OKU Fen Bilimleri Enstitüsü Dergisi
Cilt 4, Sayı 1, 86-90, 2021

OKU Journal of Natural and Applied Sciences
Volume 4, Issue 1, 86-90, 2021

Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi

Osmaniye Korkut Ata University Journal of Natural and Applied Sciences

Ödeme Terminallerinde PCI PTS Standartlarına Uygun Özgün Güvenlik Çözümü Gerçeklemesi

Kemal AŞÇI[1], Ersin HATUN[2*], Vedat NOMMAZ[3], Aaron NOMMAZ[4]

[1,2,3,4]Hugin Yazılım Teknolojileri A.Ş., Ar-Ge Merkezi, 34427, İstanbul

[1]https://orcid.org/0000-0003-4092-9458
[2]https://orcid.org/0000-0001-7524-7460
[3]https://orcid.org/0000-0001-9181-1965
[4]https://orcid.org/0000-0001-9732-0411
*Sorumlu yazar: ersin.hatun@hugin.com.tr

Araştırma Makalesi

Makale Tarihçesi:
Geliş tarihi: 24 Kasım 2020
Kabul tarihi:1 Ocak 2021
Online Yayınlanma: 2 Mart 2021

Anahtar Kelimeler:
Ödeme terminali
PCI PTS
Harici sensör
Akıllı kart
Tuş takımı
Kurcalama atakları

ÖZET

Ödeme terminalleri (EFT-POS) üzerinden finansal ve kişisel veriler geçtiği için dışarıdan müdahale ile bilgilerin ele geçirilememesi çok önemlidir. O yüzden yazılımsal ve donanımsal çözümlerle çeşitli önlemler alınmaktadır. Alınacak önlemlerle ödeme kartı endüstrisi (PCI) tarafından yayınlanan yönergelerde bulunan şartlar sağlanmaktadır. Teknoloji geliştikçe yeni saldırı methodları ortaya çıkmaktadır. Yönergeler belli aralıklarla güncellenerek yeni saldırılara karşı da koruma sağlanmaktadır. Bunlardan en önemlisi cihazın güvenlik sinyalleri ile kurcalama ataklarını algılamasıdır. Bu çalışmada EFT-POS cihazı için kurcalamalara karşı korumalı güvenli bölgenin oluşturulması anlatılmıştır. Güvenliği sağlamak için özgün bir tasarım kullanılmıştır. Maxim işlemcinin kullanıldığı EFT-POS terminali güvenliği için akıllı kart ve tuş takımı koruması kısımları üstünde yoğunlaşılmıştır.

Implementation of Unique Security Solution according to PCI PTS Standards for POS Devices

Research Article

Article History:
Received: 24 November 2020
Accepted: 1 January 2021
Published online: 2 March 2021

Keywords:
EFT-POS
PCI PTS
External sensor
Smart card
Keypad
Tamper attacks

ABSTRACT

Since financial and personal data pass through point of sales (EFT-POS) terminals, it is crucial that information can not be intercepted by external intervention. Therefore, various measures are taken with software and hardware solutions. With the precautions to be taken, the conditions in the payment card industry (PCI) directives are met. As technology develops, new attack methods are emerging. The directives are updated periodically to protect against new attacks. The most important of these is that the device detects tamper attacks. In this study, the implemention of a tamper-proof safe zone for EFT-POS device is described. Unique solution is implemented to ensure safety. For the security of the EFT-POS terminal where the Maxim processor is used, the focus is on smart card and keypad protection sections.

To Cite: Aşçı K., Hatun E., Nommaz V., Nommaz A. Ödeme Terminallerinde PCI PTS Standartlarına Uygun Özgün Güvenlik Çözümü Gerçeklemesi. Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi 2021; 4(1): 86-90.

1. Giriş

Ödeme kartı sektöründe, saldırganlar EFT-POS (Electronic Funds Transfer-Point of Sale) cihazlarında kullanılan kredi kartı, para kartı gibi kartların içindeki özel bilgilere [1] odaklanırlar. Saldırganlar teknolojik alandaki gelişmelerden faydalanıp güvenlik duvarlarını [2] aşarak bu bilgilere ulaşmaya çalışırlar. Buna karşılık güvenlik önlemleri de PCI (Payment Card Industry) tarafından belli aralıklarla aktif saldırılara önlem alınacak şekilde güncellenir. Güncellemenin amacı güvenlik kontrol testlerinin daha sıkı yönergelerle yapılması ve yapılacak

saldırılara karşı hedef cihazların direncini artırmaktadır [1,2].

PCI PTS (Payment Card Industry PIN Transaction Security) güvenlik gereksinimleri, belirli işlevler ile ilgili olan modüllerden oluşmuştur. Değerlendirme altında olan cihazın veya bileşenin form faktörü ne olursa olsun, sağladığı işlevler yönergelerin uygulanabilirliğini sağlamalıdır.

EFT-POS özelliği olan ödeme kaydedici cihazlar, Ödeme Kartları Endüstrisi PIN İşlem Güvenliği Standartlarına [1] göre PCI seviye 3 veya PCI seviye 3 üstü güvenlik sertifikasına ve EMV (Europay, Mastercard, Visa) sertifikasyonuna sahip olmalıdır. PCI güvenlik standardının amacı kart verilerinin çalınmamasını sağlamaktır. Bu sayede yapılan işlemlerin güvenliği sağlanır. EMV ise verilerin çalınması durumunda içeriğinin işe yaramaz hale getirilmesini garanti etmektedir. EFT-POS özellikli YNÖKC (Yeni Nesil Ödeme Kaydedici Cihaz) üreticileri güvenlik yönergelerine uygun olarak çeşitli çözümler geliştirip PCI testlerini [1, 2] başarılı bir şekilde sonuçlandırmaktadırlar.

Çalışma kapsamında PCI güvenliği [1] donanımsal olarak kurcalamaya karşı koruma mekanizmasının sensörleri [3,4,5] ile sağlanmıştır. Yapılan çalışma ile akıllı kart ve tuş takımı koruması kısımları ele alınmıştır. İlerleyen bölümlerde sensörlerin nasıl kullanıldığı ve bu kullanım sırasında güvenlik sinyallerinin nasıl işlendiği açıklanmaktadır.

2. Koruma Mekanizması

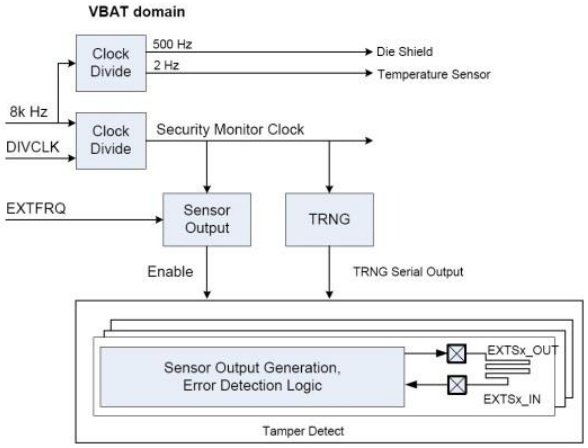
Güvenlik standartlarının yerine getirilmesi için fiziksel korumalar ve kurcalamaları algılamak (Tamper) için dinamik harici sensörler kullanılır [3]. PCI yönergelerine göre en az ekstradan dahili bataryayla destekli altı ayrı koruma noktası ile güvenlik sağlanmalıdır. Bu koruma mekanizması, yüksek korumalı mikroişlemcilerin içinde bulunan dinamik harici sensörlerin donanımsal çözümler ile beraber kullanılmasından meydana gelir.

Her bir dış müdahale algılama sensörü bir çift data hattından oluşmuştur. Şekil 1'de sensör çiftlerinin EXTS_IN ve EXTS_OUT bağlantıları gösterilmiştir. Sensörler tarafından dış müdahale algılandığında yüksek güvenlikli mikroişlemciler koruma moduna geçer.

3. Koruma Mekanizmasının Çalışması

3.1. Güvenlik Sinyalleri

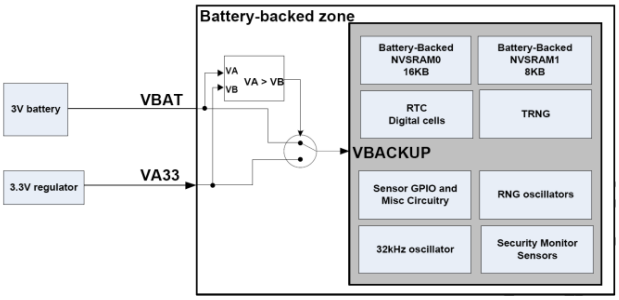
Dış müdahale algılama sensörleri EXTSCN [5] yazmacı üzerinden aktif edildikleri zaman kilitlenmiş olurlar ve artık değiştirilemezler. Sadece pilin bağlantısı (Şekil 2) kesilirse bu yazmacın kilidi açılabilir.



Şekil 1. Sensör bağlantıları

İşlemci içinde bulunan TRNG [6] (true random number generators) modülü rastgele sayılar gerektiren tüm uygulamalar tarafından kullanılmaktadır. Tamper sensörler için TRNG tarafından beslenen ayrı bir LFSR [5] (Linear Feedback Shift Register) tarafından verimli bir şekilde 128 bit gerçek rastgele sayılar üretilir. Örneğin, şifrelemeye hazır 128 bit AES rastgele anahtarı elde etmek için yalnızca dört ardışık okuma erişimi (32 bitlik erişim) gerekir.

Güvenlik monitor bloğu saldırı koşullarını izlemek için, Şekil 3'te gösterildiği gibi örüntüler üretmektedir. Soldaki şekil, EXTSCN yazmacında etkin kontrol bitini maksimum 2 kHz tarama frekansıyla (EXTFRQ = DIVCLK = 0xb) ayarladıktan sonra harici sensör sinyali taramasının başlangıcını gösterir. Sağdaki şekil, tarama işleminden bir süre sonra bir tarama döngüsünü gösterir.



Şekil 2. Batarya korumalı alan

Şekil 3. Güvenlik sinyal örüntüleri

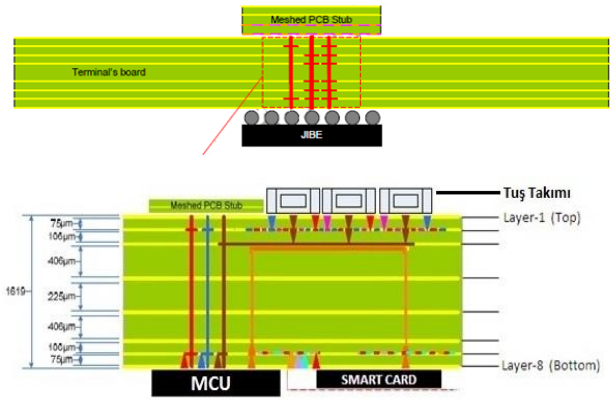
Her bir sensör çifti benzersiz bir sinyal üretir ve bağımsız olarak etkinleştirilebilirler.

Mesh bağlantıları ile korunan bölge veya bölgeler, fpc veya pcb layout ile sarmalanarak "tuzak" oluşturulmuştur. Herhangi bir delme, prob'lama veya iletken sıvı teması ile giriş/çıkış hatlarına ulaşmak amacıyla yapılacak saldırı girişimleri başarısızlığa uğrayacaktır.

Bir sensör çifti aktif olduktan sonra giriş piminde herhangi bir uyumsuzluk tespit edildiğinde, yazılımsal olarak cihaz yıkıcı bir resetlemeyi tetikleyerek, cihazı kullanım dışı bırakır. Bu işlemden sonra cihaz yapılan isteklere cevap veremez.

3.2. Güvenli Bölge Oluşturma Modeli

Buradaki koruma modelinde; Şekil 4'te görüldüğü gibi, üzerinden tamper sinyallerinin geçtiği bir örgülü mesh ile kaplı lehimlenebilir stup PCB [3] elektromekanik bileşen olarak ana pcb'de güvenlik işlemcisinin karşı yüzeyine lehimlenmiştir. Böylece ana işlemci ile stub PCB arasındaki tüm bağlantılar için güvenli bir bölge oluşturularak hassas bilgiler içeren sinyaller koruma altına alınmıştır.

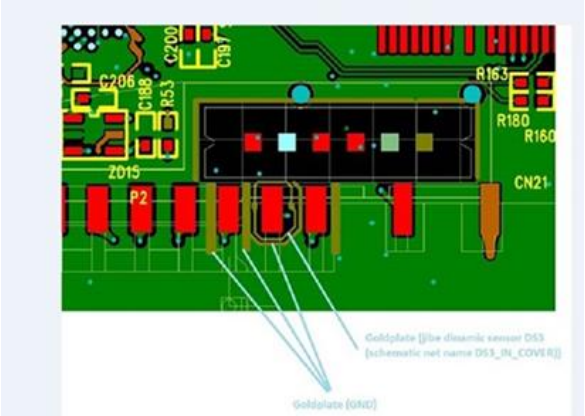


Şekil 4. Tamper ve I/O sinyalleri koruma alanı

3.3. Akıllı Kart Koruması

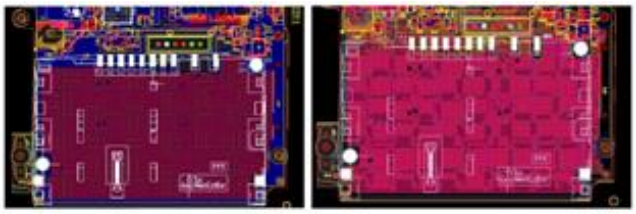
Bu çalışmada, akıllı kart okuyucu'nun giriş/çıkış data hattının bağlantısı Şekil 4 ve Şekil 5'te gösterildiği gibi dışarıdan yapılabilecek ataklara karşı tamper sensörleri kullanılarak korumaya alınmıştır. Bu sayede akıllı kart okuyucu konnektörüne yapılacak bir atağın önlenmesi ve başarısızlığa uğratılması sağlanmıştır.

Şekil 6'da soldaki şekil, akıllı kart okuyucu konnektörünün pcb üzerindeki bir katmanının bakır yollar ile kaplanmasını, sağdaki şekil ise farklı bir katmanının da kaplandıktan sonraki son durumunu göstermektedir.

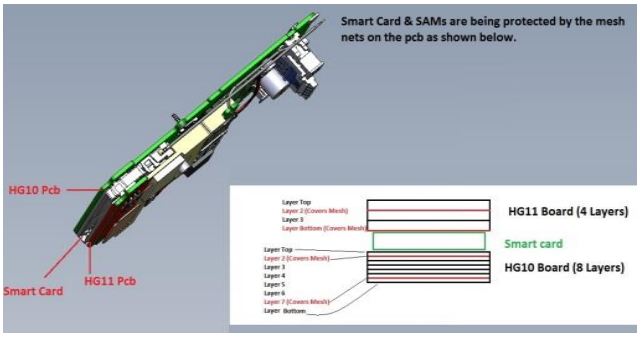


Şekil 5. I/O sinyali koruma alanı

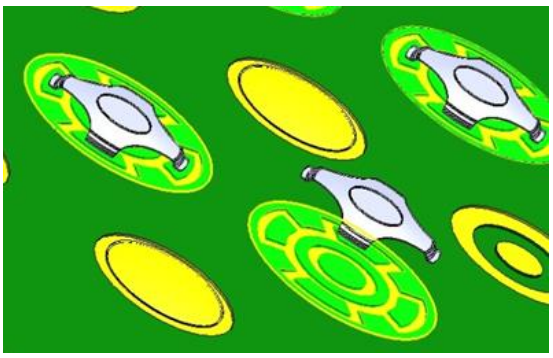
Böylece akıllı kart okuyucuya dikey olarak bir yönden ulaşılması engellenmiş olmaktadır. Aynı şekilde konnektörün diğer yüzeyi için de ayrı bir PCB kartta farklı katmanların da bakır yollar ile kaplanmasıyla diğer dikey yönden de ulaşılması engellenmiş olmaktadır. Böylece her iki yönden de yapılacak saldırılar [1] güvenlik sinyalleri ile koruma altına alınmıştır (Şekil 7).



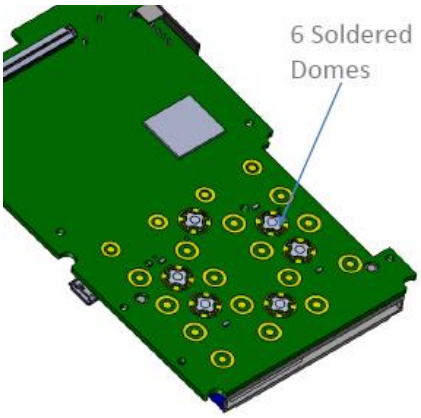
Şekil 6. Akıllı kart konnektörünün bakır yollar ile kaplanması



Şekil 7. Akıllı kart korumasının katman gösterimi



Şekil 8. Anahtar sensörlerin yerleşimi



Şekil 9. Sensörlerin tuş takımı üstündeki yerleşimi

3.4. Yazılımsal İşleyiş

Koruma mekanizması aktif edildikten sonra güvenlik sinyallerinde bir uyumsuzluk olması durumunda (Örneğin; cihaz kapaklarının kontrolsüz açılması) yazılımsal olarak bu durum anında algılanmaktadır. Atak algılandığında bu durum için kayıt tutulmakta ve yetkili servis müdahalesi tamamlanana kadar bu kayıt silinmemektedir. Sadece yetkili servisin giriş yapabileceği bir modda kullanıma izin verilmektedir. Teknik müdahale yapılmadığı sürece cihaz normal modda kullanılamamaktadır. Yetkili servis üreteceği tekil bir şifre ile giriş yapabilmektedir. Tutulan olay kayıtları yardımıyla cihazın durumu değerlendirmektedir. Fiziksel incelemeyle cihaza müdahale olup olmadığına karar verilmektedir. Sorun giderildiğinde yetkili servis müdahalesi ile normal çalışma moduna dönülebilmektedir. Normal çalışma moduna dönüldüğünde koruma mekanizması işleyişine aynı şekilde devam etmektedir.

4. Sonuç

Ödeme terminalleri üzerinden geçen kişisel veriler nedeniyle saldırganların hedefi konumundadır. Bu sebeple uluslararası yönergelerle güvenlik sertifikasyonlarına tabi tutulmuşlardır. Her geçen gün saldırganlar atak yöntemlerini yeni teknolojilerle geliştirirken sertifika otoriteleri de güvenlik standartlarını güncel ataklara uygun hale getirmektedirler. Yönergedeki güvenlik şartlarını sağlamak için üreticiler farklı çözümler uygulamaktadırlar. Çalışma kapsamında akıllı kart ve tuş takımı güvenliğine yoğunlaşılmıştır. Geçmiş bölümlerde açıklanan uyguladığımız çözümler ile PCI-PTS POI yönergelerine [1], [2], [6]-[10] uygun bir cihaz geliştirilmiştir. Tamper güvenlik sinyalleri kullanılarak dış müdahaleyi engellemek için özgün bir tasarım oluşturulmuştur. Sonuç olarak güvenli mikroişlemcinin özgün tasarımla birleşmesiyle gelişmiş bir ödeme terminali üretilmiştir.

Çıkar Çatışması Beyanı

Makale yazarları aralarında herhangi bir çıkar çatışması olmadığını beyan ederler.

Araştırmacıların Katkı Oranı Beyan Özeti

Yazarlar makaleye eşit oranda katkı sağlamış olduklarını beyan ederler.

Teşekkür

Bu çalışma, Tübitak TEYDEB destekli 1120190 no'lu proje ve 2017/11114 patent başvurulu ürün üzerinde gerçekleştirilmiştir. EMV çalışmalarında FIME firmasının Fransa laboratuvarıyla ortak çalışma yapılmıştır.

Kaynakça

[1] ISO 9564-1: 2011 Personal Identification Number Management and Security, Part 1:PIN Protection Principles and Techniques

[2] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements, PCI Security Standards Council LLC Version 3.1, October 2011

[3] Maxim referans tasarım https://www.maximintegrated.com/en/products/microcontrollers/MAX32590.html/tb_tab2

[4] DS21H10RevD-MAX32590JIBE_Datasheet https://datasheets.maximintegrated.com/en/ds/MAX32590.pdf

[5] UG21H05RevE-max32590_UserGuide.pdf https://www.maximintegrated.com/en/products/microcontrollers/MAX32590.html/tb_tab2

[6] Designing Next Generation Payment Terminals That Meet PCI PTS 3.x Requirements By: Yann Loisel- Application Note 4809 – Maxim

[7] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Detailed Test Procedures, PCI Security Standards Counicl LLC, Version 3.1, October 2011

[8] PCI PTS POI Modular Security Requirements, PCI Security Standards Council LLC, Version 3.1, October 2011

[9] PCI PTS POI Evaluation Vendor Questionnaire, PCI Security Standards Council LLC, Version 3.1, October 2011

[10] Payment Card Industry (PCI) PTS POI Security Requirements v3 FAQ, PCI Security Standards Council LLC, Version 3.1, October 2011