Journal of Korea Multimedia Society Vol. 19, No. 5, May 2016(pp. 918-923)
http://dx.doi.org/10.9717/kmms.2016.19.5.918

IoT 환경에서의 보안위협 분석과 모바일 키 복구

이윤정†, 박용준††, 김철수†††, 이봉규††††

Threats Analysis and Mobile Key Recovery for Internet of Things

Yunjung Lee†, Yongjoon Park††, Chul Soo Kim†††, Bongkyu Lee††††

ABSTRACT

IoT should be considered security risk environments such as various platforms and services including smart devices that can be mounted on household electric appliances, healthcare, car, and heterogeneous networks that are connected to the Internet, cloud services and mobile Apps.. In this paper, we provide analysis of new security threats, caused by open-platform of IoT and sensors via the Internet. Also, we present the key recovery mechanism that is applied to IoT. It results to have compatibility with given research, reduces network overhead, and performs key recovery without depending on key escrow agencies or authorized party.

Key words: IoT Security, Smart Devices, Sensor, Mobile Key Recovery

1. 서 론

사물인터넷(IoT, Internet of Things)이란 사용자의 제어에 의하여 동작하는 스마트기기뿐만 아니라 자원제한적인 센서를 포함한 모든 기기들을 인터넷과 연결할 수 있는 기술로서, 가트너는 2020년까지 260억 개 이상의 기기들이 상호 연결되어 다양한 혁신과 사업기회가 창출될 것이라고 전망하고 있다 [1]. IoT은 우리 실생활에 사용되는 모든 기기에 활용할 수 있어 IoT 플랫폼의 개방화, 다양한 이기종 스마트기기 및 센서의 인터넷을 통한 상호 연결로 인한 새로운 보안위협들이 등장할 것으로 예상되므로 사전에 발생할 수 있는 보안위협을 대비하여 보안침해 사고의 확률을 최소화하여야 한다.

IoT 보안을 위하여 가전, 의료, 자동차 등에 탑재할 수 있는 스마트기기, 인터넷과 연결되는 이종네트워크, 클라우드 서비스 모바일 앱 등 각종 플랫폼 및 서비스와 같은 환경의 보안위험을 고려하여야 하며, IETF·ITU-T·ISO와 같은 국제표준단체는 IoT 서비스 공동플랫폼 개발, 경량 인증/암호화 기술 표준화를 활발히 진행 중이며 IoT 보안 요구사항에 대한 논의가 시작되는 단계이다 [3, 4, 13]. 본 논문에서는 스마트카·스마트홈·항공기와 같은 주요 IoT 보안위협에 대하여 분석하고 IoT을 위한 네트워크 표준 확립에 고려할 사항을 제시하여 안전한 IoT 서비스를 제공받기 위하여 향후 연구고려사항을 제시하고자 한다.

암호는 본래 가지고 있는 키 관리의 어려움으로 인해 키의 분실이나 손실로 인해 사용자가 자신의 키(또는 암호문)에 접근할 수 없는 경우가 생기거나,

※ Corresponding Author : Chul Soo Kim, Bongkyu Lee, Address: (690-756) Ara-dong, Jeju-si, Korea, TEL : +82-64-754-3592/ +82-64-754-3593, FAX : +82-64-725-2579, E-mail : kimcs@jejunu.ac.kr/ bklee@jejunu.ac.kr
Receipt date : Mar. 22, 2016, Revision date : Apr. 19, 2016
Approval date : Apr. 22, 2016
† Dept. of Computer Science and Statistics, Jeju National University (E-mail : rheeyj@jejunu.ac.kr)
†† Dept. of Computer Science and Statistics, Graduate School, Jeju National University (E-mail : joony82@jejunu.ac.kr)
††† Dept. of Computer Science and Statistics, Jeju National University
†††† Dept. of Computer Science and Statistics, Jeju National University
※ This research was supported by the 2015 scientific promotion program funded by Jeju National University

Fig. 1. Interent of Things [2].

국가가 범죄 수사 등의 적법한 이유로 키에 접근해야 할 필요가 있을 때, 또는 암호가 오용됨으로써 발생할 수 있는 잠재적인 위협 등의 문제점이 나타난다[10].이러한 점을 해결하기 위해 제시된 방안은 키 복구기반 방식이다. 키 복구는 합법적 단체가 기기 오류 또는 악의적인 공격에서 비롯되는 키와 관련된 데이터의 손실 또는 파괴로부터 키를 복구함으로써 암호화된 데이터로부터 원래데이터를 복구 할 수 있도록 하는 시스템이다. 키 복구는 각 특성에 따라 키 위탁 방식, 캡슐화 방식, TTP 기반의 방식으로 나눌 수 있다[11].

IoT 기기들 중에는 계산 능력이 낮은 단말들도 포함되어 있기 때문에, IoT 환경에서는 효율적이면서도 안전한 서로 상반되는 목적을 만족시키는 암호 시스템이 필요하다. 모바일 환경을 위하여 공개키 암호방식을 사용하여 키를 분배하고 분배된 키를 대칭키 방식을 사용하는 시스템이 제안되었다. 따라서 IoT 환경도 이를 따르게 될 것이다. 그러나 키를 분실한 경우 정당한 사용자도 암호문을 복호화 할 수 없거나, 암호가 범죄에 이용되는 경우 합법적인 수사를 방해할 수 있다는 역기능이 발생할 수 있다. 더 나아가, IoT 환경에 연결된 수많은 단말들로부터 유의미한 암호화된 데이터들이 발생되는 경우, 키의 분실로 인해 어려움에 처할 가능성은 폭발적으로 증가할 것이다[12].

본 논문에서는 앞서 기술한 IoT 환경 특성에 적합한 효율적이면서도 안전한 키분배 및 키복구 메커니즘을 제안한다. 제안하는 시스템은 암호의 역기능을 방지하기 위하여 요구되는 키 복구 기능을 추가하였으며, 키 복구가 통신단말 한쪽이 일방적으로 키 복구를 할 수 없는 구조로서 양쪽 모두에게 안전성을 제공한다. 또한, IoT 환경에 적합하도록 키복구 시 전송되는 정보가 적어 효율적이다.

2. IoT 환경에서의 보안위협과 보안 고려사항

블랙햇 2014는 세계적인 정보보안 콘퍼런스로서 2014년 8월 2일부터 7일까지 미국 라스베이거스에서 개최됐다. 이 콘퍼런스를 통하여 '모든 것은 해킹 당할 수 있다'는 사실을 재확인하였으며 스마트카 · 스마트홈 · 항공기와 같은 주요 IoT에 대한 해킹을 시연 및 취약점을 제시하였다[5].

IoT은 저사양 기기 사용으로 인하여 백신, 암호화, 인증 등 보안을 적용하기 곤란하고 Zigbee, Wi-fi, Bluetooth 등 이종 네트워크 사이에 상호접속을 통하여 동작하므로 보안문제가 해결되지 않고는 이용 확산이 불가능하다. 특히, 인터넷을 통하여 이종 네트워크 사이 상호접속이 일어나므로 기존 인터넷 환경에 부합하는 보안요구사항을 충족하여야 한다[6].

IETF·ITU-T·ISO와 같은 국제표준단체는 IoT 관련 기술 표준화를 활발히 진행 중이며 IETF는 Fig. 2와 같이 6LoWPAN 워킹그룹을 통하여 IEEE 802.15.4 기반의 센서(Sensor) 네트워크를 TCP/IP 프로토콜 스택에 접목하는 표준화를 진행하였다[7]. 하지만 6LoWPAN 워킹그룹의 표준은 IEEE 802.15.4 기반의 센서의 인터넷환경 접목을 목적으로 하였기에 현재 IoT 환경에 부적합하다.

IETF의 core 워킹그룹에서는 네트워크 환경에서 사용 가능한 웹 기반 응용 프로토콜로 CoAP(Con-

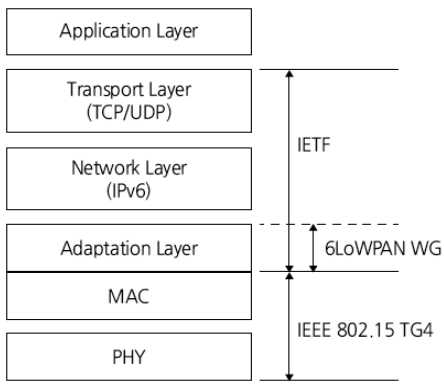

Fig. 2. 6LoWPAN.

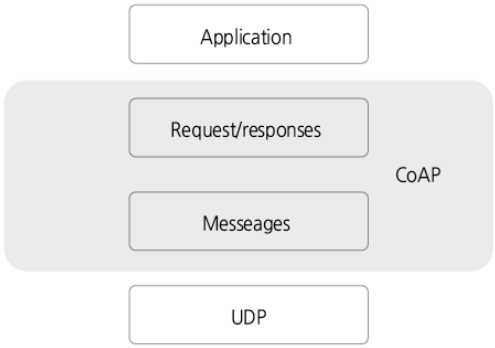

Fig. 3. CoAP Protocol Strack

strained Application Protocol)을 개발해 왔다 [8]. Fig. 3에서와 같이 CoAP은 전송계층 프로토콜로 UDP 사용을 채택하고 있으며 서버/클라이언트 방식으로 이벤트 메시지를 전달하며 송수신을 위해 비동기적 전송 방식을 가지고 있다. 하지만 UDP와 같은 데이터 그램 프로토콜을 사용하므로 한 패킷이라도 손실될 경우 전체 메시지를 다시 전송해야 한다.

이상의 표준들의 장단점과 IoT 네트워크 환경을 고려한 IoT 네트워크 보안요구사항은 다음과 같다 [9].

- 기존 네트워크 스택에 부합하는 보안프로토콜 개발
  - IoT과 센서네트워크 기술 사이 중요한 차이는 센서네트워크를 구성하는 센서들은 인터넷과 연결되지 않은 자체적인 네트워크를 구성하여 통신하였지만, IoT은 사용자의 제어에 의하여 동작하는 스마트기기뿐만 아니라 자원제한적인 센서를 포함한 모든 기기들을 인터넷과 연결
  - 기존의 IP 기반 네트워크 프로토콜 스택에서 문제없이 동작하는 보안프로토콜 개발 필요

- 이종네트워크 상호운용성 확보
  - IoT은 센서와 스마트기기, 네트워크, 플랫폼(하드웨어 플랫폼, 개방형 소프트웨어 플랫폼, 특정 OS 플랫폼등), 웹 서비스, 데이터 분석/예측, 빅데이터 처리, 보안/프라이버시 보호 기술 등으로 구성
  - 이러한 요소 기술은 각각 특정기능을 제공하며, 서로 통합되어 새로운 기능을 제공하기도 하지만 각 요소 기술에 존재하던 보안 기술의 연동에 문제 발생 가능
  - 특히 이기종 기기의 상호 접속 시 공통적으로 적용할 수 있는 보안 기술의 개발이 필요

- 데이터 압축 기술 개발
  - IoT은 자원(CPU, 메모리, 전력 등)이 제한적인 일상의 사물들과 이들이 연결되는 저전력 네트워크로 구성
  - 인터넷을 구성하는 이종 네트워크 사이에서 데이터 전송 매체가 전송할 수 있는 최대 프레임 크기인 최대 전송 단위(MTU)의 차이를 보상하기 위하여 프레임을 나눠서 송수신하는 단편화 기능사용
  - 단편화 기능은 처리 절차와 수신 장치의 자원 제한적인 특성(특히 적은 메모리 공간)으로 인하여 중간자 공격 등 많은 보안위협에 노출
  - 단편화를 최소화하고 시간 효율적인 통신을 위하여 데이터 압축 기술 개발 필요

3. IoT 환경에서 적합한 키분배 및 키복구 메커니즘

본 절에서는 IoT 환경에 적합한 모바일 키분배 및 키복구 메커니즘을 제안한다. [10, 11, 12]의 키 복구 연구들은 앞으로의 IoT 환경에서 요구되는 이동성 및 멀티홈 확장 등의 필요성을 충족시키지 못한다. 제안하는 메커니즘은 앞서의 문제점을 해결하고 통신 주체의 안전성을 확보할 수 있는 방법을 제시한다. 여기서는 4개의 메시지 교환으로 세션키와 그에 필요한 SA 협상이 모두 이루어지며, 서비스거부 공격 방지를 위해서는 추가로 2개의 메시지 교환이 필요하다.

3.1 키복구 정보를 포함하는 키분배 과정

제안하고 있는 키 복구 메커니즘에서 사용될 세션키-암호화키 K_{skr} 를 도출하는 SA의 흐름을 나타낸다. 이 흐름은 키 생성 요청자(A) 응답자(B) 사이에서 발생한다.

① A→B: $g^a \ mod \ p$, crypto offered, n_A, [certreq]
② B→A: $g^b \ mod \ p$, crypto offered, n_B, [certreq]
③ 각각의 A, B : Key = f(nonces, SPIs, $g^{ab} \ mod \ p$) 연산
④ A→B: Key {“A”, sign on ½ msgs, [cert],

child, $g^x \bmod p$}

⑤ B→A: Key {"B", sign on ½ msgs, [cert], child, $g^y \bmod p$}

⑥ A→TTP_A: $K_{TTP-A-pu}$ {x, child }, g, p

⑦ B→TTP_B: $K_{TTP-B-pu}$ {y, child }, g, p

1. ①와 ②의 메시지교환과 ③의 Key 도출은 [10]의 SA 방법을 따른다.

2. ④ 메시지에서 A는 세션키-암호화 키 도출을 위한 Diffie-Hellman 키교환을 위해, 개인값 x를 선정하고 $g^x \bmod p$ 를 기존의 메시지에 추가하여 전송한다.

3. ⑤ 메시지에서 B는 Diffie-Hellman 개인값 y를 선정하고 $g^y \bmod p$ 를 A에게 보낸다.

4. A와 B사이의 메시지 교환이 종료된 후, A와 B는 다음의 방법으로 동일한 세션키-암호화키 K_{skr} 를 각각 생성한다.

$$K_{skr} = f2(g^{xy} \bmod p) \quad (1)$$

$$C = E\{SK\}_{K_{skr}} \quad (2)$$

(1)에서 f2 함수는 단방향 해시함수이다. 이 해시함수와 K_{skr}를 적용할 세션키-암호화 알고리즘은 3번째와 4번째의 SA인 child 안에서 동시에 협상된다. (2)에서 A는 세션키 SK를 세션키-암호화 키인 K_{skr}로 암호화하여 암호화된 세션키 $C=E\{SK\}K_{skr}$ 를 생성한다.

5. ⑥에서 A 는 세션키의 복구를 위하여, 본인의 키 위탁 기관인 TTP-A 에게 세션키-암호화키 K_{skr}의 재료인 x, child, g, p 를 암호화하여 안전한 형태로 전송한다. ⑦에서 같은 방법으로 B도 자신의 키 위탁 기관 TTP-B 에게 y, child, g, p 를 전송하여 위탁한다.

3.2 키복구 과정

시간이 지난 후 A와 B이 해당 세션의 세션키 SK, K_{skr} 나 그와 관련된 정보를 갖고 있지 않은 상태에서, 공공의 목적을 이유로 정부나 그 밖의 다른 권위기관이 해당 패킷을 복호화하기 위하여 세션키를 요구할 때에 키복구가 요구될 수 있다. 이때 권위기관(AP)는 A와 B의 동의하에 TTP-A로부터는 (x, child, g, p)를, TTP-B로부터는 (y, child, g, p)를 전송받는다. 그 후 다음의 연산으로 세션키 SK를 도출하여 키 복구를 완성할 수 있다.

① AP→A, AP→B: *Request for agreement*

② A→TTP_A: *Grant of agreement*

③ B→TTP_B: *Grant of agreement*

④ TTP_A→AP: K_{AP-pu} {x, child }, g, p

⑤ TTP_B→AP: $K_{TTP-B-pu}$ {y, child }, g, p

1. ①에서 AP 는 A, B 각각에게 키 복구를 위한 요청을 전송한다.

2. ②에서 A는 TTP_A에게, ③에서 B는 TTP_B에게 키 복구에 대한 허락을 전송한다.

3. ④는 TTP_A가 AP에게, ⑤는 TTP_B 가 AP에게 키 복구 재료들인 x, y, child, g, p 등을 전송한다.

4. 그후, AP는 다음을 계산하여 세션키 SK를 도출한다.

$$K_{sky} = f2(g^{xy} \bmod p)$$
$$SK = D(C)_{K_{skr}} \quad (3)$$

3. 3 제안된 메커니즘의 안전성 분석

이 장에서는 본 논문에서 제안하는 메커니즘의 안전성을 분석한다. 제안된 메커니즘은 위탁 메커니즘을 기반으로하고 있으며, IoT 환경을 위한 세션키 분배 및 복구 메커니즘을 제공한다.

제안하는 메커니즘은 키분배에 있어서 기존의 IETF 표준을 따르며, IoT 환경의 다른 프로토콜들과 호환성을 갖는다. 또한 전송되는 정보가 비교적 적어 IoT 네트워크 환경에 부하를 크게 증가시키지 않는다. 또한 키 복구를 요청하는 정부와 같은 권위기관은 통신 주체인 A와 B 모두의 동의를 받아야하며, 각각의 키 위탁 기관인 TTP-A, TTP-B 로부터 키 재료들을 전송받아야 세션키 복구가 가능해진다. 통신주체 한쪽이라도 동의하지 않는다면 권위기관은 키복구가 불가능하게 되기 때문에 사용주체들의 안전성이 보장된다. Table 1는 기존의 [10, 11, 12] 연구와 본 논문에서 제안하는 메커니즘을 비교하고 있다.

4. 결 론

본 논문에서는 주요 IoT 보안위협에 대하여 분석하고, IoT를 위한 네트워크 표준 확립에 고려할 사항을 제시하였다. 또한 IoT 환경에서 안전성이 확보되

Table 1. Comparison of protocols

	[10]	[11]	[12]	The Proposed
Compatibility with IETF	○	○	○	○
Interoperability with IoT	×	×	×	○
Reducing overhead of network	×	△	△	○
Key Recovery Agreement of Communicating Entities	×	○	△	○

(O: high, △: low, X: not support)

는 키분배 및 키복구 메커니즘을 제안하였다. 제안하는 메커니즘은, IoT 환경에서 이러한 휴대의 불편함이 없으면서 기존의 키 위탁방법으로 발생할 수 있는 여러 가지 위협으로부터 보호하고, 사용자 양쪽의 동의 없이는 키 복구가 불가능한, 안전하고 신뢰성 있는 키분배 및 키복구 모듈을 제공한다.

향후에는 제시한 고려사항을 토대로 본 논문에서 제안하는 메커니즘에 대한 구현을 진행할 예정이다.

REFERENCE

[1] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 (2012), http://www.gartner.com/newsroom/id/2636073. (accessed Mar., 2, 2016)

[2] VPN Haus, *The Internet of Vulnerable Things: Why Remote Access Security is Critical*, 2014.

[3] Y. Park and Y. Lee, "A Study on Countermeasure for Privacy in Mobile Office," *Journal of Korea Multimedia Society*, Vol. 18, No. 2, pp. 178-188, 2015.

[4] Ministry of Sciencem, *Information Security Load-Map for IoT*, 2014.

[5] Blackhat, https://www.blackhat.com/us-14/. (accessed Mar., 2, 2016)

[6] Y. Park and Y. Lee, "A Study on Security Threats and Countermeasures for Internet of Things," *Proceedings of the Summer KICS Conference*, pp. 41-42, 2015.

[7] 6LoWPAN, http://www.ietf.org/wg/concluded/6lowpan.html/. (accessed Mar., 2, 2016)

[8] K. Hartke, *Observing Resources in CoAP*, IETF Internet Draft, 2014.

[9] Y. Lee and D. Kim, "Threats Analysis, Requirements and Considerations for Secure Internet of Things," *International Journal of Smart Home*, Vol. 9, No. 12, pp. 191-198, 2015.

[10] Y. Rhee, "Key Recovery for IETF Internet Protocol Based on TTP," *The Journal of the Korea Contents Association,* Vol. 6, No. 6, pp. 56-63, 2006.

[11] Y. Rhee and T.Y. Kim, "Practical Solutions to Key Recovery Based on PKI in IP Security," *Lecture Notes in Computer Science,* Vol. 2434, pp. 44-52, 2002.

[12] Y. Rhee, C.S. Kim, and B. Lee, "IPSec Key Recovery for IKEv2," *Journal of the Korea Academia-Industrial Cooperation Society,* Vol. 11, No. 4, pp. 1260-1265, 2010.

[13] N. Moon, S. Yong, J. Oh, and T. Cho, "A Study on Privacy for the Services in Digital Convergence," *Journal of Korea Multimedia Society,* Vol. 10, No. 4, pp. 24-32, 2006.

이 윤 정

2002년 고려대학교 컴퓨터학과 이학박사
2004년 9월~현재 제주대학교 전산통계학과 교수
관심분야 : 정보보안, 네트워크 보안, 유무선통신 보안, IoT 보안

박 용 준

2006년 전남대학교 컴퓨터정보학부 이학사
2010년 전남대학교 정보보호협동과정 이학석사
2014년~현재 제주대학교 전산통계학과 박사과정
관심분야 : 개인정보보호, 정보보호관리체계, 디지털 포렌식

김 철 수

1988년 연세대학교 수학과 이학박사
1989년~현재 제주대학교 전산통계학과 교수
관심분야 : 데이터마이닝, 통계응용

이 봉 규

1995년 서울대학교 컴퓨터공학과 공학박사
1996년~현재 제주대학교 전산통계학과 교수
관심분야 : 영상처리 SoC 설계, 패턴인식