웨어러블 디바이스 데이터 보안을 위한 안전한 세션 키 수립 및 데이터 암호 키 사용

Secure Session Key Establishment and Data Encryption Key Use for Data Protection of a Wearable Device

저자 (Authors)
문지연, 이부형, 이종혁
Ji-Yeon Moon, Boo-Hyung Lee, Jong-Hyouk Lee

출처 (Source)
한국정보과학회 학술발표논문집 , 2015.12, 1479-1481(3 pages)

발행처 (Publisher)
한국정보과학회
The Korean Institute of Information Scientists and Engineers

URL
http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE06602770

APA Style
문지연, 이부형, 이종혁 (2015). 웨어러블 디바이스 데이터 보안을 위한 안전한 세션 키 수립 및 데이터 암호 키 사용. 한국정보과학회 학술발표논문집, 1479-1481

웨어러블 디바이스 데이터 보안을 위한 안전한 세션 키 수립 및 데이터 암호 키 사용*

문지연 ○ 이부형 이종혁
상명대학교 컴퓨터소프트웨어공학과
jiyeon@pel.smuc.ac.kr, boohyung@pel.smuc.ac.kr, jonghyouk@pel.smuc.ac.kr

Secure Session Key Establishment and Data Encryption Key Use for Data Protection of a Wearable Device

Ji-Yeon Moon○ Boo-Hyung Lee Jong-Hyouk Lee
Dept. of Computer Software Engineering, Sangmyung University

요 약

최근 스마트 워치와 같은 웨어러블 디바이스의 폭발적인 사용 증가로 인해 웨어러블 디바이스로부터 수집되는 데이터에 대한 보안이 중요한 과제로 떠오르고 있다. 본 논문에서는 스마트 워치로부터 스마트 폰으로 전송되는 생체정보를 포함한 데이터가 안전하게 전송되고 이용될 수 있도록 하는 새로운 기법을 제안한다. 제안된 기법은 스마트 워치와 스마트 폰 간의 안전한 인증을 통한 세션 키 수립과 데이터 암호 키를 이용해 데이터에 대한 추가적인 보안성을 제공한다.

1. 서 론

신체에 장착하는 컴퓨팅 기기라는 의미의 웨어러블 디바이스는 이전부터 많은 연구와 실험적인 제품이 있었지만, 최근 들어 피트니스를 위한 밴드형 디바이스, 손목에 차는 스마트 워치, 안경형태의 구글 글라스 등의 사용 제품의 출시로 인해 그 사용이 폭발적으로 증가하고 있다[1].

웨어러블 디바이스는 사용자의 생체정보를 포함한 민감한 개인정보를 수집하고 외부기기(예를 들어 스마트 폰)에 전송하기에 이러한 데이터를 안전하게 전송할 수 있는 보안 기법이 요구 된다. 또한, 한 어플리케이션이 다른 어플리케이션의 데이터에 접근하는 것을 차단하는 샌드박스 환경을 우회하는 스마트 폰 앱 교차 공격(XARA: Cross-App Across Attack)의 존재가 발표 되었다[2]. 이는 스마트 워치와 같은 웨어러블 디바이스에서 스마트 폰과 같은 외부기기로의 안전한 데이터 전송 만이 요구되는 것이 아니라 스마트 폰 내부에서도 접근이 가능한 어플리케이션만이 데이터에 대해서 접근이 가능하게 하는 추가적인 데이터 보안이 요구 된다는 것을 의미한다.

본 논문에서는 웨어러블 디바이스의 데이터 보안을 위한 안전한 세션 키 수립과 데이터 암호 키 사용을 제안한다. 제안된 기법은 스마트 워치와 같은 웨어러블 디바이스가 스마트 폰과 안전한 인증을 수립하게 하고 그 결과로 세션 키를 수립할 수 있게 한다. 또한, 데이터 암호 키을 사용하여 데이터에 대한 추가적인 보안성을 제공한다.

본 논문의 2 장에서는 관련 연구로 블루투스 페어링과 웨어러블 디바이스로부터 수집될 수 있는 생체정보를 살펴 본다. 제 3 장에서 제안하는 기법을 소개하고 제 4 장에서 본 논문의 결론을 맺는다.

2. 관련 연구

2.1 블루투스 페어링

블루투스는 노트북, 휴대폰, PDA 등 무선 주파수를 사용하는 휴대기기를 위한 저전력의 근거리 무선 통신 기술이다. 일대일 또는 일대다 연결 형태를 지원하는 블루투스는 하나의 마스터 장치에 최대 7 개의 슬레이브 장치가 연결 된다[3].

마스터 장치와 슬레이브 장치는 블루투스의 인증 및 암호화 과정에 필요한 링크 키를 생성하기 위해 PIN code 를 공유한다[4]. 본 논문에서는 스마트 폰과 웨어러블 디바이스는 블루투스를 통해 연결되며, 연결(페어링) 과정에서 생성된 링크 키를 이용해 블루투스 통신을 암호화 한다.

2.2 웨어러블 디바이스를 통해 수집되는 데이터

[표 1]은 웨어러블 디바이스에 의해 수집 되는 데이터 종류를 나타낸다[5]. 본 논문에서는 웨어러블 디바이스로 스마트 워치로 가정하고 [표 1]과 같은 데이터가 스마트 워치에서 스마트 폰으로 전송한다고 가정한다.

표 1. 웨어러블 디바이스를 통해 수집되는 데이터 종류

데이터 종류	설명
심박수	단위시간당 심장박동수의 수로 일반적으로 분당 멱의 수로 표현되는 숫자
혈압	혈관을 따라 흐르는 혈액이 혈관의 벽에 주는 압력

* 본 연구는 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2014R1A1A1006770).

혈당	혈액 속에 함유되어 있는 포도당의 농도
호흡량	사람이 호흡하고 있을 때 출입하는 공기양

3. 제안하는 기법

3.1 시나리오

스마트 워치(즉, 웨어러블 디바이스)와 스마트 폰은 블루투스를 이용해 서로를 인증한다. 스마트 폰의 운영체제 위에는 스마트 워치와 통신하여 얻은 데이터와 키를 관리하는 매니저 응용 프로그램이 존재한다. 지금부터 매니저 응용 프로그램은 '매니저'로 줄여서 표기한다. 여기서 매니저와 스마트 워치는 서로를 인증하며 이 과정에서 세션 키가 수립된다.

매니저와 스마트 워치의 인증 과정이 끝나면, 스마트 워치는 매니저에게 데이터 암호 키로 암호화된 데이터를 전송한다. 이후에 매니저가 관리하는 어플리케이션이 매니저에게 필요한 데이터의 타입을 요청하면, 매니저는 스마트 워치와 인증과정에서 생성된 세션 키로 이를 암호화하여 워치에게 전송하고, 스마트 워치는 매니저에게 암호화된 데이터의 식별자를 얻어 이를 복호화한 뒤, 이와 매치되는 키를 세션 키로 암호화하여 매니저에게 전송한다. 매니저는 암호화된 키를 얻어 이를 복호화한 뒤, 데이터를 요청한 어플리케이션에게 데이터를 전송한다.

3.2 동작과정

제안하는 기법의 전반적인 동작 과정을 설명하기 앞서 제안하는 기법의 전제 조건과 주요 표기법을 설명한다. 그 후 스마트 워치와 스마트 폰 매니저 간의 인증 과정을 설명한 후, 스마트 폰 어플리케이션이 암호화된 데이터에 대한 접근을 요청하는 과정을 설명한다.

제안 기법의 전제 조건은 다음과 같다.

- 스마트 폰과 스마트 워치는 블루투스를 이용하여 각 장치를 인증한다.
- 스마트 폰의 운영체제 위에는 스마트 워치와 통신하여 얻은 데이터와 키를 관리하는 매니저 응용 프로그램이 존재한다.
- 스마트 워치는 데이터의 종류에 따라 식별자를 두어 키를 분류하여 보관하고, 매니저는 데이터의 종류에 따라 식별자를 두어 데이터와 키를 분류하여 보관한다.
- 매니저 위에 존재하는 스마트 워치의 데이터를 필요로 하는 어플리케이션과 통신한다.

제안하는 기법에서 사용되는 주요 표기는 [표 2]와 같다.

표 2. 제안하는 기법에서 사용하는 용어 정의

용어	정의
ID_p	스마트 폰 p의 아이디
ID_w	스마트 워치 w의 아이디
K_l	블루투스 설정 과정에서 생성된 링크 키
$a \parallel b$	a와 b를 연결
$h(x)$	입력값 x에 대해 일방향 해시함수를 수행
K_a	매니저와 스마트 워치 사이의 비밀 키
r_i	i번째 생성한 난수
g^x	디피-헬만 알고리즘을 사용하기 위해 사전에 공유된 정수 g와 임의의 정수 x
$E_k(x)$	대칭 키 k를 이용하여 입력 값 x에 대해 대칭 키 기반 암호화를 수행
K_s	매니저와 스마트 워치 사이의 인증 과정에서 생성되는 세션 키
t_i	매니저와 스마트 워치가 생성한 i번째 타임스탬프
Δt	메시지 최대 전송지연 허용 시간
K_{c_i}	데이터 타입 c의 i번째 데이터 암호 키
D_{c_i}	데이터 타입 c의 i번째 식별자
ID_m	매니저 응용 프로그램의 아이디
ID_{a_i}	매니저가 관리하는 i번째 어플리케이션 아이디

[그림 1]은 스마트 워치와 스마트 폰의 매니저 간의 인증 과정을 나타낸다.

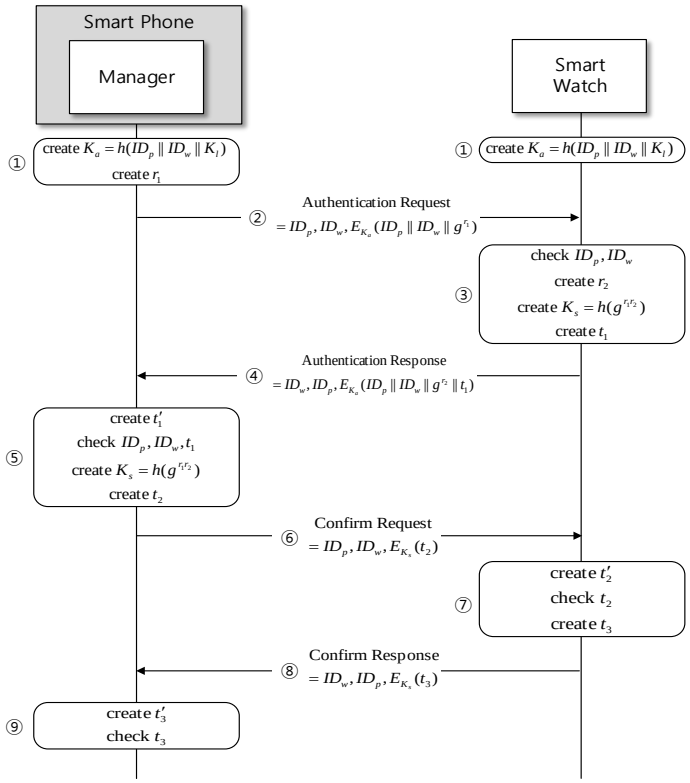

그림 1. 스마트 워치와 스마트 폰의 매니저 간의 인증 과정

① 먼저 매니저는 스마트 폰의 아이디 ID_p와 스마트 워치의 아이디 ID_w 그리고 링크 키 K_l을 이어 붙인 값을 해시화하여 비밀 키 K_a를 만들고 난수 r_1을 생성한다. 이때, 스마트 워치도 같은 방법으로 비밀 키 K_a를 생성한다.

② 매니저는 스마트 워치에게 비밀 키 K_a로 암호화된 스마트 폰의 아이디 ID_p와 스마트 워치의 아이디 ID_w 그리고 디피-헬만 알고리즘 난수 g^{r_1}를 송신한다.

③ 매니저가 비밀 키 K_a로 암호화된 스마트 폰의 아이디

ID_p와 스마트 워치의 아이디 ID_w 그리고 난수 g^{r_1}를 수신하면, 이를 복호화한다. 송수신 기기의 아이디 값을 확인한 후, 난수 r_2를 만들어 세션 키 $K_s = h(g^{r_1 r_2})$와 타임스탬프 t_1을 생성한다.

④ 스마트 워치는 매니저에게 비밀 키 K_a로 암호화된 스마트 폰의 아이디 ID_p와 스마트 워치의 아이디 ID_w와 디피-헬만 알고리즘을 사용한 난수 g^{r_2} 그리고 타임스탬프 t_1을 송신한다.

⑤ 매니저가 비밀 키 K_a로 암호화된 스마트 폰의 아이디 ID_p와 스마트 워치의 아이디 ID_w와 난수 g^{r_2} 그리고 타임스탬프 t_1을 수신하면 이를 복호화한다. 현재 시간 기준으로 타임스탬프 t_1'을 만들어 $|t_1' - t_1| \leq \Delta t$를 검사하고 송수신 기기의 아이디 값을 확인한 후, 세션 키 $K_s = h(g^{r_1 r_2})$와 타임스탬프 t_2를 생성한다.

⑥ 매니저는 스마트 워치에게 타임스탬프 t_2를 세션 키 K_s로 암호화하여 송신한다.

⑦ 매니저가 세션 키 K_s로 암호화된 타임스탬프 t_2를 수신하면, 이를 복호화한다. 현재 시간 기준으로 타임스탬프 t_2'를 만들어 $|t_2' - t_2| \leq \Delta t$를 검사하고 송수신 기기의 아이디 값을 확인 후, 타임스탬프 t_3를 생성한다.

⑧ 스마트 워치는 매니저에게 세션 키 K_s로 암호화 된 타임스탬프 t_3을 송신한다.

⑨ 마지막으로 세션 키 K_s로 암호화 된 스마트 워치에게 타임스탬프 t_3를 수신하면 이를 복호화한다. 현재 시간 기준으로 타임스탬프 t_3'를 만들어 $|t_3' - t_3| \leq \Delta t$를 검사하고 송수신 기기의 아이디 값을 확인한 후, 인증 과정을 마친다.

스마트 폰의 매니저와 스마트 워치 간의 인증 과정이 끝나면, 각 장치는 세션 키 K_s를 공유한다. 그 후, 스마트 워치는 스마트 폰에게 암호화된 여러 타입의 데이터를 전송하기 위해서 타입별로 데이터 암호 키를 생성한다. 이렇게 생성된 데이터 암호 키를 이용하여 데이터를 암호화하여 스마트 폰에게 데이터를 전송한다.

[그림 2]는 스마트 워치와 스마트 폰의 매니저가 관리하는 어플리케이션 간의 데이터 통신 과정을 나타낸다.

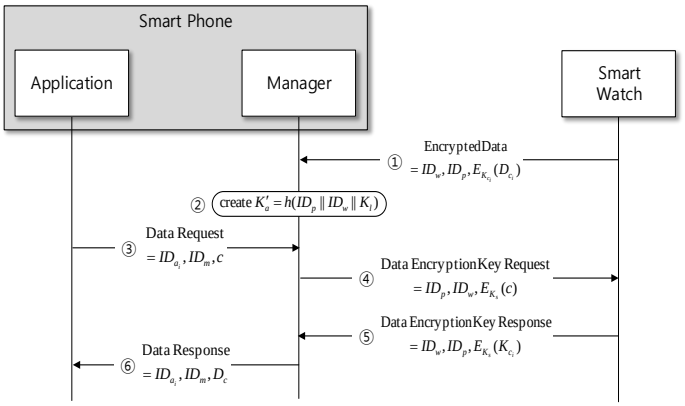

그림 2. 스마트 워치와 스마트 폰의 매니저가 관리하는 어플리케이션 간의 데이터 통신 과정

① 스마트 폰의 매니저와 스마트 워치 간의 인증이 완료되면, 먼저 스마트 워치는 매니저에게 데이터 암호 키 K_{c_i}로 암호화된 데이터 D_{c_i}를 송신한다.

② 매니저가 스마트 워치에게 데이터 암호 키 K_{c_i}로 암호화된 데이터 D_{c_i}를 수신하면, 송수신 기기의 아이디와 링크 키 K_l을 이어 붙인 값을 해시화하여 K_a'을 만들어 비밀 키 K_a와 비교하여 송수신 기기의 아이디 값을 확인한다.

③ 매니저가 관리하는 어플리케이션 i가 데이터 타입 c가 필요하다면, 매니저에게 데이터 타입 c를 송신한다.

④ 매니저는 스마트 워치에게 데이터 타입 c를 세션 키 K_s로 암호화하여 송신한다.

⑤ 스마트 워치가 세션 키 K_s로 암호화된 데이터 타입 c를 송신하면, 이를 세션 키 K_s로 복호화한다. 만약 데이터 타입 c가 존재한다면, 매니저는 바로 어플리케이션 i에게 데이터 암호 키 K_{c_i}로 암호화된 데이터 D_{c_i}를 데이터 암호 키 K_{c_i}로 복호화하여 송신한다. 데이터 타입 c가 존재하지 않는다면, 스마트 워치는 매니저에게 데이터 타입 c에 맞는 데이터 암호 키 K_{c_i}를 세션 키 K_s로 암호화하여 송신한다.

⑥ 매니저가 세션 키 K_s로 암호화된 데이터 암호 키 K_{c_i}를 수신하면 이를 세션 키 K_s로 복호화한다. 그 후, 매니저는 어플리케이션 i에게 데이터 암호 키 K_{c_i}로 암호화된 데이터 D_{c_i}를 데이터 암호 키 K_c로 복호화하여 송신한다.

4. 결론

본 논문은 웨어러블 디바이스를 사용하는 사용자의 데이터를 외부기기에 안전하게 저장하는 방법을 제안한다. 스마트 폰의 매니저 응용프로그램과 스마트 워치 간의 인증과정을 통해 세션 키를 수립하고, 스마트 워치에서 수집되는 데이터를 보호하기 위해 데이터 암호 키를 사용한다. 이를 통해 웨어러블 디바이스가 외부기기에 전송한 사용자의 중요한 데이터가 유출되거나 침해되지 않고 다른 어플리케이션으로부터 교차 공격을 받지 않도록 안전하게 보호할 수 있다.

참고문헌

[1] 박광만, 석왕헌, 고순주, The Next Smart Thing : 웨어러블 디바이스", 한국전자통신연구원, 2014.05

[2] Luyi Xing, Xiaolong Bai, Tongxin Li, XiaoFeng Wang, Kai Chen, Xiaojing Liao, "Unauthorized Cross-App Resource Access on MAC OS X and iOS", May 2015

[3] 제현우, 양오, "스마트폰과 블루투스 통신을 이용한 태양광 인버터 모니터링 시스템 구현", 한국정보통신학회, 제 16 권, 제 10 호, 2012.08

[4] 강동호, 백광호, 김기영, "블루투스 보안 기술", 정보통신연구진흥원, 주간기술동향 통권 1380 호, 2009.1

[5] 김정도, 박성대, 임승주, 황선필, 이상국, "모바일 헬스케어를 위한 정보 시각화", 한국정보기술학회, 제 10 권, 제 12 호, 2012.12.