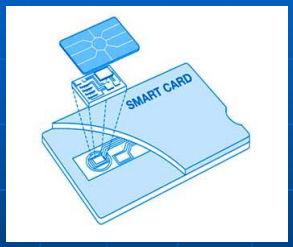
1

0113841
Mesleki Terminoloji

Akıllı Kart
(Smart Card)
Teknolojisi



Yard. Doç. Dr. A. Tevfik İNAN
Bilgisayar Mühendisliği Bölümü

(2012/1 Dönemi)

Akıllı Kart Nedir ?

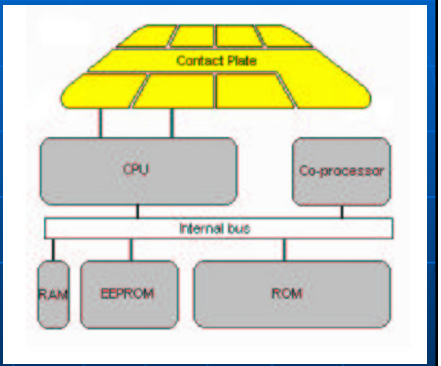
- İçinde bir işlemci ve/veya bellek birimi bulunduran, bir okuyucu ile eşleştiği zaman farklı uygulamalar için gerekli işlem gücüne sahip olabilen, plastik bir karttır.
- Kontrollü erişim sağlayabilme özelliği sayesinde kişisel veya ticari bilgilerin uygun (yetkili) kişiler tarafından görülebilmesini sağlar.
- Veri taşıma, taşınınan verinin güvenliği ve taşıma kolaylıkları nedeni ile her geçen gün çeştilenen ve daha yaygın olarak kullanılan bir teknolojidir.

3

Akıllı Kartın Genel Yapısı

Akıllı kartın genel yapısı incelendiğinde genel olarak bir bilgisayar sisteminde olan temel parçaları (daha düşük hız ve kapasitelerde olmak kaydı ile) bünyesinde barındırdığı görülür.

- Kredi kartı veya SIM kartı büyüklüğünde,
- Küçük işlem hacimli gömülü bir işlemci (8-bit işlemci ve 5 MHz hızdan başlar)
- Bellek (4 Kb RAM, 16 Kb EEPROM, 64 Kb ROM'dan başlar)
- Güvenli bir yapı (tamper-resistant)
- Ucuz sahip olma maliyeti (3-5 Euro)



4

Sahip Olduğu Donanım

- CPU
  - Veri işleme, şifreleme algoritmalarını ve uygulamalarda tanımlı kuralları çalıştırmak
- ROM (flash EEPROM)
  - Kart üzerindeki işletim sistemini barındırmak
- RAM
  - Veriyi geçici süreli saklamak
- EEPROM
  - Kullanım amacına bağlı olarak değişkenlik gösterebilen (kart sahibinin bilgileri, şifreler ve yapılan işlem detayları gibi) türde bilgileri saklamak
- Co-Processor
  - Şifreleme işlemlerinin daha hızlı yürütülmesini sağlamak
- Internal–Bus
  - Tüm birimler arasındaki veri/adres/kontrol haberleşmesini sağlamak
- Dedicated HW security
  - Kart üzerinde yer alan uygulama yazılımı veya kart üzerinde saklı bulunan bilgilere fiziksel veya mantıksal saldırılar ile erişilmesini (ele geçirilmesini) engelleyen ek donanım özellikleri

5

Kısa Tarihçe

- İlk akıllı kart uygulaması Fransadaki haberleşme ve bankacılık sektörelerindeki dolandırıcılık/sahtekarlık (fraud) faaliyetlerinin ortaya çıkardığı aşırı maliyet ile savaşabilmek için Motorola firmasının 1979 da ilk tek yonga mikro denetleyiciyili (single chipmicrocontroller) banka kartlarını Fransız bankaları için üretmesi ile başlar.
- 1980'lere gelindiğinde biri haberleşme sektörü için seri bellekli entegre devre (serial memory IC), diğeri ise bankacılık uygulamaları için daha üstün güvenlik özellikli mikro kontrolcü bulunduran devre (MCU-Micro Controller Unit - CPU, RAM, ROM, EEPROM, I/O birimleri barındırır.) olmak üzere iki tip kullanılmaya başlandı.
- Akıllı kartların evrimi kişisel bilgisayarlarınkine (PC) çok benzemektedir. Ancak günümüzdeki kartların işlem güçleri, 1980'lerdeki kişisel bilgisayar sistemlerinin işlem güçlerinin oldukça ötesindedir.

6

Kart Tipleri

- **Bellekli – Mikroişlemcili (Memory vs. Microprocessor)**
  Bellek kartları bir disket veya USB bellek biriminin yaptığı gibi (ancak ek güvenlik seçenekleri ile) veri depolama imkanı sağlarken, üzerinde mikro kontrolcü veya mikro işlemci olanlar küçük bir bilgisayar sistemi gibi, sahip oldukları bellek, güvenlik özellikli depolama alanı, G/Ç birimleri ve işletim sistemini kullanarak çok çeşitli işlemler yapabilir.
- **Temaslı-Temassız (Contact vs. Contactless)**
  Akıllı kartlar temaslı ve temassız olarak iki cinstir. Temaslı olanlar bir kart okuyucu biriminin içine kartın sokulması ve okuyucu ile fiziksel temasın sağlanması prensibine göre çalışırken, kontaksız olanlar, kart içine gömülmüş minik bir anten sayesinde okuyucuya fiziksel temas sağlanmadan kullanılabilirler. Bazı kartlarda her iki teknolojide birlikte bulunabilir. Bunlara melez (hybrid) kartlarda denir.

7

Akıllı Kart Yazılımları

- Geleneksel Akıllı Kartlar
  - Tek kart = tek işlev
  - Yazılım, ROM üzerinde ve güncelleme mümkün değil
  - Kart üreticisi tarafından üretilmiş tescilli (propietary) yazılım kullanılıyor
  - C veya assembly ile kod üretiliyor.
- Modern Akıllı Kartlar (Java Card, MultOS)
  - Bilginin kontrollü şekilde paylaşılması ile birden fazla uygulama tek kart üzerinde çalışabiliyor.
  - Sonradan uygulama (cardlets) yükleme imkanı var.
  - Yazılım Java ile üretiliyor (bir Java alt kümesi kullanılır)
  - Yazılım çoğu zaman kart üreticisinden bağımsız olarak hazırlanıyor.

8

Kart Üzerindeki Yazılımlar

- İşletim sistemi (Card OS)
  - Native OS: işletim sistemi ve kart üzerine yüklenmiş uygulama birbirleri ile sıkı biçimde eşlenmiştir.
  - Open OS (Java Card of MULTOS): Uygulamalar kullanılan bir API sayesinde işletim sisteminden ayrılmıştır. Böylece uygulamalar işletim sisteminden bağımsız olarak geliştirilebilir. Bu türde, sistem içindeki senkronizasyonun güvenliği, işletim sistemi ve uygulamaları birbirinden ayıran bir firewall tarafından sağlanmaktadır.
  - Uygulamaların yüklenmesi, çalıştırılması ve yönetilmesi için işletim sistemi aşağıdaki görevleri yerine getirmelidir.
    - Kart üzerinde yer alacak bir veya daha fazla uygulamayı kontrol etmek
    - Seri terminal bağlantısı üzerinden yapılan iki yönlü veri aktarımı
    - Çalışmanın kontrolü ve komutların işlenmesi
    - Veri erişiminin korunması
    - Bellek yönetimi
    - Dosya yönetimi
    - Şifreleme algoritmalarının yönetimi ve çalıştırılması
- Uygulama yazılımları
  - Bir uygulamanın gereği olarak yazılmış programlardır. Bir kart üzerinde birden fazla uygulama desteklenmesi mümkündür.

9

Güvenlik ??

- Akıllı kartlar finansal bilgilerin saklanması için kullanılan depolama çözümlerinin hepsinden daha fazla güvenlik ve mahremiyet sağlar. Bu kapsamda özel anhtralar (private key), hesap numaraları, şifreler ve kişisel bilgiler gibi değerli verinin saklanması için son derece elverişli bir ortamdır.
- Özellikle sahip olduğu hesaplama kabiliyetini kullanarak kendi üzerinde (başkalarına açık etmeden) açık veya kapalı anahtar şifreleme yapabilmektedir.
- Kart sahibinin onaylanması PIN ve/veya biometrik işlemler ile sağlanarak üstün güvenlik hizmeti verilebilmektedir.

10

Çoklu Uygulama Desteği

- Farklı işler için kullanılan çok sayıdaki kartın fonksiyonelliği yazılım olarak tek bir kart üzerinde toplanarak taşınması gereken kart sayısı azaltılmaktadır.
- Sonradan karta yüklenebilen yazılımlar (cardlets) çok büyük esenklik sağlamak ile bilrlikte bazı güvenlik tehditleri de oluşturabilir. Kotü amaçlı yazılım;
  - Kart üzerindeki önemli veriyi bozabilir, değiştirebilir (integrity)
  - Hassas verinin dışarı çıkmasına neden olabilir. (confidentiality)
  - Kart üzerindeki diğer uygulamaların hatalı çalışmasına neden olabilir (availability)
  - Uygulamaların sayısal imza ile imzalanmış olmaları o yazılımın menşei hakkında bir bilgi sağlamak ile birlikte onun zararasız olduğunu garanti eden bir güvenlik önlemi değildir. (Bu durum web appletleri gibi uygulamalar için de böyledir.)

11

Standartları Nedir?

- **ISO 7816** Temaslı akıllı kart standarını belirler. Kartın fiziksel yapısı, boyutları, temas elemanlarının yeri, iletişim protokolü, değiş-tokuş için kullanılması gerken komut kümesi, uygulamaları belirlemek için kullanılan kimlik sistemi (application identifier systems) ve veri elemanları ile ilgilidir.
- **ISO 14443** Temassız akıllı kart standardını belirler Fiziksel kart özellikleri, kullanılan radyo frekans gücü ve sinyal karışmaları, başlatılma (initialization) çarpışma önleyici (anti-collision) ve iletim protokollerini belirler. Sistem 13.56 MHz frekansını kullanarak 10 cm kadar bir uzaklıktan temassız işlem yapılmasına imkan vermektedir. A ve B olmak üzere iki tipi vardır.
  - ISO 14443 A en yaygın kullanılan tipdir. Veri aktarım hızı nispeten düşüktür.
  - ISO 14443 B Özllikle bankacılık uygulamalarında tercih edilen tipdir. Daha yüksek veri iletim hızına sahip olması nedeni ile biometrik ve benzeri türde yoğun bilgi aktarılması gerektiği durumlarda tercih edilmektedir.
- **ISO 15693** Benzers şekilde 13.56 MHz teknolojisini kullanmak ile birlikte daha geniş bir alandan okunabilme özelliğine sahiptir. Bu özeliği nedeni ile yüksek trafige maruz kalan erişim kontrolü uygulamaları için tercih edilmektedir.
- **Proximity (Yakınlık)** Bu bazen temassız özelliğinden ötürü ISO14443 veya daha eskiden erişim kontrolü amacıyla kullanılan 125 kHz teknolojisini ifade etmek üzere kullanılan bir terimdir. 125 kHz proximity "smart" olarak adlandırılabilecek bir teknoloji olmadığı gibi ISO tarafından standarda bağlanmamış, kart ve okuyucusunun ayni firmanın tescilli (proprietary) ürünü olmasının gerekli olduğu durumları ifade etmektedir.

12

NFC operates at 13.56 MHz and transfers data at up to 424 Kbits/second.

Temassız Teknolojinin Artıları

Temassız teknolojinin, temaslı veya 125 kHz ile çalışan proximity card teknolojisine göre üstün olduğu noktalar şöyle özetlenebilir.

1. **Uygunluk (Convenience):** Temassız teknolojide kartı nereye ve hangi yönde sokmak gerektiği, sürtemek gerekiyor ise hangi hızda bunu yapmak gerektiği konusunda endişe edilmesi gerekmez.
2. **Düşük Bakım/Garanti (Less Maintenance/Warranty):** Temassız kartların hareketli bir parçası olmaması nedeni ile bozulma, temas etmemesi nedeni ile aşınma gibi problemeri yoktur. Ömür boyu garanti kapsamındadır.
3. **Yüksek Güvenlik (Higher Security):** Temassız kartlar veri iletimi yapmadan önce birbirlerinin kimliklerini denetler (authentication). Bu kimlik denetleme işlemi üç yönlü (three-way) bir işlem olup, saklı anahtar (secret key) açık edilmeden, bir kıyım (hash) fonksiyonu ile şifreli olarak gerçekleştirilir.
4. **Geniş Bellek (Large Memory):** Temassız kartların bellek kapasiteleri proximity karlardan yüzlerce kat fazla olabildiği gibi veri hesaplama (computation) kabiliyetleri de vardır.

13

Temassız Teknolojinin Artıları (devam)

5. **Geliştirilmiş Gizlilik (Enhanced Privacy):** Son derece fazla yer kapyabilen biometric şablonlar kullanılarak özel bilgilerin mahremiyeti garanti altına alınabilir.
6. **Çeşitli Kart Biçimler (Versatile Form Factors):** Temaslı kartlarda olduğunun aksine, bunlar amaca uygun farklı şekillerde kimlik belirleme (credential) teknolojilerinde kullanılabilirler. Anahtar, saat, hatta cama yapısabilen etiketler temassız kimlik belirleme amaçlı olarak kullanılabilir.
7. **Çoklu Uygulama (Multiple Applications):** Temassız kart taşımak farklı amaçlar için kullanılan pekçok kartı taşımak gibidir. Birden fazla uygulama için aynı kartı kullanmak mümkündür. Geçiş kontrolünden, nakit ödeme, ön ödeme, ulaşım vb. amaçlar için tek kart yeterli olabilir. Ek ihtiyaçlara bağlı olarak uygulamaların sayısı da arttırılabilir.
8. **İleriye Yönelik Koruma (Future Protection):** Temassız kart teknolojisi manyetik ve proximity kart teknolojisinin yerini almıştır. Bu teknolojinin seçilmesi zamanı geçmiş teknolojilerin kullanımının önüne geçeceği gibi sistemin genişletilebilir olması nedeni ile yapılan yartırımın da ileride korunabilir olmasına imkan verecektir.

14

Kullan at – Doldurulabilir

(Disposable vs Reloadable)

Günümüzde kullan-at (disposable) ve tekrar doldurulabilir (reloadable) olarak adlandırılan kartlar kullanılmaktadır.

- **Kullan at kartlar: Tek bir amaç için kullanılabilen, işi bittiğinde atılabilen (hatta bazıları tarafından kolleksiyon amacıyla saklanan) türde kartlardır. Birkaç biniş imkanı tanıyan ulaşım kartları, ön ödeme ile alınarak para yerine kullanılabilen, kredisi tükendiğinde degeri kalmayan kartlar (telefon kartları, fotokopi makinaları için kartlar vb.)**
- **Doldurulabilir kartlar: Para çekmek/yatırmak, elektronik cüzdan, kimlik, sağlık ile ilgili işlemler vb. için kullanılan türde üzerinde farklı uygulamaların yer aldığı kartlar olarak karşımıza çıkmaktadır. Özellikle ulaşım, elektronik cüzdan vb uygulamalarda üzerine yeniden kredi (para) yüklenmek kaydı ile tekrar tekrar kullanılabilir olması kullanıcılar tarafından daha çok tercih edilmesine de imkan vermektedir.**

15

Akıllı Kart – Manyetik Kart

(Smart vs Magnetic Stripe)

- **Akıllı Kart**
  - Mahremiyet ve güvenliğin ön planda olduğu uygulamaların vazgeçilmez parçasıdır. Üzerindeki işlem ve şifreleme kabiliyeti sayesinde taşıdığı bilgiye sadece yetkilendirilmiş arayüzler tarafından erişilmesine izin verdiği için kartı verenin geçerli bir kurum olup olmadığı, kart üzerindeki bilgilerin bir sahtecilik ile değiştirilip değiştirilmediği kontrol altında tutulabilir.
  - Bir smart card 4KB-256MB veriyi güvenliği tehdit etmeksizin saklayabilir, veri güncellenmesi (yetkiler dahilinde) mümkündür. Örneğin sağlık kayıtları, var olan alerji vb kornik hastalıklar, kullanılan ilaçlar, görüntüleme ve tahlil sonuçları vb. bilgi farklı erişim seviyelerindekiler tarafından görülebilir, üzerinde değişiklik yapılabilir (kimin tarafından yapıldığına dair bilgileri saklamak kaydıyla).
  - Sağlanan değişik fonksiyonlar sayesinde uzerindeki bilgileri kullanarak olası bürokrasi ve kagıt işlemini ortadan kaldırmak, servis kalitesini yükseltmek mümkündür. Denetleme (audit) ve yapılan erişimlerin raporlama özelliği vardır. Kapalı çevrim okuyucular ile üzerinde yer alan bilgilere erişim mümkündür.
  - Birden falza uygulama birbirinin çalışmasını etkilemeden/engellemeden aynı kart üzerinde çalışabilir. Benzer şekilde kart üzerinde bulunan uygulamalar etkilenmeden var olanlar silinebilir veya yenileri karta yüklenebilir.
- **Manyetik Kart**
  - Veri güvenliği son derece zayıftır. Bilginin çalınması ve kartın çoğaltılması için 25$'lık cihazlar yeterli olmaktadır.
  - Sınırlı kapasitede (2KB), sonradan içeriği değiştirilemeyen bir depolama alnı vardır.
  - En alt düzeyde fonksiyonelliğe sahiptir.
  - Veri ve uygulamalara erişebilmek için sürekli bağlı olması (online) gereklidir
  - Son 30 yıl içinde çok yaygın kullanılmış bir teknoloji olmak ile birlikte artık pazar payını kayıp etmektedir.

16

		Smart Card	Magnetic Strip Card
Technology Features	Storage capacity	●	○
	Security features	●	○
	Post-issuance modification	●	◑
	Cost of ID device	◑	●
	Cost of reader	●	◑
	Support for multiple sets of application data on the card	●	No
	On-card biometric storage	●	No
	On-card biometric match	●	No
Legend	Worst ○ ◔ ◑ ◕ Best		

17

Akıllı Kart Teknik Özellikleri

	Typical	***High Density***
Confidential Operating system	ROM (512 KB)	CodeFlash (512 KB NOR Flash)
Application Data, Secret Keys	EEPROM (256 KB)	Emulated EEPROM (128 KB NOR FLASH)
RAM	5 KB	24, 48, 64 KB
User Data	In EEPROM	4 to 256 MB (OR)NAND FLASH
Interface	ISO 9600 bit/s	+ USB, MMC High-speed protocols
Die Size	25 mm^2 in 0,13µm technology	75 mm^2 in 90nm technology

18

Ürünler

- **MIFARE®** , Philips tarafından 13.56 MHz temassız teknoloji ile üretilmiş en yaygın chipset'tir. ISO 14443 uyumludur.
- **DESFire®** , MIFARE ailesi içindeki en üst chip settir. Government Smart Card Interoperability Specification (GSC-IS) uyumludur.
- **MIFARE DESFire EV1** kullanılan haberleşme (air interface) ve şifreleme metodları açısından açık dünya standardıdır. ISO / IEC 14443 A uyumlu olup optional ISO / IEC 7816-4 komut setini desteklemeketdir. MIFARE DESFire EV1 28 kadar farklı uygulama, uygulama başına 32 dosya saklayabilir. Dosya boyutlarının yaratım sırasında belirlenebilir olması sayesinde çok esnek ve her iş için uygun bir çözümdür.
- **my-d®** , Infineon Technologies tarafından 13.56 MHz temassız teknoloji ile üretilmiş bir chipsettir. Kullanılan ileri güvenlik algortimaları sayesinde ISO 15693 uyumlu kartlar arasında lider konumdadır.
- **iCLASS®**, HID Corporation tarafından ISO 15693 uyumlu 13.56 MHz temassız teknoloji kullanılarak oluşturulmuş özel (propriarity) ürün ailesidir.

19

Dış Dünya İle Haberleşme ?

- Akıllı kart ve onu okumak ile görevli olan cihaz (Card Accepting Device-CAD) APDU (Application Protocol Data Units) adı verilen küçük veri paketleri kullanarak haberleşirler.
- Akıllı kart ve CAD areasında kullanılan karşılıklı (mutual) kimlik belirleme (authentication) protokolü sayesinde uçlar birbirlerinin kim olduğunu tespti edebilirler. Kart rasgele (random) bir sayı üreterek bunu CAD'a yollar, CAD yollanan sayıyı paylaşılan anhta(public-key) ile şifreler ve karta yollar. Kart kendi üzerindeki şifrelenen mesajı çözer ve elde edilen deger ilk yollanan sayı aynı ise iki taraf birbirini tanımış, böylece bağlantı sağlanmış olur.
- Bağlantı tesis edildikten sonra her ikisi arasında tüm mesajlar bir mesaj doğrulama kodu ile kimlik denetiminden geçirilir. Bu doğrulama kodu, şifreleme anahtarı ve rasgele bir sayı kullanılarak yollanacak veri üzerinden elde edilmektedir. Veri yol boyunca (hata nedeni veya aradaki kötü amaçlı müdahale ile) bir değişikliğe ugrayacak olursa mesajın yeniden yollanması gerekecektir.
- Alternatif olarak kart üzerindeki bellek kapasitesi ve işlem gücüne bağlı olarak veri bir sayısal imza ile de kontrol edilebilir. Bunun için simetrik çalışan DES (Data Encryption Standard), 3DES (triple DES) ve açık anahtarlı RSA (Rivest-Shamir-Adleman's algorithm) kullanılarak 56, 168, ve 1024 bit uzunluğunda anahtarlar kullanılarak güvenliğin arttırılması mümkündür. (Hiçbir güvenlik sistemi kırılamaz nitelikte değlidir. Bunun için ne kadar zaman ve ne kadar işlem gücü harcanması gerektiği ve bunun sonucunda elde edilecek olan kazancın ne olacağı önemlidir.)

20

Kullanılan Şifreleme Algortimaları

- DES, gizli bilginin korunması için geliştirilmiş güçlü bir şifreleme algortimasıdır. National Institute of Standards and Technology (NIST) tarafından geliştirilmiş, açık, ucuz yaygın kullanımlı ve çok güvenlidir.
- Triple DES, DES'den daha yavaş olmak ile birlikte daha uzun anahtar kullanılması ve üç defa şifreleme yapılması sayesinde milyarlarca defa daha güçlü bir şifreleme imkanı sunar. DES tabanlı, açık ve kendini ispatlamış bir algortimadır.
- AES (Advanced Encryption Standard), simetrik anahtar şifreleme standardıdır. AES, DES den yavaş, Triple DES'den hızlıdır. AES-128 (128 bit key) çok gizli bilgilerin korunması için kullanılan ilk halka açık, National Security Agency tarafından onaylanmış algoritmadır.

21

Şifreleme ile Sağlanan Güvenliğin Önemli Olduğu Alanlar

- PC ve Ağ kullanıcıları için güvenli bağlantı ve kimlik tespiti (doğru kişi olduğunun anlaşılabilmesi için PIN kullanımı)
- Güvenli B2B ve B2C e-ticaret uygulamaları için
  - Bankacılık/e-cüzdan vb ödeme sistemi
  - Sadakat (Loyalty) ve promosyon
  - Erişim Kontrolü
  - Veri saklama
  - Kimlik
  - Bilet (ulaşım)
  - Park ve otoyol geçiş ücreti ödeme
- Sayısal sertifikaların, sicil, kimlik ve şifre bilgilerinin saklanması için
- Hasas nitelikteki verinin şifrelenmesi için

22

Yapılan Saldırılar

- Kart üzerinde yer alan tüm veri ve şifrelerin EEPROM üzerinde saklandığı bilindiğine göre beklenmedik bir gerilimin uygulanması sonucunda bu bilgilerin tahrip edilmesi, değiştirilmesi mümkün olabilmektedir. (veya kart üzerinde çalışan programın doğru çalışması engellenerek bazı bilgilerin elde edilmesine yönelik salsırılar olabilir.)
- Bu nedenle kart üzerinde bazı algılayıcılar vasıtası ile olası değişklikleri takip etmek için güvenlik işlemcileri kullanılmaktadır. Ayrıca değişiklik yapabilmek için uygun gerilim seviyesinin belirlenmesi de çok kolay olmadığı (veya karta ciddi zarar verme ihtimali olduğu) için çok yaygın kullanılmaz.
- Diğer bir yönetm kart üzerindeki kontrolcüyü ısıtmak veya EEPROM üzerine UV ışınları düşürerek üzerindeki güvenlik kilidini kırmaya yöneliktir.
- En saldırgan ve tahrip etmeye yönelik saldırı ise kart üzerinde yer alan devreyi sökerek tersine mühendislik (reverse-engineering) yöntemleri kullanmaktır.
- Differential Power Analysis (DPA), ise şifreleme algoritmasına yönelik istatistiksel bir saldırıdır. Amaç hipotezin yapılan ölçümler ile karşılaştırılarak şifreleme anahtarının tespit edilmesine yöneliktir.
- Simple Power Analysis (SPA) ise kayıt edilmiş güç verisinin (power data) analizi yapılarak eylem ve verinin (actions and data) tespit edilmesine yöneliktir.

23

SPA/DPA Saldırılarına Karşı Çözümler

- 0.6 micron teknolojisi kullanımı ile ebat küçülürken güç tüketimi ve bunların çalışma sırasındaki değişimleri arasındaki farklar azaltılmıştır. Bu sayede SPA/DPA türü tehditlerin kart üzerinde yapılan işlemlerin olsturuğu dalgalanmaların normal işlemlerden mi yoksa veri ile ilgili işlemlerden mi olduğunu anlamak zorlaşmıştır.
- Kullanılan özel Clock Software Management facility sayesinde gömülü programlar çalışırken çok değişken yazılım zamanlaması (highly variable software timing) sağlanmıştır.
- Kesme mekanizmalı bir zamanlayıcı devre (built-in timer) ve tahmin edilemeyen bir sayı üreteci (Unpredictable Number Generator) kullanımı ile yazılımın çalışma biçiminde tahmin edilemeyen değişikenlikler ve güç kullanımında farklılıklar yaratılmıştır. (changes in the pattern of power consumption)
- Güçlü modüler tasarım ile yeni donanım değişiklikleri hızlı ve ve etkin şekilde yapılabilir olmuştur. Böylece yeni saldırı senaryoları için tedbir almak kolaylaştıtılmıştır.
- Geliştirilen bellek erişim yöntemleri ile işletim sisteminin, çoklu uygulamaya güvenilir bir şekilde destek vermesi sağlanmıştır.
- Kurulan gelişmiş güvenlik mekanizmaları ve firmware işlevleri ile uygulamaların saldırı olması muhtemel koşulları (invalid operating conditions, bad opcodes, bad addresses and violations of chip integrity) tespit etmesi ve bunlara karşı cevap vermesi (include interrupts, program reset, immediate erasure of all RAM data and flash programming of the entire EEPROM array) sağlanmıştır.

24

Diğer Karşı Önlemler

- Fiziksel koruma katmaları (Birkaç metal katman, İletken metal zırh –shield-)
- Chip'i gizleme (Obfuscation) Üretim teknolojisini küçültmek
- Memory bus üzerinde şifreleme
- Bellek eşiminin donanım olarak kontrolü
- Tahrip edici saldırılar için periyodik self-test ve verinin güvenilir olarak depolanması –redundant-
- Düzensiz Saldırılara karşı data ve kontrol bilgisi üzerinde checksum vb. mekanizmalar kullanılması
- İzlemeye yönelik saldırılar için rasgele çalıştırma -randomized execution-
- Güvenlik algılayıcıları (VCC, Temp, Light, UV, Clock, glitches)
- Glue Logic
- NOR FLASH Memory
- Karıştırma –Scrambling-
  - Current
  - Data
  - Address

25

İşletim Sistemi Güvenliği

- Akıllı karlar üzerindeki veri bir ağaç yapısı şeklinde tutulmaktadır. Bir tane master file (MF or root) olup altında pekçok elementary file (EF) ve yine pekçok dedicated file (DF) barındırabilir.
- DF ve MF, bilgisayarlarımızdaki dosya sistemindeki klasörlere, EF ise dosyalara özdeş kabul edilebilir. Ancak bundan farklı olarak DF içinde veri de barındırabilir.
- Alışıla gelmiş işletim sisteminde dosya/klasörler olduğu gibi DF, EF ve MF başlıklarında (header) güvenlik ile ilgi öznitelikler (attributes) vardır. Bir uygulama ağaç yapısı üzerinde ilerleyebilmek ile birlikte sadece yetkisi olan kısma girebilir.
- **Dosyalar (DF ve EF için) Erişim Hakları – sıralı-**
  1. Always (ALW): Sınırlama olmadan erişim, herkese açık
  2. Card holder verification 1 (CHV1): Geçerli CHV1 değeri olana açık
  3. Card holder verification 2 (CHV2): Geçerli CHV2 değeri olana açık
  4. Administrative (ADM): Yönetim. Diğer kademeler ve onların gereksinimlerini karşımak için yapılması gerkenlerden sorumlu yönetici erişimi
  5. Never (NEV): Erişim yasak
- CHV2 ye sahip olunması bununla CHV1 isteyen bir dosyaya eirşilebileceği anlamında degildir. CHV1 ve CHV2 kart üzerindeki iki ayrı PIN'dir. Biri kullanıcıyı belirlemek için kullanılırken diğeri ilkinin bloke olduğu durumlarda kullanılır.

26

Worldwide Smart Secure Device shipment - 2011 and 2012 forecasts
Millions of Units (Mu)
(General Assembly, Brussels, 25 April 2012)

	2011	2012 forecast	2012 vs 2011 % growth
Telecom	4 700	5 200	11%
Financial services	1 050	1 260	20%
Government - Healthcare	240	300	25%
Transport	100	120	20%
Pay TV	125	135	8%
Others	80	90	13%
Total	6 295	7 105	13%

Included in the above forecasts are the following contactless shipments:

Worldwide Smart Secure Contactless market figures – 2011 and 2012 forecasts
Millions of Units (Mu)
(General Assembly, Brussels, 25 April 2012)

	2011	2012 forecast	2012 vs 2011 % growth
Financial services	200	260	30%
Government - Healthcare	130	170	31%
Transport	100	120	20%
Others	50	60	20%
Total	480	610	27%

27

Kaynaklar

- What's so smartabout What's so smartabout Smart Cards?, Smart Card Forum.
- An Overview of Smart Card Security, http://people.cs.uchicago.edu/~dinoj/smartcard/security.html
- Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications, Smart Card Alliance
- Smart card security from a programming language and static analysis perspective, Xavier Leroy, INRIA Rocquencourt & Trusted Logic
- Security Challenges for High Density Smart Cards, Dr. Helena Handschuh, Spansion EMEA
- Basic Overview of Smart Card Technology, http://w3.securitytechnologies.com/products/credentials/Solutions/Pages/details.aspx?InfoID=96
- http://www.eurosmart.com/index.php/publications/market-overview.html
- HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements, Smart Card Alliance

28

Sorular/Cevaplar

29