Wearable Token 기반의 무선단말간 통신 기법

송세화*, 최형기*
*성균관대학교 전자전기컴퓨터공학부
e-mail : {dreaminsh, hkchoi}@ece.skku.ac.kr

A Study on Tools for Agent System Development

Sehwa Song*, Hyoung-Kee Choi *
*Department of Electrical and Computer Engineering, Sungkyunkwan University

요 약

PDA, 노트북과 같은 무선 장비들은 가볍고 이동이 편리하기 때문에 널리 사용되고 있다. 하지만 이들 장비들은 그 편리성만큼 분실, 도난 등에 취약하다. 그리고, 각 무선 장비에는 사용자의 비밀번호와 같이 외부에 노출되어서는 안 되는 데이터가 포함되어 있을 수 있다. 기존에 이러한 문제를 보완하고자 프로토콜이 제시된 바 있다. 이들 기법은 사용자가 손목시계와 같이 항시 착용하는 작은 기기(Wearable Token)와 Bluetooth 와 같은 근거리 통신을 사용하여 사용자와 무선 장비가 떨어져 있을 시 다른 사람은 해당 기기를 사용할 수 없고, 데이터를 습득할 수 없도록 한다. 본 논문에서는 더 나아가 동일한 Wearable Token 의 통제를 받는 기기들간에 안전하게 인증하면서 통신할 수 있는 기법을 제안한다.

1. 서론

PDA, 노트북, 휴대폰과 같은 무선 장비들이 폭넓게 사용되고 있다. 이들 장비들은 사용자에게 근접되어 사용되므로, 사용자들이 외부에 노출하고 싶지 않는 자료도 포함할 수 있다. 개인의 패스워드, 사진 등이 그것이다. 하지만, 이들 무선 장비들은 작고, 고정되지 않기 때문에 분실 및 탈취의 위험을 가지고 있다. 노트북의 경우, 사용자가 로그인한 상황에서 잠시 자리를 비운 사이에, 사용자가 아닌 다른 자가 사용자의 민감한 정보를 빼낼 수 있는 위협이 존재한다. 이를 막기 위해서는 빈번한 사용자의 인증이 있어야 하지만, 이는 사용자의 편의를 침해한다.

사용자의 편의를 유지하면서 각 단말이 사용자의 근처에 있어야만 동작하도록 하는 방법이 이미 연구된 바 있다. D.Corner 등은 Zero-Interaction Authentication (ZIA) [1] 이라는 시스템을 제안하였다. 이는 사용자가 착용할 수 있는 Wearable Token 을 사용하여 사용자가 수행해야 하는 인증을 Wearable Token 이 대신 수행하도록 한다. 또한, Sun 등은 위의 ZIA 를 수정하여 인증서를 사용하지 않고, 보다 간단하게 위의 사항을 수행하는 프로토콜을 제안하였다[2].

(그림 1) Wearable Token System

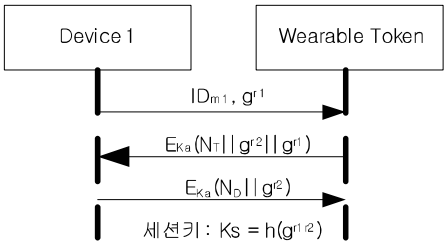
하지만 이들은 동일한 사용자의 여러 단말들 사이에서의 통신에 대해서는 정의를 하고 있지 않다. 예들 들어 휴대폰에서 사진을 블루투스 인터페이스를 사용하여 노트북으로 전송하는 일이 있을 수 있다. 이런 상황에서 Wearable Token 이 있어야만 데이터를 암/복호화 할 수 있는 장비들은 통신하고자 하는 상대방 장비 역시 동일한 Wearable Token 의 통제를 받는 장비인지 확인할 필요가 있다.

본 논문에서는 각 기기가 동일한 Wearable Token 의 통제하에 있음을 확인하도록 하는 방법을 제안한다.

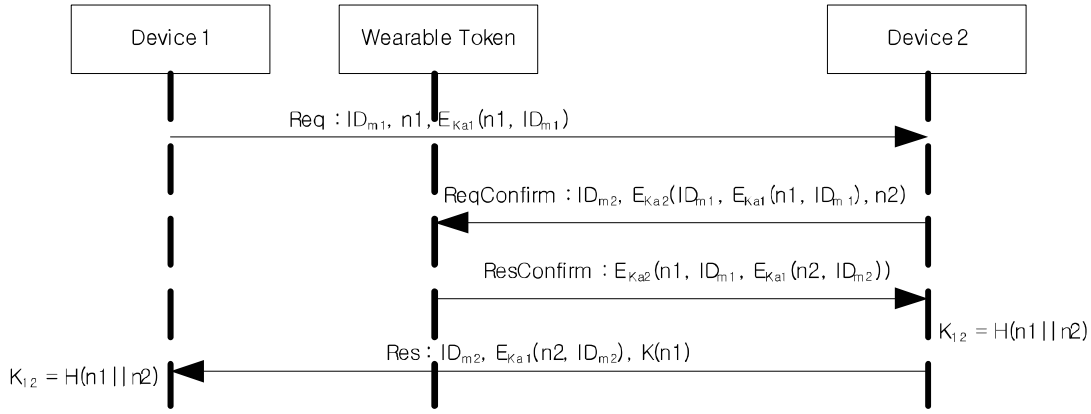
제 2 장에서는 본 논문에서 기본으로 하는 SUN 의 Wearable Token System 에 대해서 설명한다. 제 3 장에서는 Wearable Token 기반의 기기간 연동에 대해 설명한다. 그리고 제 4 장에서 본 논문의 결론을 맺는다.

2. SUN 의 Wearable Token System

논문의 주된 내용은 크게 키 생성 및 분배, 인증 프로토콜로 나눌 수 있다.



(그림 2) 인증 및 세션키 설정



(그림 3) 제안하는 Wearable Token 기반 장비간 통신 기법

키 생성 및 분배 : 각 모바일 장치는 저장하는 데이터를 file Key (K_f) 로 암호화 하고, 각 K_f 는 Wearable Token 이 저장하는 root key (K_r)로 암호화되어 저장된다. 그리고, 각 모바일 장치와 Wearable Token 은 shared Key 인 K_a 를 $K_a = h(ID_m||K_r)$ 와 같이 생성한다. K_a 는 각 모바일 장치에 미리 계산하여 탑재되고, Wearable Token 에서는 각 장치의 ID 인 ID_m 을 받으면, K_a 를 계산하여 통신의 암/복호화에 사용한다.

인증 및 세션 키의 생성 : (그림 2)는 상호인증 및 세션 키 생성 과정을 보여준다. 일반적인 Diffie-Hellman 키 생성을 사용하고 있으며, 키 생성과정을 K_a 로 암호화하여 men-in-the-middle 공격을 막고 있다.

Token loss : Wearable Token 의 분실 시 K_r 의 노출을 막기 위해 일상적으로 K_r XOR PW 를 Wearable Token 은 저장하고 있다.

3. 제안하는 장비간 통신 기법

사용자의 Wearable Token 의 통제를 받는 장비간의 통신은 보다 사용자의 정보를 안전하게 보호할 수 있는 방안이 된다. 본 논문에서는 Wearable Token 을 각 장비의 인증의 매개체로써 동작하도록 하여 각 장비들이 인증할 수 있도록 한다. ((그림 3)은 제안하는 프로토콜을 보여준다. Wearable Token 은 Device1 과 Device2 와의 세션 키인 K_{a1} 과 K_{a2} 를 가지고 있다. ID_{m1}, ID_{m2} 는 Device1 과 Device2 의 ID 이다. N1 과 n2 는 Device1 과 Device2 가 각각 생성하는 랜덤 값이다. H()는 one-way Hash 함수이다. 최초에 Device1 이 Device2 와 통신을 하고자 할 때, Req 메시지를 전송한다. 이때, ID_{m1}, 랜덤 값인 n1, 그리고 ID_{m1} 과 n1 을 Wearable Token 과의 세션 키인 K_{a1} 으로 암호화한 값이 Req 메시지에 포함된다. K_{a1} 으로 암호화된 값은 오직 Wearable Token 만 복호화 할 수 있다. Req 를 받은 Device2 는 Device1 이 Wearable Token 의 통제를 받는 단말인지 확인하기 위해 ReqConfirm 을 Wearable Token 에 전송한다. Wearable Token 은 K_{a2} 로 우선 복호화 하고, 그 내부에 있는 내용을 K_{a1} 을 통해 복호화 한다. 그래서 ID_{m1} 과 K_{a1} 으로 암호화 되어 있는 IDm1 이 동일한지 확인하고, ResConfirm 메시지를 생성하여 Device2 에 전송한다. ResConfirm 에는 Device1 이 생성한 n1 이 포함되어 있으며, K_{a1} 으로 암호화된 IDm2 와 n2 가 포함되어 있다. Device2 는 n1 과 n2 로 Device2 와 Device1 과의 세션 키인 K 를 생성한다. 그리고 최종적으로 Res 메시지를 생성하여 Device1 에 전송한다. Res 를 받은 Device1 은 우선 K_{a1} 으로 암호화된 내용을 복호화 하여 n2 를 확인하고, 세션 키 K 를 생성한다. 그리고 K 로 암호화된 n1 을 확인하므로 서 정상적으로 세션 키가 생성되었음을 확인한다.

4. 결 론

본 논문은 기존에 SUN 등이 제안한 Wearable Token 기반 무선 장비 인증 및 보호 시스템에 덧붙여 각 장비간에 Wearable Token 의 인증 여부를 확인하고 세션 키를 생성하는 기법을 제안하였다. 향후, BAN Logic 등을 활용한 보안분석 및 RFID 등을 통한 테스트베드를 통해 성능분석을 진행하여 제안하는 기법의 유효성을 검증할 것이다.

참고문헌

[1] D. C. Mark and D. N. Brian, "Zero-interaction authentication," in *Proceedings of the 8th annual international conference on Mobile computing and networking* Atlanta, Georgia, USA: ACM, 2002.

[2] S. Da-Zhi, H. Jin-Peng, S. Ji-Zhou, Z. Jia-Wan, and F. Zhi-Yong, "A new design of wearable token system for mobile device security," *Consumer Electronics, IEEE Transactions on,* vol. 54, pp. 1784002D1789, 2008.