한 단계로 신원확인을 위한 패스워드

김용훈* · 조범준*

One-Pass Identification Processing Password

Yong-Hun Kim* · Beom-Joon Cho*

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 방법으로 일회용 패스워드, Challenge-Response 인증 방식이 유용하게 사용되며, 클라이언트/서버 환경에서는 별도 동기가 필요 없는 시간을 이용한 일회용 패스워드 방식이 특히 유용하게 사용될 수 있다. 안전성은 Square root problem에 기초를 두고 있고, 프리플레이 공격, 오프라인 사전적 공격 그리고 서버 등을 포함하여 지금까지 잘 알려진 공격들에 대해서 안전성을 높이기 위한 OPI(One Pass Identification)을 제안한다. OPI는 패스워드를 생성하는데 특별한 키를 생성할 필요가 없다는 것이다. OPI는 승인된 자를 확인된 데 걸리는 시간이 적게 소요되면서 뛰어났다.

ABSTRACT

Almost all network systems provide an authentication mechanism based on user ID and password. In such system, it is easy to obtain the user password using a sniffer program with illegal eavesdropping. The one-time password and challenge-response method are useful authentication schemes that protect the user passwords against eavesdropping. In client/server environments, the one-time password scheme using time is especially useful because it solves the synchronization problem. It is the stability that is based on Square Root Problem, and we would like to suggest OPI(One Pass Identification), enhancing the stability, for all of the well-known attacks by now including Free-playing attack, Off-line Literal attack, Server and so on. OPI does not need to create the special key to read the password. OPI is very excellent in identifying the approved person within a very short time.

키워드
Identification, Pre-Play Attack, Off-Line Dictionary Attack, Server Comprise

Ⅰ. 서 론

신원조회는 관리자가 사용자의 신원에 관하여 다른 사람처럼 되어지는 것을 막고 명확히 확신시켜주는 과정이다[1],[2]. 패스워드 시스템의 장점들은 즉 쉬운 실행, 낮은 가격 그리고 사용능력들 때문에 가장 널리 사용되어지는 신원확인 체계이다. 패스워드 시스템에서 보호되어져야만 하는 공격(해킹)들은 다음을 포함한다. 즉 시스템 외부에서의 패스워드 노출, 시스템 안에서 라인 상에 엿듣기, 그리고 둘 모두는 연속적인 리플레이 공격을 허용하고, 오프라인 상의 사전적 공격을 포함한 패스워드 추측 등이다[5],[6]. 여러 기법의 기술들은 패스워드 시스템의 안전성을 증진시킬 수 있다는

*조선대학교
접수일자 : 2005. 1. 6

것을 대변하여 왔었다. 그러나 어떤 기법 기술이 서버 협상이후 리플레이 공격 혹은 프리플레이 공격[3],[4]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[7],[8].

본 논문에서는 OPI라고 하는 새로운 신원확인 도식을 제안한다. OPI의 안전성은 다음과 같은 사실이 즉 n이 두 소수의 산물이라면, 그 때 제곱근 모드 n을 계산할 수 있는 능력이 인수 n에 대한 능력과 계산 수치상으로 동등하다는 것에 달려 있다. OPI는 리플레이 공격, 프리플레이 공격, Man- in-the-middle 공격, 엿듣는 공격, 오프라인 사전적 공격, 서버협상 그리고 서버협상 후에 오프라인 사전적 공격들과 같은 잘 알려진 공격에 대해서도 안전하다. OPI는 challenge response 신원확인 프로토콜과 ZK(Zero Knowledge) 근본 신원확인 프로토콜을 비교하여볼 때, OPI는 패스워드를 소유하지만 키는 사용하지 않는다. 그리고 OPI 패스의 숫자는 하나이다. 오로지 OPI와 ZK근본 신원확인 도식을 비교하여 보면, OPI는 사용자가 관리자에 의해 직접적으로 재사용하게 하는 것을 막고 있다는 것을 또한 만족시킨다.

OPI와 ZK근본 신원확인 아이디어를 비교하여보면, OPI는 대화식 증명을 사용하지 않고 있으며, 해커가 사용자를 성공적으로 의인화 할 확률은 ZK 근본 신원확인 도식의 확률에 대해서 동등하지 않다.

II. 관련연구

패스워드 시스템 보안의 위협이란 사용자의 패스워드가 불법적으로 노출되는 것을 말한다. 시스템에 불법 침입하려는 자는 아래의 네 가지 방법으로 사용자의 패스워드를 알아낼 수 있다.

첫째, 시스템의 패스워드 파일을 읽어내는 방법이 있다. 패스워드 파일은 사용자들의 패스워드와 식별자를 저장한 파일로서 만약 노출되면 시스템과 모든 사용자들의 자료는 위험에 빠지게 된다. 따라서 패스워드파일은 일반 사용자에게 접근을 제한하며 오직 보안 관리자만이 권리를 갖게 한다. 그러나 시스템의 고장이 생겨 일반 사용자들도 패스워드 파일에 접근 가능하다거나 보안 관리자가 불순한 마음을 품었을 때에는 이와 같은 패스워드 시스템은 전혀 안전하지 못하다. 보다 확실한 방법은 패스워드를 일방함수를 사용하여 그 결과를 식별자와 함께 파일에 저장하여 패스워드 파일이 노출되어도 안전을 유지하게 하는 것이다. 이 방법은 입력된 패스워드에 일방함수를 적용하여 그 결과를 저장된 것과 비교함으로써 사용자의 인증을 한다.

둘째, 사용자와 시스템 간에 패스워드를 주고받는 통신을 도청할 수 있다. 통신회선의 도청은 엿듣기만 하는 수동적 라인 태핑(passive line tapping)과 적극적 라인 태핑(active line tapping)이 있다. 만약 보안 관리자가 패스워드 시스템의 도청의 위험이 크다고 판정하면 통신되는 패스워드는 입력 장소에서 암호화되어 비교 장소까지 전달되는 방법을 취해야 한다[9],[10].

셋째, 패스워드가 부주의하게 만들어져 쉽게 추측할 수 있는 경우이다. 실제로 사용자들은 자신들과 연관되거나 흔히 사용하는 단어를 패스워드로 선택하는 경우가 많으므로 패스워드의 추측이 용이한 경우가 많다. 패스워드의 추측을 어렵게 하려면 사용자가 보다 무작위로 선택하거나 자동으로 시스템에서 패스워드를 무작위로 골라주는 방법이 있다[7],[8].

넷째, 사용자가 입력하는 것을 직접 보고 확인하는 방법이 있다. 이 방법은 가장 확실하게 패스워드를 알아낼 수 있는 방법이다. 하지만 이 방법은 사용자가 긴 패스워드를 사용하고, 빠르게 입력한다면 충분히 예방이 가능한 방법이다[11].

본 논문에서는 이러한 두 번째의 문제를 해결하기 위한 방법으로 OPI를 제안한다.

III. OPI: One Pass Identification

본 논문에서는 신원확인 도식을 제시하고자 한다. 즉 (1)은 사용자에 의해 입력 되어진 비밀 정보를 소유하고 있고, (2)는 많은 패스들을 최소화 시키고 있고, 그리고 (3)는 잘 알려진 공격들에 대해 (4)가 안전하도록 보전하게 하고 (5)가 사용자의 확인에 소요되는 시간적인 면을 아주 훌륭히 이행하도록 하는 동안에 키를 필요로 하지 않는다. 다음에서 언급된 OPI는 사용자가 그의 패스워드를 입력할 때 실행되어진다.

1. Protocol: OPI

(1) 시스템 매개변수: 신뢰된 중심은 n이 인수에 대해 계산 수치상으로 불가능하게 한 p와 q의 두 비밀 소수를 선택한 후에 일반적인 modulus n=pq를 모든 사용자들에게 발행을

한다.

(2) 사용자들 매개변수들의 선택: 사용자는 임의의 정수 $X_{1i}(1 \le X_{1i} \le n-1)$를 선택하고 i가 시스템 원천에 대한 i 번째 접근을 나타내주는 곳인 time stamp T_i를 획득한다. 사용자는 $X_{2i} \equiv (pwd-X_{1i}) \bmod n$인 X_{2i}를 결정한다.

(3) 관리자의 패스워드 파일에 저장되어진 매개변수: $Y_1^2 \bmod n$과 Y_2는 $Y_1(1 \le Y_1 \le n-1)$가 무작위로 그리고 $Y_2 \equiv (pwd-Y_1) \bmod n$에서 선택되어진 곳에 저장된다.

(4) protocol message: 사용자는 관리자에게 T_i, X_{2i} 그리고 $(X_{1i}+T_i)^2 \bmod n$을 보낸다.

(5) protocol action: 만약 다음의 식 (1)이 유지된다면, 관리자가 사용자의 신원을 받아들인다. $C^2 \bmod n=(4(Y_1^2 \bmod n)(X_{1i}+T_i)^2 \bmod n) \bmod n$이 있는 곳이며

$$C=((X_{1i}+T_i)^2+Y_1^2-(X_{2i}^2+Y_2^2+T_i^2)+(2X_{2i}Y_2+2X_{2i}Ti-2Y_2T_i)) \quad (1)$$

OPI가 사용자에게 시스템 자원을 점유하도록 허락하는지 그리고 공격자가 사용자를 의인화하는지, 그런 후에 전자는 Theorem 1에서 나타난 반면 후자는 섹션 4에서 보여준다.

Theorem 1 관리자는 사용자가 OPI에서 시스템 자원을 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. 관리자는 T_i, X_{2i} 그리고 $(X_{1i}+T_i)^2 \bmod n$을 사용자로부터 받으며 $Y_1^2 \bmod n$과 Y_2를 패스워드 파일에 저장한다. 그 결과 관리자는 C를 계산할 수 있다. 따라서 관리자는 만약 $C^2 \bmod n=(4(Y_1^2 \bmod n)(X_{1i}+T_i)^2 \bmod n) \bmod n$이 된다면, 관리자는 사용자가 pwd를 입력한 것으로 확신하기 때문에 사용자에게 시스템 자원에 접속하도록 허용하게 된다.

IV. OPI의 분석

1. 안전성

제곱근 modulo n(SQROOT) 문제는 주어진 합성 정수 n과 정방형의 잔여분 a modulo n에 대한 a modulo n의 제곱근을 발견하는 것이다. 인수 p와 q가 알려진다면, 그 때 SQROOT 문제는 다항식의 시간에서 해결될 것이다. 인수 p와 q가 알려지지 않는다면, 그 때는 n의 인수적 문제가 다항식의 시간에서 SQROOT 문제에 처해지게 될 것이다. 그리고 n의 소인수적 문제는 NP-complete 될 것이다.

Property

n=pq, 그리고 두 인수 p와 q가 n이 인수에 대해 계산상으로 불가능한 것으로 선택되어지게 한다. 그런 다음, 주어진 t, 정방형의 잔여분 a module n과 n에 대한 $(x+t)^2 \bmod n$에서 x를 발견하는 문제는 NP-complete 이다.

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

OPI에서 X_{1i}와 pwd의 두 비밀 정보가 존재한다. 그러나 불완전한 채널과 관리자에게 있는 비밀 정보는 X_{1i}이다. 본 논문은 신원확인 도식이 공격자가 다음의 온라인상 사전적 공격에서 pwd를 습득하려는 시도를 방지해 가는지를 기술한다. 또한 OPI가 온라인상 사전적 공격을 제외하고, 잘 알려진 공격들에 대해서 안전하다는 것을 보여줄 것이다.

1) Replay Attack

공격자는 과거에 이루어졌던 통신상에서 보내진 메시지를 기록하고, 그것을 후에 다시 그들에게 보낸다. 사용자가 단지 X_{2i}와 $X_1^2{}_i \bmod n$을 보냈다고 가정한다. 그때, 사용자는 X_{1i}가 무작위로 선택되어졌기 때문에 관리자에게 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 $X_1^2{}_j \bmod n$을 다시 보냈을 때, 관리자가 공격자에게 시스템 자원을 접할 수 있도록 허용한다. time stamp T_i는 $2 \le i$와 $j<i$에 대해 $T_j \ne T_i$이기 때문에 T_i의 재사용을 방지한다. 이런 이유 때문에 OPI는 리플레이 공격에 대해서 안전하다.

2) Pre-play Attack

공격자는 과거 통신상에서 보내졌던 메시지를 기록하고 기록된 메시지에서 현재의 메시지들을 결정한다. 사용자가 T_j, X_{2j}와 $X_1^2{}_j \bmod n$을 보내는 것을 가정한다. 그렇게 되면, 공격자가 $2 \le i$와 $j \le i$에 대해 T_j, X_{2j}와 $X_1^2{}_j \bmod n$,을 보냈을 때, 공격자가 T_i를 결정할 수 있기 때문에 관리자가 공격자에

게 시스템 자원을 접근하도록 허용할 것이다. 그 두 경우에 있어서 프리프레이 공격에 대한 OPI의 안전성을 숙고해야 한다. 즉 공격자가 (a) $(X_{1i}+T_i)^2$ mod n, (b) $2 \le i$와 $j \le i$에 대해 T_j, X_{2j}와 $(X_{1j}+T_j)^2$ mod n에 대한 $(X_{1i}+T_i)^2$ mod n이다.

(a)의 경우에 있어서, 공격자는 T_j, T_i, X_{2j} 그리고 $(X_{1i}+X_{2i})$ mod n을 알게 되고 X_{2i}를 결정하게 된다. 또한 $(X_{1j}+T_j)$ mod n=$(X_{1i}+X_{2j})$ mod n과 Ti=Tj+T와 같은 T를 알게 된다. 그러면 공격자는 X_{2i}를 선택하게 되고 $(X_{1j}-X_{1i})$ mod n=$(X_{2i}-X_{2j})$ mod n을 얻게 된다. $X_{1i}=(X_{1j}-D)$ mod n이 되도록 한다. 공격자가 Tj+T, X_{2i}와 $((X_{1j}-D)+(Tj+T))^2$ mod n에서 $((X_{1j}-D)+(Tj+T))^2$ mod n을 결정하는 것이 가능한 지를 숙고해야 한다. 공격자는 D1=(X1i+Tj)2 mod n, D2=(D-t)와 D3= (D-t)2-2Tj(D-1)가 되는 곳인, $(D_1-2X_{1j}D_2+D_3)$ mod n=$((X_{1j}-D)+(Tj+T))^2$에서 D1 mod n과 D3 mod n을 결정할 수 있다. 그러나 $(D_1-2X_{1j}D_2+D_3)$ mod n에서 $2X_{1j}$ D_2를 찾는 어려움은 Property에 달려있다. (b)의 경우에 있어서, 공격자는 T_j, T_i, X_{2j} 그리고 $(X_{1i}+T_j)^2$ mod n을 알게 된다. 공격자는 $T=T_i-T_j$와 $E=2T_j+T^2$인 $(D_1-2X_{1j}T+E)$ mod n=$(X_{1j}+(Tj+T))^2$에서 D1 mod n과 E mod n을 결정할 수 있다. 그리고 D1은 (a) 경우와 같다. 그러나 $(D_1-2X_{1j}T+E)$ mod n에서 $2X_{1j}T$를 발견하는 어려움은 Property에 달려있다. 따라서 OPI는 (a)와 (b)의 경우에 있어서 프리플레이 공격에 대해서 안전하다.

3) Eavesdropping Attack

공격자는 라인 상의 메시지를 엿듣는 수가 있고, 진행되어지고 있는 통신으로부터 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 알려고 시도할 때, $(X_{1j}+Tj)^2$ mod n으로부터 유용한 정보 X_{1j}를 아는 어려움은 Property에 달려있다. 따라서 OPI는 엿듣는 것에 대해서 안전하다.

4) Man-in-the-Middle Attack

공격자는 집단들 사이에 보내진 메시지를 가로채고, 그것을 공격자들 자신의 메시지들로 교체한다. 공격은 이것이 서버에 보내는 메시지에서 사용자 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 대해서 안전하다.

5) Password Guessing Attack

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 이것을 사용하려고 시도한다. 만약 이런 의인화가 실패한다면, 공격자는 사전으로부터 이 패스워드를 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. 오프라인 사전적 공격에서, 공격자는 과거 통신을 기록하고 그런 다음 사전에 기록되어진 통신과 함께 일치하는 패스워드를 찾는다. 만약 같은 패스워드를 발견한다면, 공격자는 공격 패스워드라고 결론지을 것이다. OPI의 가능한 오프라인 사전적 공격을 위해서는 공격자가 기록되어진 통신과 일치하는 패스워드를 찾기 이전에 유지하여야 한다. 거기에는 사용자가 무작위로 그리고 $1 \le X_{1i} \le n-1$에서 X_{1i}를 선택하기 때문에 pwd에 대한 2^{n-1} 가능성이 존재하게 된다. 또한 n은 n이 계산상으로 요소에 대해 실행 불가능한 어떤 크기로 구성되어 있기 때문에 2^{n-1} 기록을 저장하는 것이 비실용적이다. 따라서 OPI는 오프라인 사전적 공격에 대해서 안전하다.

6) Server Compromise

관리자가 사용자를 의인화한다면 신원확인 도식에 대해 가능하게 한다. OPI에서 관리자는 Y_1^2 mod n과 Y_2를 저장해왔다. 그러나 Y_1^2 mod n으로부터 Y_1를 결정하는 것은 NP-complete 문제이다. 따라서 OPI는 서버 협상에 대해서 안전하다.

2. 실행(Performance)

(1) OPI 패스워드의 숫자는 하나이다. 패스워드들의 숫자는 트래픽 오버헤드와 연관이 있고 트래픽 오버헤드는 직접적으로 신원확인 도식이 상업적으로 사용되어질 수 있는가와 연관이 있다.

(2) OPI는 키를 필요로 하지 않다. 신원확인 도식은 그것이 키를 필요로 한다면 또 다른 문제를 갖게 된다. 예를 들자면, 친숙한 키를 사용한 신원확인 도식은 친숙한 키를 분배하는데 있어

서 기술적인 면을 필요로 할 것이다.

(3) OPI는 사용자에 의해 입력되어진 패스워드를 소유하고 있다. 사용자는 신원 확인 도식이 패스워드를 소유하고 있지 않다면, 그가 사용하는 모든 시스템에 그의 비밀 정보를 저장하여야만 한다.

사용자는 하나의 modular 곱셈 $(X_{1i}+T_i)^2$ mod n을 실행한다. 관리자가 오프라인 상태에서 Y_1^2 mod n을 계산하고 사용자로부터 $(X_{1i}+T_i)^2$ mod n을 받을 수 있기 때문에 관리자는 온라인상에서의 식 (1)에서 우변의 결과를 획득할 수 있는 하나의 modular 곱셈을 실행한다. 그리고 또한, 관리자는 식 (1)에서 좌변의 결과를 얻을 수 있는 세 개의 제곱 곱셈과 세 개의 곱셈 그리고 하나의 modular 곱셈을 실행한 후에 식 (1)에서 C를 얻을 수 있는 하나의 modular 덧셈을 실행한다. 표 1에서 OPI에서 실행된 조작된 숫자를 함축한다.

표 1. OPI에서 실행된 조작된 숫자
Table 1. Summarization of the number of the operations

사용자	관리자 (오프라인 상태)	관리자(온라인 상태)
modular 제곱곱셈: 1	modular 제곱곱셈: 1	제곱곱셈 : 3 곱셈 : 3 modular 덧셈 : 1 modular 제곱곱셈 : 1

V. 결 론

OPI라고 불리는 새로운 신원확인 도식에 대해 안전성은 SQROOT 문제를 기본으로 하고 있다. OPI는 프리플레이공격, 오프라인 사전적 공격 그리고 서버 협상에 대해서 안전하다. OPI 패스워드의 숫자는 하나이고 패스워드를 소유하고 있을 뿐이지 키를 사용하고 있지 않다. OPI는 사용자를 확인하는데, 소요하는 시간에 대해서 평균적으로 60%정도 단축되었으며, 향후 안전성과 시간 단축에 대한 연구가 필요할 것이다.

참고문헌

[1] A. Hill, A. D. Brett, and C. J. Taylor, "Automatic landmark identification using a new method of non-rigid correspondence" in Proceedings of IPMI '97 Conference, vol. 1230, pp. 483-488, 1997.

[2] 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, pp. 516-525, 1995.

[3] J. Andreoni, and H. Varian, "Pre-play Contracting in the Prisoners' Dilemma", mimeo, University of Wisconsin, 1999.

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

[5] Bao, F., R. Deng and W. Mao. Efficient and practical fair exchange protocols with off-line TTP. 1998 IEEE Symposium on Security and Privacy. Oakland, IEEE Compute Society. pp. 77-85. 1998.

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

[7] Neil Haller. The s/key(tm) one-time password system. In Proceedings of the 1994 Symposium on Network and Distributed System Security, pp.151-157, 1994.

[8] Neil Haller. The s/key(tm) one-time password system. Symposium on Network and Distributed System Security, pp.151-157, February 1994.

[9] 박중길, 장태주, 박봉주, 류재철, "시간을 이용한 효율적인 일회용 패스워드 알고리즘", 한국정보처리학회 논문지, 제8-c권 제4호, pp.373-378, 2001.

[10] 양대헌, 이석준, "무선 인터넷을 위한 패스워드 기반의 인증 및 키 교환 프로토콜", 한국정보과학회 논문지, 제29권 제3호, pp.324-332, 2002.

[11] 박종민, 김용훈, 조범준, "타인의 관찰에서 안전한 패스워드 시스템", 한국해양정보통신학회 논문지, 제8권 제8호, pp.1790-1795, 2004.

김용훈(Yong-Hun Kim)

2000년 전남대학교 교육대학원 졸업 (교육학석사)
2005년 조선대학교 컴퓨터공학과 박사과정
※관심분야 : 패턴인식, 인공지능, 정보보호 및 보안

조범준(Beom-Joon Cho)

1980년 조선대학교 전기공학과(공학사)
1988년 한양대학교 전기공학과(공학박사)
2004년 한국과학기술원 전자전산학과(공학박사)
1980년~ 현재 조선대학교 전자정보공과대학 컴퓨터공학부교수
2002년~ 현재 한국멀티미디어학회 부회장
※관심분야 : 인공지능, 패턴인식, 뉴로컴퓨터