임베디드 시스템 환경하에서 인증시스템 설계

윤치웅*, 양재수**, 류대현*, 신승중*
*한세대학교 IT학부, **경기도청
e-mail:expershin@hansei.ac.kr

Design of Authentication System under the Embbeded System Environment

Chy-Woong Youn*, Jea-Su Yang**, Dae-Hyun Ryu*, Seung-Jung Shin*
*Dept of IT, Han-Sei University, **Gyeong-Gi Provincial Goverment

요 약

전송되는 데이터는 항상 공격자에게 노출되어 있기 때문에, 간단한 아이디나 패스워드 기법을 이용한 인증 기법은 취약점을 갖는다. 따라서 인터넷과 같은 개방형 네트워크상에서 안전한 통신을 하기 위해서는 전송될 정보의 암호화가 필요하며, 이를 위해서 통신 상대자간에 공통으로 사용할 수 있는 키의 공유가 우선되어야 한다. 본 연구에서는 인증 요청자와 인증 검증자간의 암호화된 키를 공유할 수 있는 새로운 키 교환 프로토콜을 제안하고 임베디드 환경에 적합한 암호화 알고리즘과 해시함수 알고리즘을 제안하고자 한다.

1. 서론

정보화 사회를 맞이하여 인터넷은 정보를 얻기 위한 핵심적인 기술로 발전하였을 뿐아니라 인터넷의 보급과 함께 네트워크 기술의 급속한 발전은 사이버 공간상에서 방대하고 다양한 정보가 빠른 속도로 송·수신 될 수 있는 환경이 마련되었다. 이러한 네트워크의 발전은 전자상거래, 유비쿼터스 환경 등으로 발전하면서 다양한 서비스와 편의성을 가져다주는 이점뿐 아니라 불법적인 시스템 침입과 정보의 유출 등이 쉬워짐으로써 개인 정보보호 침해와 같은 역기능을 초래하였다. 따라서 최근에는 이러한 위험으로부터 정보를 보호하고 안전하게 통신을 하기 위한 방법으로 암호화 기법이 필수적으로 사용되고 있으며 전송될 정보를 암호화하기 위해서는 통신 상대자간에 공통으로 사용할 수 있는 키의 공유가 우선되어야 하는데, 이 때 통신을 통해 정보를 교환하고 있는 상대가 실제 의도한 상대인지를 확인하는 인증 과정은 반드시 필요하며 이러한 인증기능은 사용자가 응용 서버로부터의 서비스를 받기 위해서도 필요하다. 따라서 개방형 네트워크 상에서 암호화키를 공유하고 사용자를 인증하는 문제는 안전한 정보교환을 위해 해결해야 할 중요한 문제이며, 이 문제를 해결하기 위해서 보다 효율적인 프로토콜 개발이 필요하다. 유비쿼터스 시대로 발전하면서 점점 소형기기도 인터넷과 연결되고 있는 현재 소형기기의 보안문제는 매우 중요한 문제로 부각되고 있다. 따라서 소형기기 특히 본 연구에서는 임베디드 시스템 환경하에서 일회용 암호방식의 프로토콜에 대한 설계 및 소형시스템에 적합한 암호 알고리즘과 해쉬 알고리즘을 제시하고자 한다.

2. 관련연구

인증이란 특정 시스템의 서비스를 사용하기 위해서 사용자가 권한을 얻기 위한 절차를 말하며, 인터넷을 통하여 원격 시스템에 로그인을 한다거나, 전자적인 거래를 하려할 때 반드시 사용자 인증이 필요하다. 사용자 인증방식 중 가장 보편적으로 사용되어지고 있는 것이 패스워드 인증방식이다. 그러나 이러한 패스워드 인증 방식은 보안상으로 매우 취약성을 가지고 있어 보안성을 강화할 필요성이 있다. 보안을 강화하기 위해 주로 사용되는 것이 암호화 기술이다.

암호가 처음 사용되지 시작한 이후 1970년대 초반까지 암호 방식에서 대칭 암호만이 존재하는 것으로 알려졌었다. 이러한 대칭 암호는 키의 분배 및 관리의 어려움이 있다. 이러한 키의 분배 및 관리의 어려움은 1976년 W. Diffie와 M. Hellman의 논문[2]에서 계산적 복잡도가 암호 알고리즘의 설계에 응용되는 새로운 방향을 제시하면서 해결되었다. 그들이 제시한 새로운 방향은 트랩도어 일방향 함수를 이용하여 암호화키 E와 복호화키 D 사이의 관계가 독립이 되도록 설계되는 암호이다. 이러한 암호 알고리즘을 공개키 암호 알고리즘이라고 한다. 공개키 암호 알고리즘(Public-Key Crypto Algorithm)은 암호화하거나 복호화 하는데 쓰이는 키가 두개가 존재하는 알고리즘으로 비대칭 암호알고리즘(Asymmetric Crypto Algorithm)이라고도 한다. 두 개의 키는 수학적 함수를 기반으로 서로 연관이 있는 키 쌍으로 하나의 키는 누구든지 사용할 수 있게 공개하고 다른 하나는 외부에 공개되지 않도록 보관한다. 이때 공개하는 키 E를 공개키(public key)라고 하며, 자신만이 보관하는 키 D를 개인키(private key)라고 한다.

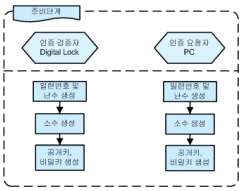
암호학적 해쉬 함수[1][5]는 현대 암호학에서 중요한 역할을 수행하고 있다. 해쉬 함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해쉬값 또는 해쉬 코드라고 불리는 값을 출력한다. 해쉬 함수는 다양한 길이의 입력을 고정된 짧은 길이의 출력으로 변환하는 함수로서, 다음과 같은 식으로 표현할 수 있다.[4]

$$y = H(x)$$

일회용 패스워드(One-Time-Password)는 매번 다른 비밀번호로 사용자를 인증할 수 있도록 하는 인증 방식을 의미하며 현재 사용하는 비밀번호로부터 다음번에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능한 특성을 가진다.[3] 일회용 패스워드 방식은 한번 사용한 패스워드는 재사용하지 않는 동적인 특성 때문에, 공격자가 네트워크 도청을 통하여 사용한 패스워드를 알아냈다 할지라도 더 이상 사용할 수 없으므로 이러한 위험을 방지할 수 있다. 또한 일회용 패스워드 방식은 단어, 숫자 패턴, 특정 사용자와 연관된 문자 등으로 구성되어있지 않아, 기억 가능하거나 쉽게 유추할 수 없다. 또한 일회성 패스워드는 매번 다른 비밀번호를 생성해내는 특성을 가지기 때문에 사회공학기법이나 네트워크 스니핑 등을 통해 의미있는 패스워드를 획득하여 재사용하는 공격방식을 무력하게 만든다.

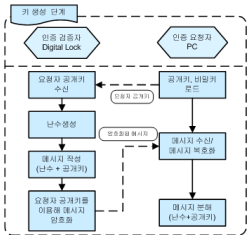
3. 제안된 프로토콜

본 연구에서 제안한 OTP를 이용한 확인자 기반 키 교환 프로토콜은 준비 단계, 키 생성 단계 그리고 인증 단계로 이루어진다. 준비 단계는 마이크로컨트롤러 즉 임베디드 시스템인 인증 검증자가 암호화를 하기위해 필요한 두 개의 소수를 생성하고 이를 바탕으로 RSA 암호화 키를 생성하여 이를 마이크로컨트롤러의 저장공간인 EEPROM에 데이터를 저장하는 단계이다. 준비 단계에 대한 내용은 (그림 1)과 같다.

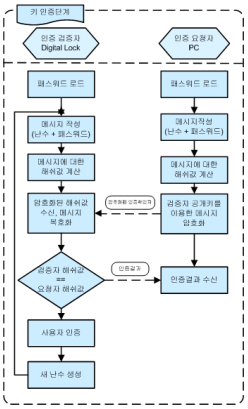


(그림 1) 준비단계

키 생성 단계는 인증 검증자는 저장 공간에 저장된 RSA 키를 로드하고 인증 요청자는 난수를 발생시켜 RSA 키를 생성하고 서로 교환하는 단계이다. 일회용 패스워드 생성을 위해 인증 검증자는 난수를 생성하고 인증 요청자에게 전달하는 과정이 포함된다. 키 생성 단계에 대한 과정은 (그림 2)와 같다.



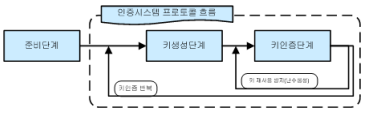
(그림 2) 키 생성단계



(그림 3) 인증단계

인증 단계는 인증 요청자가 인증 검증자가 보내준 난수와 공개키를 이용하여 일회용 패스워드 즉, 인증 확인자를 생성하여 인증 검증자가 인증을 결정하는 단계이다. 인증 단계에 대한 흐름은 다음 (그림 3)과 같다.

다음 (그림 4)는 제안된 프로토콜의 전체 처리 흐름도를 보여준다.



(그림 4) 인증시스템 프로토콜 흐름도

4. 결론 및 향후 연구

제안한 프로토콜은 인증 요청자와 인증 검증자 간의 일방향 함수 HAS-160의 해시함수와 RSA 암호 알고리즘을 바탕으로 구현되었다. 기존의 사용된 해시함수와 RSA 암호 알고리즘은 낮은 사양의 마이크로프로세서에서는 제대로 실행되지 않는 문제점을 가진다. 따라서 향후 소형 프로세서에 알맞은 암호화 알고리즘에 대한 수정 연구를 계속 할 예정이다.

참고문헌

[1] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental cryptography : The case of hashing and signing," Advances in Cryptology-CRYPTO '94, LNCS, Issue 839, 1994, pp. 216-233.

[2] W. Diffie and M.E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory IT-26, No. 6, 1976, pp. 644-654.

[3] N. Haller, "A One-Time Password Standard", IETF RFC 1938, 1996.

[4] R. Merkle, "One way hash functions and DES", In Advance in Cryptology CRYPTO'89, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, 1989.

[5] B. Preneel, "Cryptographic hash functions," European Transactions on Telecommunications and related technologies, Vol. 5, No. 4, 1994, pp. 431-448.