특집

출입통제 시스템 및 스마트카드 솔루션의 현황 및 전망

이철욱 (HID Global-Korea)

I. 서 론

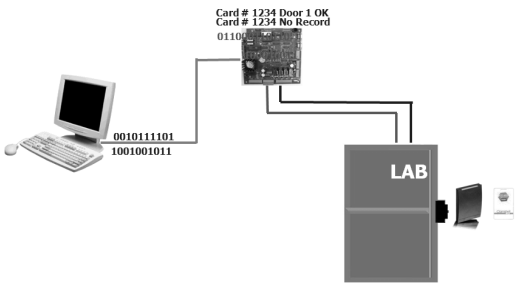
최근 수년간 산업 스파이 기밀 유출 사건 사고가 급증하면서 출입통제에 대한 관심도 부쩍 높아지고 있다. 그러나 해외 여러 다른 나라들에 비해 국내의 출입통제 시스템의 보안 수준은 많이 뒤쳐져있고 보안에 대한 경각심이 IT보안이나 영상 감시에 비해 상대적으로 부족한 상황이다. 출입통제 시스템은 전체 물리적인 보안 시스템과 IT 보안 시스템에 있어 필수 요소이며 기본이 되는 보안 시스템으로 전체 시스템의 보안 레벨 향상 및 리스크 매니지먼트의 효율성에 미치는 영향이 크다.

다른 여러 산업과 마찬가지로 출입통제 시스템도 IT화 되고 있으며, 시장의 요구와 IT부품의 신뢰성 향상으로 IT화의 속도가 급 가속되고 있다. 이에 더불어서 보안시장에도 점차 각각의 시스템의 통합화 바람이 불며 다양한 통합 솔루션이 나오고 있으며, 최근에는 물리적인 보안과 IT보안 시스템을 연결하는 통합솔루션들도 시장에 나오고 있다. 또한, 비접촉식 스마트카드(13.56Mhz)의 기술이 읽고 쓰기가 가능함으로 향상된 확장성, 호환성, 향상된 보안성 등을 이유로 우리나라를 포함한 전 세계 시장에 전통적인 비접촉식 Proximity(125Khz) 기술을 대체하여 출입통제 시스템에 적용되며 기존의 카드와 리더를 대체해 나가고 있다. 하지만, 최근 2년간 중국, 영국 등에 발생된 여러 ID 카드 불법 복제 사고에서 보여지듯이 스마트카드를 바르게 도입하여 사용하지 않는 경우 오히려 기존의 시스템보다도 보안성이 취약해 질수 있기에 출입통제의 구성과 스마트카드, 스마트카드의 바른 도입/사용 방법, 물리적인 보안과 IT보안 시스템을 연결하는 통합솔루션을 알아보고자 한다.

II. 출입통제 시스템의 구성

출입통제는 간단히 말해 인증된 사람은 쉽게 출입이 가능하고 인증되지 않은 사람은 출입은 허용하지 않기 위한 시스템이다. 물리적인 출입제어, 정보에 대한 접근 제어, 네트웍에 대한 접근 제어로 나누어 볼 수 있다.

출입통제 시스템은 <그림 1>에서 보는 바와 같이 사용자는 출입용 ID카드(비접촉식 RF카드)를 소지하고 출입문에 카드리더기와 락이 설



〈그림 1〉 출입통제 시스템 구성도

〈그림 2〉 물리적인 보안 시스템 구성도

치되고 이것은 컨트롤러로 연결되고 다시 PC의 소프트웨어로 연결되어 시스템이 완성된다.

또한 출입통제 시스템은 <그림 2>에서 보는바와 같이 다른 다양한 어플리케이션과 같이 구성되어 전체 물리적인 보안 시스템을 구성한다.

출입통제에 사용되는 RFID는 Radio Frequency Identification 의 약자로 카드리더의 유효한 영역 안에 카드가 들어왔을 때 카드의 데이터(ID번호)를 리더에 전달하는 방식이다. 현재 가장 흔히 출입통제에 사용되고 있는 카드의 데이터(ID번호) 구성은 아래 <그림 3>과 같다.

이와 같이 ID번호를 구성, 등록하여 출입통제에 사용할 경우 카드 ID번호의 중복문제로 보안성이 상대적으로 취약할 수 있기에 여러 특수 포맷/구성 또한 널리 사용되고 있다.

출입통제 시스템에서의 컨트롤러 역시 과거의

```
PAAAAAAAABBBBBBBBBBBBBBBP
00100101100000100110100100
EXXXXXXXXXXXX
                XXXXXXXXXXXX0
```

P = Parity
O = Odd Parity
E = Even Parity
X = Parity mask
A = Facility code, range = 0 to 255
B = Card ID, range = 0 to 65,535

〈그림 3〉 standard 26bit 카드 포맷 구성도

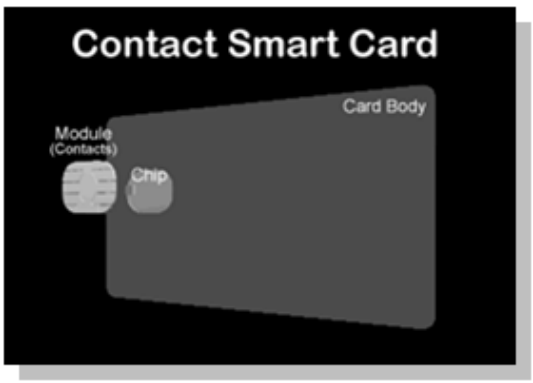
시리얼 통신방식에서 TCP/IP기반 통신 방식으로, Firmware방식에서 훨씬 강력해진 CPU의 Linux등 내장방식으로, 단순 출입통제용에서 영상감시, 알람 모니터링 등을 포함하는 통합시스템으로 전환되어왔고 전환되고 있다.

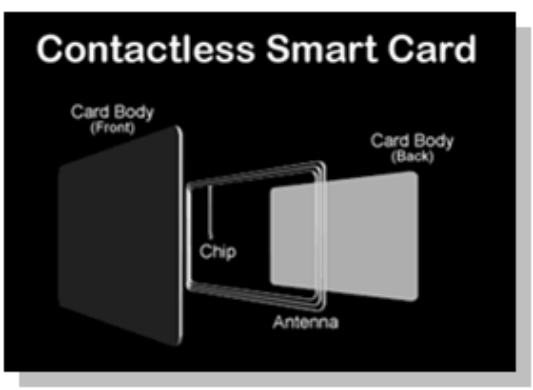
III. 스마트카드

물리적 출입통제 어플리케이션을 위한 비 접촉식 스마트카드를 중심으로 알아보고자 한다.

1. 스마트카드의 정의

컴퓨터 칩이 내장된 "신용카드" 크기의 장치로 접촉식과 비 접촉식이 있다. 접촉식 스마트카드는 카드와 리더를 전기적으로 연결하는 커넥터가 있고, 비 접촉식 스마트카드는 RF 주파수를 사용하며 무선통신으로 리더에서 카드로 전원을 공급한다. 또한, 메모리 전용이나 마이크로 프로세스 기반 등의 스마트카드가 존재한다. 아래의 그림은 접촉식 스마트카드와 비접촉식 스마트카드의 물리적 구성을 보여준다.





2. 비접촉식 Proximity(125Khz)카드와 비접촉식 스마트 카드(13.56Mhz)의 비교

125Khz	13.56Mhz
Prox	iCLASS, Mifare, Desfire, Sony Felica
"읽기"만 가능	"읽기"와 "쓰기" 모두 가능
한 개의 어플리케이션 가능	다중 어플리케이션 가능
작은 메모리 용량 (256bits)	큰 메모리 용량 (2K bits ~ 32K bits)
Low Security	High Security

위의 표에서 보여지는바와 같이 가장 큰 차이점은 향상된 보안성, 호환성, 확장성이다. 비접촉식 Proximity(125Khz)카드에 비해 비접촉식 스마트카드(13.56Mhz)는 다양한 보안 알고리즘, 특수키 사용, 암호화 기술, 상호인증 기술들을 사용할 수 있도록 함으로서 보안성이 크게 향상될 수 있게 되었고 스마트카드에서 "읽기"와 "쓰기"가 가능하게 되어 다양한 어플리케이션이 카드와 리더간에 구현되게 되면서 적용 가능한 어플리케션이 많아지고 강력해 졌다.

3. 출입통제에 주로 비접촉식 스마트카드를 사용하는 이유

가. 향상된 보안성

데이터는 암호화 알고리즘, 특수키와 Mutual Authentication등으로 보호되어 불법복제나 해킹으로부터 안전하다.

나. 편리성

접촉식은 카드를 리더기에 삽입하여야 하는 것에 반하여, 비접촉식의 경우 리더기에 가까이 근접시키기만 하면 되므로 편리하고 제품 수명이 길다(반영구적).

다. 우수한 상호 운용성

표준 ISO (14443A, 14443B, 15693)를 충족한다.

라. 증가된 메모리 사이즈

상대적으로 접촉식의 메모리 용량이 비접촉식에 비해 크지만, 비접촉식도 출입통제에 사용하기에는 충분한 메모리 용량을 가지고 있고, 현재 제품이 지속적으로 업그레이드되면서 메모리 용량도 계속 증가하고 있어서 현재 사용할 수 있는 여러 다양한 어플리케이션을(사진 등의 개인 정보저장, 사내 전자 결재, 생체인식 등) 적용하기

에 메모리가 부족하지 않다.

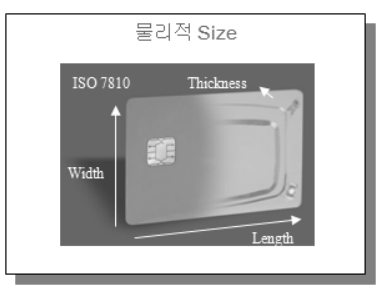
마. 다중 어플리케이션 지원

비접촉식 스마트카드는 출입통제, PC 및 네트워크 로그온, 생체인식 등의 다양한 어플리케이션을 제공 할 수 있어서 출입통제와 같이 요구될 수 있는 어플리케이션들을 충족할 수 있어서 선호되고 있다.

4. 비접촉식 스마트카드에서의 ISO Standard

가. ISO가 규정하는 것들

• Part 1 : 물리적 특징들



• Part 2 : RF 신호, 전원 인터페이스
• Part 3 : 초기화와 충돌방지
• Part 4 : 전송 프로토콜

나. ISO가 규정하지 않는 것들

• 메모리 할당
• 키, Mutual Authentication
• 보안 알고리즘
• 리더의 시리얼 프로토콜

위와 같이 ISO는 보안과 관련된 “키, Mutual Authentication”, “보안 알고리즘”, “리더의 시리얼 프로토콜”에 대해서는 규정하고 있지 않기 때문에 어떤 ISO standard (ISO 14443A, 14443B, 또는 15693)의 제품(카드, 리더)인지 여부는 보안 수준/등급과는 관련이 없다.

5. 바람직하지 않은 스마트카드 사용 형태

현재 출입통제에 CSN을 사용하는 경우가 많은데(특히 한국), 이것은 손쉽게 구할 수 있는 간단한 장비만으로 누구나 카드를 복제할 수 있기 때문에 보안에 심각한 문제를 불러일으키게 된다.

가. CSN 이란?

모든 비접촉식 스마트카드내의 불특정의 고유번호(일반적으로 32bit ~ 64bit 임)로서 ISO standard가 규정하고 있고, 아래와 같이 다양한 명칭이 있다.

• UID : Unique ID
• PUPI : Pseudo Unique Proxcard Identifier
• CSN : Card Serial Number
• CUID : Card Unique ID

CSN을 사용하는 리더는 항상 보안과 인증 없이 데이터를 읽는다.

CSN은 집주소의 번지와 같이 모든 사람이 읽을 수 있다. 하지만 들어가기 위해서는 열쇠가 필

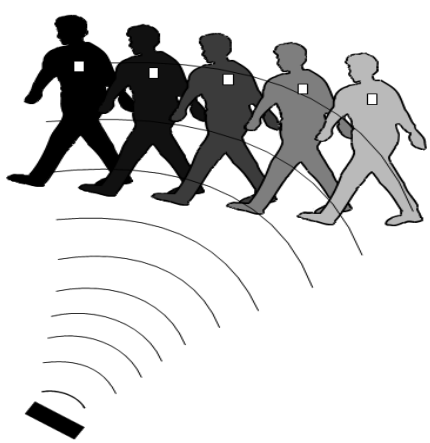
요하다. 다시 말해 CSN는 누구나 읽을 수 있게 오픈되어 있으므로 보안 솔루션에 사용하기에 부적합하다.

나. CSN의 존재 이유

카드 리더기의 RF영역에서 동일시간에 읽혀진 다수의 카드를 개별적으로 구별하기 위해 존재하고, 한번에 하나의 카드만 읽도록 충돌방지 기능(Anticollision)을 사용한다. ISO Standard는 CSN을 위의 이유 외에 다른 용도로는 디자인하지 않았다.

다. 충돌방지 기능(Anticollision)

충돌방지 기능(Anticollision)은 비접촉식 스마트카드에서 사용되는 프로토콜의 하나로서 아래 그림에서 보여지듯이 다수의 카드와 동시에 통신할 수 있는 기능을 제공하며, 장거리용 리더기에 매우 중요한 기능이다. ISO Standard는 충돌방지 기능(Anticollision)을 위해 몇 가지 방법을 규정하고 있다.



라. 출입통제에 CSN의 적용 현황

대다수의 리더기들은 카드에서 CSN을 읽어서 2진수의 데이터를 추출하여 26bit, 32bit, 34bit Wiegand나 다른 출력 포맷으로 변환하여 사용한다. 이러한 CSN의 사용은 비접촉식 스마트카드에 내장된 보안 기능을 무시하는 것과 다르지 않다.

마. 출입통제에 CSN의 적용시 문제점들

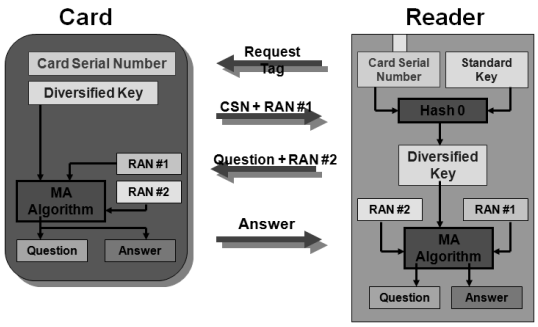
- 사용시 문제
  - CSN을 사용해서는 기존과 같이 임의로 원하는 ID번호를 등록하여 사용할 수 없으므로 추가의 비용(장비, 인력)과 소프트웨어 등에 복잡함을 초래하게 된다.
- 보안 문제
  - CSN 복제 : 프로토콜 분석기 같은 많은 스마트카드 개발툴은 ISO14443이나 ISO15693의 CSN을 손쉽게 복제할 수 있다.

바. CSN 리더의 사용

CSN 리더기는 기존의 보안이 취약한 카드리더 시스템에서 보안 알고리즘이 적용된 시스템으로 전환할 때 한시적으로 유용하다. 전체 카드가 보안 알고리즘이 적용된 안전한 카드들로 전부 교체가 완료된 후에 리더에서 CSN 리딩 기능을 끈다.

6. 바람직한 스마트카드 사용 형태

- 모든 데이터는 암호화하여 전송 한다.



〈그림 4〉 Mutual Authentication

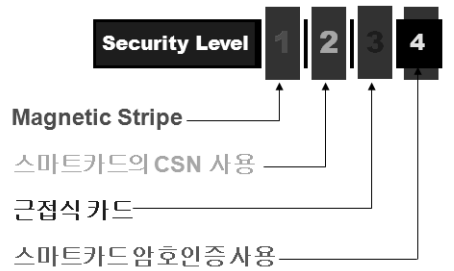
- Default상태의 키(Key)대신에 Hash등의 알고리즘이 적용된 특수키(key)를 사용한다.
- <그림 4>와 같은 카드와 리더간의 상호인증이 키(key) 매칭 방식이 아닌 아래와 같은 Mutual Authentication으로 인증한다.
- 고객 맞춤형 커스텀 키(custom-made key) 사용

대다수의 교통용 스마트카드, 전자결재/금융거래 스마트카드, 출입통제 전용 스마트카드 시스템들은 보안성을 이유로 위와 같은 방식을 적용하고 있다.

7. 각 카드 기술별 보안등급 비교

<그림 5>는 카드기술과 사용되는 방법에 따른 보안등급을 보여준다. (1: 최저, 4: 최고)

- Magnetic Stripe은 보안 레벨이 가장 낮다.
  - 표준 ISO 규격에 잘 문서화 되어있다.
  - 데이터 보호를 위한 보안이 거의 또는 전혀 없다.
  - 카드를 엔코딩 할 수 있는 장비를 어디서나 쉽게 구할 수 있다.
  - 증거 : 수많은 복제된 신용카드, 인터넷에



〈그림 5〉 카드 기술별 보안등급

떠도는 수많은 카드 복제 정보 및 지식, 해커전시회에서 데모시연.

- CSN 사용 스마트카드 역시 보안 레벨이 낮다
  - 표준 ISO 규격에 잘 문서화 되어있다.
  - CSN 인증에는 그 어떤 보안도 사용되지 않는다.
  - 증거 : 현재 시장에서 발견되는 수많은 13.56MHz CSN 복제 활동들.

- CSN 사용 스마트카드보다 Prox(125khz) 카드가 더 높은 보안 레벨을 제공한다.
  - 이 기술에 대한 정보는 문서화가 잘 되어 있지 않는다.
  - 모든 Prox 제조업체들은 카드를 엔코딩하고 데이터를 보호하는데 각각 그들만의 고유 방법을 사용한다.
  - 증거 : 현재 상대적으로 적은 수의 Prox 카드 복제 활동들.

- 여러 보안 알고리즘, 특수키를 적용한 스마트카드는 최고의 보안 레벨을 제공한다.
  - 여러 암호화 보호방법을 사용한다.
  - 안전한 상호인증(mutual authentication)을 사용한다.
  - 알고리즘이 적용된 특수키 및 맞춤형 키

(custom-made key)를 사용한다.

- 증거 : 여러 암호화 기술, 알고리즘, 상호인증 등으로 보안된 각 산업별 선두의 비접촉식 스마트카드들의 경우 불법 복제된 경우가 없다.

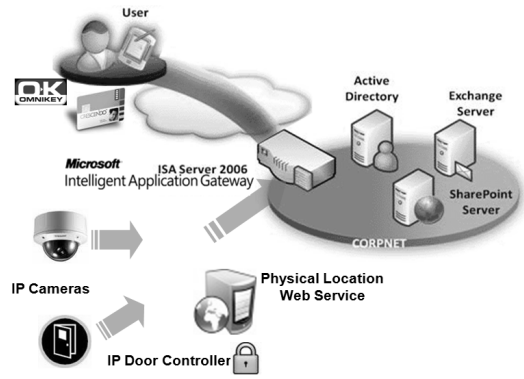
Ⅳ. 통합솔루션

이 장에서는 최근 시장에서 요구되고 출시되고 있는 물리적인 보안과 IT보안 시스템을 연결하는 통합솔루션에 관하여 살펴보기로 한다.

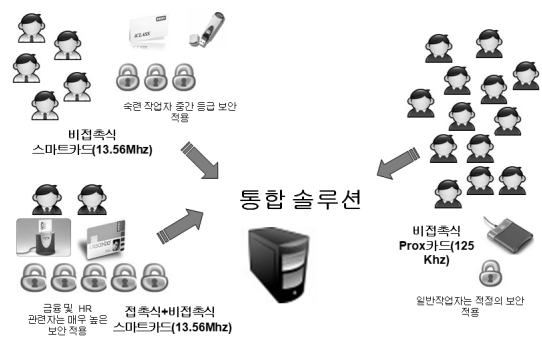
현재 대다수 기업에 가장 귀중한 자산은 "정보"와 "인재"이다. 대다수 기업, 조직에서 지속적으로 급증하는 산업 기밀 유출, 해킹 등의 사건, 사고로부터 보호하고자 하는 "정보"에는 설계도, 고객 정보, 환자 정보, 계약서 등이 있고 이를 보호하기위하여 많은 비용과 노력을 기울이고 있다. 지난해 말부터 닥쳐온 전세계 경기 불황에도 각 기업의 소중한 자산을 지키기 위한 노력은 계속되고 있고, 더 신중해 지고 있다. 시장에서 물리적인 보안과 IT보안 시스템을 연결하는 솔루션의 필요가 증가하고 있고, 네트워크는 점점 더 보안인프라의 한부분이 되어가고 있고, 좀 더 효율적이고 편리하며 경제적인 솔루션의 요구가 증가함에 따라 물리적인 보안과 IT보안 시스템을 연결하는 통합솔루션이 출시되고 있다.

출입통제 시스템에 사용하는 RF카드로 PC 로그온 및 서버 접속, PKI 어플리케이션 등을 사용함으로서 전체 리스크 매니지먼트 효율성을 높이고 도입, 관리, 유지비용을 절감하며 물리적인 보안과 IT보안 시스템의 보안등급을 동시에 향상 시킬 수 있다.

<그림 6>은 다양한 위치, 환경에서의 시스템



〈그림 6〉 다양한 위치의 접속 인증



〈그림 7〉 다양한 기술의 카드시스템 통합

접속 인증을 보여준다. 사무실 직원의 누군가가 인증된 카드와 패스워드만으로 접속 승인이 되는것이 아닌 실제 그 사람이 사무실에 들어왔는지도 확인하여 승인하게 된다. 시스템이 IP기반 카메라와 함께 통합 구축되어 사고 발생시 영상 검색도 지원하게 된다.

<그림 7>은 다양한 카드 기술의 시스템을 통합하는 예를 보여준다.

1. PC 로그온 관리

현재 많은 사용자가 윈도우에서 기본적으로 제공하는 ID와 패스워드를 사용하여 자신의 PC

Average annual number of help desk calls per user[1]	3.8
Average cost per password reset call[2]	$25
Wasted time by end-user	$13
Loss of productivity by end-user and help-desk	$20
Annual Password Reset Cost Per User	~$220

	200 Employees	500 Employees	1000 Employees	5000 Employees
Estimated Annual Cost of Password Resets	$44,000	$110,000	$220,000	$1,100,000

〈그림 8〉 ID & 패스워드 로그온 사용에 따른 손실

에 로그온하고 기업 내 서버에 접속하고 있다. 하지만 이 ID와 패스워드는 보안이 취약하기에 대다수 기업들이 3개월에서 6개월마다 변경을 요구하고 있고 특수문자 조합 등을 요구하고 있다. 하지만, ID, 패스워드의 홍수에 살고 있는 많은 사용자들은 ID와 패스워드를 메모해서 PC에 부착해두거나 사무실 책상 서랍에 넣어두곤 한다.

<그림 8>은 많은 사람들이 무료라고 생각하는 ID와 패스워드방식의 PC로그온 사용으로 초래되는 실제 북미 지역 기업들의 평균 손실 비용이다. 대부분 사무실 직원들은 패스워드를 잊었을 때 시스템에 로그온 하기위해 헬프데스크에 연락하여 어카운트를 리셋(Reset)하게 되고 이에 따라 발생하는 비용들(헬프데스크 직원, 시설 유지비, 이 작업으로 발생하는 사무실 직원과 헬프데스크 직원의 소비되는 시간, 생산성 등)을 보여주고 있고, 이 보고서에 따르면 북미 기업들은 연간 개인당 평균 $200에서 $300의 손실이 발생되고 있다.

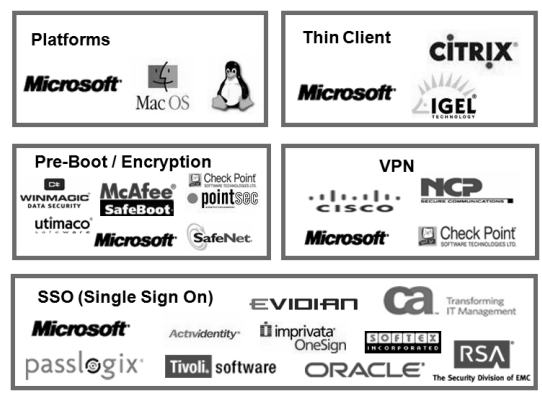
이에 따라 점점 더 많은 기업들이 스마트카드를 이용한 PC 로그온, 서버 접속 시스템을 도입하고 있다.

2. 서버 : 모니터링, 히스토리 추적

이러한 솔루션은 기본적으로 서버에서 관리자들이 시스템 접속자들을 실시간 모니터링 할 수 있고 특정 개인의 접속 히스토리를 트래킹(tracking) 할 수 있다.

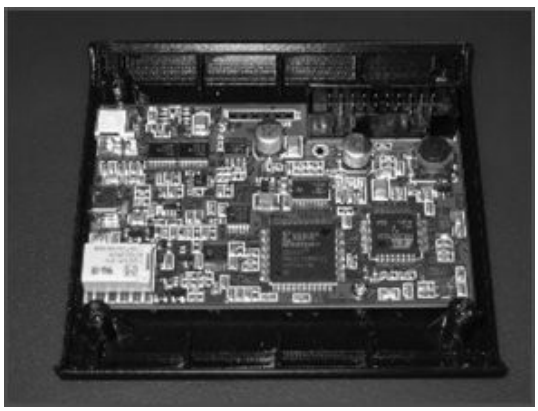
3. PKI 어플리케이션

이러한 솔루션은 사용자 각각의 환경/요구에 맞게 다양한 OS, PKI 어플리케이션들을 지원한다. 이에 따라 과거와는 달리 새로운 PKI 솔루션을 도입할 때 마다 기존 시스템의 변경 교체 없이 add on 개념의 추가 설치가 가능하다.



V. 향후 전망

앞서 기술한 CSN 리딩 스마트카드 시스템은 그 보안의 취약성이 알려짐에 따라 점진적으로 안전한 보안 알고리즘 탑재 스마트카드 시스템으로 전환되어 질것이다. CSN 리딩 스마트카드 시스템 이외에도 섹터에 특정 데이터를 입력하여 사용하는 방식도 아래와 같은 복제 장비(Proxmark III)로 누구나 손쉽게 칩 정보를 복제할 수 있으므로 안전한 보안 알고리즘 탑재 스마트카드 시스템으로의 전환은 시장상황에 따라 현재 보다 훨씬 빨리 전환이 이루어 질수도 있을



〈그림 9〉 Proxmark III, http://proxmark3.com

것이다.

점차 커져가는 각 보안 어플리케이션의 통합화 요구에 의해 현재 이미 많은 시스템이 영상과 출입통제를 결합하는 솔루션을 출시 또는 개발하고 있고 최근에는 물리적인 보안과 IT보안 시스템을 연결하는 통합솔루션들도 시장에 나오고 있다. 조만간 영상보안, 알람 모니터링, 출입통제 등의 물리적인 보안과 다양한 어플리케이션(사내 전자 결재, 근태/식수 관리, 주차 관리 등), IT 보안 시스템을 하나로 연결하는 TCP/IP기반 통신 방식의 통합솔루션이 시장을 주도하게 될 날이 멀지 않았다.

참고문헌

[1] Gartner's report in 2008

[2] Common Access Card Pre-Issuance Technical Requirements v 4.1.2 2/9/05

[3] http://proxmark3.com

저자소개

이 철 욱

1995년 2월 Bachelor of Commercial Art, Central Texas College at Killeen, Texas, US

1998년 2월 Bachelor of Business Administration, University of Texas at Arlington, Texas, US

2004년 7월~현재 HID Global-Korea, 한국지사장