PCI PTS 요구사항을 충족하는 안전한 PEK(PIN Encryption Key) 업데이트 방법

허제호* 정기현* 최경희**
*아주대학교 전자공학과
**아주대학교 컴퓨터공학과
e-mail : hurdol@ajou.ac.kr

A Study on Method to update PEK(PIN Encryption Key)

Je-Ho Heo*, Ki-Hyun Chung*, Kyung-Hee Choi**
*Dept. of Electronics, A-jou University
**Dept. of Computer Engineering, A-jou University

요 약

금융 사기로 인한 피해로부터 카드 사용자의 금융 정보를 보호하기 위한 노력이 지속되고 있다. 금융 카드에 대한 보안은 IC 금융 카드의 사용 등의 방법으로 지속적으로 보완되고 향상되어 가고 있다. 이런 시점에 상대적으로 취약한 결재 시스템인 카드 단말기에 대한 보안에 또한 관심을 기울여야 하는 시점이다. 이런 의미로 카드 단말기에 대한 보안성 평가 스킴인 PCI PTS(Payment Card Industry Payment Transaction Security) 요구사항을 소개하고 카드 단말기의 필수적 키인 PEK(PIN Encryption Key)를 주입하는데 있어 PCI PTS 의 논리적 요구사항을 충족하는 방법을 제시한다.

1. 서론

금년 3 월 2 일부터 금융 IC(Integrated Circuit)카드 전용 사용이 시범운영 실시된다. 기존의 금융 MS(Magnetic Strip)카드의 불법 복제 등의 보안에 대한 취약성을 보완하기 위한 대안으로 만들어진 IC 카드를 사용하기 시작하는 것이다. 수학적으로 해독이 거의 불가능한 암호화 기법과 물리적인 공격으로부터 카드를 보호하기 위한 여러 가지 방법들로 제작된 IC 카드는 더 이상 카드를 통한 금융 사기는 불가능하게 만들어가고 있다. 하지만, 상대적으로 크기가 크고 접근이 쉬운 카드 단말기에 대한 보안은 국내에서 크게 부각되지 않고 있다. 그러나 유럽, 미국, 일본, 중국, 호주 등은 금융정보를 사용하는 기기에 대한 보안 또한 지속적으로 관심을 가지고 있다. 그 대표적인 표준이 세계적 카드브랜드 회사인 VISA, MasterCard, American Express, Discover, JCB 의 협의체인 PCI SSC (Payment Card Industry Security Standard Council)에서 제정되어 운영되고 있는 PCI PTS(Payment Card Industry PIN Transaction Security) 요구사항이다. 위의 나라들은 PCI PTS 요구사항뿐만 아니라 자국 내 사정을 고려하여 그 이상의 보안 요구사항을 요구하고 있고 일부 국가에서는 카드단말기를 사용하기 위해서는 PCI PTS 인증을 필수로 요구하는 경우도 있다. 이런 실정에 본 논문을 통해 PCI PTS 요구사항을 소개하고 금융 단말기에 필수적으로 필요한 PEK(PIN Encryption Key)를 주입하는데 있어 PCI PTS 의 논리적 요구사항을 충족하기 위한 방법을 제시하고자 한다.

2. PCI PTS 요구사항

PCI PTS 요구사항은 ATM(Automated Teller Machine)과 POS(Point Of Sale, 카드단말기) 기기에서 카드 사용자의 정보를 보호하기 위한 물리적, 논리적 보안 요구사항이다.

이 요구사항은 PCI(Payment Card Industry) 에서 받아들여지기 위한 최소한의 기준을 제시하고 있다. 이 요구사항은 카드사용자의 정보가 유출되는 것을 원천적으로 제거하기 위한 방법은 아니지만 유출에 대한 가능성을 최소화 하기 위한 요구 사항이다.

이 요구사항은 기기에 물리적으로 침투해서 버그 삽입하고 카드 사용자의 정보를 유출한다든지, 기기의 오 동작(Malfunction)을 유발시켜 키 값을 유추하는 공격 등으로부터 기기를 보호하기 위한 물리적, 논리적인 특징들을 요구하고 있다. 그리고 이것에 대한 평가를 CC(Common Criteria)에서 사용하고 있는 Attack Potential 이라고 하는 객관적인 지표를 사용하여 기기를 평가하게 된다. 또한 기기에 대한 생산, 관리, 전송, 저장 등 기기에 대한 전반적인 life cycle 에 대한 요구사항 또한 명시하고 있다.

PCI PTS 요구사항은 3 년을 주기로 메이저 업데이트가 되고 수시로 이슈 사항이 있을 때마다 마이너 업데이트를 시행하고 있다. 현재 3.x 버전이 release 되어 운영되고 있고 다음과 같이 5 개의 평가 모듈로

구성되어 있다.

1) Core Requirement : 물리적, 논리적인 핵심 요구사항을 기술하고 있다.
2) POS Terminal Integration : 물리적, 논리적 요구사항을 적용하는 범위에 따라 Approval 종류가 바뀐다. 이에 따르는 요구사항을 기술하고 있다.
3) Open Protocols : TCP/IP 프로토콜을 사용하는 기기에 대한 요구사항을 기술하고 있다.
4) Secure Reading and Exchange of Data : 카드 사용자의 정보를 보호하기 위한 요구사항을 기술하고 있다.
5) Device Management : 기기의 Life cycle 전반에 관련된 요구사항을 기술하고 있다.

3. 키와 관련한 PCI PTS 논리적 요구사항

PCI PTS 의 핵심 요구사항 중에 하나인 논리적 요구사항에서는 다음과 같이 키와 관련된 요구사항을 기술하고 있다.

"The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA key bundle."

"기기상에 운영되는 키 관리 방법은 ISO 11568 과 ANSI X9.24 에 부합해야 한다. 키 관리 방법은 TDES 키 번들을 유지하는데 있어 ANSI TR-31 키 생성 방법이나 그와 동등한 수준의 방법을 사용해야 한다."

본 논문에서는 기기를 실제로 사용하기 위해 필요한 PEK(PIN Encryption Key)와 관련하여 해당 요구사항에 어긋나지 않는 PEK 주입 방법에 대해 기술하려고 한다.

4. 안전한 PEK 주입을 위한 사전 조건

안전한 키 주입을 위해서 물리적, 절차적, 논리적인 보안이 필요하다. 본 논문에서 물리적, 절차적으로 안전한 환경에서 키 주입이 이루어지는 것을 가정한다.

안전하게 PEK 를 주입하기 위해서는 다음과 같은 키의 생성을 가정한다.

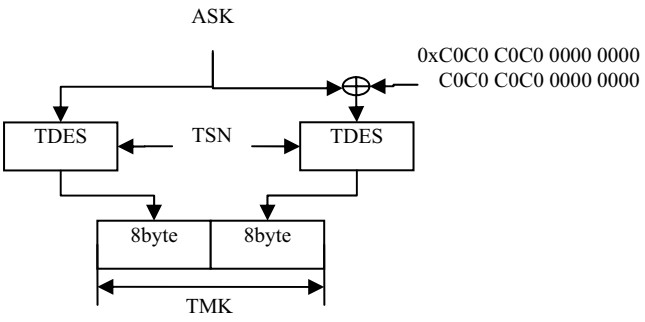
- PEK(PIN Encryption Key) : 랜덤으로 생성된 112-bit TDES 키, 카드 사용자의 PIN 을 암호화 하기 위해 카드 단말기에서 사용되는 키이다.

- UBK(User Base Key) : 랜덤으로 생성된 112-bit TDES 키, 카드단말기 내부의 TMK 을 생성하기 위한 키이다.

- TSN(Terminal Serial Number) : 카드단말기를 구별하기 위해 카드단말기가 가지는 유일한 8-byte 값이다. TMK 을 생성하기 위한 입력 값으로도 사용된다.

- TMK(Terminal Mater Key) : PEK 를 카드단말기에 주입할 때 PEK 을 암호화하는 키다. TMK 는 다음과 같은 방법을 통해 생성된다. (ANSI X9.24 참조)

1) UBK1 = UBK
2) Left of TMK = 3DES_ENC (KSN, UBK1)
3) UBK2 = UBK XOR (0xC0C0 C0C0 0000 0000 C0C0 C0C0 0000 0000)
4) Right of TMK = 3DES_ENC (KSN, UBK2)
5) TMK = Left of TMK || right of TMK.

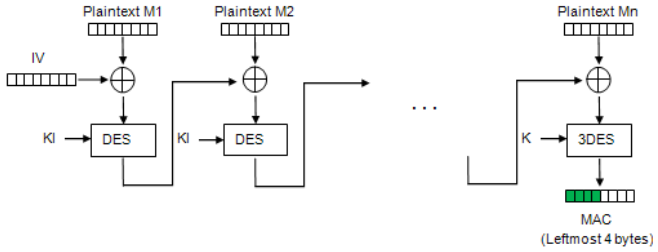


(그림 1) TMK 생성 방법

카드단말기는 생산 공정에서 안전한 방법으로 TSN 과 TMK 가 주입되어 생산된다. 이렇게 만들어진 카드단말기는 제조사로부터 구매자에게 전달되고 카드단말기 구매자는 자신들이 사용할 PEK 를 카드단말기에 주입해야 한다. 이때 주입하는 절차는 다음과 같다.

5. 안전한 PEK 주입 절차

1) 카드단말기는 TSN 과 TMK 의 KCV 값을 포함하여 호스트로 키 주입 요청 메시지를 전송한다. TMK 의 KCV 값은 TMK 의 무결성을 검증하기 위한 방법으로 ANSI X9.24 에서 정의하고 있는 KCV 생성방법을 사용한다. 이 값은 CBC-MAC 값의 좌측 4-byte 의 값으로 한다.



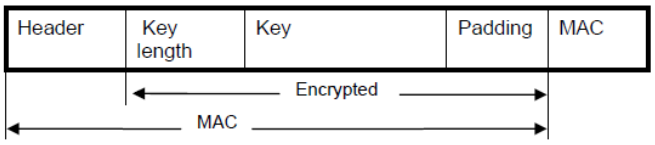
M = M1||M2||….Mn
K = KI||Kr
IV = 0x0000000000000000

(그림 2) KCV 생성 방법

2) 호스트는 전달받은 TSN 과 UBK 값을 가지고 호스트에서 TMK 를 생성하고 이 TMK 의 KCV 값을 구하여 수신된 KCV 값과 일치하는 여부를 확인하여 인증한다.

3) 카드단말기에 대한 인증이 성공하면 TMK 를 이용하여 PEK 를 암호화하고 X9 TR-31 에서 정의하고 있

는 키 교환 방식을 사용하여 다음과 같은 키 메시지를 생성한다.



(그림 3) KCV 생성 방법

3-1) 다음과 같이 전송할 블록을 생성한다.

<표 1> 암호화 전 키 블록

Key Block	2	키 길이 (Key length)
	16	전송하려는 PEK 값
	6	임의 값

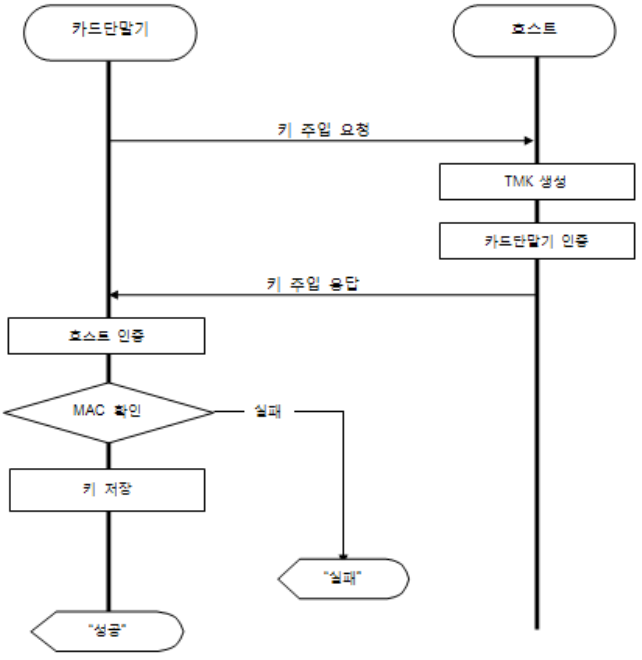
3-2) encTMK 을 다음과 같은 방법을 통해 생성한다.
encTMK = (Left 8-byte of TMK) XOR (“EEEEEEEE”) || (Right 8-byte of TMK) XOR (“EEEEEEEE”)

3-3) encTMK 을 이용하여 TDES CBC 방식으로 해당 블록을 암호화 한다. IV 값은 Header 의 왼쪽 8-byte 값을 한다.

3-4) macTMK 을 다음과 같은 방법을 통해 생성한다.
macTMK = (Left 8-byte of TMK) XOR (“MMMMMMMM”) || (Right 8-byte of TMK) XOR (“MMMMMMMM”)

3-5) macTMK 을 이용하여 TDES CBC 방식으로 Header 부터 암호와 블록의 MAC 값을 생성한다.

4) 수신된 암호화된 키 블록을 CBC-MAC 으로 인증한다. 인증이 성공하면 해당 PEK 값을 저장하고 PEK 주입절차를 완료한다. 실패 시, PEK 주입을 거절한다.



(그림 4) 키 주입 절차

6. 결론

본 논문을 통해 PCI PTS 을 소개하고 그 요구사항 중의 일부인 PEK 주입에 대한 내용에 대해 서술하였다. 이 것을 통해 카드에 대한 보안에 비해 상대적으로 취약한 금융 단말기에 대한 관심을 환기할 수 있었으면 한다. 이 논문에서 다룬 내용은 PCI PTS 에서 요구하는 내용에 비해 극히 일부의 내용을 다루었기에 추후에 물리적 및 다른 논리적 요구사항들에 대한 추가적인 연구를 진행하고자 한다.

참고문헌

[1] PCI Security Standards Council LLC, “Point of Interaction (POI) Modular Security Requirements v3.1”, 2011.
[2] PCI Security Standards Council LLC, “Device Testing and Approval Program Guide”, 2011
[3] ANSI, ANS X9.24-2004 : Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques, 2004
[4] ANSI, TR-31 2005 : Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms, 2005
[5] ISO, ISO 11568-1 : Banking-Key management (retail)-Part 1: Principles, 2005
[6] ISO, ISO 11568-2 : Banking-Key management (retail)-Part 2: Symmetric ciphers, their key management and life cycle, 2005
[7] ISO, ISO 11568-4 : Banking-Key management (retail)-Part 3: Asymmetric cryptosystems-Key management and life cycle, 2007
[8] 한국인터넷진흥원, “부채널 공격 취약성 평가방법론 및 기준개발”, 2009
[9] 한국정보통신기술협회, TTAS.KO-12.0004 : 128 비트 블록암호알고리즘 표준, 1999