스마트 카드의 보안 기술 및 동향 분석

이지민 [1], 조승렬 [1], 박재혁 [1], 전경훈 [1], 박상희 [1], 오현영 [2*]
[1] 가천대학교 AI 소프트웨어학부 학부생
[2] 가천대학교 AI 소프트웨어학부 교수

dlwlals1207@gachon.ac.kr, rs0103@gachon.ac.kr, hyuk5248@gmail.com, ktxsky999@gachon.ac.kr, psh010209@gachon.ac.kr, hyoh@gachon.ac.kr

A Survey on Security Technologies in Smart Card

Ji-Min Lee, Seung-Yeol Cho, Jae-Hyeok Park, Kyoung-Hoon Jeon, Sang-Hui Park, Hyunyoung Oh
Dept. of AI · Software, Gachon University

요 약

스마트카드 기술은 현대 사회의 다양한 영역에서 광범위하게 활용되고 있으며, 그 중 보안은 가장 중요한 고려 사항으로 인식되고 있다. 본 연구에서는 스마트카드에 적용된 다양한 보안 기술의 구현 방식과 실제 상용화된 카드에서의 적용 사례를 분석한다. 이를 통해 스마트카드 보안 기술의 최신 연구 동향을 파악하고, 향후 기술 발전 방향에 대한 전망을 제공하고자 한다.

1. 서론

스마트카드는 내장된 집적회로(IC) 칩을 통해 고도의 사용자 식별 및 인증 기능을 제공하는 보안 장치로, 물리적 접근 제어와 논리적 접근 제어를 동시에 지원하는 특성으로 인해 다양한 분야에서 활용되고 있다. 스마트카드 기술의 지속적인 발전을 위해서는 소비자의 신뢰와 수용성이 핵심적인 요소이며, 특히 보안성은 사용자 만족도와 기술 수용에 결정적인 영향을 미치는 요인으로 작용한다. 본 연구에서는 스마트카드에 적용된 다층적 보안 기술들의 기술적 특성과 실제 구현 사례를 조사하였다. 이를 통해 스마트카드 보안 기술의 현재 상태와 최신 동향을 파악하고, 향후 기술 발전 방향에 대한 전망을 제시하고자 한다.

2. 스마트 카드 보안 기술

스마트카드에 적용된 보안 요소는 사람이 읽을 수 있는 보안 기능 (Human-readable Security Features), 스마트카드 칩의 보안기능 (Security Features of The Smart Chip), 운영체제의 보안기능 (Security Features of The Operating system), 네트워크 보안 (Security Features of The Network)으로 분류할 수 있다[1].

사람이 읽을 수 있는 보안 기능에는 사진 라미네이션, 홀로그램, 미세 인쇄, 엠보싱, 보안 패턴, 레이저 각인 등이 포함된다. 이러한 기능들은 육안으로 식별 가능한 물리적 보안 요소로, 카드의 위조나 변조를 방지하는 역할을 한다.

스마트카드 칩의 보안 기능은 칩의 보안 모드, 암호화된 내부 회로, 외부 공격 탐지 회로 등으로 구성된다. 칩의 보안 모드는 생산 후 외부 접근을 차단하며, 암호화된 내부 회로는 데이터 변경을 어렵게 만든다. 외부 공격 탐지 회로는 비정상적인 접근 시도를 감지하여 칩을 보호한다.

운영체제의 보안 기능에는 PIN 코드 보호와 카드 비활성화 기능이 포함된다. PIN 코드는 카드 데이터 접근을 제어하며, 카드 비활성화 기능은 반복된 인증 실패 시 카드를 잠근다. 다중 보안 프로그램이 탑재된 스마트카드의 경우 각 프로그램별로 PIN 보호 기능을 설정할 수 있다.

네트워크 보안은 스마트카드와 카드 리더기 간의 통신 과정에서 데이터 변조 및 유출을 방지하기 위해 암호화된 통신 프로토콜을 사용한다.

이 외에도 양자 내성 암호 (Post-Quantum Cryptography)는 미래의 양자 컴퓨터 위협에 대비한 새로운 암호화 기술이다[2]. 이 기술은 양자 알고리즘으로도 해독이 어려운 수학적 문제를 기반으로 암호화 시스템을 구축한다. 또한, 백도어(backdoor)는 정상적인 보안 조치를 우회하여 시스템에 접근할 수 있는 방법을 의미한다[3]. 이는 IoT 장치의 보안에 중요한 고려사항으로, 장기간 감지되지 않은 채 전체 네트워크에 영향을 미칠 수 있다.

3. 전자결제 환경에서의 카드 적용 보안 기술 분석

본 연구에서는 국내에서 사용되는 주요 스마트카드에 탑재된 마이크로컨트롤러 유닛(MCU) 종류 및 사용 빈도를 조사하였다. 조사 대상에는 농협, 하나은행, 카카오뱅크, IBK 기업은행, 토스뱅크, 신한은행, KB 국민은행, 현대카드, SC 제일은행, 가천대학교 등 다양한 기관에서 발행한 스마트카드가 포함되었다. 특히 최

* 교신저자

근 발급된 카드(예: 하나 JCB 포인트카드 24/03 제조, NEXON 현대카드 23/06 제조, 현대 대한항공 24/01 제조)와 일부 구형 카드(예: 농협 법인카드 travel wallet, 가천대학교 학생증 구형)를 포함하여 다양한 시기의 23 종의 카드를 조사하였다. 조사 결과는 다음 표와 같다:

(표 1) 다양한 스마트카드에 탑재된 MCU 분포

MCU 제조사	모델명	사용 빈도
NXP	D321	8
NXP	5068	2
NXP	6C14	1
Samsung	190E	7
Infineon	7733	2
Infineon	1861	2
Infineon	540A	1

분석 결과, 몇 가지 주목할 만한 특징이 발견되었다. 첫째, NXP 사의 MCU 가 가장 널리 사용되고 있으며, 특히 D321 모델이 8 회로 가장 높은 사용 빈도를 보이고 있다. 이는 NXP D321 Secure Element[4]가 RSA-4096 및 ECDSA 와 같은 현대 암호학의 주요 알고리즘을 지원하는 등 높은 보안성을 제공하기 때문으로 판단된다.

둘째, Samsung 의 190E 모델이 7 회의 사용 빈도로 NXP D321 에 이어 두 번째로 많이 사용되고 있다. 이는 국내 기업인 Samsung 의 기술력이 국제적 수준에 근접해 있음을 시사하며, 특히 국내 금융 기관들이 국산 기술을 적극적으로 채택하고 있음을 보여준다.

셋째, Infineon 사의 제품도 사용되고 있으나, 세 가지 모델(7733, 1861, 540A)이 각각 적은 빈도로 사용되고 있다. 이는 Infineon 제품이 특정 용도나 요구사항에 맞춰 선택적으로 사용되고 있을 가능성을 시사한다. 예를 들어, 정부에서 발행하는 나라사랑카드와 같은 특수 목적 카드에 사용될 수 있다.

넷째, 최근 발급된 카드(24/03, 23/06, 24/01 제조)에서도 다양한 MCU 가 사용되고 있다는 점은 주목할 만하다. 이는 각 금융 기관이나 서비스 제공업체가 자사의 요구사항에 가장 적합한 MCU 를 선택하고 있음을 시사한다.

다섯째, 구형 카드와 최신 카드의 MCU 를 비교 분석함으로써, 시간에 따른 기술 발전 추이를 관찰할 수 있었다. 최신 카드에서는 더 높은 보안성과 성능을 제공하는 MCU 모델이 선호되는 경향이 있다.

이러한 분포는 2018 년을 전후로 RSA-4096 및 ECDSA 지원이 가능한 플랫폼(예: NXP 의 JCOP 4+)으로의 전환 추세를 반영하고 있다. 이는 컴퓨팅 성능 향상에 따른 새로운 보안 위협에 대응하기 위한 조치로 해석된다. 그러나 이러한 기술적 진보에도 불구하고, 몇 가지 우려사항이 존재한다. 국내 제조사의 MCU 점유율이 상대적으로 낮아, 해외 공급망에 대한 의존도가 높은 상황이다. 이는 잠재적인 보안 위협(예: '스파이칩')에 대한 우려를 야기할 수 있다. 특히 APDU(Application Protocol Data Unit) 명령으로 데이터를 교환하는 스마트카드의 특성상, MCU 의 출력값 신뢰성 확보가 중요한 과제로 대두되고 있다.

또한, 일부 스마트카드의 플래시 메모리 용량이 320KB 에서 256KB 로 감소하는 경향이 관찰되었다. 이는 암호화 알고리즘의 효율성 증가로 인해 더 적은 메모리로도 동일한 수준의 보안을 제공할 수 있게 되었음을 시사한다. 그러나 이러한 변화가 향후 새로운 보안 기능의 추가나 기존 기능의 개선에 제약을 줄 수 있는지에 대해서는 추가적인 연구가 필요할 것으로 보인다.

4. 결론 및 향후 발전 방향

집적회로 기술의 발전과 암호화, 전자서명 알고리즘의 개선으로 인해, 향후 더욱 비용 효율적이고 저용량 플래시 메모리를 사용하는 Secure Element 개발이 가능할 것으로 전망된다. 그러나 현재의 Secure Element 들이 양자 내성 암호(예: Poly1305)에 대한 대응이 미흡한 점은 주목할 만하다. 따라서 향후 양자 컴퓨터 발전에 대비한 양자 내성 Secure Element 의 개발이 필요할 것으로 보인다. 또한, 전자 결제 등에서 사용되는 Secure Element 의 외산 의존도가 높은 현 상황은 공급망 공격에 대한 취약성을 내포하고 있다. 이에 대응하기 위해 국산화된 Secure Element 기술 개발 및 생태계 구축의 필요성이 대두되고 있다.

사사문구

이 논문은 2024 년도 정부(산업통상자원부)의 재원으로 한국산업기술기획평가원의 지원(No. RS-2024-00406121, 자동차보안취약점기반위협분석시스템개발(R&D))과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2022-00166529)을 받고 과기정통부 정보통신기획평가원의 정보보호핵심원천기술개발사업(No. RS-2024-00337414)으로 수행한 결과임.

참고문헌

[1] Hamed Taherdoost et al., "Smart Card Security; Technology and Adoption," International Journal of Security, 2011

[2] Daniel J. Bernstein and Tanja Lange, "Post-quantum cryptography," Nature, 2017

[3] Soheil Hashemi and Mani Zarei, "Internet of Things backdoors: Resource management issues, security challenges, and detection methods," Wiley, 2020

[4] NXP, "Secure Microcontroller SmartMX3 P71D321 Fact Sheet, " [online access: 2024.09] https://www.nxp.com/docs/en/fact-sheet/P71D321.pdf