal boyutuyla ilgili endişeler fazla olmamakla birlikte, asıl sorun teknolojinin dikkatsiz kullanımı ve sistem yöneticileriyle kullanıcıların beceriksizliği olarak görülmektedir. Bu nedenle ilgili yasanın 17. maddesine göre verilerin çalınmasına, kazara kaybolmasına veya izinsiz kullanımına karşı koruma sağlayacak gerekli ve yeterli önlemleri almayan kuruluşlar ve şirketler cezalandırılacaktır. Avrupa Birliği'nin 18 Aralık 2000 tarihli 45/2001 nolu kararındaysa kişisel bilgilerin kullanımıyla ilgili güçlü düzenlemeler getirilmiştir.

ABD'de yıllarca süren yasal düzenleme yokluğu sonrasında Amerikan Kongresi HIPAA'yı (Sağlık Sigortası Taşınabilirliği ve İzlenebilirliği Yasası)1996 yılında çıkarıldı (Loncton V, Rosenberg S. R, 2005). Bu yasa insanlara uygulanan RFID implantlarının ilk etaptaki güvenliğini sağlayabilmektedir. Kişisel verileri korumayla ilgili olarak ABD genel anlamda otokontrole dayalı bir anlayışı benimsemiş olsa da elektronik kimliklerin çalınması, kaybolması ya da satılması demek olan kimlik hırsızlığı Amerikan Federal Ticaret Komisyonu'nun aktif rol üstlenmeye karar vermesine neden olacak düzeye ulaştı(FTC2005). Komisyon yaptığı araştırmalar ve anketler sonucunda otokontrolün yetersiz olduğunu ve federal yasalara ihtiyaç duyulduğunu ifade etti. Federal Ticaret Komisyonu'nun konuyla ilgili sunduğu talimatlar yine otokontrole dayalıydı fakat etkili olmadı. ABD'de bu alanda çok daha kapsamlı yasalara ihtiyaç vardır.

Yeni Türk Ceza Kanunu'nun 525 b/1 maddesi elektronik verilerin silinmesi, tahrip edilmesi ve değiştirilmesi, sistemlerin yanlış biçimde işlemesine neden olmak ya da işlemesine tamamen engel olmak konularına yaptırımlar getirmektedir (Dülger, V,M, 2004). . Bu yaptırımlar her ne kadar veri güvenliği konusunda temel oluşturmuş olsa da RFID'nin uygulama alanlarını yeterince kapsamamaktadır. Bunun için yasalar ürün ve uygulama alanı odaklı yapılmalıdır.

8. SONUÇ

Elektronik iletişim suçlarına ilişkin yasalar mevcut olmasına rağmen, RFID'ye özel yasalar bulunmamaktadır. Bu konuda daha belirli yasa tasarıları hazırlanması mümkündür. Özellikle sistemi uygulayan organizasyonlara yeterli veri güvenliğini sağlamak amacıyla çok iş düşmektedir. RFID çiplerinden sağlanan veriler ilgili kişiyle eşleştirilmemelidir. Kişisel bilgilere yönelik ortaya çıkabilecek tehditler ve tehlikeler önceden hesaba katılmalı ve önlemleri alınmalıdır. İzinsiz veri erişimi ya da kişisel bilgilerin kullanımı gibi durumlar yaşandığında kişi bunun sonucunda oluşabilecek zarardan ve rahatsızlıktan korunmalıdır. Burada organizasyonlara da büyük görevler düşmektedir. Organizasyonlar kullandıkları sistemler hakkında kullanıcıları ve tüketicileri bilgilendirmek zorundadırlar. Aksi taktirde tükeicileri koruyan yasalar çerçevesinde cezalandırılabilirler.

KAYNAKLAR

Want,R *An Introduction to RFID Technology*. Published By IEEE CS and IEEE ComSoc. 2006.31.s

Da, Ruan(Ed.). *Applied Artificial Intelligence : Proceedings of the 7th International FLINS Conference*. River Edge, NJ, USA: World Scientific, 2006. 338.s

Asif,Z & Madviwalla,M Integrating *The Supply Chain with RFID: A Technical And Business Analysis*. Fox School of Business Management, Temple University.2005. 27.s

Parlikad,K,A&McFarlane. *RFID-based product information in end-of-life decision making*. Institute for Manufacturing, Cambridge University Engineering Department, Cambridge CB2 1RX, UK. 2007. 1359.s

Brown,D,E. *RFID implementation*. McGraw-HillProfessional, 2006. 466 s.

Krishna,P & Husak,D. RFID Infrastructure.IEEE Applications &Practice. 2007.s. 4-7

Lindstrom, P. *RFID Security*. Rockland, MA, USA: Syngress Publishing, 2005 s.58-63.

Riscure, Privacy Issues with new digital passport, 2005. http://www.riscure.com/news/passport.html

Angeles, R. *Rfid Technologies: Supply-Chain Applications and Implementation Issues*, Information Systems Management journal, 2005. 22:1,s. 63-64

Locton, V & Rosenberg, S, R. RFID:The Next Serious Threat to Privacy. Ethics and Information Technology, 2005 7:s. 224-225

PESLAK, R, A,. *An Ethical Exploration of Privacy and Radio Frequency Identification*, Journal of Business Ethics, 59, Springer 2005 DOI 10.1007/s10551-005-2928-8,2005 s:328

Lonckton V,& Rosenberg S. R,. *RFID: The Next Serious Threat to Privacy*, Ethics and Information Technology, Springer 2006 DOI 10.1007/s 10676-006-0014-2, 2005 p: 224

[FTC2005] http://www.consumer.gov/idtheft/

Dülger, V,M,. *Bilişim Suçları*, Seçkin Yayıncılık, Ankara, 2004 s:154-156