디지털산업정보학회 논문지 제13권 제1호-2017년 3월
http://dx.doi.org/10.17662/ksdim.2017.13.1.069

스마트폰 기반에서 안전한 디바이스 모니터링을 위한 디바이스 식별 및 통신 기법 설계

진 병 욱* · 안 희 학** · 전 문 석***

A Design of Device Identification and Communication Method for Secure Device Monitoring based Smart Phone

Jin Byungwook · Ahn Heuihak · Jun Moonseog

〈Abstract〉

As the smartphone-based devices are diffused and developed rapidly, they provide the convenience to the users. The abovementioned sentence technologies are being used not only in the existing sensor and wireless network technology but also in the application services of the diverse fields application services such as smart appliance, smart car, smart health care, etc. and the new fusion paradigm from the industry is presented by undertaking the researches in diverse area by the enterprises and research institutions. However, the smart environment exposes its weaknesses in the mobile terminal area, existing wireless network and IT security area. In addition, due to new and variant ways of attack, not only the critical information are disclosed However also the financial damages occur. This paper proposed the protocol to perform the smartphone-based safe device monitoring and safe communication. The proposed protocol designed the management procedure of registration, identification, communication protocol and device update management protocol and the safety against the attack techniques such as the an-in-the-middle-attack, impersonation attack, credential threat, information leaks and privacy invasion was analyzed. It was observed that the proposed protocol showed the performance improved by approximately 52% in the communication process than the existing system.

Key Words : Authentication, Communication Method, Smart Device, Management Protocol.

Ⅰ. 서론

스마트 디바이스 및 센서를 활용한 기술은 생활환경에 밀접한 부분에 장착되어 사용자에게 편의성을 제공하고 있으며 지속적으로 성장할 것으로 전망되고 있다. 현재 스마트 카 , 스마트 홈, 스마트 시티, 스마트 헬스케어와 같은 다양한 서비스 산업이 발전

* 숭실대학교 컴퓨터학과 박사수료
** 가톨릭관동대학교 컴퓨터공학과 교수(교신저자)
*** 숭실대학교 컴퓨터학부 교수

하고 있으며 국내외 대기업, 공공기관 뿐만 아니라 국가적인 차원에서도 전폭적으로 지원하고 있다[1,2].

스마트 환경의 융합기술은 이러한 편의성 및 생활환경에서 효율성을 제공하고 있지만, 보안 영역에서 취약점이 노출되고 있으며 크게는 금적전인 피해가 발생하고 있다. 기업 내부를 침투한 디바이스에 대한 공격기법이 증가하고 있으며, 정보유출에 대한 피해가 막심해져서 이에 대한 대응체계가 요구되고 있다[3].

본 논문에서는 스마트기반의 디바이스 관리와 안전한 통신을 수행하기 위해서 식별 및 통신 프로토콜을 설계하였다.

본 논문은 5장으로 구성되어 있다. 2장에서는 스마트 디바이스와 ICT 융합기술의 활용사례와 스마트폰 기반의 보안위협 및 보안요구사항에 대해서 관련연구를 작성하였다. 3장은 제안부로 시스템의 구성도, 디바이스 식별 및 등록절차, 통신 프로토콜, 갱신된 디바이스 관리 프로토콜을 설계하였다. 4장은 안전성 분석, 보안성 및 효율성에 대해서 성능 평가를 평가하였다. 5장에서는 향후 연구 방향 및 논문의 결론은 맺는다.

Ⅱ. 관련연구

2.1 스마트 디바이스 기반의 ICT 융합기술의 활용사례

스마트폰 기반의 디바이스와 융합된 서비스가 활발히 진행되고 있으며, 건설, 공공복지 및 건설 분야, 자동차, 헬스케어 등과 융합하여 부가적인 가치를 창출하고 있다[1,4].

스마트폰의 기반의 사물인터넷은 저 전력, 다양한 센서를 활용하여 확장된 환경에서 데이터를 수집하고 손쉽게 관리 할 수 있는 환경을 제공하는 특징이 있다[3,5].

대표적인 예로 스마트폰 기반의 헬스케어를 활용한 서비스 분야에서는 국내의 S사의 원격에 대한 서비스를 제공하고 있다. 사용자들은 스마트 폰 기반의 디바이스를 활용하여 데이터를 전송 및 검진을 하여 편의성을 제공받고 있다. 또한 국외의 미국의 S사는 스마트 디바이스와 센서 네트워크를 활용하여 지능형 주차제공을 제공하고 있으며 미국의 V사는 빌딩용 센서와 스마트 폰을 결합하여 건물의 생활환경을 분석하여 에너지 관리에 대한 응용 시스템을 선보이고 있다[2,5,6].

스마트 디바이스를 활용한 서비스는 사용자들로부터 다양한 연구 및 개발이 이루어질 것을 예측하고 있으며 기존의 기반 기술이 아닌 새로운 융합 산업을 창출할 것으로 기대하고 있다[4,7].

하지만 스마트 폰은 개방적인 네트워크와 오픈 플랫폼을 적용하여 다양한 보안위협들이 발생하고 있다. 무선 네트워크 기반의 공격, 바이러스, 웜등과 같은 공격이 발생하고 있으며, 디바이스와의 융합으로 인하여 신규 공격기법들이 발생하고 있다[6,8].

2.2 스마트폰 기반의 보안위협 및 보안요구사항

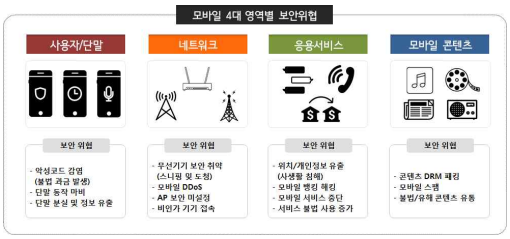
스마트폰의 확산에 따라서 사용자들로부터 시간과 장소에 구애 받지 않고 다양한 서비스를 제공할 수 있다는 장점이 있으나, 기존의 PC에서 발생하는 보안위협을 포함할 수 있다. 또한 신종 공격에 대한 새로운 공격기법이 발생한다.

스마트폰 기반에서 발생하는 대표적인 보안 위협은 개인정보 침해, 도청, 피싱 및 파밍, 서비스 거부, 권한 탈취, 악성코드·해킹, 정보 유출 등이 있다.

그림 1 과 같은 보안위협에 대한 피해를 감소하기

위해서 다각면의 보안정책이 요구되어지고 있으며, 대응기술에 대한 연구가 필요하다[4].

우선 단말기 영역에서는 데이터의 암호화, 디바이스에 대한 분실 및 도난 방지 솔루션이 요구되며, 네트워크에서는 연동된 디바이스 인증, 데이터의 암·복호화 기술이 요구된다[9]. 마지막으로 서비스 영역에서는 사용자 개인정보에 대한 보호, 스토리지에 대한 접근제어, 인가되지 않는 사용자에 대한 접근 기술이 요구되고 있다[6,8].

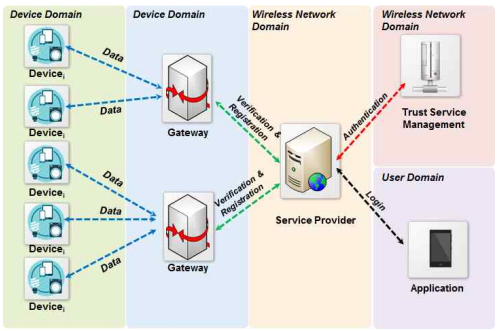


<그림 1> 스마트 기반의 환경에서 영역별 보안위협

Ⅲ. 스마트폰 기반에서 디바이스 모니터링 및 안전한 통신을 위한 프로토콜 설계

3.1 제안된 시스템 구성도

본 논문에서 제안하는 시스템 구성도는 디바이스, 게이트웨이, Service Provider, Trust Service Management로 구성되어 있으며 디바이스 도메인, 무선 네트워크, 사용자 도메인으로 나누어져 있다.



<그림 2> 제안된 시스템 구성도

제안된 시스템은 사용자가 Device를 설치 후 식별 및 등록 단계를 수행한다. 이후 식별 및 등록단계에서 생성된 값을 기반으로 인증을 완료 후 통신을 수행하는 절차이다. 디바이스 및 통신 과정에서 메시지의 무결성을 보완하기 위해 디바이스 관리하는 갱신 프로토콜을 설계한다. 제안된 시스템 구성도는 그림 2와 같다.

3.2 디바이스 식별 및 등록 절차

사용자는 Device를 활용하여 Service Provider에 등록하는 과정이다. 사용자의 스마트 폰의 Application에서 등록 완료 메시지를 수신 후 사용자의 정보 및 암호(Password)를 입력 후 Device를 식별하고 등록한다. 제안된 과정은 <그림 3> 과 같다.

1. Device는 Gateway로 등록 요청 메시지를 전송한다. 이후 Gateway에서는 Service Provider로 등록 요청 메시지를 전송한다.

$$E_k(Deivce_{SN})$$

$$E_k(Deivce_{SN}), E_k(Gateway_{SN})$$

2. Service Provider에서는 $Device_{SN}, Gateway_{SN}$을 확

인 후 식별 값을 Gateway를 통해 Device로 요청한다.

3. 사용자는 디바이스에서 $Code_{Value}$를 입력 후 이를 기반으로 $Device_{IV}$를 생성한다. 이후 $TimeStamp$를 연접 후 Gateway로 전송한다.

$E_k(Device \| Time\ stamp)$

4. Gateway에서는 $Cert_{value}$를 첨부 후 Service Provider로 전송한다.

$E_k(Device \| Time\ stamp), E_k(Cert_{value})$

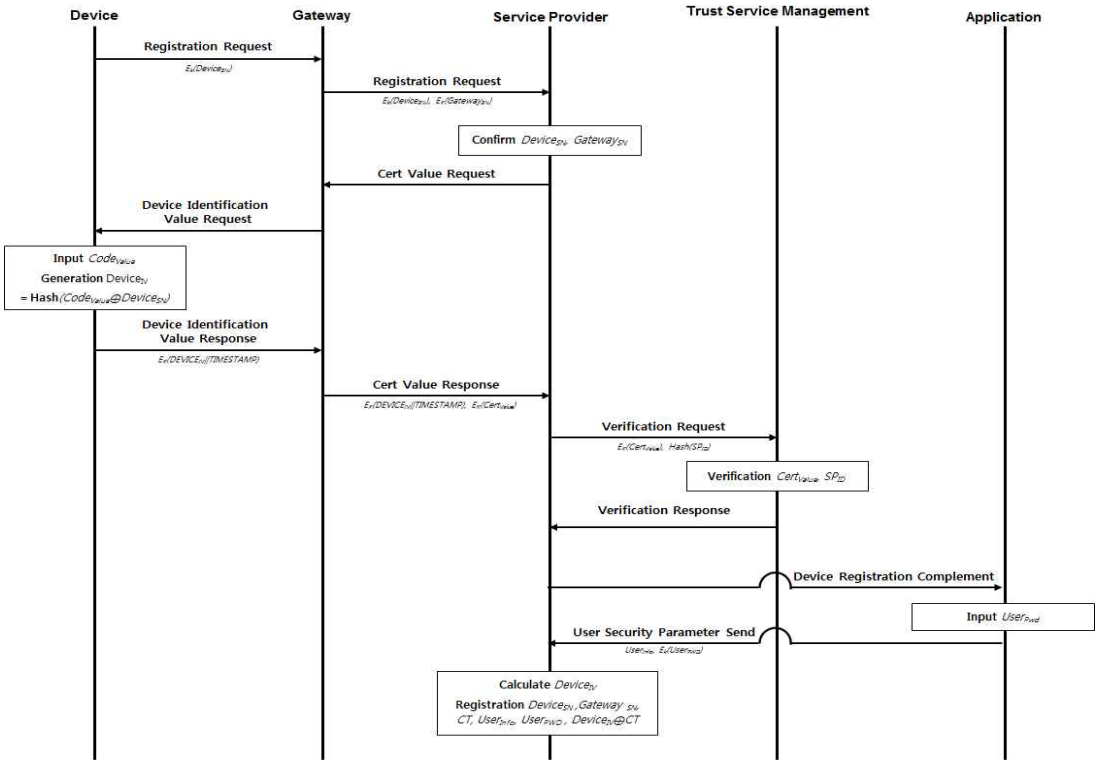
5. Service Provider에서는 자신의 식별 값을 해쉬함수를 통하여 해쉬값을 생성한 다음 Trust Service Management로 검증 요청 메시지를 전송한다.

$E_k(Cert_{Value}), Hash(SP_{ID})$

6. Trust Service Management에서는 $Cert_{Value}$, SP_{ID}를 검증 후 검증완료 메시지를 Service Provider로 전송한다.

7. Service Provider에서는 Application으로 등록완료 메시지를 전송한다. Application에서는 사용자의 $User_{Pwd}$를 입력 후 $User_{Info}$, $E_k(User_{Pwd})$를 Service Provider로 전송한다. 이후 $Deice_{IV}$를 계산 후 검증한 다음 Device와 사용자의 정보를 저장한다.

$Device_{SN}, Gateway_{SN}, CT, User_{info}, User_{PWD}, Device \oplus CT$



<그림 3> 디바이스 식별 및 등록 단계

3.3 메시지 인증 및 통신 프로토콜

본 절은 메시지 인증 및 통신 프로토콜 절차로 사용자의 정보 및 암호를 Trust Service Management에 인증 후 안전하게 메시지를 전송하는 프로토콜을 제안한다. 제안된 프로토콜은 그림 4와 같다.

1. 사용자는 Application으로 $User_{Info}$, $User_{Pwd}$를 입력 후 Servier Provider로 로그인 메시지를 전송한다.

$User_{info}, E_k(User_{Pwd}), E_k(User_{Cert})$

2. 사용자의 메시지를 Trust Management Server로 인증 요청 메시지를 전송한다.

$User_{info}, E_k(User_{Cert})$

3. Trust Management Service에서 사용자의 $User_{info}$, $User_{Cert}$를 검증 후 Service Provider로 인증 완료 메시지를 전송한다. 이후 Service Provider에서는 $User_{\infty_i}, User_{Pwd}$를 확인한다.

4. 이 후 Service Provider에서는 Gateway로부터 디바이스로부터 추출된 데이터를 요청한다. Gateway에서는 연동된 Device로부터 데이터를 요청한다.

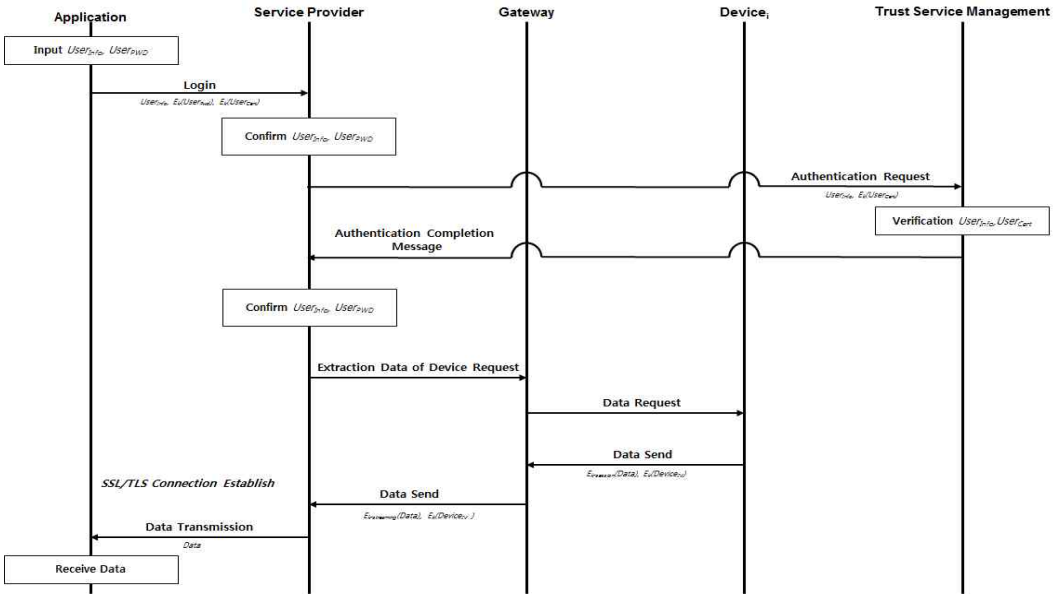
5. $Device_i$에서는 Gateway로 추출된 데이터를 전송한다.

$E_{k-session}(Data), E_k(Device_{IV})$

6. Gateway에서 Service Provider로 Data를 스트리밍방식의 암호화를 사용하여 Service Provider로 발송한다.

$E_{k-Streaming}(Data), E_k(Device_{IV})$

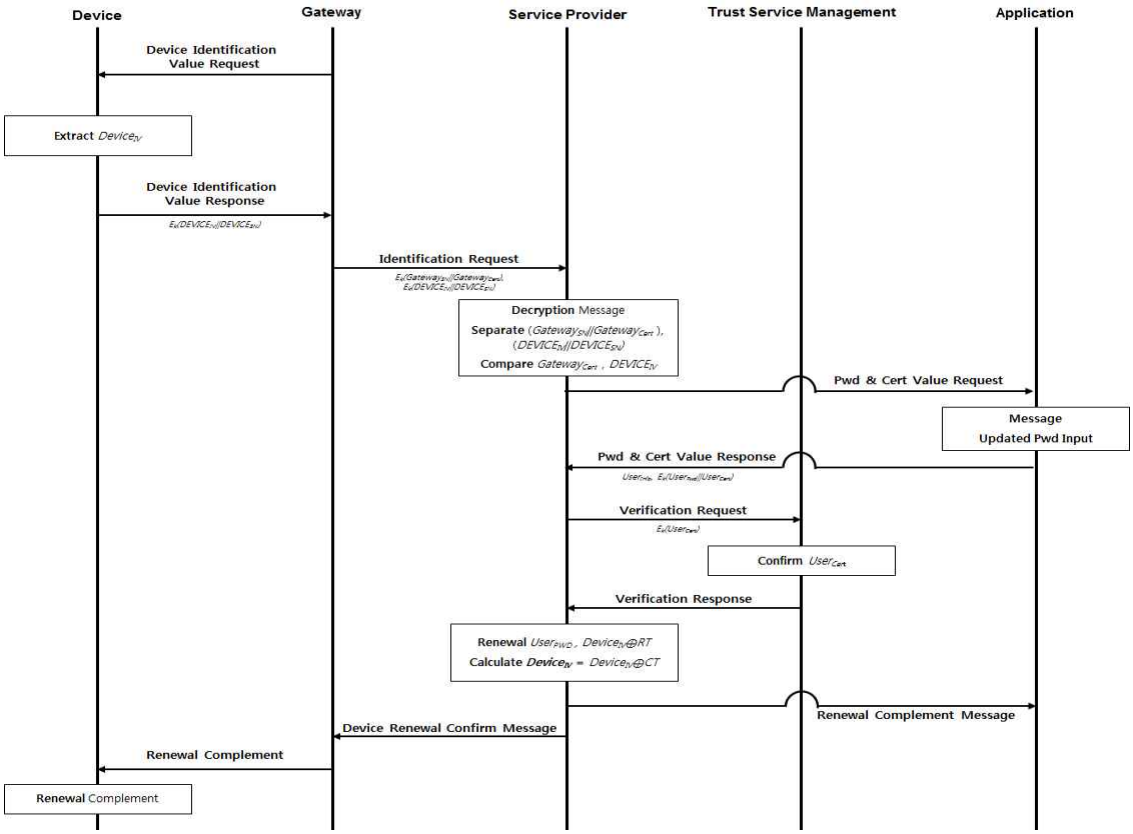
7. Service Provider와 Application에서는 SSl/TLS Connection을 설정 후 데이터를 Secure Channel로 발송한다.



<그림 4> 메시지 인증 및 통신 프로토콜 절차

3.4 갱신된 디바이스 관리 프로토콜

본 절에서는 디바이스 관리 프로토콜을 설계한다. 갱신된 값을 확인 후 Service Provider에서는 Trust Service Management 에서는 검증 후 응답메시지를 확인한다. 이후 Service Provider에서는 값을 재등록 후 제안된 프로토콜을 마친다. 제안된 프로토콜은 그림 5와 같다.



<그림 5> 디바이스 식별값 갱신 관리 절차

1. Gateway에서는 Device로부터 식별 값을 요청한다. Device에서는 식별 값을 추출 후 Gateway로 발송한다.

$E_k(Device_{IV}||Device_{SN})$

2. Gateway에서는 Service Provider로 식별 요청 메시지를 전송한다.

$E_k(Gateway_{SN}||Gateway_{Cert}), E_k(Device_{IV}||Device_{SN})$

3. Service Provider에서는 메시지를 복호화 후 연접된 값을 분리 후 $Gateway_{Cert}$와 $Device_{IV}$를 비교한다.

4. 비교 후 값이 일치하면 Application으로 암호와 인증 값을 요청한다. 사용자는 메시지를 확인 후 인증 갱신된 인증 값을 입력 후 Service Provider로 발송한다.

$User_{info}, E_k(User_{pwd} || User_{Crt})$

5. Service Provider에서는 Trust Service Management로 인증 값을 포함한 검증 요청 메시지를 전송한다.

6. Trust Service Management에서는 $User_{Crt}$를 확인 후 검증 응답 메시지를 전송한다.

7. Service Provider에서는 갱신된 $User_{PWD}$, $Device_{IV}$를 확인 후 $Device_{IV}$를 갱신한다.

8. Application과 Gateway로 Device 갱신 완료 메시지를 전송한다. 이후 Gateway에서는 Device로부터 갱신 완료를 전송한다.

Ⅳ. 성능평가

4.1 보안성 평가 및 효율성 분석

본 절에서는 제안된 프로토콜의 보안성 및 효율성을 분석하였다. 기존의 시스템에서는 무선 통신 채널 WPA2를 활용하여 송수신자로부터 데이터를 전송한다. 제안된 프로토콜에서는 디바이스와 게이트웨이의 식별 값의 노출을 방지하기 위해서 $Device_{IV}$를 생성하여 이를 기반으로 안전한 통신을 수행하도록 하였다. 그리고 식별값 갱신을 수행하기 위해서 식별값 갱신 프로토콜을 설계하여 주기적으로 변경하도록 하였다. 보안 요구사항을 기반으로 네트워크기반에서 디바이스 인증, 접근제어에 대한 시스템을 설계하였다. 제안된 프로토콜과 기존 시스템을 비교한 결과는 표 1과 같다.

다음은 기존의 시스템에서 사용하던 알고리즘과 제안된 시스템의 성능 평가를 나타낸다.

- 성능분석 환경 : Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz 3.40GHz, RAM 8.00GB, OS :Windows7 Enterprise K 64bit, Software : Eclipse JCA(Java EE Connector Architecture)
- 알고리즘 비교대상 : Public Key Cryptography (RSA2048, ECC), Hash Function(MD5, Sha256, 512), Symmetric-key Cryptography(DES, SEED, AES)

<표 1> 기존시스템과의 보안성 비교분석

	기존 시스템	제안된 프로토콜
사용자 권한에 따른 보안정책	지원안함	지원
갱신방법	지원안함	지원 ($Device_{IV}$를 식별함으로서 주기적으로 인증 및 식별값 갱신)
인증경로	유/무선	무선
통신채널	WPA2	WPA2 & EAP-TLS

기존의 시스템의 암호화 환경은 [ZigBee기반]공개키(RSA2048), 대칭키(AES-CBC or SEED)를 활용한다. 제안된 프로토콜에서는 공개키 (ECC), 대칭키 (AES-CCMP)를 사용하여 통신 프로토콜을 설계하였다.

제안된 프로토콜에서는 저 전력 및 경량 암호 시스템을 적용하기 위해서 ECC기반의 암호화기법(WPA2 & EAP-TLS)을 사용하여 사용자 인증에 대한 성능을 기존의 시스템(WPA2) 대비 대략 38%감소하였다.

또한 기존의 시스템 대비 통신 절차(Public Key :

RSA, Symmetric Key : DES or SEED, Hash Algorithm : SHA-512)에서 제안된 프로토콜(Public Key : ECC, Symmetric Key : AES, Hash Algorithm : SHA-256)은 대략 52%를 향상된 결과가 나타났으며, 해당된 수치는 표 2와 같다.

<표 2> 암호화 성능 분석

	Publick Key		Symmetric Key			Hash Algorithm		
	RSA	ECC	DES	SEED	AES	MD5	HA-256	HA-512
ncryption	1907062	1592951	23032535	4159842	4937512	36110668	15111667	5424059
ecryption	3996590	2575745	7677191	132040	137045	-	-	-
Key eneration	770333840	50663832	4594477	3287262	6313444	-	-	-
otal Time	776237492	54837028	45304203	0620608	21388001	36110668	15111667	5424059

4.2 안전성 분석

중간자 공격(Man In The Middle Attack) : 스마트폰기반의 무선 네트워크 환경에서 통신 내용을 조작하는 중간자 공격이 발생하고 있다. 본 논문에서는 디바이스의 식별 및 등록을 수행하며, $Device_{IV}$, $Cert_{value}$를 Trust Service Management에서 검증한다. 그리고 사용자의 스마트폰의 $User_{pwd}$, $User_{Cert}$를 확인함으로서 중간자 공격은 실패로 끝난다.

가장 공격 : 가장공격은 공격자가 사용자의 정보를 이용하여 사용자로 위장하는 공격기법이다. 제안된 프로토콜에서는 Trust Service Management에서는 사용자의 $User_{Cert}$를 검증하여 판별할 수 있으며, 디바이스 갱신 관리 프로토콜을 설계하여 디바이스에 대한 $Device_{IV}$를 Service Provider에서도 주기적으로 갱신함으로써 사용자를 위장할 수 없다.

자격증명의 위협: Smart기반의 환경에서는 식별 모듈에 인증토큰에 대한 디바이스 복제 및 훼손에 대한 위협이 노출된다. 이러한 경우를 보안하귀 위해서 Service Provider에서는 Gateway을 경유하여 Device에 대한 식별값을 확인하고 있으며, 또한 $Gateway_{SN}$, SP_{ID}를 검증함으로써 자격증명에 대한 위협에서 벗어날 수 있다.

정보유출 및 프라이버스에 대한 침해 : 스마트폰 기반의 Device가 연동된 환경에서는 정보유출 및 프라이버시 피해 사례가 발생하고 있으며, 중요이슈로 떠오르고 있다. 이를 해결하기 위해서 디바이스 및 게이트웨이뿐만 아니라 Service Provider에서도 Trust Service Management에서 식별값, 인증값, 해쉬값 등을 검증하도록 설계하였다. 그리고 갱신을 주기적으로 수행함으로써 디바이스와 사용자의 정보를 보완하도록 강화하였다.

Ⅴ. 결론

본 논문은 스마트폰 기반에서 디바이스 모니터링 및 안전한 통신을 위한 프로토콜을 제안하였다. 디바이스를 식별 및 등록 단계를 거쳐서 생성된 식별값 인증값을 기반으로 안전한 통신 프로토콜을 설계하였다. 그리고 디바이스 관리와 사용자 정보를 보호하기 위해서 갱신 관리 프로토콜을 추가하여 통신을 수행할 때 메시지에 대한 보완성을 높였다.

성능분석에서는 기존의 시스템과 제안된 프로토콜에서 기존의 통신수행 대비 대략 52%의 향상된 결과를 확인하였다. 또한 기존의 스마트 기반의 디바이스와 연동 환경에서 발생하는 보안위협에서 중간자 공격, 가장공격, 자격증명에 대한 위협, 정보유출에 대한 프라이버시에 대한 부분에서 안전성을 분석하였다.

스마트폰 기반의 디바이스가 활용된 환경의 취약성은 디바이스를 가장하여 정보를 탈취, 데이터의 무결성을 위협하는 것이다. 본 논문에서는 디바이스 등록 및 갱신 프로토콜을 설계하여 식별값을 강화하였으며, 통신 프로토콜에서 상호인증을 수행하여 보안성을 강화하였다. 향후 신규 및 변종 공격에 따른 보안기법에 관한 연구가 필요하며, 사용자로부터 안전하게 활용할 수 있는 보안 정책 수립이 요구된다.

참고문헌

[1] TTA, “Functional Requirements for Wireless Device Identification in WLAN,” 2013. 12.

[2] 서승현, 전길수, “스마트폰 보안 위협 및 대응전략,” TTA 저널, 통권 제132호, 2010, pp. 44-48.

[3] 고정길, 홍상기, 이병복, 김내수, “스마트 디바이스와 사물인터넷 (IoT)융합 기술 동향,” ETRI, 2013.

[4] Young-Do Joo, “Analysis on Security Vulnerabilities of a Biometric-based User Authentication Scheme for Wireless Sensor Networks,” The Journal of The Institute of Webcasting, Internet Television and Telecommunication, Vol. 14, No. 1, 2014, pp. 147-153.

[5] Kwansik Yoon, “A Mechanism for Controlling Accesses Dynamically in Smartwork Environment,” Vol. 19, No. 2, 2012. 11, pp. 877-880.

[6] 진병욱, 정동욱, 차시호, 전문석, “Design and Estimation of a Session Key based Access Control Scheme for Secure Communications in IoT Environments,” 디지털산업정보학회 논문지, Vol. 12, No. 1, 2016, pp. 35-41.

[7] 진병욱, 김종화, 차시호, 전문석, “Design and Evaluation of Secure Framework for User Management in Personal Cloud Environments,” 디지털산업정보학회 논문지, Vol. 12, No. 1, 2016, pp. 81-87.

[8] 최도현, 박중오, “M2M 환경의 디바이스 키 보호를 위한 암호 알고리즘 응용 기법,” Vol. 13, No. 10, 2015, pp. 343-351.

[9] 강동호 외 6명, “스마트폰 보안 위협 및 대응 기술,” ETRI, Vol. 25, No. 3, 2010. 6.

■ 저자소개 ■

진 병 욱
(Jin Byungwook)

2013년 3월~현재
숭실대학교 컴퓨터학과 박사수료
2011년 2월 숭실대학교 컴퓨터학과
(공학석사)
2010년 2월 청운대학교 멀티미디어학과
(문학사)

관심분야 : IoT, 인증 시스템, 접근제어
E-mail : quddnr4511@naver.com

안 희 학
(Ahn Heuihak)

1984년 4월~현재
가톨릭관동대학교 컴퓨터공학과 교수
1981년 2월 숭실대학교 전자계산학과(공학사)
1983년 2월 숭실대학교 전자계산학과(공학석사)
1994년 8월 숭실대학교 전자계산학과(공학박사)

관심분야 : 정보보안, 컴퓨터통신,
시스템소프트웨어,
E-mail : hhahn@cku.ac.kr

전 문 석
(Jun Moonseog)

1991년 3월~현재
숭실대학교 컴퓨터학과 정교수
1991년 2월 New Mexico State University
Physical Science Lab. 책임연구원
1989년 2월 University of Maryland
Computer Science 박사
관심분야 : 정보보호, 암호학, 네트워크 보안
E-mail : mjun@ssu.ac.kr

논문접수일 : 2017년 01월 19일
수 정 일 : 2017년 02월 16일(1차), 02월 27일(2차)
게재확정일 : 2017년 03월 06일