BİLGİ GÜVENLİĞİ ve AKILLI KARTLAR

Mustafa BAŞAK
Fehime BIYIKLIOĞLU
TÜBİTAK-UEKAE, Gebze
mbasak@uekae.tubitak.gov.tr
fehime@uekae.tubitak.gov.tr

ABSTRACT

Today, as the smart cards are frequently used in Information Technologies, smart card security has become an important issue. In this paper, security attacks that are specific to smart cards are described. Security considerations that need to be taken into account when developing a secure smart card are studied. AKiS, a secure smart card operating system which we designed according to these security considerations is introduced. AKiS is a secure and robust smart card which has CC EAL 5+ certificate for its chip and CC EAL4+ certificate for its smart card operating system. AKiS will be used in e-government applications such as health care card, national id card, and transportation card for municipality.

Key words: AKiS, Smart Card, Security, APDU, DES, PIN, PUK, SPA.

1. GİRİŞ

Akıllı kartlar günümüzde Bilgi Teknolojileri alanında çok önemli bir rol oynamaktadırlar. Akıllı kartlar temel olarak iki sınıfa ayrılırlar: *bellek kartları ve mikroişlemcili* kartlar. Bellek kartları, telefon kartı ve ön ödemeli olarak kullanılan kartlardır. İçerisinde basit bir seri numarası ve sayaç barındırırlar. Bu kartlarda yüksek güvenlikli ve büyük miktarda bilgi saklanması olanaklı değildir. Mikroişlemcili kartlar, yüksek seviyede güvenlik gerektiren alanlarda kullanılan kartlardır. Bu tip kartlar, yetenekli bir mikroişlemci, gelişmiş bir şifreleme modülü, verilerin saklandığı EEPROM ve RAM bellekten oluşur. Mikroişlemcili kartların en belirgin özelliği içerisindeki ROM alanında bir işletim sisteminin bulunması ve işletim sistemi tarafından verilerin güvenli ve düzenli bir şekilde tutulabilmesidir. Bu tip akıllı kartlar özellikle cep telefonları için SIM kartı, bankacılıkta kredi kartı, ulusal kimlik kartı, pasaport, sağlık kartı veya geçiş denetimi kartı olarak kullanılmaktadırlar. Akıllı kartlar veri iletimi yöntemine göre de iki sınıfa ayrılırlar: *temaslı ve temassız*. Temaslı kartların çalışması için ihtiyaç duyduğu enerji temas noktaları üzerinden iletilir. Temassız kartlarda ise herhangi bir elektriksel bağlantı olmaksızın kartın ihtiyaç duyduğu enerji belli bir mesafede havadan iletilir. Temassız kartlar genellikle pasaport, geçiş denetimi, ulaşım, uçak bileti gibi uygulamalarda kullanılmaktadır. Temaslı ve temassız ara yüz özelliklerini tek kartta taşıyan dual interface (çift ara yüz) kartlar da mevcuttur. Bu bildirinin giriş bölümünde akıllı kart kavramı, Akıllı kartlarda güvenlik başlığı altında akıllı kartlara saldırı yöntemleri, son bölümde Güvenli bir akıllı kart, AKiS başlığı altında bir işletim sistemi olarak AKiS'in güvenlik önlemleri anlatılmaktadır.

2. AKILLI KARTLARDA GÜVENLİK

Akıllı kartların manyetik kart ya da disket gibi diğer veri saklama araçlarına olan üstünlüğü veriyi güvenli olarak saklayabilmeleridir.
Akıllı kartlarda güvenlik dört bileşen ile sağlanmaktadır. İlki fiziksel olarak kartın kendisidir. Diğer bileşenler yonga, işletim sistemi ve kart üzerindeki uygulamalardır. Bir akıllı kartın güvenli olduğunu söyleyebilmek için kartın tüm bu bileşenlerinin saldırılara karşı savunma mekanizmaları olmalıdır. Bu bileşenlerden herhangi biri güvenlik gereksinimlerini karşılamıyorsa o akıllı kartın güvenliğinden bahsedilemez.
Akıllı kartların kullanımı yaygınlaştıkça kartlara olan saldırılar da çoğalmaktadır. Aşağıda akıllı kartlara uygulanan genel saldırı yöntemleri anlatılmaktadır.

- **Veri iletişiminin dinlenmesi:** Kart okuyucu ve kart arasındaki hattın dinlenerek gelen/giden verinin ele geçirilmesi.
- **Veri iletişiminin manipülasyonu:** Yonga modülünün temas noktalarına tel iliştirilerek okuyucu ve kart arasındaki veri istenilen şekilde değiştirilebilir.
- **UV ışığı kullanarak EEPROM'un silinmesi:** UV ışığıyla EEPROM silinerek kartın güvenli durumu bozulabilir.
- **Gücün kesilmesi:** PIN kontrolü sırasında güç kesilerek hata sayacının sıfırlanması önlenebilir.
- **Saat işaretinin kesilmesi:** Saat işareti kesilip elektron ışın test edici ile RAM içeriği gözlenebilir.

- **Mikroişlemcinin lazerle kesilmesi:** Mikroişlemcinin üst tabakaları lazerle kesilerek içyapısı bozulabilir.
- **Zamanlama saldırısı:** Kriptografik algoritmalarda anahtara bağlı olarak işlem süresi değişebilmektedir. Bu değişimden yararlanarak anahtarlar ortaya çıkabilir.
- **DES anahtarı analizi:** Süper bilgisayarlar kullanılarak deneme yanılma yöntemiyle DES anahtarları ele geçirilebilir.
- **Yan kanal analizleri (SPA/DPA)**: Kart çalışırken karttan sızan bilgileri inceleyerek yapılan işlemleri ve gizli verileri açığa çıkarmaya yönelik bir saldırıdır. Yan kanal analizlerinin zamanlama analizi, güç analizi, elektromanyetik analiz gibi türleri vardır.
- **Hata enjeksiyonu:** Belli mekanizmalar kullanarak kart işlemcisine hata yaptırmayı amaçlar. Gerilimdeki değişimler işlemcinin komutları atlamasına ya da yanlış yorumlamasına sebep olabilir. Saat işaretindeki değişimler verinin yanlış okunmasına sebep olabilir. Sıcaklıktaki değişimler işlemcide tutarsız davranışlara yol açabilir. İşlemciye yöneltilen lazer ışığı ya da beyaz ışık devrelerde hataya sebep olabilir. Elektromanyetik değişimler RAM'deki verilerin değişmesine sebep olabilir.

3. GÜVENLİ BİR AKILLI KART, AKİS

Akıllı kartlara yönelik geliştirilen saldırılara karşı akıllı kartlarda hem donanımsal hem de yazılımsal önlemler alınmalıdır. Güvenli bir akıllı kartta bulunması gereken güvenlik önlemleri aşağıda sıralanmıştır.

Anomali sensörleri

Akıllı kartlarda anormal durumları sezmek için çok sayıda donanımsal anomali sensörü yer almaktadır. Bu sensörler karta uygulanan gerilim, saat işareti, sıcaklık, ışık gibi etmenlerin tanımlı alt ve üst limitlerin dışında olduğu anormal bir durum sezdiğinde, kart yongası bu durum ortadan kalkana kadar çalışmasını keserek kendini güvenli duruma alır (reset durumu). Bu sensörler sayesinde UV ışığı kullanarak EEPROM'un silinmesi, saat işaretinin kesilmesi gibi saldırılara karşı koruma sağlanmış olur.

Akıllı kart yongasının güvenlik önlemleri

Akıllı kart yongalarında yonganın yüzeyinin kazılarak analiz edilmesini önlemek için değişik yöntemler uygulanmaktadır. İlk olarak önemli bloklar yongaya rasgele yerleştirilirler. Bir başka yöntemde mikroişlemcinin lazerle kesilmesi saldırısına karşı yonganın üzerine ikinci bir metal tabaka konarak yonganın özelliklerinin ortaya çıkması engellenir. Güçlü akıllı kart yongalarında, yonga yüzeyinden değerli verileri okumayı engellemek için etkin kalkan (active shield) olarak adlandırılan bir mekanizma kullanılmaktadır. Bu mekanizmada yonga yüzeyinde gelişigüzel dizilmiş ve rasgele sayı üretecinden elde edilen verilerle beslenen çok ince veri yolları bulunmaktadır. Etkin kalkan mekanizması bu veri yollarındaki değişken verilerin doğruluğunun denetlenmesi prensibine göre çalışmaktadır. Eğer bu yüzey aşındırılacak olursa veri yollarındaki veriler hatalı olacağından yonga kendisini güvenli konuma sokar (reset durumu).

Akıllı kart işletim sisteminin güvenlik önlemleri

- Algoritmaların işlem süreleri sabitlenerek yan kanal analizleri ve zamanlama analizleri ile gizli bilginin açığa çıkarılması önlenir. Eğer herhangi bir işlemin gerçekleşme süresi gizli bilginin içeriğine bağlı olarak değişiyorsa, bu bilgi güç analizi ile ortaya çıkabilir. Bu nedenle giriş değerleri ne olursa olsun işlem süreleri sabit tutulmalıdır. Bunun için gerekiyorsa algoritmanın değişik noktalarına rasgele gecikmeler eklenir.
- Güvenlik açısından önemli olan verilere (anahtarlar, PIN, PUK, vs) toplama sınaması konularak verinin bütünlüğü denetlenir. Herhangi bir nedenle bütünlük bozulduğunda kart kendini korumaya alır.
- Algoritmalarda gerçeklenen işlemlerin işleyiş sırası değiştirilerek algoritmanın ne yaptığının saptanması güçleştirilir.
- Algoritmalarda gerçekleştirilen karşılaştırma işlemleri gibi kritik işlemlere çift kontrol konulup sonuçlar karşılaştırılarak hata enjeksiyonunun önüne geçilebilir.
- Güvenlik açısından önemli verilerin birden fazla kopyası birden fazla formda tutularak (verinin üssü, vs) verinin değiştirilmesi durumu sezilebilir.
- Yan kanal analizlerinde yanlış PIN girilmesi sonucu PIN hata sayacının azaltılma işlemi tespit edilip o sırada güç kesilerek hata sayacının azaltılması engellenebilmektedir. PIN doğrulaması yapılırken PIN'in doğruluğuna bakılmadan sayaç azaltılıp PIN doğru girilirse eski değerine çekilerek bu saldırı önlenebilir.
- Veri iletişiminin dinlenmesi ve veri iletişiminin manüpülasyonu saldırılarına karşı akıllı kartlar ve ara yüz yazılımı arasındaki veri iletişimi güvenli mesajlaşma metodu kullanılarak korunabilir. Böylece giden gelen veri araya giren saldırganlar tarafından anlaşılamaz. Güvenli mesajlaşmada kart ve yazılım ara yüzü karşılıklı simetrik bir kriptografik algoritma anahtarı oluştururlar. Komut içerisinde yer alan

veri oturum anahtarı denilen bu anahtar ile şifrelenerek iletilir.

- DES algoritmasının zayıflığından dolayı veri şifreleme ve deşifreleme için DES yerine 3DES algoritmasının kullanılması önerilir.
- PIN ve PUK gibi yüksek güvenlik gerektiren verilere uzunluk sınırlaması getirilerek deneme yanılma yöntemiyle tahminleri güçleştirilir.

Yukarıdaki paragraflarda akıllı kartlarda güvenlik için dikkat edilmesi gereken konular üzerinde duruldu. Aşağıdaki paragraflarda bu güvenlik gerekleri dikkate alınarak gerçekleştirilen AKiS işletim sistemi hakkında bilgiler verilecektir.

AKiS işletim sistemi, donanım platformu olarak, yüksek güvenliğe sahip Infineon firmasının SLE66CX680PE ve NXP firmasının P5CC080 yongaları üzerine yüklenebilmektedir. Bu yongalar CC EAL 5+ (BSI0002 uyumlu) sertifikasına sahiptir. Bu yongalar üzerine kazılan AKiS işletim sistemi de CC EAL4+ güvenlik sertifikasına sahiptir. AKiS'in hem donanımı hem de işletim sistemi yukarıda sıralanan güvenlik önlemlerini uygulamaktadır.
Donanım platformu olarak bu yongalar 8051 tabanlı gelişmiş bir mikroişlemciden, ROM, EEPROM, RAM, Gelişmiş Kripto Makinesi (ACE), güvenlik onayı almış Rasgele sayı üreteci, MMU, UART, Zamanlayıcılar ve MED olarak adlandırılan Bellek şifre/deşifre modüllerinden oluşur. Akıllı kart işletim sistemleri akıllı kart yongalarının ROM olarak adlandırılan bölümlerinde bulunurlar. Ayrıca bazı işletim sistemlerinin bir bölümü kullanılan uygulamalara bağlı olarak sonradan EEPROM olarak adlandırılan bellek alanına yüklenir. Bu işlem güvenlik açısından karmaşık bir sürecin tamamlanması sonrasında gerçekleştirilir (uygulamanın sertifikalandırılması süreci). AKiS işletim sistemi native bir işletim sistemidir ve koşturulabilir bölümü tamamıyla ROM üzerinde bulunmaktadır. Ancak kullanılacak uygulamaya bağlı olarak uygulama verileri EEPROM olarak adlandırılan bellek alanında AKiS Dosya/Bellek yönetim sistemi tarafından gelişmiş güvenlik önlemleri alınarak saklanmaktadır. Akıllı kart işletim sistemleri dış dünya ile iletişmini iki adet iletişim ucu üzerinden, APDU olarak adlandırılan uygulama protokol veri paketleri aracılığıyla gerçekleştirmektedir. Bu protokol ISO7816-2/3/4 standartlarıyla tanımlanmıştır.

4. AKİS'İN KULLANIM ALANLARI

AKiS işletim sistemli akıllı kartlar, elektronik devlet uygulamalarında kişinin kendisini elektronik ortama ispat edebilmesi için kullanılacak bir araç olarak tasarlanmıştır. Kişinin kendisini elektronik ortama tanıtması kendisine verilen akıllı kart ve bu akıllı kart içerisindeki sertifika ile mümkün olmaktadır. Akıllı kart içerisindeki sertifika ve verilerin işlenmesi/yönetilmesi akıllı kart içerisindeki işletim sistemi aracılığıyla sağlanmaktadır. Bu nedenle akıllı kartların son derece güvenli olması ve içerisindeki verilerin doğru yönetilmesi önem arz etmektedir.

AKiS işletim sistemli akıllı kart, güvenli bilgi taşıma aracı olarak tasarlandığından e-devlet uygulamalarında kullanılması planlanmış ve ilk olarak e-ID ve Sosyal Sigorta işlemlerinde kullanılmasına karar verilmiştir. Bu durumda kişi AKiS işletim sistemli akıllı kartı ve içerisinde bulunan sayısal imza sertifikası aracılığıyla sayısal imza atma ve e-devlet uygulamalarını kullanma olanağına kavuşmuştur. AKiS kartlarının yakın gelecekte şehircilik uygulaması dahil birçok uygulamada kullanılması planlanmaktadır.

5. SONUÇLAR

Bu bildiride öncelikle akıllı kart kavramı ve akıllı kart çeşitleri incelendi. Akıllı kartlarda güvenlik başlığı altında, akıllı kartlarda güvenliğin önemi ve akıllı kartlar için geliştirilen saldırı yöntemleri incelendi. *Güvenli bir akıllı kart, AKiS* başlığı altında akıllı kartlara yönelik saldırılara karşı akıllı kart donanımlarında ve akıllı kart işletim sistemlerinde bulunması gereken güvenlik tedbirleri irdelendi. Geliştirdiğimiz AKiS işletim sisteminin bu güvenlik önlemlerini kullanması ve sahip olduğu güvenlik sertifikaları ile ilgili bilgiler verildi.

KAYNAKLAR

[1] W. Rankl, W. Effing, *Smart Card Handbook,* Giesecke & Devrient Gmbh, Munich, Germany, 2003

[2] K. E. Mayes, K. Markantonakis, *Smart Cards, Tokens, and Applications,* University of London, UK, 2008

[3] S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks,* Graz University of Technology Graz, Austria, 2007