Smart kartların təhlükəsizlik problemləri və onların qiymətləndirilməsi

Murad Qurbanov

Azərbaycan Respublikası Rabitə və Yüksək Texnologiyalar Nazirliyi, Məlumat Hesablama Mərkəzi
murad@rabita.az

***Xülasə*— Hazırda smart kartlar bir çox tətbiqlərdə təhlükəsizliyi təmin edən mexanizmə çevrilib. Bu da smart kartlara olan hücumların, bu sahədə araşdırmaların və nəticədə təhlükəsizlik problemlərinin ortaya çıxarılmasını aktual məsələyə çevirir. Bu tədqiqatda smart kartların təhlükəsizlik problemləri və bu problemlərin qarşısının alınması üsulları araşdırılır. Həmçinin, tədqiqat smart kartların təhlükəsizlik səviyyəsinin müəyyən edilməsi üçün istifadə olunan qiymətləndirmə sxemlərini də əhatə edir. Məqalədə smart kartların hazırki təhlükəsizlik səviyyəsinin, smart kartların müdafiə mexanizmlərinin və Ümumi Meyarlar təhlükəsizliyi qiymətləndirmə standartının icmalı da əks olunub.**

Açar sözlər— smart kart; Ümumi Meyarlar; smart kartlara hücumlar; kibercinayətkarlıq; kibertəhdid.

I. GİRİŞ

Smart kartlar autentifikasiya ve identifikasiya üçün unikal imkanlar açır. Smart kartların inkişafı, fiziki açarların, autentifikasiyanı təmin edə biləcək ekvivalent mexanizmlə əvəz olunması tələbindən başlamışdır. Bu tip autentifikasiya subyektin yalnız biliyinə deyil, həmçinin sahib olduğu cismə əsaslanır (multifaktor autentifikasiya). Bir çox həllərdə, bu təhlükəsizlik üstünlüyü smart kartları əvəzedilməz edir. Smart kartlar mobil operatorların SIM kartlarında, kredit və ödəniş kartlarının bir hissəsi olub, ödəniş sistemlərində istifadə olunur.

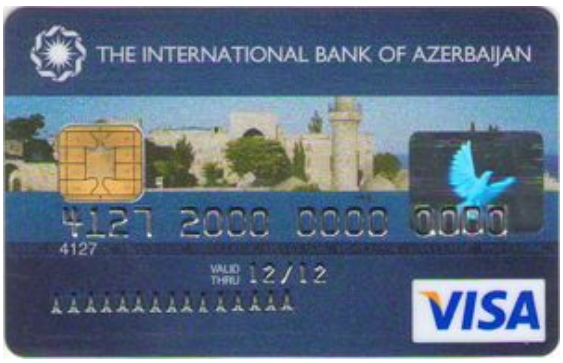
Smart kartlar əsasən kritik tətbiqlərdə təhlükəsizliyi təmin etmək üçün istifadə olunur, buna görə də onların təhlükəsizliyi ciddi məsələdir. Təhlükəsizliyi smart kartlara əsaslanan və təhlükəsizliyi yüksək səviyyədə təmin edəcək infrastrukturların həyata keçirilməsi üçün smart kartların təhlükəsizliyi hansı dərəcədə təmin edə biləcəyi müəyyən edilməlidir.

II. SMART KARTLARIN İCMALI

Smart kart quruluşuna görə digər elektronika ilə əlaqə üçün kontaktlara malik olan və özündə inteqral sxemlər (çip) saxlayan kartdır. Kontaktlar tətbiqlərdən asılı olaraq fərqlənə bilər. Kontaktlar əsasən qızılı və ya gümüşü rəngdə, üzərində mis məftil konturları olan, dördbucaq metal sahə formasındadırlar.

Smart kartlar kontaktlar olmadan belə fəaliyyət göstərə bilir. Bunlara kontaktsız smart kartlar deyilir. Kontaktsız smart kartlar çip ilə əlaqəni radio-tezlikli identifikasiya (RFİD)

texnologiyası vasitəsilə həyata keçirir. RFID texnologiyası standard smart kart texnologiyasından radikal olaraq fərqlidi və ayrıca araşdırma sahəsidir. RFID texnologiyasında fiziki interfeysin olmaması ilə əlaqədar bir çox təhlükəsizlik boşluqları vardır [5]. Bu məqalədə biz yalnız fiziki kontakta malik smart kartların təhlükəsizliyini araşdırmışıq.



Şəkil. 1. Kredit kartlarında gücləndirilmiş autentifikasiya üçün smart kartlar tətbiq edilə bilər

Smart kartlarla bağlı ilk araşdırmalar 1960-cı illərdə, ödəniş sistemləri üzrə ixtisaslaşmış, Alman şirkəti olan Giesseck & Devrient tərəfindən başlanmışdır. Bu işin davamçıları olaraq, bir neçə şirkət 1970-ci illərdə çip üzərində yaddaş və 1978-ci ildə mikroprosessor yerləşdirməyə nail olmuşdurlar. Sonradan 1992-ci ildə smart kartlar bank ödənişləri üçün qəbul edilmişdir və ardınca GSM mobil telefoniya standartında mobil telefonun autentifikatoru kimi təsdiqlənmişdir.

Smart kartlar çox hallarda ISO 7810 [7] standartına uyğun olaraq dizayn olunur. Burada onların standart ölçüləri, çipin forması və xarakteristikaları, çiplə kommunikasiya protokolları təyin edilir. Qeyd etmək lazımdır ki, smart kartlar batareya saxlamırlar. Çipin interfeyslərinin dizaynı isə İSO 7816 [8] standartı ilə müəyyən edilir.

III. SMART KARTLARA HÜCUMLAR

Smart kartlara hücumları bir neçə sinfə bölmək olar [4]:

- *İnvaziv* - smart kartın inteqral sxemlərinin və proqramının quruluşunu ortaya çıxaran hücumlar.
- *Qeyri-invaziv* - smart karta fiziki təsir olmadan hücumlar.
- *Qapanma tipli hücumlar* - smart kartların kommunikasiya kanallarında süni səhvlər yaratmaqla həyata keçirilən hücumlar.

3.1 Əks istiqamətdə mühəndislik

Əks istiqamətdə mühəndislik hücumları smart kartlara qarşı tətbiq edilə bilən ən təsirli hücumlardır [1][2]. Bu hücum zamanı smart kartın inteqral sxemləri müxtəlif kimyəvi maddələr və cihazlar istifadə edilərək ortaya çıxardılır. Əksər hallarda bu prosesdən sonra çip normal istifadə üçün yararsız hala gəlir. Bəzi hallarda, çipin quruluşu müxtəlif açıq

mənbələrdən götürülə bilər. Bu yolla çipin istifadə etdiyi kommunikasiya kanalları, kriptoqrafik sxemləri və təsadüfi ədəd generatorları öyrənilə və hücum edilə bilər.

Çipin dizaynı zamanı ehtimal edilməlidir ki, hücumçu sistemin quruluşunu bilir və təhlükəsizliyi bu ehtimal əsasında təmin etmək lazımdır. Praktikada bir çox smart kartlar zəif təsadüfi ədəd generatorları, köhnəlmiş kriptoqrafik protokollar və kommunikasiya kanallarından istifadə edirlər. Misal olaraq, 1994-1999-cu illərdə Amerika, Asiya və Avropada dizayn olunmuş bütün smart kartlar bu tip hücumlara davam gətirə bilməmişdilər [9].

3.2 Zondlama hücumları

Zondlama hücumları zamanı çipin daxili kommunikasiya kanalları ilə ötürülən elektrik siqnalları analiz edilir. Bunu etmək üçün çipin kommunikasiya kanallarına mis məftillər birləşdirilir və gərginlik ölçüləri götürülür [2]. Çipin üzərində müdafiə qatı olduqda isə ion lazeri vasitəsilə bir çox müdafiə qatlarını sıradan çıxarmaq olar.

Çipdəki elektrik siqnalları oxunula bildikdə gizli açarlar və məlumatlar əldə edilə bilər.

3.3 Zamanlama analizi

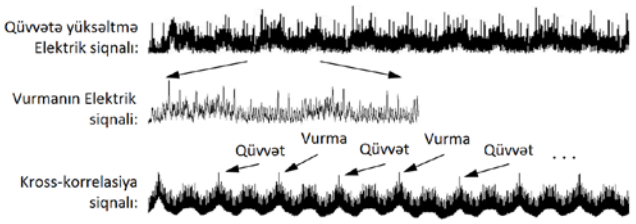
Smart kartlarda gedən proseslərə sərf olunan zamanı analiz edərək proseslər barədə müəyyən fikirlər yürütmək mümkündür. Çip - kriptoprosessorların proseslərə sərf etdiyi zaman, emal edilən məlumatın və açarların uzunluğundan, kriptoqrafik alqoritmlərin növündən asılı olaraq dəyişir. Bir sıra ölçmələr apararaq bu məlumatlar və açarlar barədə informasiya əldə etmək mümkündür. Məsələn, kartın PİN-kodunu daxil edərkən ilk rəqəm doğru olduqda, smart kart səhv barədə məlumatı, PİN-in tamamilə səhv olduğu haldan daha gec çatdıracaqdır. Bu üsulla smart kartın tam PİN-ini öyrənmək mümkündür.

Zamanlama analizi çox zaman digər hücumlarla birgə istifadə edilir və bəzi hallarda yalnız statistik analizin əldə edilməsi ilə nəticələnir.

3.4 Elektrik istifadəsinin analizi

Elektrik istifadəsinin analizi zamanlama analizinə bənzəyir və eyni növ hücum kateqoriyasına aiddir. Smart kartlarda gedən proseslərin elektrik sərfinə görə istifadə olunan kriptoqrafik protokollar, açarlar, emal edilən məlumatlar və hesablamalar barədə statistik məlumatlar əldə etmək olar. Məsələn, bitin 0 vəziyyətindən 1 vəziyyətinə gətirilməsi üçün əks prosesdən daha çox elektrik sərf olunur. Bunu bilərək və xüsusi ölçmələr apararaq emal edilən məlumatları əldə etmək mümkündür.

Daha bir misal olaraq qüvvətə yüksəltmə və vurma əməliyyatlarını yerinə yetirən, RSA və El-Gamal kriptoqrafik sxemlərində istifadə edilən "square-and-multiply" (SAM) alqoritmi bu tip hücumlar zamanı gizli açar barədə məlumatları sızdırır [10].



Şəkil. 2. SAM alqoritmində eksponentin bit ardıcıllığı

3.5 Süni səhvlərin yaradılması hücumları

Bəzən qısa qapanma hücumları kimi də tanınan bu hücum vektoru smart kartın normal əməliyyatlarının qarşısını alır və müəyyən məlumatları ələ keçirməyə imkan verir. Bu növ hücumlar əsasən üç kateqoriyaya bölünür:

1. *DoS hücumları* − çipin müəyyən hissələrinin müraciətlərə cavab verə bilməməsinə gətirib çıxarır.
2. *Yüksək tezlikli saat hücumları* − bəzi xüsusi siqnallar vasitəsilə kriptoprosessorun saat tezliyini dəyişmək və bununla da bəzi əməliyyatların sırasını və hətta yerinə yetirilməməsini təmin etmək olar. Bu hallarda kriptoqrafik açarlar barədə məlumatlar sıza bilər.
3. *Optik və ya elektromaqnit hücumları* − düzgün nöqtələrdə, xüsusi tezlikli işiq şüaları ilə təsir edərək və ya güclü elektromaqnit sahəsi yaradaraq bit-ləri dəyişdirmək imkanı vardır. Bu isə bir sıra əməliyyatların tamlığına təsir edir və nəticədə məlumat sızmasına gətirib çıxarır.

IV. TƏHLÜKƏSİZLİK TƏDBİRLƏRİ

Smart kartlarda istifadə edilə biləcək bütün mudafiə mexanizmlərini bir məqalə çərçivəsində təsvir etmək mümkün deyildir. Bu səbəbdən bəhs edilən hücumların qarşısını almaq üçün istifadə olunan bəzi müdafiə mexanizmlərini təsvir etməklə kifayətlənəcəyik

4.1 Fiziki təhlükəsizlik

İnvaziv hücumlar zamanı smart kartlarda olan çiplərin müdafiə örtüyü çıxarılır. Bunu etmək üçün xüsusi kimyəvi maddələr (korroziyalaşdıran azot turşusu [9]) mövcuddur. Bu mərhələdə hücumun qarşısını almaq üçün çipin müdafiə örtüyünü kriptoprosessorun və ya məlumat daşıma blokunun bir hissəsi etmək olar. Bu vaxt hücum zamanı çipin funksional blokları yararsız vəziyyətə düşür. Əlavə olaraq, riskləri azaltmaq üçün örtük anti-korroziv materiallardan (məsələn, titan) hazırlana bilər.

Digər bir üsul isə örtüyün altında metal tor təbəqəsinin qoyulmasıdır [9]. Çip torun vəziyyətini daimi yoxlayır. Tor təbəqəsi çip açıldıqda zədələnir və növbəti yoxlama zamanı torun əlaqələri arasında kəsilmə və ya qısa qapanmalar aşkar edilərsə, bütün gizli məlumatlar çipdən silinir. Bu üsul çiplərin açılmasını olduqca cətinləşdirir, amma çiplərin qiymətini də olduqca yüksəldir. Sübut olunmuşdur ki, elektrik dövrələrin bu tip fiziki hücumların riyazi olaraq mümkünsüz olmasını təmin edəcək layihələndirilməsi mümkündür [6].

4.2 Çip kommunikasiyalarının gizlədilməsi

Çip üzərində kommunikasiyalar ələ keçirilməkdən qoruna bilər. Prinsipcə, çip uzərindəki kommunikasiyaları anlaşılmaz

formada layihələndirdikdə, zondlama tipli hücumlardan müdafiəni təmin etmək olar. Misal olaraq, sadəcə XOR əməliyyatından istifadə edərək, kanalın dinlənməsinin qarşısını alan yeni sistem tətbiq edilmişdir [2].

4.3 Süni səhvlərin yaradılması hücumlarına qarşı müdafiə

Bu kateqoriyadan olan hücumlar kriptoprosessorun proqnozlaşdırıla bilinməsindən və uyğun anda qısa qapanma yerinə yetirilməsindən irəli gəlir. Bunun üçün, kriptoprosessorun proqnozlaşdırabilinmə risklərini azaldan texnikalardan istifadə etmək lazımdır. Araşdırmaların nəticəsi olaraq bu riskləri azaltmaq üçün iki metod təklif edilir.

Birinci metod təsadüfi saat siqnalının tətbiq edilməsi və bununla da instruksiyaların icra edilmə uzunluğunu və anını daima dəyişməkdir.

İkinci metod isə saat sinxronlaşmasını sıradan çıxaran qısa qapanmaların qarşısını ala biləcək modulun çipə əlavə edilməsidir. Bu modul, sinxronizasiya üçün vacib olan reyestrləri və digər məlumatları saxlayacaq [11,9].

4.4 Təsadüfi gecikmələr

Zamanlama analizi növlü hücumların qarşısını almaq üçün prosessor əməliyyatlarını təsadüfi gecikmələrlə həyata keçirmək tövsiyyə olunur. Öncəki bölmədə bəhs edilən təsadüfi saat siqnalı yetərli dərəcədə təhlükəsizliyi təmin etməyə qadir deyildir. Belə ki, prosessor instruksiyalarının böyük bir hissəsi binomial statik analiz metodu ilə təyin edilə bilər. Bu problemin həlli yollarından biri Seitz idarəedici elektrik komponentinin çipə əlavə edilməsidir [2]. Seitz idarəedici komponenti resurslara müraciətləri təsadüfi zaman və sıra ilə icazə verir. Məsələn: bu komponent prosessor şinini idarə etdiyi zaman məlumatların yaddaşa yazılması təsadüfi sıra ilə yerinə yetirilir.

4.5 Məlumatdan asılı elektrik istifadəsinin azaldılması

Elektrik istifadəsinin analizi növlü hücumlar prosessorun 0 və 1 bitləri emal edərkən fərqli dərəcədə elektrik istifadə etməsinə əsaslanır. Bu tip məlumat sızmalarının qarşısını almaq üçün müxtəlif kodlama texnikaları mövcuddur. Məsələn: kommunikasiya xətlərinə təsadüfi siqnalların ötürülməsi və bununla da ötürülən bitlərin gizlənilməsi mümkündür. Amma bu tip müdafiə mexanizmlərinin effektivliyi statistik analiz metodları vasitəsilə azaldıla bilər.

V. ÜMUMİ MEYARLAR STANDARTI

Ümumi Meyarlar standartı [3] smart kartlar üçün təhlükəsizliyin qiymətləndirilməsi modelini təsvir edir. Ümumi Meyarların qiymətləndirmə kriteriyalarını iki bölməyə ayırır: smart kartların özlərinə aid olan − funksional tələblər və onların istifadə olunduğu mühitə aid olan − təhlükəsizlik təminləri.

Funstional tələblər − Ümumi Meyarlar standartının təyin etdiyi funksional tələblər smart kartların ümumən, bütün daxili və xarici imkanlarını əhatə edir. Bu tələblər olduqca çox olduğundan, Ümumi Meyarlar standartı çərçivəsində smart kartların istifadə ssenarisindən asılı olaraq bu tələblər alt çoxluqlara bölünmüşdür [3].

Təhlükəsizlik təminləri - bu mərhələdə smart kartlar onların istifadə olunacağı mühitə uyğun test edilir və bu mühitdə təmin etməli olacaqları təhlükəsizlik səviyyəsi qiymətləndirilir.

Son olaraq, tətbiqlərdən asılı olaraq qiymətləndirmələr dəqiqlik dərəcəsinə görə sıralanır. Bu dəqiqlik dərəcələrinə qiymətləndirmənin təmini dərəcələri (evaluation assurance levels - EAL) deyilir. Hər EAL müəyyən etibarlılıq səviyyəsinə nail olmaq üçün həyata keçirilmiş qiymətləndirmələri təsvir edir.

Cədvəl. 1.* Ümumi Meyarların *qiymətləndirmə modeli

EAL	Açıqlamalar
EAL 1	Funksional olaraq test edilmişdir və problemsiz tətbiq edilir
EAL 2	Strukturlu test edilmişdir
EAL 3	Metodik olaraq test edilmişdir
EAL 4	Metodik olaraq dizayn, test edilib və qiymətləndirilib
EAL 5	Qeyri-formal dizayn və test edilib
EAL 6	Qeyri-formal yoxlanılıb, dizayn və test edilib
EAL 7	Formal olaraq yoxlanılıb, dizayn və test edilib

NƏTİCƏ

Smart kartlar, sadə quruluşa malik olmasına baxmayaraq bir çox hücum vektorlarına məruz qalırlar. Bu məqalədə smart kartlara qarşı olan hücumların təsnifatı təqdim edildi. Təhlükəsizlik mexanizmləri smart kartları müəyyən dərəcədə bu hücumlardan qorumağa qadirdir. Smart kartlar tətbiq elediyi təhlükəsizlik mexanizmlərinə əsasən qiymətləndirilə bilir. Bu qiymətləndirməni aparmaq üçün Ümumi Meyarlar standartından istifadə etmək məqsədəuyğundur. Ümumi Meyarlar smart kart çipləri üçün funksional tələbləri və təhlükəsizlik təminlərini təyin edir, qiymətləndirməni smart kartların təhlükəsizliyinin bütün aspektlərini nəzərə alaraq həyata keçirməyə imkan verir.

ƏDƏBİYYAT

[1] C. M. Amsuss. Reverse engineering smart cards, 2010.

[2] S. Moore, R. Anderson, P. Cunningham, R. Mullins, G. Taylor, “Improving smart card security using self-timed circuits,” Proc. of the 8th International Symposium on Asynchronous Circuits and Systems, pp. 211-218, 2002.

[3] Common Criteria (CC) v3.1. Release 4. http://www.commoncriteriaportal.org/cc/.

[4] I. El Farissi, M. Azizi, M. Moussaoui, “Classifcation of smartcard attacks,” International Conference on Multimedia Computing and Systems (ICMCS), pp. 1-5, 2011.

[5] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, R. Schreur, “Crossing borders: Security and privacy issues of the european e-passport,” 1st Int. Workshop on Security, LNCS 4266, pp. 152-167, 2006.

[6] Y. Ishai, A. Sahai, D. Wagner. “Private circuits: Securing hardware against probing attacks,”. Proc. of CRYPTO 2003, pp. 463-481, 2003.

[7] Identifcation cards - Physical characteristics, 2003.

[8] Identifcation cards - Physical characteristics, 1998.

[9] O. Kmmerling, M. G. Kuhn, O. Kmmerling, M. G. Kuhn. Design principles for tamper-resistant smartcard processors. 1999.

[10] T. Messerges, E. Dabbish, R. Sloan. “Power analysis attacks of modular exponentiation in smartcards,” Ko and C. Paar, editors, Cryptographic Hardware and Embedded Systems, LNCS 1717, pp. 724-724, 1999.