The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 3, pp.13-19, Jun. 30, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.3.13
JIIBC 2016-3-3

NFC를 OOB 채널로 활용한 사물인터넷 보안 설정 기술

Secure Configuration Scheme for Internet of Things using NFC as OOB Channel

김정인*, 강남희**

Jeongin Kim*, Namhi Kang**

요 약 PSK(Pre-shared Secret Key) 기반 방식은 공개키 기반 알고리즘을 사용하여 세션키를 설정하는 방식보다 적은 계산 시간과 에너지를 사용하므로 경량화 장치로 구성되는 IoT 환경에 적절하다. PSK 기반 방식의 주요한 전제는 사전에 통신 주체 간에 PSK가 안전하게 설정되어야 한다는 것이다. 그러나 IoT 환경의 작은 센서나 액추에이터의 경우 설정을 위해 필요한 키보드, 모니터 같은 입출력장치가 부재하므로 기존 인터넷 장치들보다 PSK를 안전하게 설정하기가 어렵다. 특히 일반 사용자의 경우 보안전문지식이 부족하기 때문에 설정에 어려움이 있다. 따라서 공장에서 제조 시 설정되는 기본 값을 사용하거나 장치의 설치자가 설정하는 경우가 일반적이다. 이 경우 모든 설치자들과 제조사들을 신뢰할 수 있는지는 생각해 볼 문제이다. 이를 해결하기 위해 본 논문에서는 자원이 제한적인 소형 장치들을 대상으로, NFC(Near Field Communication)를 OOB(Out-Of-Band) 채널로 활용한 안전한 초기 설정 (secure bootstrapping) 기술을 제안한다.

Abstract The PSK (Pre-shared Secret Key) based method is appropriate for the IoT environment consisting of lightweight devices since this method requires less computing time and energy than the method to configure the session key based on the public key algorithm. A fundamental prerequisite for the PSK based method is that PSK should have been configured between the communication entities safely in advance. However, in case of a small sensor or actuator, no input and output interface such as keyboard and monitor required for configuration exists, so it is more difficult to configure PSK for such lightweight devices safely in the IoT environment than the previous Internet devices. Especially, normal users lack expertise in security so they face difficulty in configuration. Therefore, the default value configured at the time of manufacturing at factories is used or the device installer configures PSK in most cases. In such case, it is a matter for consideration whether all installers and manufacturers can be trusted or not. In order to solve such problem, this paper proposes a secure bootstrapping scheme, which utilizes the NFC (Near Field Communication) as an OOB (Out-Of-Band) channel, for lightweight devices with limited resources.

Key Words : Secure bootstrapping, Internet of Things, Resource-constrained devices, NFC, OOB

*준회원, 덕성여자대학교 디지털미디어학과
**정회원, 덕성여자대학교 디지털미디어학과(교신저자)
접수일자 : 2016년 5월 14일, 수정완료 : 2016년 6월 8일
게재확정일자 : 2016년 6월 10일

Received: 14 May, 2016 / Revised: 8 June, 2016 /
Accepted: 10 June, 2016
**Corresponding Author: kang@duksung.ac.kr
Dept. of Digital Media, Duksung Women's University, Korea

Ⅰ. 서 론

최근 사물인터넷(IoT: Internet of Things) 기술을 적용한 다양한 장치들과 응용 서비스들이 개발되고 있다. IoT 기반 응용들은 기존의 컴퓨터 통신 시스템은 물론 인터넷과의 연결을 고려하지 않았던 주변의 사물들까지 연결하여 상호 정보를 주고받는다[1, 11]. 향 후 수년 이내에 수백억 개의 장치들이 연결될 것으로 예측되고 있고, 많은 산업체들은 IoT 기술 기반 서비스가 수십 조 달러 이상의 경제적 가치를 창출할 것으로 기대하고 있다[1].

IoT 기술이 적용되는 응용 도메인이 증가하고 신규 서비스가 활성화되기 위해 정보 보호와 보안 기술은 반드시 제공되어야 한다[2, 3, 12]. 인터넷과 연결되는 장치 수의 증가는 다양한 정보가 노출될 수 있는 공격 대상의 확장을 의미한다. 그러나 다양한 IoT 장치들을 위한 보안 기술의 개발은 쉽지 않다. IoT 환경은 이종의 장치들과 이종의 네트워크 기술이 혼재되어 있고, 센서와 같은 소형 경량 장치는 보안 기술을 탑재하기에 자원이 제한적이기 때문이다[2]. IoT 장치를 설계할 때 제조 단가를 고려하여 최소의 CPU와 메모리를 탑재할 것이고 많은 경량 장치는 배터리 전원에 의존한다. 또한 인터넷에 연결되는 접속 구간에서 에너지 사용의 효율을 위해 저전력 네트워크의 기술을 사용하기 때문에 데이터 전송량이 작고, 무선 통신의 특성으로 인한 손실과 지연이 발생할 수 있기 때문에 보안기술의 경량화가 필요하다[2].

정보의 기밀성과 무결성을 제공하고, 사용자를 식별하고 인증하는 보안 서비스에서 가장 선행되어야 하는 기능은 안전하게 키를 분배하고 관리하는 설정 기능이다. 계산 시간과 에너지 사용의 장점으로 인해 다양한 보안 시스템에 적용되고 있는 PSK(Pre-shared Secret Key) 기반 방식은 공개키 알고리즘을 기반으로 세션키를 설정하는 방식보다 적은 비용으로 보안 기술을 구축할 수 있으므로 경량화 장치로 구성되는 IoT 환경에 적절하다[3, 4].

PSK 기반 보안 시스템에서 중요한 전제는 보안 서비스게 제공되기 전에 두 통신 주체 사이에는 PSK가 안전하게 설정되어 있어야 한다는 것이다. 그러나 대부분의 기존 연구들은 IoT 장치를 위한 PSK는 안전하게 설정되어 있다고 가정하고 시스템을 설계하고 있다[5]. 그러나 경량 장치들로 구성되는 IoT 환경에서는 사전에 PSK를 안전하게 설정하기 어렵다[3].

IoT 경량 장치들은 설정을 위해 필요한 입출력 장치(예, 키보드와 모니터)가 없거나 제한된 방식(예, 설정 버튼과 LED 표시등)을 채택한다. 따라서 기존에 사용되었던 매뉴얼에 의존하는 수동 설정 방식을 직접 적용하기에는 제한이 따른다. 또한 다양한 장치들로 구성된 IoT 환경에 적용되는 보안 기술을 전문지식이 부족한 일반 사용자가 안전하게 설정하기는 무리다.

IoT 장치의 설정을 해결하기 위한 가장 직관적인 방식은 장치의 제조 시점에 기본값을 할당하는 것이다. 또는 IoT 장치를 서비스 도메인에 설치하는 설치자나 시스템 관리자가 설정하는 방식을 사용할 수 있다. 그러나 이 방식들은 설치자들과 제조사들을 신뢰할 수 있어야 가능하다[3].

이를 해결하기 위해 본 논문에서는 자원이 제한적인 소형 장치들을 위해 'NFC(Near Field Communication)를 활용한 안전한 초기 설정 (secure bootstrapping) 기술'을 제안한다. NFC는 RFID의 개념을 확장시킨 저 비용의 근거리 무선통신 기술로 대부분의 스마트폰에 적용되고 있고 최근 전자 결제 등 많은 응용에서 활용되고 있다[6, 7]. NFC 기술은 근거리 통신 기술로 많이 사용되는 블루투스나 WiFi 기술보다 전송속도가 느린 단점이 있다. 그러나 본 논문에서 제안하는 기술은 NFC를 이용하여 많은 정보를 주고받는 것보다 초기 설정시 안전한 데이터 전송을 주목적으로 하기 때문에 전송 속도는 크게 고려대상이 되지 않는다.

제안 기술은 NFC의 다양한 장점을 활용한다. NFC는 통신반경이 작아서 안전한 데이터 전송에 상대적으로 적합하다. 일반적인 표준문서에서 NFC의 통신반경은 약 10cm지만 실제 구현 환경에서의 반경은 1~2cm정도로 더 근접하므로 초기 설정을 진행하는 사용자는 초기 설정 과정에서 공격자의 여부를 눈으로 확인 할 수 있다. 짧은 통신 반경에서도 NFC의 데이터를 도청할 수 있다[8]. 그러나 특별한 장치가 있어야만 공격이 가능하기 때문에 IoT 초기 설정 과정에서의 공격 가능성은 저하된다. 다른 장점으로 NFC는 P2P(Peer to Peer) 모드를 제공하는데, 이를 통해 두 통신 주체는 상호 정보를 읽고 쓸 수 있는 양방향 통신이 가능하다. NFC는 다른 근거리 통신 기술 대비 두 주체 사이의 통신 설정이 0.1초 이내로 매우 짧은 장점도 있다[6].

기존 연구들이 PSK가 안전하게 설정되어 있다고 가정했다면, 본 논문에서는 NFC를 활용하여 PSK를 안전하게 설정하고 재설정 할 수 있는 방법론을 제시한다. 특

히, 제안 기술은 사용자의 관여를 최소화하면서 안전하게 설정 할 수 있도록 설계하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해서 기술한다. 이어서 3장에서는 제안 시스템을, 4장에서는 제안시스템의 동작시험 및 보안 분석을 기술한다. 끝으로 5장에서 본 논문의 결론을 맺는다.

II. 관련연구

IoT환경에서 사용되는 소형 장치들은 자원이 제한적이고 입출력 장치가 부재하기 때문에 사용자가 장치의 초기설정을 하는데 어려움이 있다[3]. 이를 해결하기 위한 방법으로 QR코드, 빛, 소리를 이용하는 기술들이 제안되고 있다. 그림1은 QR코드를 이용하여 신규장치를 컨트롤러에 등록하는 시스템의 동작과정을 나타낸다[9].

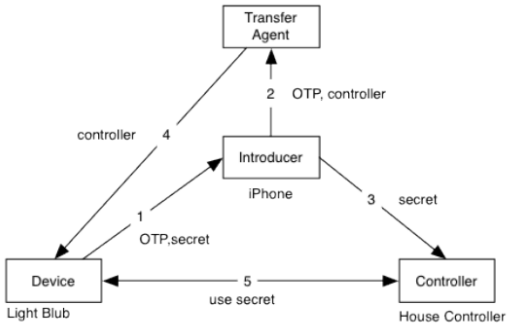


그림 1. 간단한 정보 흐름
Fig. 1. Simplified high-level information flow

중재자(그림 1의 Introducer)는 스마트폰처럼 QR코드를 읽을 수 있는 장치이다. 장치가 설치되면 중재자는 장치에서 QR코드를 스캔 하여 장치가 가지고 있는 OTP와 secret을 가져온다(메세지1). OTP는 장치등록을 위해 제조자가 생성한 One Time Password이고 secret은 장치와 컨트롤러가 통신을 할 수 있도록 제조사가 생성한 비밀 값이다. 이후 중재자는 전송 에이전트(Transfer Agent)에게 장치가 사용 할 컨트롤러의 네트워크 정보와 OTP를 전달하고(메세지2), 컨트롤러에게 secret을 전송한다. 장치가 처음으로 부팅되고 네트워크연결을 하면 전송 에이전트와 연결을 한다. 전송 에이전트는 장치에게 컨트롤러의 네트워크 정보를 전송한다(메시지4). 장치는 컨트롤러의 네트워크 정보를 알기 때문에 이후 장치의 작동 시 컨트롤러와 직접 통신을 할 수 있다(메시지5).

이 시스템은 제한된 메모리와 처리능력을 가지는 장치에 사용 할 수 있다. 장치를 설치할 때 네트워크나 전원을 필요로 하지 않으며 인증에 사용되는 OTP가 이미 사용된 경우에는 설치자가 감지 할 수 있다. 사용자가 QR코드를 스캔함으로써 장치 등록을 할 수 있도록 사용자의 관여를 최소화 하였지만 QR코드가 가지는 인증정보를 암호화하지 않고 그대로 제공하기 때문에 보안에 취약할 수 있으며 적용할 수 있는 환경이 제한적이다.

미국 카네기 멜론 대학은 자동차와 스마트폰 사이의 불루투스 통신을 안전하게 사용하기 위해 빛과 소리를 OOB(out-of-band) 채널로 사용하여 보안키를 초기 설정해주는 MVSec 기술을 제안하였다[10]. 제안 기술의 주요 목표는 공격자의 중간자 공격(Man In The Middle Attack)에 대응하는 것이다. OOB 채널은 WI-Fi나 블루투스에서 사용하는 기본 채널과 다른 빛, 소리, 진동 등 별도의 통신 매체를 의미한다.

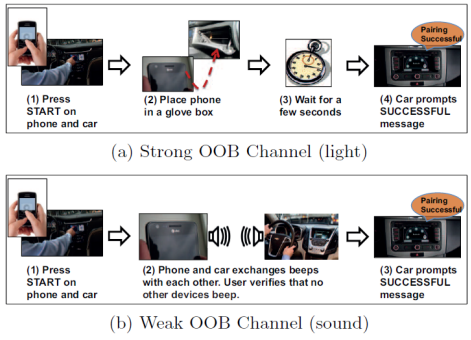


그림 2. OOB채널로 빛과 소리를 사용하는 MVSec
Fig. 2. MVSec using light and sound as OOB channels

그림 2에 나타낸 것처럼, 빛을 OOB 채널로 사용하는 경우 차량 내부 글로브 박스에 스마트폰을 넣고 빛의 깜빡거림을 통해 신호를 전송하여 차량과 페어링을 수행하게 된다. 이 경우 중간자 공격이 불가능하므로 강한 OOB로 생각할 수 있다 (그림 2의 (a)). 이와 달리 소리를 OOB 채널로 사용하는 경우 차량과 스마트폰의 경고음을 교환하여 페어링을 수행한다. 강한 OOB와 달리 소리는 공격자가 도청할 수 있으므로 약한 OOB로 정의될 수 있고, 스마트 폰과 차량은 데이터 무결성과 기밀성을 검증할 수 있도록 초기 설정 프로토콜을 설계해야한다.

Ⅲ. 제안 시스템

본 장에서는 NFC를 이용한 자원이 제한된 장치들의 안전한 PSK설정 기술을 제안한다. 신규장치가 설치된 후, 사용자는 제어장치를 이용하여 장치의 등록/인증/키 설정을 개시한다. 다음 표1은 본 논문의 제안 시스템에서 사용하는 파라미터들이다.

표 1. 시스템 파라미터
Table 1. System Parameter

Parameter	Context
ID_i	장치 i의 식별값 (32bit identifier)
RN_i, RN_{AS}	장치(i)와 인증서버(AS)가 생성한 랜덤숫자 (128bit)
TS_0, TS_1	타임스탬프
TID	트랜잭션 식별값
IK_i	신규장치를 위한 사전 설정키 (128bit 대칭키)
SK_{cs}	제어장치와 인증 서버를 위한 128bit 세션키
PSK	장치와 인증 서버의 128bit Pre-Shared key
$Sock_i$	장치의 IP, PORT 정보
$Sock_{GW}$	네트워크의 기본 게이트웨이 정보
VT_i	PSK의 유효기간(Valid Time)

그림 3은 제안하는 기술이 동작되는 시스템 구성의 예를 나타낸다. 제안하는 초기 설정 기술은 두 종류의 채널(즉, two-channel)을 사용하는데, 신규장치와 제어장치 간 통신은 NFC를 사용하고 제어장치와 인증서버, 신규장치와 인증서버 간 통신은 WiFi 나 Zigbee 등 인터넷 통신을 적용한다.

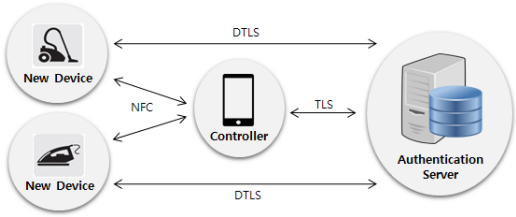


그림 3. 시스템 구성도
Fig. 3. System Configuration

동작과정은 다음과 같다 (그림 4. 참조).

1) 새로운 장치가 네트워크에 설치된 후 제어장치는 NFC를 이용하여 신규 장치의 ID_i, RN_i, IK_i 값을 받아온다. 제어장치로는 스마트폰이나 스마트 패드와 같이 이동이 용이한 장치가 사용될 수 있다.

2) 제어장치는 장치로부터 받은 ID_i, IK_i, RN_i 값과 $Sock_i$, TID, TS_0 정보를 SK_{cs}로 암호화 하여 보안 관리 서버(인증 서버)에 전송한다. 그림 4에 표시된 AE()함수는 인증과 암호를 동시에 제공되는 authenticated encryption 함수로 ISO/IEC 19772:2009에 표준화된 암호 모드나 SSL/TLS, SSH에 적용된 방식을 사용할 수 있다. 인증서버는 SK_{cs}를 이용하여 복호화한 뒤 ID_i를 가등록하고 RN_{AS}를 생성한다. 이후, RN_{AS}와 수식 (1)을 이용하여 PSK를 생성한다.

$$PSK_i = E_{IK_i}(RN_I \oplus RN_{AS}) \quad (1)$$

3) 인증 서버는 PSK와 RN_{AS}를 IK_i로 암호화하고 현재의 트랜잭션을 구분할 수 있는 TID, TS_1와 함께 SK_{cs}로 암호화하여 제어장치에 전송한다.

4) 제어장치는 전송받은 값을 SK_{cs}를 이용하여 복호화한다. TID, TS_1로 트랜잭션이 위장되지 않았음을 확인하고 3)과정에서 암호화한 $AE_{IK}(PSK, RN_{AS})$ 값과 네트워크 설정 정보인 $Sock_i$, $Sock_{GW}$를 NFC 채널을 이용하여 신규장치에 전송한다. 신규장치는 IK_i로 복호화하여 PSK와 RN_{AS}값을 확인하고, 제어장치가 설정 값으로 전달해준 IP 주소와 PORT 번호로 통신 소켓을 개설한 후, 보안 관리 서버로부터 전송될 데이터의 수신을 대기한다.

5) 인증 서버는 제어장치로부터 받은 $Sock_i$정보를 이용해 신규 장치에 소켓 개설을 요청한다. 신규 장치와 서버 사이에 인터넷 통신 소켓이 개설되면 인증서버는 ID_i, RN_i, VT_i를 PSK로 암호화하여 신규 장치에 전송한다. ID_i와 RN_i는 신규장치가 자

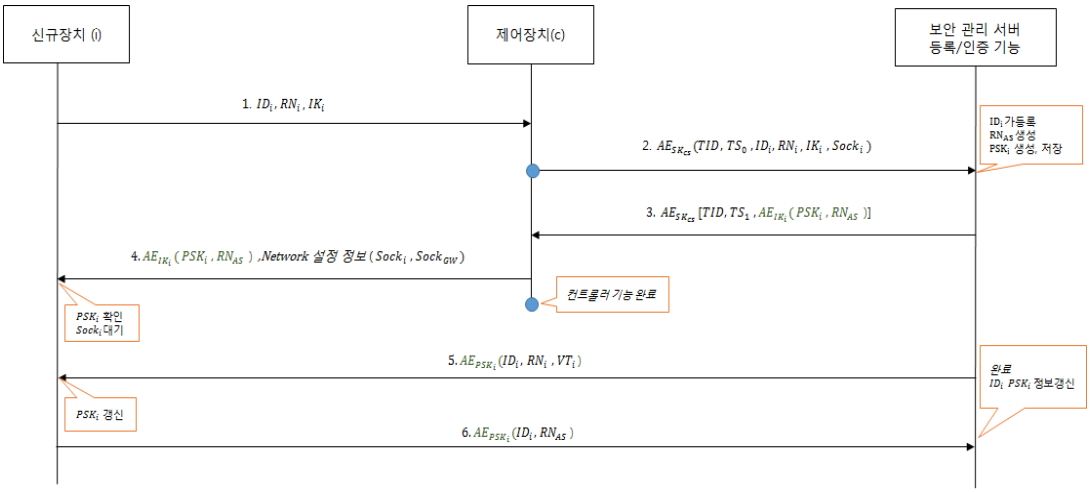


그림 4. PSK 설정을 위한 동작 과정
Fig. 4. Proposed system flow about PSK configuration

신이 보낸 값과 일치하는지 확인하여 인증 서버를 검증한다.

6) 신규 장치는 도착한 메시지를 PSK로 복호화하여 자신이 최초에 보낸 ID_i와 RN_i가 동일 한지 확인하여 인증 서버를 인증한다. 이후, 신규장치는 PSK로 ID_i와 RN_{AS}를 암호화하여 인증서버에 전송한다. 이를 수신한 인증서버는 자신이 생성한 RN_{AS}가 맞는지 확인하고 2)과정에서 가등록한 값을 확정한다.

Ⅳ. 동작 시험 및 보안 분석

1. 동작 시험

본 절에서는 제안한 시스템을 구현하여 시험 한 결과를 기술한다. NFC를 통한 OOB 채널의 양방향 통신을 제공하기 위해 안드로이드 장치를 사용하였다. PSK 설정을 위환 동작시험은 그림 5와 같다.

초기설정이 수행될 때 신규장치는 그림5-1의 1번 값을 NFC를 이용하여 제어장치에게 전송한다. 제어장치는 신규장치로부터 전송받은 값과 초기설정에 필요한 값을 나타내는 그림 5-2의 1번 값을 암호화하여 인증서버로 전송한다.

인증서버는 전송받은 값을 복호화하여 PSK를 생성한다(그림5-3 1번). 신규장치에게 전달 할 PSK, RN_{AS}를 IK_i로 암호화하고 TID와 TS_1으로 한 번 더 암호화하여 컨트롤러에게 전달한다(그림 5-2의 2번). 제어장치는 전송받은 값을 복호화하여 IK_i로 암호화한 값만 신규장치에 전송한다(그림5-2의 3번).

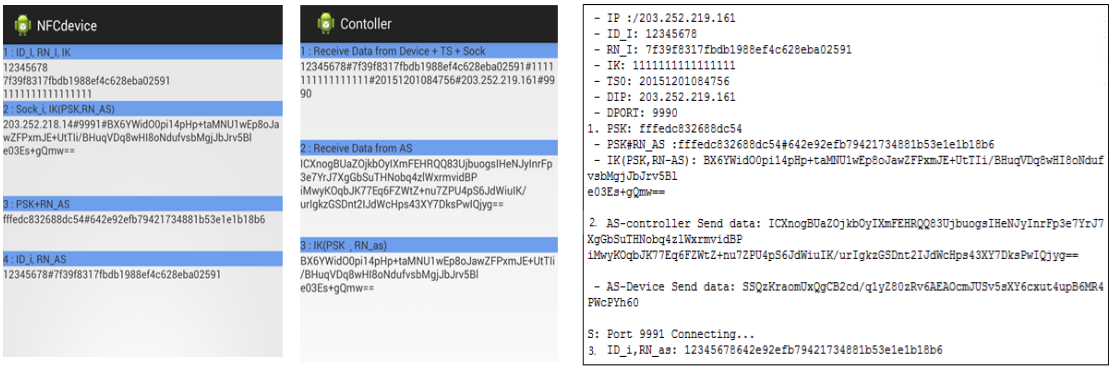
신규장치는 복호화하여 PSK를 확인 할 수 있다(그림 5-1의 3번). 이후 신규장치의 소켓이 개설되면 인증서버는 신규장치에게 인증을 위한 값을 전송하여 신규장치가 인증 서버를 검증할 수 있도록 한다(5-1의 4번). 신규장치도 인증을 위한 값을 인증서버에 암호화하여 전송하여 신규장치를 검증할 수 있도록 한다(그림5-3의 2번).

2. 보안 분석

본 논문에서 제안하는 시스템의 안전성을 분석하기 위해 신규장치의 초기 설정 시 발생할 수 있는 대표적인 공격인 재전송 공격, 위장 공격, 중간자 공격에 대해 보안 분석을 하였다.

- **재전송 공격**

신규 장치와 제어 장치 사이는 NFC 채널을 사용하고, 사용자가 주변의 공격자를 확인 한 후 메시지 전송을 시작하므로 메시지 가로채기가 어렵다. 따라서 재전송 공격이 가능한 구간은 제어 장치와 인증 서버 사이이다. 공



5-1 신규장치　　5-2 제어장치　　5-3 인증서버

그림 5. 제안 시스템 동작 시험
Fig. 5. system operational test

격자가 2)와 3)과정에서 전송되는 정보를 가지고 있다가 일정시간 이후 재전송 공격을 시도하더라도, 매 세션마다 생성하는 랜덤 숫자 RN_i와 시간정보인 TS_0와 TS_1를 사용하기 때문에 재전송 공격에 대응 할 수 있다.

• 위장 공격

본 제안 시스템의 구성 요소는 신규 장치, 제어 장치, 그리고 인증 서버로 구성되므로 각 장치로 위장하는 공격을 분석한다.

(1) 신규장치로 위장: 서론에서 기술했듯이 NFC는 특별한 장비 없이는 공격이 어렵고 10cm 내외의 짧은 통신반경을 가진다. 두 기기는 물리적으로 가까운 곳에 위치하여 공격자의 접근을 확인할 수 있으므로 공격자가 신규장치로 위장하는 것에 대응할 수 있다.

(2) 제어장치로 위장: 공격자가 제어장치로 위장하여도 제어장치와 인증 서버가 사전에 공유한 대칭키 SK_{cs}를 알 수 없기 때문에 2)과정에서 올바른 암호화 값을 인증서버에 전송할 수 없다. 또한 TID와 TS_0, TS_1로 트랜잭션이 위장되지 않았음을 확인 할 수 있다.

(3) 인증서버로 위장: 공격자가 인증서버로 위장하여도 제어장치와 인증서버가 사전에 공유한 대칭키 SK_{cs} 알 수 없기 때문에 전송받은 값을 복호화 할 수 없고, 컨트롤러에게 전송하기위한 3)값을 생성할 수 없다.

• 상호인증

신규장치는 5)에서 받은 값을 복호화하여 1)에서 자신이 전송했던 ID_i, RN_i 값과 같은지 확인하고, 값이 같다면 인증 서버를 인증 할 수 있다. 인증서버는 6)에서 수신한 값을 복호화하여 3), 4)에서 암호화하여 전송한 RN_{AS}와 같은 값이면 사용자를 인증할 수 있다.

• 중간자 공격

제어장치와 인증서버 사이에 공격자가 존재할 수 있다. 하지만 2), 3)과정 모두 제어장치와 인증 서버가 사전에 공유한 대칭키를 이용하여 암복호화하기 때문에 중간자공격에 대응할 수 있다.

V. 결 론

본 논문에서는 보안 서비스(기밀성, 무결성, 가용성 등)를 안전하게 제공하기 위해 반드시 선행되어야 하는 보안 설정 기술을 살펴보았다. 특히, 자원이 제한적인 사물인터넷 경량 기기에 많이 적용될 것으로 예상되는 PSK의 안전한 설정/재설정 방안을 제안했다. 제안하는 기술은 NFC를 OOB 채널로 활용하여 자원이 제한적인 소형 장치들이 제조나 설치 시 설정된 초기 비밀키 값을 안전하게 재설정할 수 있는 방안이다. 제안 기술은 재전송 공격, 위장 공격, 중간자 공격에 대응할 수 있고, Two-Channel 기술을 활용하여 상호인증을 제공한다.

References

[1] Gartner, http://www.gartner.com/newsroom/id/2905717, Nov. 2014.
[2] Namhi Kang, "Survey on standard technologies for Internet of Things security," Information and Communications Magazine, Vol.31, No.9, pp. 40-45, 2014.
[3] Jeongin Kim, Namhi Kang, "Secure Configuration Scheme of Pre-shared Key for Lightweight Devices in Internet of Things," The Journal of the Institute of Internet, Broadcasting and Communication, Vol.15, No.3, pp.1-6, 2015.
[4] Jiye Park, Saemi Shin, Namhi Kang, "Mutual Authentication and Key Agreement Scheme between Lightweight Devices in Internet of Things,"The journal of KOREAN Institute of Communication and Information Science," Vol. 38, No. 9, pp. 707-714, 2013
[5] P. Eronen, H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", IETF Standard, RFC 4279, 2005.
[6] Myny, Kris, et al. "Flexible thin-film NFC tags," IEEE Communications Magazine, Vol.53, No.10, pp.182-189, 2015.
[7] Atzori, Luigi, Antonio Iera, Giacomo Morabito, "The internet of things: A survey," Computer networks, Vol.54, No.15, pp. 2787-2805, 2010.
[8] Kortvedt, Henning, and S. Mjolsnes. "Eavesdropping near field communication." The Norwegian Information Security Conference (NISK). Vol. 27. 2009.
[9] C. Jennings, "Transitive Trust Enrollment for Constrained Devices," IETF Internet Draft, draft-jennings-core-transitive - trust -enrollment-01, 2012.
[10] Han, J., Lin, Y. H., Perrig, A., & Bai, F, "MVSec: Secure and Easy-to-Use Pairing of Mobile Devices with Vehicles," CMU White Paper, CMU-CyLab-14-006, 2014.
[11] Jiye Park, Namhi Kang, "Design of Smart Service based on Reverse-proxy for the Internet of Things," The Journal of the Institute of Internet, Broadcasting and Communication, Vol.14, No.06, pp.1-6, 2014.
[12] Yong-Soon Im, Eun-Young Kang, Jae-Pyo Park, "Security of Image Information using Steganography and QR Code in IoT," The Journal of the Institute of Internet, Broadcasting and Communication, Vol.15, No.02, pp.31-37, 2015.

저자 소개

김 정 인(준회원)

- 2015년 2월 : 덕성여자대학교 디지털미디어학과 졸업
- 2015년~현재 : 덕성여자대학교 디지털미디어학과 석사과정

<주관심분야 : 네트워크 보안, 사물인터넷 보안>

강 남 희(정회원)

- 1999년 2월 : 숭실대학교 공학사
- 2001년 2월 : 숭실대학교 공학석사
- 2004년 12월 : University of Siegen, 공학박사
- 2009년 3월~현재 : 덕성여자대학교 디지털미디어학과 부교수

<주관심분야 : 유무선 인터넷통신, 네트워크 보안, 사물인터넷보안>

※ 본 연구는 덕성여자대학교 2015년도 교내연구비 지원에 의해 수행되었음