특집논문-08-13-1-07

부채널 분석을 이용한 원거리 사용자 인증 기법의 사전공격

김 용 훈[a], 윤 택 영[a], 박 영 호[b], 홍 석 희[a]‡

Dictionary attack of remote user authentication scheme using side channel analysis

Yong Hun Kim[a], Taek Young Youn[a], Young Ho Park[b], and Seok Hee Hong[a]‡

요 약

원거리 사용자 인증 기법은 원거리에 존재하는 사용자의 인증을 제공하는 프로토콜이다. 2007년 Wang 등은 2004년 Ku 등의 원거리 사용자 인증 기법[6]이 전력분석과 같은 부채널 공격을 사용해 카드의 비밀값을 알아 낸 후 이 정보를 기반으로 사전 공격이 가능함을 보였다. 또한 Wang 등은 이러한 문제점을 개선해 공격자가 스마트카드에 저장된 정보를 획득하게 되는 경우에도 안전한 원거리 인증 기법을 제안했다[11]. 본 논문에서는 Wang 등의 원거리 사용자 인증 기법을 분석한다. Wang 등이 제안한 기법은 부채널 분석과 같은 방법으로 카드 내에 있는 정보가 공격자에게 유출되더라도 사전 공격에 안전하다고 주장되었으나 그러한 카드 내부의 정보가 공격자에게 유출되는 경우 적용 가능한 사전 공격방법을 제안한다.

ABSTRACT

Remote user authentication scheme is a cryptographic tool which permits a server to identify a remote user. In 2007, Wang et al. pointed out that Ku's remote user authentication scheme is vulnerable to a dictionary attack by obtaining some secret information in a smart card using side channel attacks. They also proposed a remote user authentication scheme which is secure against dictionary attack. In this paper, we analyze the protocol proposed by Wang et al. In the paper, it is claimed that the protocol is secure even though some values, which is stored in a smart card, are revealed to an adversary. However, we show that their protocol is insecure if the values are disclosed to an adversary.

Keyword : dictionary attack, authentication scheme, smart card, side channel attack

Ⅰ. 서 론

원거리 사용자 인증 기법은 원거리에 존재하는 사용자의 인증을 제공하는 프로토콜로 인터넷을 통한 통신과 같이 상대방을 직접 확인할 수 없는 환경에서 매우 중요한 요소이다.

원거리 사용자 인증 기법은 1981년도 Lamport에 의해 최초로 제안되었고[9], 이 기법은 공유된 패스워드로 사용자를 인증하는 방식으로 구성되어 있다. Lamport에 의해 제안된 이후, 원거리의 사용자를 인증하기 위한 다양한 기법이 제안되었고, 이는 사용자를 인증하기 위한 정보로 공개키를 사용하는 것[1,2,4]과 패스워드를 사용하는 것[7,8,9,10]으로 나

a) 고려대학교 정보경영공학전문대학원
Graduate School of Information Security, Korea Univ.
b) 세종사이버대학교
Sejong Cyber Univ.
‡ 교신저자 : 홍석희(hsh@cist.korea.ac.kr)
※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2007-(C1090-0701-0025))

눌 수 있다.

공개키 기반의 기법은 연산량이 많은 대신 패스워드를 기반으로 한 기법보다 더 안전하게 설계 할 수 있다. 공개키를 기반으로 설계된 원거리 사용자 인증 기법으로는 1993년에 Chang과 Wu가 중국인의 나머지 정리를 이용하여 구성한 기법[2]과 1994년 Chang과 Liao가 ElGamal의 서명을 이용하여 제안한 기법[1]이 있다. 2002년에는 Hwang과 Yeh가 Peyravian과 Zunic의 패스워드 기반의 기법[9]을 공개키 기반으로 변형하여 제안했다[4].

패스워드를 기반으로 설계된 원거리 사용자 인증 기법은 연산량이 적기 때문에 적은 연산능력이 제공되는 환경에서 사용할 수 있는 장점을 가진다. 최초로 제안된 Lamport[7]의 기법을 시작으로 패스워드 기반의 기법도 활발히 연구가 진행 되었다. 1998년에 Shimizu 등이 Lamport의 기법의 취약점과 변형된 기법을 제시했고[10], 2000년 Peyravian과 Zunic가 패스워드를 안전하게 보호할 수 있는 사용자 인증 기법을 제시했으며[9] 2002년에는 Lee 등이 Peyravian과 Zunic의 기법을 개선한 기법을 제시했다[8]. 패스워드를 기반으로 한 기법은 적은 연산량 때문에 스마트카드에 내장이 용이해 원거리 인증 기법에 스마트카드를 활용하는 방법에 대한 연구도 수행되고 있다. 특히, 스마트카드를 활용하면 패스워드를 원거리 시스템(remote system : RS)이 보관하지 않도록 설계할 수 있으므로 RS의 패스워드 관리비용을 절감할 수 있다는 장점을 가진다.

2002년 Chien 등은 스마트카드를 사용해 사용자가 자신의 패스워드를 변경 할 수 있고 서버는 사용자의 인증을 위해 저장하는 정보 없이 사용자 인증이 가능한 원거리 사용자 인증 기법을 제안했다[3]. 그러나 2004년 Ku 등은 Chien 등의 기법은 몇몇의 공격법에 취약함을 지적했고, 그 취약점에 안전한 기법을 제안했다[6]. 그리고 최근 Wang 등은 Ku 등의 기법이 전력분석과 같은 부채널 공격을 이용해 스마트카드 내부의 정보를 획득함으로서 사전공격이 가능함을 보였다[11]. 그리고 스마트카드 내부의 정보가 노출되더라도 안전한 새로운 기법을 제안했다.

본 논문에서는 Wang 등의 원거리 사용자 인증 기법 역시 Ku 등의 기법과 마찬가지로 부채널 공격[5]을 이용해 스마트카드 내부의 정보를 알아낼 경우에 적용할 수 있는 사전공격방법을 제안한다. 사전공격은 패스워드 기반의 기법에서 필수적으로 고려되어야 하는 공격방법으로 알 수 있는 값들을 사용해 패스워드의 옳고 그름을 판단하고 패스워드를 알아내는 방법이다. 부채널 공격을 고려하는 공격 방법이므로 스마트카드 내부에 저장되어 있는 정보도 공격자가 알 수 있는 값에 포함하고 또한 이후 4장에서는 실제로 부채널 공격으로서 카드 내부의 값을 알아낼 수 있음을 보인다. Wang 등은 이러한 스마트카드 내부의 정보가 노출되더라도 자신들이 제안한 프로토콜은 사전공격에 대해 안전하다고 주장했다.

II. Ku 등의 기법에 대한 사전공격

이 장에서는 Ku 등의 원거리 사용자 인증 기법에 대한 사전공격방법에 대해 알아본다. 공격방법의 설명 전에 Ku 등의 원거리 사용자 인증 기법이나 다음 장에서 소개할 Wang 등의 원거리 사용자 인증 기법에서 사용할 기호들을 다음 표1과 같이 정의한다.

표 1. 기호의 정의
Table 1. notation

U : 사용자
ID : 사용자 U의 ID
PW : 사용자 U의 패스워드
S : 서버
x : 서버의 비밀키
$h()$: 암호학적 해쉬함수
$h_k()$: 키를 사용한 암호학적 해쉬함수

Ku 등의 원거리 사용자 인증기법에서 U의 스마트카드에 저장되는 정보는 다음과 같다:

$$R = h(EID \oplus x) \oplus h(b \oplus PW), b$$

여기서 b는 사용자가 선택한 랜덤한 값이고 $EID = (ID \| n)$이다. n은 S가 저장하고 있는 U의 재등록 횟수이다. Wang 등은 전력분석으로서 스마트카드에 저장되어 있는 위의 값

R, b를 공격자가 알아낼 수 있고 따라서 그 정보로 인해 사전공격이 가능하다고 주장했다. 그 사전공격은 다음과 같이 수행된다:

i. 공격자는 전력분석[5]과 같은 부채널 공격 방법으로 인해 스마트카드에 저장되어 있는 값 R과 b를 알아낸다. 또한 공격자는 U의 로그인 메시지인 $\{ID, c_2, T_u\}$를 얻는다.

ii. 공격자는 추측한 패스워드 PW'를 사용해 다음을 계산한다.

$$c_2' = h(R \oplus h(b \oplus PW') \oplus T_u)$$

iii. 공격자는 $c_2 = c_2'$이 성립할 때까지 위의 ii단계를 반복한다.

Wang 등은 위와 같은 방법으로 공격자는 사전공격을 수행해 사용자의 패스워드를 알아낼 수 있음을 지적하였고 이러한 공격에 안전한 기법을 제시하였다. 제시한 기법은 다음 장에서 살펴본다.

Ⅲ. Wang 등의 원거리 사용자 인증 기법

이 장에서는 Ku 등의 원거리 사용자 인증 기법의 취약점을 개선한 Wang 등의 원거리 사용자 인증 기법에 대해 알아본다.

◎ *등록단계 :*

i. U는 랜덤한 값 b를 선택하고 $h(b \oplus PW)$를 계산하고 S에게 안전한 경로로 ID와 $h(b \oplus PW)$를 전송한다.

ii. S는 다음을 계산한다:
$p = h(ID \oplus x), R = p \oplus h(b \oplus PW)$,
$V = h_p(h(b \oplus PW))$

iii. S는 $R, V, h(), h_k()$를 저장한 스마트카드를 안전한 경로로 U에게 전달한다.

iv. U는 선택했던 값 b를 스마트카드에 저장한다.

◎ *로그인 단계 :*

i. U는 ID와 PW를 입력한다. 스마트카드는 입력받은 PW를 사용해 $p = R \oplus h(b \oplus PW)$을 계산한 후 $h_p(h(b \oplus PW))$를 계산해 V와 같지 않을 경우 수행을 중단한다.

ii. 스마트카드는 랜덤한 값 r을 생성하고 타임스탬프 T_u를 사용해 다음을 계산한다:

$$c_1 = p \oplus h(r \oplus b), c_2 = h_p(h(r \oplus b) \oplus T_u)$$

iii. U는 S에게 $\{ID, c_1, c_2, T_u\}$를 전송한다.

◎ *인증 단계 :*

i. S는 U의 ID가 유효하지 않은 형식이거나 S의 타임스탬프 T_s에 대하여 $T_u = T_s$이면 수행을 중단한다. 또한 $T_s - T_u$가 허용된 시간 이상이 되면 수행을 중단한다.

ii. S는 $p = h(ID \oplus x)$와 $c_1' = p \oplus c_1$를 계산한 후, $h_p(c_1' \oplus T_u)$를 계산해 c_2와 비교한다. 두 값이 같지 않으면 수행을 중단한다.

iii. S는 $c_3 = h_p(c_1' \oplus T_s)$를 계산한 후, U에게 $\{c_3, T_s\}$를 전송한다.

iv. U는 T_s의 값이 유효하지 않은 값이거나 $T_s = T_u$이면 수행을 중단한다.

v. U는 $c_3' = h_p(h(r \oplus b) \oplus T_s)$를 계산한 후, c_3과 비교한다. 두 값이 같지 않으면 수행을 중단한다. 또한 r은 매 세션마다 선택되는 랜덤한 값이기 때문에 U와 S는 $c_1' = h(r \oplus b)$를 세션키로 사용할 수 있다.

◎ *패스워드 변경 :*

i. U는 ID와 PW를 입력한 후 패스워드 변경 요청을 한다.

ii. 스마트카드는 다음을 계산한다.

$$p^* = R \oplus h(b \oplus PW), V^* = h_p^*(h(b \oplus PW))$$

iii. 스마트카드는 저장된 V와 계산된 V^*를 비교하고 틀릴 경우 수행을 중단한다. 두 값이 같을 경우 U에게 새로운 패스워드 PW_{new}를 입력받는다.

iv. 스마트카드는 다음을 계산해 R, V대신 저장한다.
$R_{new} = p^* \oplus h(b \oplus PW_{new})$,
$V_{new} = h_p^*(h(b \oplus PW_{new}))$

Ⅳ. Wang 등의 원거리 사용자 인증 기법의 공격 방법

Wang 등은 Ku 등이 제안한 기법은 전력분석으로 인해 스마트카드 내부의 정보를 알아낸 후 사전공격이 성공함을 보였다[11]. 그리고 전력분석과 같은 방법으로 스마트카드내의 정보가 유출되더라도 사전공격에 안전한 변형된 기법을 제시하였지만 제안한 기법도 카드내의 정보가 유출 될 경우 사전공격이 가능하게 된다. 이번 장에서는 Wang 등이 제안한 기법의 사전공격 방법에 대해 기술한다.

1. 추측공격(guessing attack)과 사전공격(dictionary attack)

Wang 등이 언급한 공격 방법은 추측공격(guessing attack)이고 추측공격에 대해 자신의 기법이 안전하다고 주장했다. 본 절에서는 추측공격과 사전공격(dictionary attack)에 대해 논한다. 추측공격과 사전공격은 모두 전수조사의 효율성을 높이기 위해 나온 방법으로 패스워드에 대한 공격에서 주로 사용된다.

패스워드는 일반적으로 사람이 기억하기 쉬운 문자열이나 숫자, 혹은 그것들의 조합으로 사용된다. 이러한 점을 바탕으로 추측공격은 패스워드의 사용자에 대한 정보를 수집해 수집한 정보들에서 패스워드의 후보들을 추출하고 후보들로서 전수조사를 수행하는 방법이다.

사전공격은 추측공격과 패스워드의 후보들을 선택하는 방법에서 차이가 있다. 사전공격 역시 패스워드는 기억하기 쉬운 것을 사용할 것이라는 것에 기반을 두고 있다. 기억하기 쉬우려면 의미 있는 문자열이나 숫자를 사용할 것이고 따라서 사전공격에서는 사전에 등록되어 있는 문자열이나 숫자에서 패스워드의 후보들을 추출한다. 그 후, 추측공격과 마찬가지로 후보들로 전수조사를 수행한다. 이와 같이 추측공격과 사전공격은 패스워드 후보의 추출 방법에 차이가 있고 추출이 된 후에는 같은 방법으로 공격을 수행한다.

2. 전력분석 방법

본 절에서는 공격에 사용될 스마트카드의 정보를 알아내는 방법인 부채널 공격 중 하나인 전력분석 방법[5]에 대해 서술한다. 전력분석은 연산이 이루어지는 부분에서 소비되는 전력의 파형을 모아 분석해 연산된 값을 알아내는 방법이다. 이 방법을 사용하기 위해서는 공격자가 알고 있는 값을 입력해 볼 수 있어야 하고 고정된 비밀값과 공격자가 알 수 있는 값과의 연산이 이루어져야 한다. 간단한 예로서 설명하면, 공격자가 스마트카드 내부의 비밀값 x를 알고자 한다고 가정하자. 이때, 카드 내부에서는 카드에 입력되는 입력값과 x와의 XOR연산이 수행된다고 가정하자. 공격자는 우선 $x=(1\cdots)_2$와 같이 비밀값 x의 첫 번째 자리를 추측하고 다수의 a_i를 입력해 보면서 XOR연산 후의 전력파형을 수집한다. 이때 공격자는 다음과 같은 두 집합으로 전력파형을 분류한다.

$$A=\{a_i\text{의 파형}|a_i\text{의 첫번째 자리}\oplus 1=1\},$$
$$B=\{a_i\text{의 파형}|a_i\text{의 첫번째 자리}\oplus 1=0\}$$

이때 두 집합의 파형들의 평균을 구한 후, 'A의 평균-B의 평균' 파형을 계산한다. 이 파형이 양수로 나타나면 x의 첫 번째 자리가 올바르게 추측된 것이고, 파형이 음수로 나타나면 x의 첫 번째 자리가 0이 된다. 이와 같은 방법으로 x의 이후 모든 자리의 비트도 알아낼 수 있다.

이제 Wang 등의 원거리 사용자 인증 기법에서 공격이 수행되는 방법에 대해 서술한다. 공격자가 카드 내부의 값인 b를 알아내려고 한다고 가정하자. Wang 등의 원거리 사용자 인증 기법은 로그인을 하기 위해 카드에 패스워드와 아이디를 입력하게 된다. 여기서 패스워드는 카드 내부에서 연산에 사용되는 값이므로 위의 예에서 a_i의 역할을 할 수 있다. 스마트카드는 입력받은 패스워드로 $p=R\oplus h(b\oplus input)$를 계산하게 된다. 여기서 $input$은 공격자가 패스워드로서 입력한 값이다. 이때 스마트카드는 b와 $input$을 XOR하는 연산을 우선적으로 수행하게 된다. 공격자는 많은 값을 입력해 봄으로서 많은 b와 $input$의 XOR연산에서 많은 전력 파

형을 수집할 수 있고, 따라서 위에서 언급한 방법을 통해 b를 알아낼 수 있다. 공격자는 b를 알아낸 후에 자신이 입력한 값과 알아낸 b를 이용해 $h(b \oplus input)$의 값을 알 수 있고 이 값은 위의 예에서 a_i의 역할을 할 수 있다. 공격자는 $h(b \oplus input)$와 R의 XOR연산에서 많은 파형을 수집할 수 있고, 따라서 R도 알아 낼 수 있다.

3. Wang 등의 기법 공격방법

공격자는 올바른 사용자 U의 패스워드를 알아내려한다고 가정하자. 공격자는 다음과 같은 방법으로 사전공격을 수행한다.

i. 공격자는 위에서 설명한 전력분석과 같은 부채널 공격 방법으로 인해 스마트카드에 저장되어 있는 값 R과 b를 알아낸다. 또한 공격자는 U의 로그인 메시지인 $\{ID, c_1, c_2, T_u\}$를 얻는다.

ii. 공격자는 추측한 패스워드 PW'를 사용해 다음을 계산한다.

$$p' = h(PW' \oplus b) \oplus R$$

iii. 공격자는 위의 p'을 이용해 다음을 계산해 c_2와 비교한다.

$$c_2' = h_{p'}(c_1 \oplus p' \oplus T_u)$$

iv. 공격자는 $c_2 = c_2'$이 성립할 때까지 위의 ii, iii단계를 반복한다.

올바른 패스워드를 대입하였을 경우 다음과 같은 식이 성립하므로 위의 공격으로 사전공격이 가능하다.

$$p' = h(PW \oplus b) \oplus R = h(PW \oplus b) \oplus h(PW \oplus b) \oplus p = p,$$
$$c_2' = h_p(c_1 \oplus p \oplus T_u) = h_p(p \oplus h(r \oplus b) \oplus p \oplus T_u).$$
$$= h_p(h(r \oplus b) \oplus T_u) = c_2$$

따라서 위의 방법으로 공격을 수행하면 공격자는 올바른 패스워드를 찾아낼 수 있게 된다. 공격자는 주어진 식과 로그인 메시지로 사전공격을 수행하였는데, 이 공격 방법은 입력 후보에 대한 검증식을 유도한 것으로 Wang 등이 언급한 추측공격에도 적용 가능하다.

V. 결 론

Wang 등은 공격자가 스마트카드내의 정보를 사용하더라도 사전공격에 안전한 원거리 사용자 인증 기법을 제안하였다. 하지만 본 논문에서는 Wang 등이 제안한 기법 역시 스마트카드내의 정보가 노출되면 사전공격에 취약함을 보였다. 스마트카드 기반의 프로토콜에서는 스마트카드 내부의 정보가 안전하게 저장된다는 가정하에 프로토콜을 설계하게 되므로 카드 내부의 정보를 공격자가 알아낸다는 가정을 하는 것은 스마트카드를 사용하지 않는 프로토콜과 큰 차이가 없어진다. 그러므로 스마트카드 기반 프로토콜의 특징을 살리기 위해서는 카드 내부의 정보를 공격자가 획득하지 못하게 해야 할 것이다. 따라서 이와 같은 프로토콜의 안전성을 위해서는 스마트카드에 대한 부채널 공격을 방지하는 것이 중요한 문제가 될 것이고 많은 연구가 필요하다.

참 고 문 헌

[1] C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme", Computers and Security, vol. 13, no. 2, pp 137-144, 2002.

[2] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards", IEE Proceedings-E, 138(3), pp 165-168, 1993.

[3] H. Y. Chien, J. K. Jan and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card", Computers & Security, vol. 21, no. 4, pp. 372-375, 2002.

[4] J. J. Hwang and T. C. Yeh, "Improvement on Peyravian-Zunic's password authentication schemes", IEICE Transactions on Communications, E85-B(4), pp 823-825, 2002.

[5] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", Proc. Advances in Cryptology (CRYPTO '99), pp.388-397, 1999.

[6] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics 50 (1), pp.204-207, 2004.

[7] L. Lamport "Password Authentication with Insecure Communication", Communications of the ACM, vol. 24, no. 11, pp 770-772, 1981.

[8] C. C. Lee, L. H. Li and M. S. Hwang, "A remote user authentica-

tion scheme using hash functions", ACM Operating systems Review, vol. 36, Issue 4, pp 23-29, 2002.

[9] M. Peyravian and N. Zunic, "Method for protecting password transmission", Computers and Security, vol. 19, no. 5, pp 466-469, 2000.

[10] A. Shimizu, T. Horioka and H. Inagaki, "A password authentication methods for contents communication on the Internet", IEICE Transactions on Communication, E81-B(8), pp 1666-1673, 1998.

[11] X. M. Wang, W. F. Zhang, J. S. Zhang and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards", Computer Standards & Interfaces, vol. 29, no. 5, pp.507-512, 2007.

[12] E. K. Yoon and K. Y. Ryu, "Further improvement of an efficient password based remote user authentication scheme using smart card", IEEE Transactions on Consumer Electronics 50 (2), pp.612-614, 2004.

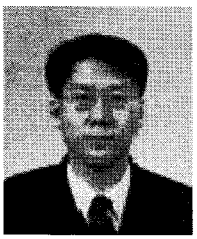
저 자 소 개

김 용 훈

- 2006년 8월 : 광운대학교 수학과 졸업
- 2006년 9월 ~ 현재 : 고려대학교 정보경영공학전문대학원 정보보호학과 석사과정
- 주관심분야 : 암호 이론, 정보보호 이론, 암호 프로토콜

윤 택 영

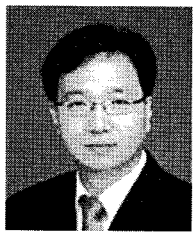
- 2003년 2월 : 고려대학교 수학과 졸업
- 2005년 2월 : 고려대학교 정보경영공학전문대학원 정보보호학과 공학석사
- 2005년 3월 ~ 현재 : 고려대학교 정보경영공학전문대학원 정보보호학과 박사과정
- 주관심분야 : 암호 이론, 정보보호 이론, 암호 프로토콜, 부채널 공격



박 영 호

- 1990년 2월 : 고려대학교 수학과 이학사
- 1993년 2월 : 고려대학교 수학과 이학석사
- 1997년 2월 : 고려대학교 수학과 이학박사
- 2002년 3월 ~ 현재 : 세종 사이버 대학교 조교수
- 주관심분야 : 정수론, 공개키 암호, 암호 프로토콜, 부채널 공격

저 자 소 개



홍 석 희

- 1995년 2월 : 고려대학교 수학과 학사
- 1997년 2월 : 고려대학교 수학과 석사
- 2001년 2월 : 고려대학교 수학과 박사
- 1999년 8월 ~ 2004년 2월 : (주) 시큐리티 테크놀로지스 선임연구원
- 2003년 2월 ~ 2004년 2월 : 고려대학교 시간강사
- 2004년 4월 ~ 2005년 2월 : K.U.Leuven 박사후연구원
- 2005년 3월 ~ 현 재 : 고려대학교 정보보호대학원 조교수
- 주관심분야 : 암호 알고리즘 설계 및 분석, 컴퓨터 포렌식