사용자 경험 데이터를 위한 PKI의 보안 요구 사항 분석 및 고찰

임형진[1], 이덕규[2],박종혁[1,*]
[1]서울과학기술대학교 컴퓨터공학과
[2]서원대학교 정보보호학과
[1]e-mail:{imhj9121, jhpark1}@seoultech.ac.kr
[2]deokgyule@gmail.com

Analyses and considerations for security requirement of PKI for user experience data

Hyungjin Im[1], Deok Gyu Lee[2], Jong Hyuk Park[1,*]
[1]Dept. of Computer Science and Engineering and Dept. of interdisciplinary Bio IT Materials, SeoulTech, Korea
[2]Department of Information Security, Seowon University, Korea

요 약

최근 사물인터넷에 대한 발전이 빠르게 이루어짐에 따라서 인터넷 상의 보안 이슈 또한 증가하고 있다. 이에 따라 데이터를 안전하고 은밀하게 통신하기 위한 공개키 기반 구조 (Public-Key Infrastructure: PKI) 기술이 발전하고 있다. PKI는 신뢰할 수 있는 기관에서 개인이나 기관을 식별할 수 있는 인증서를 저장하고 있으며 이를 활용할 수 있도록 돕는 디렉토리 서비스를 제공한다. 특히 기존의 PKI 구조에는 사용자의 경험이 담겨있는 패스워드 기반으로 개인키를 암호화 하고 있다. 이는 사용자 인증과 데이터 암호화와 같은 강력한 보안 서비스를 제공하고 있지만 이 또한 취약점을 내포하고 있다. 본 논문에서는 공개키 기반 구조의 핵심 요소에 대해 논의하며 보안 취약점을 분석한다. 이를 통해 안전한 사물인터넷 환경을 위한 연구 방향을 제시한다.

1. 서론

최근 무선네트워크 환경과 스마트 디바이스의 발전으로 인해 사물, 사람 등과 같은 객체 간의 연결이 가능한 사물인터넷 (Internet of Things: IoT)에 대한 관심이 급증하고 있다 [1]. 그러나 사물인터넷 서비스는 유·무선네트워크로 연결되기 때문에 사물인터넷 통신상에서 발생될 수 있는 정보유출, 데이터 변조, 복제 공격, 서비스 거부, 프라이버시 침해 등의 보안 문제가 나타나고 있다 [2].

이에 대한 대처로 제시되고 있는 방식 중 PKI에 대한 연구가 진행되고 있다. 이는 디지털 상에서 펌웨어를 업그레이드 할 수 있다. 또한 PKI를 통해 인증, 인가, 암호화, 서명등의 서비스를 제공함으로써 기기간의 신뢰성을 제공할 수 있다. 또한 PKI는 IoT 환경 뿐만 아니라 인터넷에서 개인의 공인인증서를 이용한 신분확인, 사이트의 인증서를 관리하고 통신 구간을 암호화하는 등의 기능을 가지고 있다 [3].

최근 사용자 경험 (User Experience: UX) DB에 관심이 모아짐에 따라 사용자의 정보가 활용되는 PKI에서의 보안 위협이 존재한다. 사용자의 습관, 기호 에 따라 비밀번호가 유추될 수 있음에 따라 이에 대한 안전한 데이터 처리가 요구된다.

*교신저자: 박종혁(서울과학기술대학교)

본 논문에서는 PKI 환경에서의 핵심 요소들에 대해 논의한다. 또한 이를 통해 PKI에서의 보안 취약점을 분석한다. 이를 통해 안전한 PKI환경을 위한 보안 요구 사항에 대해 고찰한다.

2. 관련연구

2.1 PKI 핵심 기술

공개키 암호 방식에는 공개키와 비밀키가 존재한다. 공개 키는 누구나 알 수 있는 암호키이며 비밀키는 키의 소유자만이 알고 있는 키이다. 이는 잘 알려진 공개키 암호화 알고리즘인 RSA, Elgamal, ECC (Elliptic curve cryptography) 등을 활용하여 사용된다. 공개 키 암호 방식은 공개키로 암호화할 경우 비밀키로만 암호를 해독할 수 있으며 반대로 비밀키로 생성한 암호는 공개키로만 해독이 가능하다. 이러한 기능을 이용하여 공개키 암호, 공개키 서명에 사용된다 [4].

2.2 PKI 구성요소

PKI는 수학적 연산에 의해 공개키와 개인키를 생성해야 하며 이를 관리하고 분배할 기관과 관리 대상 등이 필요하다. 따라서 PKI를 구성하는 최소 요소들을 사용자, 인증기관, 저장소로 구분할 수 있다. 다음은 각 요소 별 목적

및 설명을 나타낸다 .

사용자 : 사용자는 PKI를 사용해서 자신의 공개키를 등록하고 싶어 하는 사람과, 등록되어 있는 공개키를 사용하는 두 부류가 존재한다.

인증기관 (CA, Certificate Authority) : CA는 다른 CA 혹은 사용자에게 인증서를 작성하고 발급한다. 또한 최신의 인증서 폐지 목록을 조사해서 그 인증서의 유효성을 확인한다.

저장소: 사용되고 있는 인증서의 DB로 인증서에 대한 상태를 확인하고자 할 때 사용되며 인증서의 상태 정보를 저장하는 역할을 한다.

3. PKI 보안 요구사항 및 분석

CA는 계층적 구조로 이루어져 있다. 다음 그림 1과 같이 최상위 인증기관(Root CA)이 존재하며 하위 인증기관은 상위 인증기관의 영향을 받는다. 그러므로 상위기관일수록 그에 대한 보안의 중요도를 높여야 한다 [5]. Root CA가 Malware에 공격당할 경우 일시적으로는 하위 CA에서 인증서 발급 업무를 수행할 수 있을 수도 있지만, 장기적으로 Root CA에서의 정책 수정, 인증서 발급, 인증서 폐지 등의 업무에 지장이 있을 경우 하위 CA의 기능이 마비될 수 있다 [6].

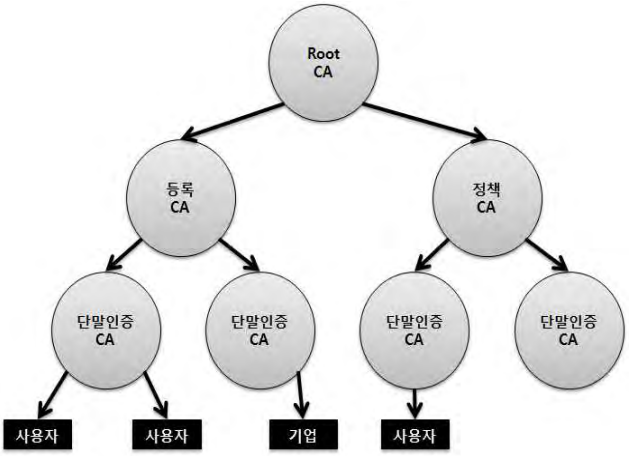

그림 1 CA의 계층적 구조

공개키 기반 구조에서 공개키와 개인키의 관리는 주요한 프로세스이다. 이 중에서 사용자의 개인키는 서명, 인증 등에서 사용되므로 가장 중요한 요소이다. 만일 사용자가 공격자에게 개인키가 유출될 경우 개인키를 이용하여 전자문서에 서명을 생성할 수 있으며 사용자 인증을 수행할 수 있다. 다음은 사용자의 개인키를 알아낼 수 있는 보안 취약점이다.

알고리즘 공격 (Algorithmic Attack): 서명 알고리즘 자체의 취약점을 이용한 공격 방법으로 서명 알고리즘의 수학적 취약점을 이용하여 개인키를 노출시킨다. 알고리즘 공격 취약점은 IT 요소가 첨가되지 않고 수학적 알고리즘에 의존하기 때문에 비교적 알아내기가 어렵다.

사회 공학적 기법 (Social Egineering): 공격자와 일반 사용자가 동일 시스템을 사용할 경우 공격자는 사용자의 PC에 접근하여 Key-logging을 통해 메모리 상에 노출되어있는 개인키의 비밀번호를 탈취할 수 있으며 이를 통해서 개인키를 노출시킬 수 있다.

전수조사 공격(Brute-force Attack): 패스워드를 통해 보호되어 있는 개인키를 노출하기 위해 패스워드로 가능한 모든 가능성에 대해 대입시켜 키를 알아내는 전수조사 공격이나 사용자들이 많이 사용하는 키를 대입시켜 패스워드를 알아내는 사전 공격 (dictionary attack)을 이용하여 개인키를 노출시키는 공격 방식이다.

4. 결론 및 고찰

모든 사물에 인터넷이 연결되는 시대에서 정보 보안은 주요한 주제이다. IoT 환경에서는 정보유출, 데이터 변조, 복제 공격, 서비스 거부, 프라이버시 침해 등의 보안 문제가 나타나고 있다. 이러한 보안 취약점을 해결하기 위하여 PKI에 대한 연구가 활발하게 진행되고 있다.

본 논문에서는 PKI 환경에서의 보안 취약점을 해결하기 위한 PKI의 핵심기술과 보안위협에 대해 분석하였다. 사용자는 PKI를 통해 안전한 서비스를 제공받을 수 있지만 PKI 환경에서는 공개키 암호화, 디지털 서명을 사용하기 때문에 기존의 공개키 암호화 방식이 갖는 취약성을 계승한다. 또한 개인키를 보호하기 위해 패스워드 암호화를 수행함으로 이에대한 취약성 또한 존재한다. 그러므로 차후에는 안전한 PKI 환경을 구축하기 위해 각각의 보안 취약성에 대한 심도있는 연구를 통해 보안 요구 사항을 정립할 수 있는 연구가 필요하다.

감사의글

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-H8501-15-1014)

참고문헌

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems, Vol.29, Iss.7, pp1645-1660, 2013

[2] Chakib Bekara "Security Issues and Challenges for the IoT-based Smart Grid" International Workshop on Communicating Objects and Machine to Machine for MissionCritical Applications (COMMCA-20144). Vol.34, pp.532-537, 2014

[3] Yong Lee, Jeail Lee, JooSeok Song, "Design and

implementation of wireless PKI technology suitable for mobile phone in mobile-commerce", Vol.30, Iss.4, pp.893-903, 2007
[4] Gabriel López Millán, Manuel Gil Pérez, Gregorio Martínez Pérez, Antonio F. Gómez Skarmeta, "PKI-based trust management in inter-domain scenarios", Computers & Security, Vol.29, Iss.2, pp.278-290, 2010
[5] Carl Ellison, Bruce Schneier, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", Computer Security Journal, Vol.16, Num.1, pp.1-7, 2000
[6] Carlisle Adams, Steve Lloyd, "Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations" Macmillan Technical Publishing, 1999