신원확인이 한번으로 가능한 패스워드

박종민, 조범준
조선대학교 컴퓨터공학과
e-mail: jmpark@ai.chosun.ac.kr

One Pass Identification of Possibility Password

Jong-Min Park, Beom-Joon Cho
Dept. of Computer Engineering, Chosun University

요 약

사용자 고유번호와 패스워드 기반의 사용자 인증 매커니즘을 수행하는 네트워크 시스템 환경에서는 스니퍼 프로그램 등을 이용하여 불법 도청함으로써 쉽게 사용자의 패스워드를 알아낼 수 있다. 이러한 불법적인 도청에 의한 패스워드 노출 문제를 해결하는 방법으로서는, 일회용 패스워드, Challenge-Response 인증 방식이 유용하게 사용되며, 클라이언트/서버 환경에서는 별도의 동기가 필요 없는 시간을 이용한 일회용 패스워드 방식이 특히 유용하게 사용될 수 있다. 안전성은 Square root problem에 기초를 두고 있고, 프리 플레이 공격, 오프라인 사전적 공격 그리고 서버 등을 포함하여 지금까지 잘 알려진 공격들에 대해서 안전성을 높이기 위한 OPI을 제안한다. OPI는 패스워드를 생성하는데 특별한 키를 생성할 필요가 없다는 것이다. OPI는 승인된 자를 확인하는데 걸리는 시간이 적게 소요되면서도 특출하였다.

1. 서론

신분조회는 확인자가 승인자의 신원에 관하여 다른 사람화 되어지는 것을 막고, 명확한 것으로 확신시켜주는 과정이다[1]. 패스워드 시스템의 장점들은 즉 쉬운 실행, 저렴한 가격 그리고 사용능력들 때문에 가장 널리 사용되어지는 신분확인 체계이다. 패스워드 시스템에서 보호되어져야만 하는 공격(해킹)들은 다음을 포함한다. 즉 시스템 외부에서의 패스워드 노출, 시스템 안에서 라인 엿듣기, 그리고 둘 모두는 연속적인 재연을 허용하고, 오프라인 상의 사전적 공격을 포함한 패스워드 추측 등이다[3]. 여러 기법의 기술들은 패스워드 시스템의 안전성을 증진시킬 수 있다는 것을 대변하여 왔었다. 그러나 어떤 기법 기술이 서버 협상이후 리플레이 공격 혹은 프리-플레이 공격[2]과 오프라인 사전적 공격을 포함한 실질적인 공격에 대항해서 안전성을 아직까지는 나타내주지는 못했다. 예를 들면 일회성 패스워드와 속이는 패스워드를 포함하고 있다. 프리 플레이 공격은 일회성 패스워드 시스템이 불안전한 상태로 만들 가능성이 존재하며, 오프라인 사전적 공격은 속이는 패스워드를 사용하는 패스워드 시스템에 적용되어질 수 있다[4]. 본 논문에서는 OPI라고 하는 새로운 신원확인 도식을 제안하고자 한다. OPI의 안전성은 다음과 같은 사실이 즉 n이 2개부호(프라임)의 산물이라면, 그 때 사각 근원 모드 n을 계산할 수 있는 능력이 벡터 n에 대한 능력과 계산 수치상으로 동등하다는 것에 달려있다. OPI는 리플레이 공격, 프리플레이 공격, 맨인더미들 공격, 엿듣는 공격, 오프라인 사전적 공격, 서버 협상 그리고 서버협상 후에 오프라인 사전적 공격들과 같은 잘 알려진 공격에 대해서도 안전하다. OPI와 도전 반응 신분확인 프로토콜과 ZK(Zero Knowledge) 근본

신분확인 프로토콜을 비교하여볼 때, OPI는 패스워드를 소유하지만 키는 사용하지 않는다. 그리고 OPI 패스의 숫자는 하나이다. 오로지 OPI와 ZK 근본 신분확인 도식을 비교하여보면, OPI는 승인자가 확인자에 의해 직접적으로 재사용하게 하는 것을 막고 있다는 것을 또한 만족 시킨다.

OPI와 ZK 신분확인 아이디어를 비교하여보면, OPI는 내부 교류 증거를 사용하지 않고 있으며, 해커가 승인자를 성공적으로 의인화 할 확률은 ZK 신분확인 도식의 확률에 대해서 동등하지는 않다.

2. OPI: One Pass Identification

이 논문에서는 신분확인 도식을 제시하고자 하는 것이다. 즉 (1)은 승인자에 의해 입력되어진 비밀 정보를 소유하고 있고, (2)는 많은 패스들을 최소화 시키고 있고, 그리고 (3)는 잘 알려진 공격들에 대해 (4)가 안전하도록 보전하게하고 (5)가 승인자의 확인에 소요되는 시간적인 면을 아주 훌륭히 이행하도록 하는 동안에 키를 필요하지 않는다. 다음에서 언급된 OPI는 승인자가 그의 패스워드를 입력할 때 실행되어진다.

Protocol: OPI

(1) 시스템 매개변수: 신뢰된 센터는 n이 벡터에 대해 계산 수치상으로 불가능하게 한 p와 q의 두 비밀부호를 선택한 후에 일반적인 모듈 n=pq를 모든 사용자들에게 발행을 한다.

(2) 승인자 매개변수들의 선택: 승인자는 임의의 정수 $X_{1i}(1 \le X_{1i} \le n-1)$를 선택하고 i가 시스템 원천에 대한 i 번째 접근을 나타내주는 곳인 타임 스템프 T_i를 획득한다. 승인자는 $X_{2i} \equiv (pwd-X_{1i})$ 계수n인 X_{2i}를 결정한다.

(3) 확인자의 패스워드 파일에 저장되어진 매개변수: Y_1^2 계수 n과 Y_2는 $Y_1(1 \le Y_1 \le n-1)$가 무작위로 그리고 $Y_2 \equiv (pwd-Y_1)$계수 n에서 선택되어진 곳에 저장되어진다.

(4) 프로토콜 메시지: 승인자는 확인자에게 T_i, X_{2i} 그리고 $(X_{1i}+T_i)^2 \bmod n$을 보낸다.

(5) 프로토콜 액션: 만약 다음의 등식(Equ.) 1이 유지된다면, 확인자가 승인자의 신분을 받아들인다. $C^2 \bmod n=(4(Y_1^2 \bmod n)(X_{1i}+T_i)^2 \bmod n) \bmod n$ 있는 곳이며 $C=((X_{1i}+T_i)^2+Y_1^2-(X_{2i}^2+Y_2^2+T_i^2)+(2X_{2i}Y_2+2X_{2i}Ti-2Y_2T_i))$ 등식 1.

OPI가 승인자에게 시스템 리소스를 점유하도록 허락하는지 그리고 공격자가 승인자를 의인화하는지, 그런 후에 전자는 Theorem 1에서 나타난 반면 후자는 섹션 3에서 언급이 되어지는지를 보여주어야 한다.

Theorem 1 확인자는 승인자가 OPI에서 시스템 리소스를 접할 수 있도록 허용한다.

Proof $X_{2i} \equiv (pwd-X_{1i}) \bmod n$ 과 $Y_2 \equiv (pwd-Y_1) \bmod n$이기 때문에 $(X_{1i}-Y_1+T_i)^2 \bmod n=(X_{2i}-Y_2+T_i)^2 \bmod n$이다. 따라서 $C \bmod n=2Y_1(X_{1i}+T_i) \bmod n$ 있는 곳에 $C=((X_{1i}+T_i)^2 \bmod n)+(Y_1^2 \bmod n)-(X_{2i}^2+Y_2^2+T_i^2)+(2X_{2i}Y_2+2X_{2i}T_i-2Y_2T_i))$이다. 확인자는 T_i, X_{2i} 그리고 $(X_{1i}+T_i)^2 \bmod n$을 승인자로부터 받으며 $Y_1^2 \bmod n$과 Y_2를 패스워드 파일에 저장한다. 그 결과 확인자는 C를 계산할 수 있다. 따라서 확인자는 만약 $C^2 \bmod n=(4(Y_1^2 \bmod n)(X_{1i}+T_i)^2 \bmod n) \bmod n$이 된다면, 확인자는 승인자가 pwd를 입력한 것으로 확신하기 때문에 승인자에게 시스템 리소스를 접속하도록 허용하게 된다.

3. OPI의 분석

3.1 안전성

사각 근원 modulo n(SQROOT) 문제는 주어진 합성 정수 n과 정방형의 잔여분 a modulo n에 대한 a modulo n의 사각 근원을 발견하는 것이다. 인수 p와 q가 알려진다면, 그 때 SQROOT 문제는 다명의 시간에서 해결될 것이다. 인수 p와 q가 알려지지 않는다면, 그 때는 n의 인수적 문제가 다명의 시간에서 SQROOT 문제에 처해지게 될 것이다. 그리고 n의 인수적 문제는

NP-complete 될 것이다.

Property 2 n=pq, 그리고 두 부호(수) p와 q가 n이 인수에 대해 계산상으로 불가능한 것으로 선택되어지게 한다. 그런 다음, 주어진 t, 정방형의 잔여분 a module n과 n에 대한 $(x+t)^2$ mod n에서 x를 발견하는 문제는 NP-complete이라는 것이다.

주어진 합성정수 n과 정방형의 잔여분 a modulo n에 대한 a modulo n의 사각 근원을 발견하는 문제가 주어진 t, 정방형의 잔여분 a module n과 n에 대한 $(x+t)^2$ mod n에서 x를 발견하는 문제의 특별한 경우이기 때문에 위의 property가 진실이라는 것을 쉽게 알 수 있다. 이런 이유 때문에 OPI의 안전성이 property 2 결론에 이르게 될 때, 공격자들에 대항하여 안전하다는 것을 입증할 것이다.

OPI에서 X_{1i}와 pwd의 두 비밀 정보가 존재한다. 그러나 불완전한 채널과 확인자에게 있는 비밀 정보는 X_{1i}이다. 우리는 어떻게 신분확인 도식이 공격자가 다음의 온라인상 사전적 공격위에서 pwd를 습득 하려는 시도를 방지해 가는지를 기술 하려고 한다. 또한 OPI가 온라인상 사전적 공격을 제외하고 잘 알려진 공격들에 대해 안전하다는 것을 보여줄 것이다.

(1) 리플레이 공격에서, 공격자는 과거의 의사교환에서 보내진 그리고 후에 그것들을 다시 보내는 메시지를 기록합니다. 승인자가 단지 X_{2i}와 $X_1^2{}_i$ mod n을 보냈다고 가정한다. 그때, 승인자는 X_{1i}가 무작위로 선택되어졌기 때문에 확인자에게 상이한 시간 매개변수를 보낸다. 그러나 공격자가 $2 \le i$와 $j \le i$에 대해 X_{2i}와 $X_1^2{}_i$ 처럼 X_{2j}와 $X_1^2{}_j$ mod n을 다시 보냈을 때, 확인자가 공격자에게 시스템 리소스를 접할 수 있도록 허용한다. 타임 스템프 T_i는 $2 \le i$와 $j<i$에 대해 $T_j \neq T_i$이기 때문에 T_i의 재사용을 방지한다. 이런 이유 때문에 OPI는 리플레이 공격에 대해서는 안전하다.

(2) 프리 프레이 공격에 있어서, 공격자는 과거 커뮤니케이션에서 보내졌던 메시지를 기록하고 기록된 메시지에서 현재의 메시지들을 결정한다. 승인자가 T_j, X_{2j}와 $X_1^2{}_j$ mod n을 보내는 것을 가정한다. 그렇게 되면, 공격자가 $2 \le i$와 $j \le i$에 대해 T_j, X_{2j}와 $X_1^2{}_j$ mod n,을 보냈을 때, 공격자가 T_i를 결정할 수 있기 때문에 확인자가 공격자에게 시스템 리소스를 접근하도록 허용 할 것이다.

(3) 엿듣는 것에서, 공격자는 라인 상의 메시지를 엿듣는 수 있고 진행되어지고 있는 커뮤니케이션으로부터 약간의 유용한 정보를 빼려고 시도한다. 공격자가 $2 \le i$와 $j \le i$에 대해 T_i, X_{2j} 그리고 $(X_{1i}+T_j)^2$ mod n으로부터 T_i, X_{2i} 그리고 $(X_{1i}+T_i)^2$ mod n에서 X_{1i}를 배우려고 시도할 때, $(X_{1j}+Tj)^2$ mod n으로부터 유용한 정보 X_{1j}를 배우려는 어려움은 Property 2에 달려있다. 따라서 OPI는 엿듣는 것으로부터 안전하다.

(4) 중간자 공격에서, 공격자는 무리들 사이에서 보내진 메시지를 가로채고 공격자 자신의 메시지들로 교체합니다. 공격은 이것이 서버에 보내는 메시지에서 승인자 역할을 한다. 중간자 공격에 대한 안전성은 OPI 패스의 숫자는 하나이기 때문에 엿듣는 것에 대한 OPI의 안전성과 같다. 그리고 공격자는 T_i, X_{2j} 그리고 $(X_{1i}+T_j)^2$ mod n에서 X_{1i}를 그의 자신의 메시지로 교체해야 할 X_{1j}를 결정하여야 한다. 따라서 OPI는 중간자 공격에 대항하여 안전하다.

(5) 패스워드 추측 공격에서, 공격자는 패스워드의 일반적 선택을 가지고 있는 상대적으로 작은 사전에 대한 접근을 갖고 있다고 가정한다. 거기에는 공격자가 온라인 사전적 공격과 오프라인 사전적 공격이 될 사전을 사용할 수 있는 우선적으로 두 가지 방법이 존재한다. 온라인 사전적 공격에서, 공격자는 반복적으로 사전에서 패스워드를 선택하고 사용자로 의인화하기 위해 이 것을 사용하려고 시도 한다. 만약 이런 의인화가 실패한다면, 공격자는 사전으로부터 이 패

스워드를 제거하고 다른 패스워드를 사용하면서 다시 시도할 것이다. 실질적으로 그와 같은 온라인 사전적 공격을 막을 수 있는 표준적 방법들은 패스워드가 만료되기 전에 갖는 사용자가 실패하는 숫자를 제한하여 사용하게 하거나 혹은 사용자가 로그인 시도를 하는데 허용되어지는 비율을 줄이는 방법들이다.

(6) 서버 협상은 확인자가 승인자를 의인화한다면 신분확인 도식에 대해 가능하게 한다. OPI에서 확인자는 Y_1^2 mod n과 Y_2를 저장해왔다. 그러나 Y_1^2 mod n로부터 Y_1를 결정하는 것은 NP-complete 문제이다. 따라서 OPI는 서버 협상에 대해서도 안전하다.

3.2 실행(Performance)

(1)OPI 패스워드의 숫자는 하나이다. 패스워드들의 숫자는 트래픽 오버헤드와 연관이 있고 트래픽 오버해드는 직접적으로 신분확인 도식이 상업적으로 사용되어질 수 있는가와 연관이 있다. (2)OPI는 키를 필요하지 않다. 신분확인 도식은 그것이 키를 필요로 한다면 또 다른 문제를 갖게 된다. 예를 들자면, 친숙한 키를 사용한 신분확인 도식은 친숙한 키를 분배하는데 있어서 기술적인 면을 필요로 할 것이다. (3)OPI는 승인자에 의해 입력되어진 패스워드를 소유하고 있다. 승인자는 신분 확인 도식이 패스워드를 소유하고 있지 않다면, 그가 사용하는 모든 시스템에 그의 비밀 정보를 저장하여야만 한다.

승인자는 하나의 모듈 곱셈 $(X_{1i}+T_i)^2$ mod n을 실행한다. 확인자가 오프라인 상태에서 Y_1^2 mod n을 계산하고 승인자로부터 $(X_{1i}+T_i)^2$ mod n을 받을 수 있기 때문에 확인자는 온라인 상태에서의 등식 1에서 우변의 결과를 획득할 수 있는 하나의 모듈 곱셈을 실행한다. 그리고 또한, 확인자는 등식 1에서 좌변의 결과를 얻을 수 있는 세 개의 사각 곱셈과 세 개의 곱셈 그리고 하나의 모듈 곱셈을 실행한 후에 등식 1에서 C를 얻을 수 있는 하나의 모듈 덧셈을 실행한다.

4. 결론

OPI라고 불리는 새로운 신분확인 도식에 대해 안전성은 SQROOT 문제를 기본으로 하고 있다. OPI는 프리 플레이공격, 오프라인 사전적 공격 그리고 서버 협상에 대해서 안전하다. OPI 패스워드의 숫자는 하나이고 패스워드를 소유하고 있을 뿐이지 키를 사용하고 있지 않다. OPI가 승인자를 확인하는데 소요하는 시간에 대해서 특출하다고 생각하며 문제점에 대한 연구를 진행할 것이다.

참고문헌

[1]E. Moulines, P. Duhamel, J.F. Cardoso, and S. Mayrargue, *Subspace methods for the blind* ***identification*** of multichannel fir filters, IEEE Transactions on Signal Processing, SP-43 (1995), pp. 516--525.

[2]Bensaid, B. and R.J. Gary-Bobo (1996), *"An Exact Formula for the Lion's Share: A Model of* ***Pre*****-Play** Negotiation," Games and Economic Behavior, 14, pp 44-89.

[3]A. W. Senior and A. J. Robinson. *An* ***off*****-line** cursive handwriting recognition system. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3):309--321, 1998.

[4]Neil Haller. The s/key(tm) **one-timepassword** system. *Symposium on Network and Distributed System Security*, pages 151--157, February 1994.