스마트카드를 이용한 패스워드 기반 인증시스템 정형분석

김현석° 김주배 정연오 최진영
고려대학교 컴퓨터학과
{hskim°, jbkim, yojeong, choi}@formal.korea.ac.kr

Formal Analysis of Authentication System based on Password using Smart Card

Hyun-Seok Kim° Ju-Bae Kim Yeon-Oh Jeong Jin-Young Choi
Dept. of Computer Science and Engineering, Korea University

요 약

인터넷의 범용적인 사용으로 많은 사용자들이 분산된 컴퓨팅 환경에서 원격 서버에 접속하는 일이 빈번해 지고 있다. 하지만 인증된 보호시스템 없이 안전하지 않은 채널을 통한 데이터의 전송은 재생공격이나 오프라인 패스워드 공격 및 가장공격등과 같은 문제점들에 노출되어 있다. 이에 따라 악의적인 공격들을 막기 위해 스마트카드를 이용한 인증프로토콜들에 대해 활발히 연구되고 있다. 본 논문은 패스워드 기반 사용자 인증시스템의 취약성을 분석하고 이에 대해 개선된 사용자 인증 시스템을 제안한다

1. 서 론

최근 유비쿼터스 컴퓨팅 환경에서는 개인 정보보호 및 프라이버시에 관심이 대두되고 있다. 특히 스마트카드를 이용한 원격 인증 시스템에서 개인정보보호를 위한 일환으로 사용자 익명성을 제공하는 인증 시스템에 대한 연구가 진행되어 오고 있다[1,2]. 그러나 기존의 익명성을 제공하는 스마트카드를 이용한 인증에 대한 연구들은 로그인 단계에서 서버에게 보내는 데이터를 통해 사용자를 구분할 수 있고 그로 인해 사용자 익명성을 제공하지 못한다는 점과 사용자 익명성을 제공하는 인증 프로토콜을 제안되고 있지만 제3자에게만 안전한 사용자 익명성을 제공하고 있는 취약점을 가지고 있다. 스마트카드를 이용한 원격 사용자 인증 프로토콜을 살펴보면, 사용자가 서버에 등록하기 위한 정보들이 존재하고, 서버는 이러한 정보들을 이용해 검증테이블에 저장 및 스마트카드에 저장한 후 이를 사용자에게 발급한다. 본 논문에서는 2008년에 Chen와 Lee [3]가 제안한 스마트카드를 이용한 패스워드기반의 원격 사용자 인증 프로토콜을 분석하여 그 취약성을 분석하고 개선된 프로토콜을 제안한다. 제안된 프로토콜에서는 Chen 과 Lee 의 프로토콜에서와 같이 처리비용이 큰 지수연산이나 비대칭 암호화 연산 없이 XOR 연산과 해쉬함수만을 사용하는 효율적인 인증절차를 수행한다는 장점을 유지하고 있다.
본 논문의 구성은 다음과 같다. 2장에서 패스워드 기반 스마트카드에 대한 보안 요구사항들을 정의하고, 3장에서는 Chen 과 Lee에 의해 제안된 프로토콜의 안전성을 분석하고 4장에서 개선된 프로토콜을 제안한다.

2. 인증시스템 보안 요구사항

패스워드 기반의 스마트카드를 이용한 인증 시스템의 필수적인 보안 요구사항에 대해 사용자의 카드 및 카드 단말기, 서버의 구성환경에 대해 많은 문헌들[1-4]에 의해 다음과 같이 3가지 보안 요구사항을 정의할 수 있다.

- Replay attack (재생공격) : 인증단계에서 메시지 값을 차후 재전송에 이용하더라도 사용자나 공격자는 이를 인식하여 공격을 방지할 수 있다.
- Offline guessing attack (오프라인 추측 공격) : 사용자와 서버와의 통신에서 패스워드 값이 직접 보내지지 않는다. 따라서 공격자는 통신채널을 통해서 패스워드를 얻을 수 없다.
- Impersonation attack (가장 공격) : 공격자가 정당한 로그인 정보를 위조하기 위해서는 암호화된 메시지 값 안에 포함된 정당한 사용자 생성값과 서버의 비밀 값을 알아야만 한다. 또한 공격자는 메시지를 도청하여 저장해 두고 재사용하여 사용자를 가장하고자 하지만 서버의 비밀값이 노출되지 않기 때문에 재사용하더라도 공격이 가능하지 않다.

3. 스마트카드 인증 프로토콜 분석 및 검증 결과

Peyravian-Zunic [1]이 제안한 효율적인 인증 프로토콜은 추측공격이 가능함에 따라 재사용공격이 가능하게 되었으며 Chen과 Lee [2]는 이러한 공격의 취약성을 막기 위한 개선 프로토콜을 제안하였다. 본 장에서는 스마트카드를 이용하고 XOR과 해쉬함수 연산만으로 구성되는 효율적인 인증 프로토콜을 분석한다. 제안된 프로토콜을 사용자 등록 단계, 로그인 및 인증 단계로 구별하여 설명한다. 사용자는 서버에 로그인을 하기 위해 자신의 스마트카드를 서버에 미리 등록해야 하는데 그 과정을 알아보기 위해 사용자 **U**의 경우를 예를 들어 설명한다.

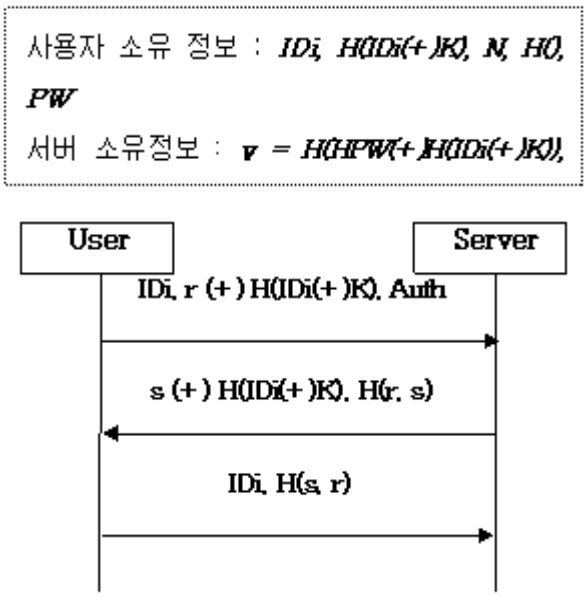

그림 1. Chen-Lee 인증프로토콜

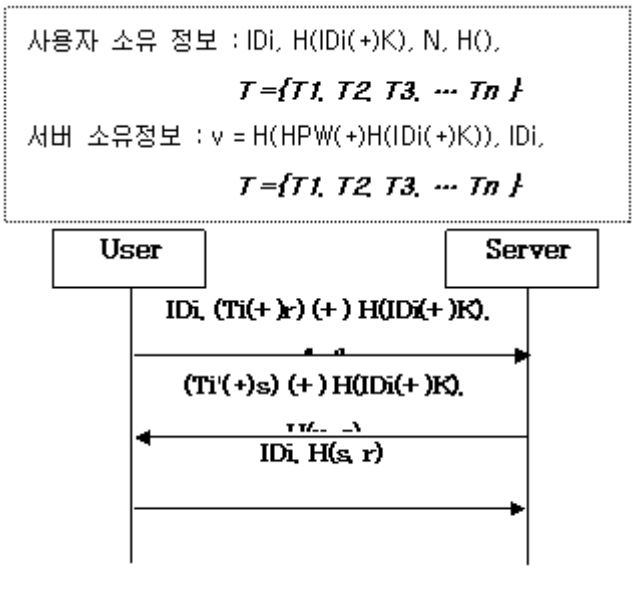

그림 2. 개선된 Chen-Lee 프로토콜

2절에서 제시된 보안 요구사항에 대해 위 분석 결과를 토대로 다음과 같이 정리할 수 있다.

- Replay attack (재생공격) : [4] 에 의한 사실로 공격자는 전력소모를 모니터링 함으로써 스마트카드에 저장된 정보를 추출해 낼 수 있다. 따라서 공격자는 스마트카드에 저장된 H(IDi(+)K) 과 N, H() 값을 획득할 수 있다. 이에 따라 공격자가 사용자의 과거 로그인 메시지 중 하나를 가로채기하여 소유하고 있다고 가정하자. 즉 메시지 1의 IDi, r (+) H(IDi(+)K), Auth 에서 H(IDi(+)K) 를 XOR 연산하여 r 값을 도출할 수 있게 된다. 이를 통해 메시지 2의 s (+) H(IDi(+)K) 또한 s 값을 생성할 수 있으며 이 두 값 r , s 를 이용하여 서버에 대한 재생공격이 가능하게 된다.
- Offline Guessing attack (오프라인 추측 공격) : 공격자는 H(IDi(+)K) 과 N, H() 정보를 가지고 있으므로 메시지 1의 값을 통해 오프라인 추측공격이 가능하다. 즉, 메시지 1의 Auth 값은 다음과 같은 값으로 구성되어 있다. H(H(HPW(+)H(IDi(+)K)),r) = H(H(*H(IDi, PW, N)* (+)H(IDi(+)K)),r). 따라서 공격자는 Auth'= H(H(H(IDi, *PW*, N) (+)H(IDi(+)K)),r) 을 연산하고 이를 통해 Auth ?= Auth'을 비교하여 패스워드 값 PW를 추측할 수 있다.
- Impersonation attack (가장 공격) : 공격자가 정당한 로그인 정보를 위조하기 위해서 암호화된 메시지 값 안에 포함된 공격자 생성값 IDx을 메시지 1과 2에서 이미 H(IDi(+)K)을 통해 획득한 s, r 값을 이용해 메시지 3에서 IDx, H(s,r) 을 전송하여 서버로부터 정상적인 사용자가 IDx인 것으로 인식하게 한다.

4 해쉬기반 프로토콜의 취약성을 수정한 제안프로토콜

이러한 Chen-Lee 프로토콜의 문제점으로 분석되었던 부분은 스마트카드 내에 저장된 정보가 DPA(차별화 전력 분석: Differential Power Analysis) 를 통해 노출되고 ,이 정보를 통해 상호 인증을 위한 난수값이 노출됨으로써 발생되었으며 이는 사용자의 OTP(일회성 패드 : One time Pad)를 이용한 난수값을 추가적으로, 인증시 입력함으로써 인증시에 사용되는 난수값과 함께 XOR 연산을 함으로써 안전성을 보장받게 되었다. 즉 제안프로토콜은 다음 (그림 2)과 같은 절차로 인증이 이루어지며 앞서 언급된 취약성은 인증과정에서 도입된 One-time-pad 기술에 의해 극복할 수 있다. 즉, 사용자는 스마트카드를 발급 받음과 동시에 OTP용 난수 집합 T={T1, T2, T3, … Tn }을 이용한 값들을 함께 가지게 된다.

5. 참고문헌

[1] J. Munilla, A. Peinado, "Off-line password guessing attack to Peyravian. Jeffries's remote user authentication protocol", A Computer Communications 30, pp. 52-54, 2006.

[2] H.Y. Chien, C.H. Chen, "A Remote Authenti-cation Scheme Preserving User Anonymity", IEEE AINA'05, Vol. 2, pp. 245-248, 2005.

[3] T.H. Chen and W.B. Lee, "A new method for using hash functions to solve remote user authentication", Computers and Electrical Engineering 34, pp.53-62, 2008.

[4] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Examining smart card security under the threat of power analysis attacks", IEEE Transactions on Computers 51 (5), pp. 541-552, 2002.