최근 정보통신 기술을 활용한 모바일 외장메모리 활용 및 보안 강화에 관한 연구

김준호, 고연서, 서우빈, 이지윤, 박준석*
국민대학교, 국민대학교, 국민대학교, 국민대학교, *국민대학교

jhk00@kookmin.ac.kr, qqqwww200410 kookmin.ac.kr, smn0419 kookmin.ac.kr,

lgy4494@ kookmin.ac.kr *jspark@ kookmin.ac.kr

A Study on the use of mobile external memory and strengthening of security using recent information and communication technology systems

Kim Jun Ho, Ko Yeon Seo, Seo Woo Bin, Lee Gi Yun, Park Jun Suk*
Kookmin Univ., Kookmin Univ., Kookmin Univ., Kookmin Univ., * Kookmin Univ.

요 약

본 연구는 스마트폰 사용 보편화와 함께 모바일 데이터의 양과 중요성이 급증함에 따라 안전한 외부 저장 장치에 대한 필요성이 대두되고 있음을 지적한다. 기존 외장 메모리 및 클라우드 백업 솔루션은 데이터 유출, 악성코드 감염, 물리적 도난 및 분실, 서비스 제공자의 보안 문제 등 다양한 보안 취약점을 내포하고 있다. 특히 휴대용 저장 장치를 통한 정보 유출은 심각한 문제로 인식되고 있으며 , 이에 대한 효과적인 대응책 마련이 시급하다. 이러한 배경 하에, 본 논문은 갤럭시 스마트폰과 라즈베리파이 기반 외장 SSD 간의 물리적 연결(맥세이프 방식 자성 결합) 상태를 자기장 센서로 감지하여, 연결 해제 시 자동으로 잠금 기능을 활성화하는 새로운 보안 외장 메모리 시스템을 제안한다. 제안 시스템은 강력한 데이터 암호화(AES-256), 하드웨어 보안 모듈(스마트폰의 Android Keystore, 라즈베리파이의 TPM)을 활용한 키 관리, 그리고 라즈베리파이의 AP(Access Point) 모드를 통한 독립적이고 안전한 통신 채널 구축을 핵심 특징으로 한다.

Ⅰ. 서 론

현대 사회에서 스마트폰은 개인의 일상생활과 업무 수행에 필수적인 도구로 자리매김하였으며, 이에 따라 생성되고 저장되는 디지털 데이터의 양 또한 기하급수적으로 증가하고 있다. 이러한 데이터에는 사진, 동영상과 같은 개인적인 기록뿐만 아니라 금융 정보, 건강 기록, 업무 관련 중요 문서 등 민감한 정보가 다수 포함되어 있어 안전한 관리가 매우 중요하다. 모바일 데이터의 급증은 단순한 양적 팽창을 넘어, 데이터의 민감도와 가치 상승을 동반한다. 과거에는 개인 사진이나 간단한 문서 저장이 주를 이루었다면, 현재는 의료 기록 , 기업 내부 자료 , 금융 정보 등 유출 시 심각한 피해를 야기할 수 있는 정보들이 모바일 환경에서 다뤄지고 있다. 이는 더욱 강력하고 다층적인 모바일 보안 솔루션의 필요성을 시사한다.

Ⅱ. 본론

본 논문에서 제안하는 모바일 보안 외장 메모리 시스템의 아키텍처, 핵심 보안 메커니즘, 안드로이드 애플리케이션 설계 방안, 그리고 사용자가 선택 가능한 계층적 보안 옵션에 대해 상세히 기술한다.

제안 시스템은 사용자 인터페이스 및 암호화 키 관리를 담당하는 갤럭시 스마트폰 애플리케이션, AP(Access Point) 모드로 동작하며 데이터 저장 및 인증을 수행하는 라즈베리파이, 실제 데이터가 암호화되어 저장되는 외장 SSD, 그리고 스마트폰과 라즈베리파이(외장 SSD 장착부) 간의 물리적 연결을 담당하는 맥세이프 방식 자성 결합부로 구성된다. 라즈베리파이를 단순한 스토리지 컨트롤러가 아닌, 독립적인 AP 기능과 하드웨어 보안(TPM) 기능을 갖춘 '보안 게이트웨이'로 활용하는 것이 이 아키텍처의 핵심이다.[1] 이는 스마트폰과 외장 SSD 사이에 신뢰할 수 있는 중간 계층을 형성하여, 외부 네트워크의 위협으로부터 데이터를 격리하고, 장치 간 인증을 강화하는 역할을 한다.

핵심 보안 메커니즘으로는 물리적 연결 및 근접 감지 기반 잠금, 데이터 암호화 및 키 관리, 보안 통신 프로토콜이 있다. 본 시스템의 특징은 맥세이프 방식의 자성 결합을 이용한 물리적 연결 상태 감지 및 이에 연동된 자동 잠금 메커니즘이다.[2][3] 스마트폰 앱은 내장 자기장 센서를 이용해 결합 상태를 모니터링한다. 결합이 약해지거나 분리되어 자기장 세기가 임계값 이하로 떨어지면, 앱은 이를 비정상 상태로 간주하고 즉시 DevicePolicyManager API 를 통해 설정된 수준의 잠금(앱 잠금 또는 OS 잠금)을 실행한다. 이는 '소유 증명'의 한 형태를 실시간으로 강제하는 효과가 있다. 즉, 데이터 접근을 위해서는 논리적 인증뿐 아니라 '물리적 결합 상태'를 지속적으로 유지해야 한다. 이는 기기

탈취나 분실 시 데이터 노출 위험을 즉각적으로 줄이는 선제적 방어 수단이다.

저장되는 모든 사용자 데이터는 AES-256 알고리즘으로 암호화된다. 암호화 키는 다음과 같이 분리되어 하드웨어 보안 모듈에 안전하게 저장된다(스마트폰: 데이터 암복호화용 AES 키는 Android Keystore 에 저장되어 키 추출을 방지한다. 키 사용 시 생체 인증 연동이 가능하다)
(라즈베리파이: 장치 인증용 Device Key 는 TPM 내부에 저장되어 물리적/소프트웨어적 공격으로부터 보호된다). 이러한 듀얼 하드웨어 기반 키 저장 방식은 매우 강력한 보안 아키텍처를 구성한다. 어느 한쪽 장치가 손상되더라도 다른 쪽 장치의 키와 그 키로 보호되는 정보는 안전하게 유지될 가능성이 높다. 즉, 공격자가 시스템 전체를 장악하기 어렵게 만든다.

스마트폰과 라즈베리파이 간 통신은 라즈베리파이 AP 모드가 생성하는 독립적인 Wi-Fi 네트워크를 통해 이루어진다. 이는 외부 네트워크 공격 표면을 최소화한 격리된 보안 통신 채널을 구축하는 전략이다. WPA2/WPA3 보안 프로토콜을 적용하여 채널 보안성을 강화한다. 초기 연결 시, 앱은 라즈베리파이에 인증을 요청한다. 라즈베리파이는 TPM 에 저장된 Device Key 를 활용한 Challenge-Response 방식으로 자신이 정당한 장치임을 증명한다. 인증 후, 데이터 쓰기 시 스마트폰은 AES 키로 데이터를 암호화하여 전송하고, 라즈베리파이는 이를 SSD 에 저장한다. 데이터 읽기 시 라즈베리파이는 암호화된 파일을 전송하고, 스마트폰은 이를 AES 키로 복호화한다.

스마트폰 애플리케이션은 시스템의 핵심 제어 및 사용자 인터페이스 역할을 수행한다. 사용자 경험(UI/UX)을 중시하여 갤러리 관리, 백업/복원, 보안 설정 등을 직관적으로 수행할 수 있도록 설계해야 한다. 앱은 백그라운드에서 SensorManager 를 통해 자기장 센서 값을 지속적으로 모니터링하고, 임계값 비교 로직을 수행한다. 분리 감지 시 DevicePolicyManager 를 호출하여 설정된 잠금 레벨을 적용하고, 재결합 및 사용자 인증(비밀번호/생체인증) 시 잠금을 해제하는 로직을 구현한다. 또한, Android Keystore API 와 연동하여 AES 키를 안전하게 관리하고 암복호화 작업을 수행하며 , 라즈베리파이 AP 와의 Wi-Fi 통신, 인증 및 데이터 전송 프로토콜을 처리하는 모듈을 포함한다. 사용자가 계층적 보안 옵션을 쉽게 선택하고 관리할 수 있는 설정 화면을 제공한다.

본 시스템은 모든 사용자의 보안 요구 수준과 편의성 선호도가 동일하지 않다는 점을 고려하여, 사용자가 직접 보안 수준을 선택할 수 있는 계층적 옵션을 제공한다. 기본 모드일 경우 추가 암호화 서비스를 제공하지 않는다. 하지만 중간 또는 고급 모드일 경우 앱 잠금, OS 레벨 수준의 화면 잠금을 제공한다.

Ⅲ. 결론

본 논문은 모바일 데이터 저장의 보안성과 편의성을 동시에 향상시키기 위해 물리적 연결 상태 감지 기술을 통해 새로운 모바일 외장 메모리 시스템을 제안하였다. 맥세이프 방식의 자성 결합을 이용한 물리적 연결 상태를 스마트폰의 자기장 센서로 실시간 모니터링하고, 연결 해제 시 DevicePolicyManager 를 통해 앱 또는 OS 수준의 자동 잠금을 수행하는 핵심 아이디어를 제시하였다. 또한, 라즈베리파이를 AP 모드로 활용하여 독립적인 보안 통신 채널을 구축하고, AES-256 데이터 암호화, Android Keystore 및 TPM 을 활용한 하드웨어 기반 키 관리를 통해 강력한 보안 기반을 마련하였다. 마지막으로 사용자 선택형 계층적 보안 옵션을 제공하여 다양한 사용자의 요구를 만족시키고 시스템의 수용도를 높일 수 있도록 설계하였다.

본 연구의 의의는 기존 휴대용 저장 장치의 보안 문제점을 해결하기 위해 물리적 인터페이스 상태, 하드웨어 보안 모듈, 소프트웨어 암호화 및 제어 기술을 효과적으로 융합하는 새로운 접근 방식을 제시했다는 점에 있다. 제안된 시스템은 라즈베리파이와 같은 비교적 저렴한 하드웨어를 기반으로 구현 가능하여 , 비용 효율적이면서도 높은 수준의 보안을 제공하는 개인용 모바일 스토리지 솔루션의 실현 가능성을 보여준다. 이는 단순한 편의성을 넘어 '물리적 연결의 무결성'을 중요한 보안 요소로 통합하는 새로운 모바일 보안 패러다임을 제시하며, 향후 관련 기술 발전에 기여할 수 있을 것으로 기대된다.

향후 연구 방향으로는 제안된 시스템의 실제 프로토타입을 제작하여 성능 및 보안성에 대한 심층적인 실험 검증을 수행하는 것이 필요하다. 특히, 다양한 환경 조건에서의 자기장 센서 감지 정확도 및 안정성, 암복호화 속도, 데이터 전송률 등을 측정하고, 알려진 공격 시나리오에 대한 방어 능력을 평가해야 한다. 국제 표준 보안 인증인 Common Criteria EAL 등급 획득을 목표로 시스템의 신뢰성을 객관적으로 검증하는 방안도 고려할 수 있다. 또한, 다양한 스마트폰 모델 및 안드로이드 OS 버전에 대한 호환성 확보, 자성 센서 오작동 방지를 위한 알고리즘 고도화, 사용자 피드백을 반영한 UI/UX 개선 , 그리고 양자컴퓨터 시대에 대비한 양자내성암호(PQC) 적용 가능성 탐색 등이 후속 연구 과제로 제시될 수 있다.

ACKNOWLEDGMENT

Put sponsor acknowledgments.

참 고 문 헌

[1] Marcus S. E. N, "Emulation of TPM on Raspberry Pi", Lund University 2015.

[2] Anders B. " Security architecture and implementation for a TPM-based mobile authentication device", University of Cambridge, 2014.

[3] Jaemin C." MagID: Enhancing the Functionality of Off-the-Shelf Smartphones Through Magnetic Accessory Identification," IEEE Access, PP(99):1-1.

[4] Nikolay M. "MagneticSpy: Exploiting Magnetometer in Mobile Devices for Website and Application Fingerprinting" 2019, DOI: 10.1145/3338498.3358650.