한국컴퓨터정보학회 하계학술대회 논문집 제23권 제2호 (2015. 7)

아두이노를 이용한 다중 레벨 인증 시스템

유호원*°, 김용승*
*°한국교통대학교 소프트웨어학과
e-mail : ys@ut.ac.kr*, loverhwgel@gmail.com°

Multi-level Certification System Using Arduino

Ho-weon Yoo*°, Yong-seung Kim*
*°Dept. of Software, Korea National University of Transportation

● Abstract ●

최근 IT기술의 발전과 더불어 보안의 중요성이 부각되면서 Pin Number, Password, Pattern Recognition 등 인증 방식에 대한 연구가 진행되고 있지만 위와 같은 One-factor 인증 시스템에는 “Shoulder Attack”과 같은 사용자 레벨에서의 보안공격에 취약하다. 위와 같은 문제점을 해결하기 위하여 ‘Google E-mail‘ 등 일부 강화된 보안이 필요한 시스템에서는 추가 모듈을 이용한 Two-factor 인증 시스템을 적용하여 보안을 제공하고 있지만 사용상의 번거로움과 복잡성으로 인해 고도의 보안 기술의 적용을 받지 못하는 등 많은 제약사항이 남아있다.

본 논문에서는 위 와 같은 One-factor 시스템의 취약점을 파악하여 그에 따라 보안 인증 절차를 향상시키기 위해 암호화와 인증 방법으로 지문인식을 사용하여 Multi-level 인증 시스템을 제안한다. 본 시스템은 Send 디비이스를 구현한 아두이노를 통해 M2M 서비스를 수행하며, 암호와 지문 정보를 아두이노 디바이스에 저장하여 두 가지의 신뢰적인 정보를 바탕으로 인증하는 시스템이다. 아두이노를 이용하여 디바이스 분리를 통한 사용자 레벨에서의 보안을 강하고 지문인식을 통해 불편함과 복잡성을 간소화하였다.

키워드: 지문인식(Fingerprint), 아두이노(Arduino), 암호화(Cryptograph), 보안(Security)

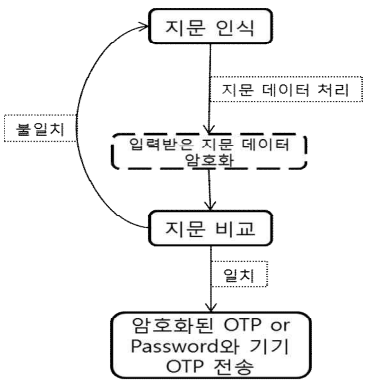
I. Introduction

IT기술이 발전하면서 IT기기들의 보급화로 인해 개인 단위의 정보 보안의 중요성이 많이 증가하고 있다. 신제품 전자기기들은 보안을 강화하기 위해 많은 추가적인 요소들을 기기 내에 구현하고 있다. 하지만 대부분이 사용하고 있는 One-factor인증 기법에는 사용자 부주의로 발생하는 보안공격에는 취약하다. 또한 공개된 장소에서의 보안 공격에 대해 취약하다. 대부분 이러한 문제를 사용자에게 책임을 부담하고 있다. 또한 이를 보완하기 위해 OTP와 같은 Two-factor인증 기법을 사용하는 기업이 간혹 있지만, 번거로움과 복잡성으로 인해 높은 수준의 보안을 보급화 시키기에는 많은 문제점이 현존한다.

II. The Proposed Scheme

Send 디바이스를 소형의 아두이노에 개발하고 Send System 아두이노는 지문인식을 통해 사용자를 인증하고 해당기기에 사용자 password 또는 OTP 번호를 암호화하여 전송함으로써, Two- factor의 인증시스템의 문제점과 통신에서의 보안 위협을 해결 한다. 암호화된 Password 혹은 OTP를 전송 받은 해당 Receive 기기에서는 기기인증과정과 복호화 과정을 거쳐 사용자를 인증하고 사용자에게 해당 Receive 기기의 사용 권한을 부여한다.

1. Send and Receive 시스템 구조

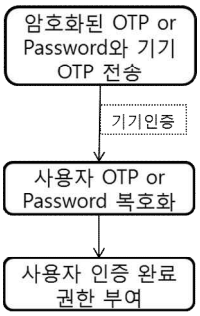


Send System Architecture

처음 지문이 들어온 시점에서 지문 데이터 처리를 한다. 지문 데이터 처리는 지문 데이터를 보다 선명하고 뚜렷하게 만들어서 데이터를 저장하기 위해 오류를 검출하고 정상적인 지문인지를 판별하는 과정을 구현한 알고리즘을 통해 진행된다.

입력받은 지문에 대한 데이터 암호화 과정은 전처리 과정을 거친 지문 데이터를 AES 알고리즘을 통해 입력받은 지문 데이터를 암호화하고 저장하고 있는 데이터와 비교하여 인가된 사용자 인지를 판별한다. 암호화 과정과 암호화 통신 기법에 대해서는 II.2에서 자세히 기술하겠다.

인가된 사용자라고 판별이 되면, 해당 디바이스에 암호화된 사용자 OTP 혹은 Password를 전송하여 암호화 통신을 수행한다.



Receive System Architecture

암호화 통신을 통해 데이터를 전송받은 해당 디바이스는 기기 인증과정을 통해 데이터를 전송한 디바이스가 정상적인 디바이스인지를 판별한다. 그리고 정상적인 디바이스라면 사용자 OTP와 Password를 복호화 하는 과정을 진행하고 사용자를 인증하여 권한을 부여한다.

2. 지문 암호화

지문데이터를 암호화하는 AES-128 알고리즘이 독립적으로 수행 가능한 ATMEGA128A를 장착한 소형의 아두이노 디바이스에 알고리즘을 구현하였다. Ciper Key의 값으로는 지문 데이터의 특징점 데이터를 가지고 사용한다. 암호화된 지문은 인증 사용자가 입력해 놓은 암호화된 지문과 비교하여 분석한다.

3. 사용자 Password 암호화 및 통신

통신 시 수준 높은 보안성을 위해 암호화된 문서를 Send 디바이스 아두이노가 해당 Receive 기기에 전송한다. Password 혹은 양방향 자동 동기화가 되는 OTP를 입력받으면 암호화를 하게 된다. 현재 공인인증서 Key 분배와 같은 공개키 알고리즘을 사용하여 사용자의 Sk(Secret key)를 받아 사용한다. 이러한 과정을 거쳐 암호화한다. 해당기기에서는 기기 인증을 통해 사용자를 판별하고 사용자의 Pk(Public key)로 복호화 하는 과정으로 암호화 통신한다.

III. Conclusions

본 논문에서는 보안 인증과정에서의 문제점을 해결하기 위하여 지문인식을 통해 공개된 장소에서의 보안을 강화하였다. OTP와 password의 암호화를 AES 알고리즘 통해 Send 디바이스 아두이노 내에 개발하고, 해당 Receive 기기와 암호화 통신하는 기법으로 Two- factor와 같은 높은 수준의 보안을 적용하였다. Send 디바이스 아두이노에 통합 개발하여 저비용으로 Two-factor 사용상의 번거로움과 복잡성을 One-factor와 같은 수준으로 최소화하여 개발하였다.

References

[1] Alexandra Dmitrienko, Christopher Liebchen, Cristian Rossow, and Ahmad-Reza Sadeghi, “On the (In)Security of Mobile Two-Factor Authentication,” Technical Report TUD-CS-2014-0029, Mar 2014.

[2] Priyansha Gupta, “Implementing Security in a Personal Security Device,” University of California, December 2013.

[3] Subhra Mazumdar, and Venkata Dhulipala, “Biometric Security Using Finger Print Recognition,” University of California, August 2008.