JOKOHTU

ISSN : 2980-1591
e-ISSN 2980-3845
Yıl/Year : September/Eylül 2023
Cilt/Volume : 1
Sayı/Issue : 2

Akıllı Kartlar ve Türkiye'deki Durumu

Ercan ÖLÇER[1]

Derleme Makale
Review Article

Geliş tarihi/Received:
23.08.2023

Son revizyon teslimi/Last revision received:
26.08.2023

Kabul tarihi/Accepted:
31.08.2023

Yayın tarihi/Published:
Ağustos 2023

Atıf/Citation:
Ölçer, E. (2023). Akıllı Kartlar ve Türkiye'deki Durumu. *Journal of Kocaeli Health and Technology University*, 1(2), 1-7.

DOI:

ÖZET

Bu makalede, Türkiye'de kullanımı hızla artan ve yerli üretim uygulamalarda güven unsuru olarak kullanılan akıllı kartların güvenliği ele alınmıştır. Genel kullanıma sahip mikroişlemci yapılarından farklı olarak gelişmiş kritoptografik yeteneklere ve üstün algılayıcılara sahip mikroişlemci yongaları kullanan akıllı kartların olası saldırılara karşı direçli yapısı ve alınan önlemler makalede detaylı olarak irdelenmiştir. Diğer yandan güvenliğin daha da arttırılması için neden yerli üretim akıllı kartların yabancı ürünlere göre tercih edilmesi gerektiğinin önemi de vurgulanmaktadır. Akıllı kartlara yapılan saldırıların ve alınan önlemlerin haricinde, kullanılan kripto anahtarlarının ve anahtar üretiminin yerli unsurlarla yapılmasının gerekliliği açıklanmıştır. Ayrıca akıllı kartların Türkiye'deki kullanımı ile ilgili güncel bilgiler yürütülen ve tamamlanan projeler ile örneklendirilerek değerlendirilmiştir.

Keywords: Saldırı, önlem, güvenlik, akıllı kart

ABSTRACT

In this paper, the security of smart cards, which are rapidly increasing in use in Turkey and used as an element of trust in locally produced applications, is discussed. Unlike common microprocessor structures, smart cards that use microprocessor chips with advanced cryptographic capabilities and superior sensors are analyzed in detail in the article. On the other hand, the importance of why domestically produced smart cards should be preferred over foreign products in order to further increase security is also emphasized. Apart from the attacks on smart cards and the precautions taken, the necessity of making the crypto keys and key generation with local elements is explained. In addition, current information about the use of smart cards in Turkey is evaluated by exemplifying the projects carried out and completed.

Keywords: Attack, precaution, security, smartcard

[1] *Kocaeli Sağlık ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Dr.Öğr.Üyesi, ercan.olcer@kocaelisaglik.edu.tr, ORCID ID: 0000-0003-3786-6230*

GİRİŞ

Özellikle bilgi güvenliği alanında yüksek teknoloji kullanımlarından biri de akıllı kartlardır. Üzerinde mikroişlemci barındıran akıllı kartlar, kişi güvenliğini sağlayan alanlarda güvenli, pratik ve ucuz bir çözüm olarak kullanılmaktadır. Bakıldığında akıllı bir kart, plastik kart gövdesi, kart üzerinde yer alan güvenlik öğeleri, mikroişlemci, flash bellek ve ram tipi bellekten oluşmaktadır. Asıl güvenliği sağlayan unsur, güvenlik yetenekleri olan ve kart üzerinde yer alan mikroişlemcidir. Güvenlik yetenekleri sayesinde akıllı kartlarda kullanılan mikroişlemciler, sıradan mikroişlemcilerden ayrılır ve çok uygun fiyata yüksek güvenlik sağlayabilirler. Mikroişlemcinin içinde gelişmiş şifreleme ve şifre çözme yeteneklerine haiz kripto modülü bulunmaktadır. Güçlü ve hızlı donanımlar gerektiren proje maliyetlerinin yanında, ucuz ve güvenilir bir alternatif olmaları nedeniyle güvenlik gerektiren pek çok uygulama alanında akıllı kartlar yaygın olarak kullanılmaktadır. Aynı zamanda akıllı kartlar akıllı şehir konusunda yine önemli bir unsur olarak tanıtılmaktadır (Akpınar, 2023). Günümüzde cep telefonları için SIM kartı, bankacılıkta kredi kartı, ulusal kimlik kartı, pasaport, sağlık kartı veya geçiş denetimi kartı olarak kullanılmaktadırlar. Hatta yeni teknolojilerden olan blokzincir uygulamalarında akıllı kartların dijital cüzdan olarak kullanımları da söz konusudur (Tanrıkulu, Yüce, & Ölçer, 2021). Blokzincir teknolojisini destekleyen akıllı kartların ödeme sistemlerinde de kullanılması da gündeme gelmiştir (Doğan, Takaoğlu, & Ölçer, 2022). Akıllı kartlar birçok açıdan yaygın olarak kullanılıyor olsa da olası güvenlik açıklıkları nedeniyle kötü niyetli kişilerin saldırılarına maruz kalabilmektedir (Ceyhan, Ceyhan, Demiryürek, & Bodur, 2018).

Akıllı kartlar, veri iletimi bakımından arayüzü farkı nedeniyle ikiye ayrılmaktadır. Temaslı ve temassız akıllı kartlar olarak sınıflandırılır. Temaslı kartlar kartın üzerinde yonga kart okuyucusuna takılıp elektriksel olarak sinyal haberleşmesi gerektirdiğinden bu ismi almaktadır. Ancak daha yaygın olan kullanımı temassız kart iletişimi tipidir. Günümüzde wifi, Bluetooth gibi temassız iletişim benzeri kart, kart okuyucusu ile temassız olarak iletişim kurar. Ancak wifi, bluetooth benzerlerinden farklı olarak en fazla 10 cm mesafeden haberleşir ve haberleşme hızı diğerlerinden çok daha yavaştır. Ancak bu yavaşlık iletişimde kullanılacak olan verinin küçük olmasından dolayı sorun oluşturmamaktadır. Genelde kart sahibine ait, çok ta büyük olmayan verilerden oluşmaktadır. Kartta kişisel veriler ve anahtar verileri olması nedeniyle kimlik doğrulama, e-imza gibi kritik işlemlerde kullanılması gerektiğinden iyi korunması gerekmektedir.

1. Akıllı Kartlarda Güvenlik

Akıllı kartlar, üzerine yüklenen verileri güvenli olarak saklayabilir. Akıllı kart üzerinde bulunan kripto işlemleri yapan modüller ve akıllı kart işletim sistemi, kartın üzerinde tutulan verilerin güvenliğini sağlamaktadır. Akıllı kartlar, şifreleme, şifre çözme, imzalama, imza doğrulama ve anahtarları depolama gibi hizmetler sunmaktadır (Akleylek, Yıldırım, & Tok, 2011). Bu güvenliği geçebilmek için saldırganlar çeşitli yöntemler denemektedir. Akıllı kartlara yapılan saldırılara karşı alınan donanım ve yazılım türü önlemler bulunmaktadır (Başak & Adalı, 2012). Akıllı kartlarda en çok bilinen saldırılar aşağıdaki gibi sıralanabilir:

• Veri iletişiminin dinlenmesi: Kart okuyucu ve kart arasındaki hattın dinlenerek gelen/giden verinin ele geçirilmesi.

• Veri iletişiminin değiştirilmesi: Çipin bağlantı noktalarına iletken tel bağlanarak okuyucu ve kart arasındaki verilerin istenilen şekilde değiştirilmesi

• Elektrik gücü üzerinde değişiklik yapılması: PIN girişi sırasında güç kesilerek hata sayacının değişmesinin önlenmesi.

• Çip saatinin kesilmesi: Saat kesilip elektron ışın test edici ile RAM içeriğinin takip edilmesi

• Ultraviyole ışığı kullanarak EEPROM'un silinmesi: UV ışığıyla bellek içeriğinin silinmesi

• Mikroişlemcinin lazerle katmanlarına ayrılması: Mikroişlemcinin üst katmanının lazerle kesilerek devreye müdahale edilmesi

• Simetrik anahtarın analizi: Deneme yanılma yöntemiyle simetrik anahtarların ele geçirilmesi

• Yan kanal analizi (SPA/DPA): Çip çalışırken sızan bilgilerin incelenerek anahtarın ortaya çıkarılmaya çalışılması

• Zamanlama saldırıları: Kriptografik algoritmalarda anahtara bağlı işlem sürelerinin değiştirilmesi ve gizli anahtarın elde edilmesi

• Hata enjeksiyonu: mikroişlemciye hata yaptırma

Akıllı kartlarda yukarıda anlatılan ve bilinen saldırı yöntemlerine karşı mikroişlemcide ve üzerindeki yazılımlarda karşı önlemler alınarak saldırganlar bertaraf edilmektedir. Buna göre saldırı ve alınan önlemler aşağıdaki gibi olabilmektedir:

1.1. Saldırı: Veri İletişiminin Dinlenmesi

Önlem: Kart okuyucu ve kart arasındaki hattın dinlenerek gelen/giden verinin ele geçirilmesi ile anahtarın ortaya çıkarılması prensibine dayanmaktadır. Buna göre araya giren dinleyicinin verileri elde etmesini önlemek için akan verinin şifrelenmesi sağlanmaktadır. Şifrelenmiş veri yapısı saldırganın veriyi elde etmesini engellemektedir. Bu sayede oturum anahtarlarının transferi ve PIN, ya da kişisel verilerde kanalda akarken şifreli olması nedeniyle saldırgan veriyi ele geçiremez.

1.2. Saldırı: Veri İletişiminin Değiştirilmesi

Önlem: Çipin bağlantı noktalarına iletken tel bağlanarak okuyucu ve kart arasına girerek veri dinlenir ve veri istenilen şekilde değiştirilir. Bu saldırıda hedef verinin değiştirilmesidir. Örneğin kullanıcı PIN'i tanımlanırken veri değiştirilerek kullanıcının PIN'i saldırganın bildiği PIN ile değiştirilebilir. Bunun için PIN tanımlanması dâhil iletişimin güvenli olması sağlanmalıdır. Oturum anahtarı üretilerek taraflar (okuyucu ve kart) simetrik bir anahtarla şifreli haberleşmeye geçirilir. Araya giren saldırgan şifreli veriyi alır ve çözemez saldırı önlenir.

1.3. Saldırı: Ultraviyole Işığı Kullanarak EEPROM'un Silinmesi

Önlem: UV ışığıyla bellek içeriğinin silinmesi saldırısında saldırgan elektronik devrelere ultraviyole ışık tutarak flash belleğin silinmesini ve işlemcinin hata yapmasını hedefler. Bunun

önlenmesi için yonga yüzeyi tel ızgara hatlarıyla ve duyargalarla donatılmaktadır. Bu sayede UV ışığın devrelere sızması engellenir ve yonganın hata yapması ile verinin yongadan kaçmasına engel olunur.

1.4. Saldırı: Elektrik Gücü Üzerinde Değişiklik Yapılması

Önlem: Saldırgan bu saldırı tipinde kullanıcının PIN girişi sırasında gücü keserek hata sayacının değişmesini önlemek ister. Kullanıcının PIN'i hatalı girmesi durumunda PIN deneme sayısına bir sayaç atanarak PIN'i sınırsız deneme saldırısına engel olunur. Ancak PIN deneme sayısının az olarak belirlenmesi saldırganın istemediği bir durumdur. Bu kota saldırganın PIN'I deneyerek bulma şansını ortadan kaldırır. Bunu aşmak için saldırgan yonga elektrik gücünü azaltarak veya kapatarak PIN denemesi sonrası sayacın artmasını engellemek ister ve bunu sağlaması durumunda sayısız PIN denemesi yaparak kartın PIN'ini bulabilir. Saldırıyı önlemek için yonga güç hattını izleyen özel bir devre bulunmaktadır. Bu devrede yer alan duyargalar hat üzerindeki güç dalgalanmalarını takip eder ve bir sorun olursa bir kesme oluşturarak işletim sistemine haber verir. İşletim sistemi üzerinde yer alan yazılım bu durum karşısında yazılım ile önlem alarak saldırıyı bertaraf eder.

1.5. Saldırı: Çip Saatinin Kesilmesi

Önlem: Saldırgan bu saldırı tipinde işlemci saatini kesip elektron ışın test edicisi ile RAM'de yer alan kritik verilerin bulunmasına çalışır. Saldırıda saat sinyali kesildiğinde yonga üzerinde program akışı durur. Bu sayede yazılım ile bir önlem alınamaz. Bellekte yer alan kritik veriler şifreli ve geçici olarak tutulur. Bu sayede bellekte verilere erişilse bile veriler açığa çıkarılamaz.

1.6. Saldırı: Mikroişlemcinin Lazerle Katmanlarına Ayrılması

Önlem: Mikroişlemcinin üst katmanının lazerle kesilerek devreye erişilmesi sağlanır. Yonganın çalışma sürecinde veri ve adres yolları, kullanılan proplar sayesinde izlenebilir. Saldırının engellenmesi için veri ve adres yollarının sırası değiştirilir. Dolayısı ile proplardan elde edilen veriler karışıktır ve çözülmesi mümkün değildir. Diğer yöntem yine akan veri şifreli olarak bloklar arasında dolaşır. Şifreli veri nedeniyle saldırgan anlamlı veri elde edemez. Ayrıca lazerle kesilmesi durumda donanımın kitlenmesini sağlayan yonga yüzeyi üzerinde çok sayıda duyarga bulunur. Bu duyargalar kesim esnasında tetiklenmesi durumunda devreyi bloke eder.

1.7. Saldırı: Zamanlama Saldırıları

Önlem: Saldırgan, kriptografik algoritmalarda anahtara bağlı işlem sürelerinin değiştirilmesi ve gizli anahtarın elde edilmesine çalışır. Buna karşılık anahtar kullanımı ve üretimi sürecinde yazılımda olumlu veya olumsuz durumlar için geçen süreler eşitlenerek bilgi elde edilmesine engel olunur.

1.8. Saldırı: Simetrik Anahtarın Analizi

Önlem: Deneme yanılma yöntemiyle simetrik anahtarların ele geçirilmesi amacıyla yapılan saldırı tipidir. Buna göre saldırgan anahtarları değiştirerek deneme yapar. Ancak zamana dayalı simetrik anahtarlar değiştirilerek saldırgan simetrik anahtarı bulsa bile anahtar değiştirildiğinden saldırı başarısız olur. Ayrıca kriptolu iletişimde oturum bazlı anahtarların kullanılması da bu saldırıyı benzer şekilde engeller.

1.9. Saldırı: Yan Kanal Analizi (SPA/DPA)

Önlem: Bu saldırı tipinde yonga çalışırken sızan bilgiler analiz ederek anahtar ortaya çıkarılmaya çalışılır. Bu saldırı güç veya sinyal hattı üzerinden sızan verilerdir. Çip çalışırken farklı harmonikler üzerine binen sinyaller incelenerek verilerin elde edilmesine çalışılmaktadır. Bunun engellenmesi için işlemcinin giriş ve çıkış hatlarına harmonik sinyallerin bastırılması için filtreler kullanılmaktadır. Ayrıca yonga içinde ve dışında dolaşan kritik veriler kriptolanarak veri saklanır. Saldırgan bu verileri elde etse bile şifreli elde eder.

1.10. Saldırı: Hata Enjeksiyonu

Önlem: Bu saldırı tipinde mikroişlemciye hata yaptırarak bir çeşit verinin kaçması sağlanmaya çalışılır. Bu tip durumlarda yonga hata yaptığında genelde kesme vektörleri üzerinden işletim sistemine sinyal gönderir ve işletim sistemindeki yazılım bu kesmeleri alarak anahtarların silinmesi veya yonganın çalışmaz hale getirilmesi gibi işlemleri yerine getirir. İyi yazılmamış kesme yazılımları nedeniyle yongaya hata yaptırılarak verinin sızması mümkün hale gelebilir. Bunun için işletim sisteminde gerekli yazılımların düzgün işlem yapması sağlanarak bu saldırı önlenebilir.

Yukarıda anlatılan saldırı tipleri en çok rastlanan ve genelde de yonga ve işletim sistemi geliştiriciler tarafından dikkate alınan saldırı ve önlemleri anlatmaktadır. Ancak akıllı kartlarda ne kadar önlem alınırsa alınsın kartlara yeni tip saldırılar geliştirilmektedir. Bu nedenle saldırganla işlemci ve işletim sistemi geliştiriciler arasında süren bir yarış vardır. Zaman içinde yeni saldırılar gerçeklenmesi durumunda yeni önlemler alınarak saldırganların çabası boşa çıkarılmaktadır. Akıllı kartların güvenlik yanında sağladığı avantajlar nedeniyle yaygın kullanımı bu rekabetin daha uzun yıllar devam edeceğini göstermektedir.

Türkiye'de Akıllı Kart Çalışmaları

Yukarıdaki bölümde açıklanan saldırılar ve bu saldırılara karşı alınan önlemlere sahip olmaları, pratik ve ucuz olmaları, akıllı kartların Dünya'da birçok uygulamada yaygın kullanılmasına neden olmaktadır. Banka kartları, kimlik kartları, pasaportlar, sürücü belgeleri, imza kartları, seyahat kartları, üniversite kartları, güvenli geçiş kartları vs. güvenlik ve kimlik doğrulama gerektiren pek çok uygulama alanında kullanılır. Bu uygulamalarda akıllı kart temelde kimliği doğrulayan ve kişisel bilgileri ve anahtarları tutan bir anahtar rolünü üstlenmektedir. Küresel çapta büyük akıllı kart şirketleri eliptik eğri algoritmalarını da desteklemesi nedeniyle akıllı kartları projelerinde kullanmaktadırlar (Lauter, 2004).

Türkiye'de, Tübitak tarafından geliştirilen Akıllı Kart İşletim Sistemi (AKİS) çalışmaları ve yine Tübitak'ta bulunan Yital grubunun akıllı kart işlemcisinin (UKTÜM) yerli imkânlarla üretilmesi sayesinde, yonga üretiminden kart basımına ve saha kullanımına kadar yabancı menşeli ürünlerin yerini almaktadır. Günümüzde elektronik imza sürecinde kullanılan akıllı kartlar tüm kamuda doküman imza süreçlerinde kullanılmaktadır. Nüfus Genel Müdürlüğünün dağıttığı Türkiye Cumhuriyeti Kimlik Kartları, kâğıt formatta olan kimlik kartlarının yerini alarak akıllı kartlara dönüşmüştür. AKiS işletim sistemli akıllı kartlar, elektronik devlet uygulamalarında kişinin kendisini elektronik ortama ispat edebilmesi için kullanılacak bir araç olarak tasarlanmıştır. Kendisine verilen akıllı kart ve içerisindeki elektronik sertifika ile kişinin kendisini elektronik ortama tanıtması mümkün olmaktadır. Akıllı kart içerisindeki sertifika ve verilerin işlenmesi akıllı kart içerisindeki işletim sistemi aracılığıyla sağlanmaktadır.

Türkiye'deki elektronik devlet uygulaması olan "e-devlet kapısı" uygulaması ile vatandaş kendisini sisteme ispat ederek sunulan e-devlet uygulamalarından yararlanır. Vatandaşların kendini sisteme tanıtmasında yöntemlerden biri akıllı kart olan Türkiye Cumhuriyeti Kimlik Kartı'dır.

Benzer şekilde Darphane'de basılan yerli pasaportlar akıllı kart uygulamalarına diğer bir örnektir. Yerli ürün olmasına rağmen hem kullanılan yerli yonganın hem de AKiS işletim sisteminin uluslararası Ortak Kriterler sertifikasyonuna sahip bulunması da ayrıca önemli bir güvenlik unsuru olmaktadır. Bu sayede bu akıllı kartlar sadece yerli projelerde değil yurtdışında projelerde de kullanılmaktadır. Örneğin, Kuzey Kıbrıs'ta Türkiye'de üretilen akıllı kart olarak kimlik doğrulama ve e-imza için kimlik kartları kullanılmaktadır.

Kurumlarda kurum kartı olarak kullanılması da özellikle Ankara'da Cumhurbaşkanlığı giriş ve güvenlik kartı olarak kullanılmaya başlanmasından sonra hız kazanmıştır. Ayrıca önümüzdeki yıllarda banka ve kredi kartlarında da yerli ürünlere geçiş beklenmektedir.

Sonuç

Yüksek güvenlik gerektiren uygulamalarda akıllı kartların pratik, ucuz ve daha önemlisi güvenli olması kullanım alanlarını hızla çoğaltmıştır. Özellikle güvenlik gerektiren uygulamalarda anahtarı tutan ve doğrulayan bir unsur olan akıllı kart ve sistemlerin yerlileşmesi akıllı kartlara olan güveni daha da arttırmış ve Türkiye'de uygulama alanlarını genişletmiştir. Bunun nedeni bugüne kadar kullanılan anahtarların üretiminin yeterince güvenilir olmaması ve yabancı şirketlerin oluşturduğu sistemlerde üretilmesi bu güveni eksik kılıyordu. Ayrıca akıllı kartlarda yer alan yabancı kaynaklı işletim sisteminin ve yongaların kişiye ait anahtar ve verileri işliyordu. Gümünüzde yonga, akıllı kart ve işletim sistemi ile akıllı kartların yerlileşmesi bu güven sorununu önemli ölçüde ortadan kaldırdı. Bundan sonraki çalışmalarda akıllı kartlarda donanım ve yazılımların yerli olanların kullanımı ile hangi güvenlik sorunlarının ortadan kaldırılabileceği detaylı olarak incelenecektir. Ayrıca kullanılan projelerde akıllı kartların oluşturduğu ve eksik olarak görülebilecek güvenlik ile ilgili bu problemlerin çözüm önerilerinin neler olacağı konusu çalışılacaktır.

Kaynakça

Akleylek, S., Yıldırım, H., & Tok, Z. (2011). Kriptoloji ve uygulama alanları: açık anahtar altyapısı ve kayıtlı elektronik posta. Akademik Bilişim, 11, 2–4.

Akpınar, M. (2023). Akıllı Şehirler ve Yapay Zeka. TYB Akademi Dil Edebiyat & Sosyal Bilimler Dergisi.

Başak, M., & Adalı, E. (2012). Dinamik Güvenlik Akıllı Kartlar İçin Dinamik Güvenlik İşlevi. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi. Dinamik Güvenlik Akıllı Kartlar İçin Dinamik Güvenlik İşlevi. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 5.

Ceyhan, E., Ceyhan, İ., Demiryürek, E., & Bodur, R. (2018, September 30). AKILLI KİMLİK KARTLARININ FİNANSAL İŞLEMLERDE KULLANIMI: OLASI GÜVENLİK TEHDİTLERİ VE ALINACAK ÖNLEMLER. International Journal of Management Economics and Business, 14, 0-0. doi:10.17130/ijmeb.2018343121

Doğan, A., Takaoğlu, M., & Ölçer, T. (2022). Smart Card Based Offline Payment System for Central Bank Digital Currencies. Smart Card Based Offline Payment System for Central Bank Digital Currencies, 114. (S. Y. Yurish, Dü.)

Lauter, K. (2004, February). The advantages of elliptic curve cryptography for wireless security. IEEE Wireless Communications, 11, 62-67. doi:10.1109/mwc.2004.1269719

Tanrıkulu, A., Yüce, H., & Ölçer, E. (2021). Afyon Kocatepe Üniversitesi Uluslararası Mühendislik Teknolojileri ve Uygulamalı Bilimler Dergisi. Afyon Kocatepe Üniversitesi Uluslararası Mühendislik Teknolojileri ve Uygulamalı Bilimler Dergisi, 4, 37–48.