인간이 기억할 수 있는 패스워드를 이용한 안전한 키교환

김성학*, 이정배, 서광석, 임종인

*전북대학교 정보통신연구소, 전북대학교 수학과, 한국정보보호교육센터,
정보보호기술연구센터(CIST)

Secure Key Exchange Using Human-Memorable Password

Sung-Hak Kim*, Jung-Bae Lee, Kwang-Suk Suh, Jong-In Lim

*Dept. of Inform. and Comm. Eng. Institute of Inform. and Comm. Chonbuk University, Dept. of Mathematics. Chonbuk University, Korea Information Security Education Center(KISEC), Center for Information Security Technologies(CIST)

요 약

패스워드는 가장 광범위한 인증의 수단으로 사용되어지고 있다. 안전성 측면에서는 패스워드의 길이가 길수록 안전하고 Dictionary Attack 등에 강할 것이다. 그러나, 긴 패스워드를 기억하고 있는 것은 어려운 일이다. 또한, 하나 이상의 패스워드가 필요한 경우 현실적으로 긴 패스워드를 모두 기억하고 있는 것은 현실적으로 불가능, 혹은 어려운 일이다. 또한, 인터넷 보안을 위한 비밀성을 보장하기 위해서 블록암호알고리즘을 사용하고 있다. 공개키보다 빠른 연산속도를 가지고 있고, 키 분배의 문제를 해결한다면 안전한 인터넷을 이용할 수 있을 것이다. 따라서, 본 논문에서는 짧은 패스워드를 이용하여 키 분배를 이루는 프로토콜을 제안한다. 또한 공격에 강한 알고리즘을 위해서 본 논문에서는 Signcryption 알고리즘을 이용하여 짧은 패스워드를 가지고 키분배를 하고, Dictionary Attack에 강한 알고리즘을 설계한다.

I. 서론

인터넷을 통한 전자상거래는 현재 많이 사용하고 있는 실생활의 상거래보다 편리함과 유용성을 가지고 있어서 사용자 수가 급증하고 있다. 이런 과정에서 거래 상호간에 인증 및 안전한 정보 교환을 위한 안전한 시스템이 필요하게 되었다. 우리는 인터넷을 통해서 패스워드를 이용한 인증을 하는 것을 많이 경험했을 것이다. 특히, 짧은 패스워드를 통한 인증 방법은 안전성에 문제가 있지만 편리성 때문에 지금도 많이 이용되고 있다. 또한, 인증 뿐 만이 아니고 전자상거래에서 상호간에 안전한 정보 교환이 이루어져야 한다. 따라서, 대칭키 암호 알고리즘을 사용한다면 상호간에 비밀키의 분배가 선행되어야 한다. 본 논문에서는 대칭키 암호 알고리즘을 위한 키분배에 초점을 맞추고 있다.

잘 알려진 키분배 프로토콜은 DH(Diffie-Hellman) 프로토콜이 있다. 이것은 공개키를 이용한 방법으로 공개키의 인프라가 필요하고 계산량이 많다. 짧은 패스워드를 이용한다면 이는 Dictionary attack에 취약성을 보이고 있기 때문에 이를 개선하는 방법이 필요하다.

S. Bellovin and M. Merritt에 의해서 패스워드를 이용한 프로토콜들이 설명되어있다[1]. EKE가 대표적인 방법으로 이는 기밀성을 보장해야 하는 정보, 즉 키 등을 패스워드로 암호화해서 보내는 방식이다. 또한, A-EKE는 패스워드을 가지고 해쉬값을 취해서 이용하는 방법을 이용하고 있다. 이러한 방법에는 기본적으로 패스워드의 길이에 대한 문제가 있다. 즉, 패스워드가 짧은 길이를 가질 경우 Dictionary Attack에 취약하게 된다. 또한 [4]는 짧은 패스워드를 이용한 키교환 프로토콜로써 설계된 프로토콜이다. 이 프로토콜은 3 pass를 가지며 복잡한 구조를 가지고 있다. 그러나, 이 프로토콜은 인증 및 무결성들을 가지고 있는 프로토콜이다.

본 연구에서는 짧은 패스워드를 이용해서 키분배 및 Signcryption에 이용할 수 있는 방법을 제안한다. Dictionary Attack에 강력한 프로토콜을 만들기 위해서는 도청자가 알아채지 못하게 하면서 송신자와 수신자만이 패스워드의 길이를 증가시키는 방법이 필요하다. 따라서, 이러한 정보 전달을 위해서 기본적으로 패스워드를 가지고 있고 이를 이용해서 패스워드 길이 확장을 위한 정보 전달값이 하나 더 필요하게 된다. 본 연구에서는 Signcryption을 이용한 방법을 가지고 설명한다.

II. 본문

본 논문에서는 Yuliang Zheng의 논문을 기초하여서 Forward Secrecy를 제공하는 프로토콜로의 변환을 하고[2], 본 논문의 최종 목표인 짧은 패스워드 기반의 키분배 프로토콜을 설계한다.

1. Yuliang Zheng의 Signcryption

A와 B의 Signcryption을 수행한다고 가정한다. 여기서, A는 하나의 수를 선택하여서 프로토콜을 수행한다. 이는 프로토콜에서 항상 변화하는 키를 만들기 위한 것이다. 따라서, B는 이 값에 대한 정보를 A로부터 받아서 동일한 키를 생성할 수 있어야 한다. 본 논문에서는 이점에 초점을 맞추고 설계를 시작한다.

[2]에서 공개변수 및 키 환경에 대한 부분은 생략하고 랜덤한 x를 선택하여서 B에게 그에 대한 정보를 보내는 부분을 살펴본다.

[A(signcryption)]
$x \in_R [1,2,\cdots,q-1]$
$k = hash(y_b^x \bmod p)$
$k_1 \| k_2 = k$
$c = E_{k_1}(m)$
$r = KH_{k_2}(m)$
$s = x/(r+x_a) \bmod q$

[정보전달]
A $\Rightarrow$ B : (c,r,s)

[B(singcryption 확인]
$k = hash((y_a g^r)^{s \cdot x_b} \bmod p)$
$k_1 \| k_2 = k$
$m = D_{k_1}(c)$
accept m only if $KH_{k_2}(m) = r$

위의 프로토콜에서 랜덤한 x를 선택하여서 항상 변화하는 키값을 생성한다. B는 A와 동일한 키를 생성하여서 Singcryption된 정보를 확인하기 위해서는 x에 대한 정보를 얻어야 한다.

2. Forward Secrecy Signcryption

[3]은 [2]에 대해서 Forward Secrecy를 제공하는 프로토콜을 제안하였다. 프로토콜에서 공개변수, A와 B의 키는 [2]와 동일한 환경이다.

[A(signcryption)]
$x \in_R [1,2,\cdots,q-1]$
$k = hash(y_b^x \bmod p)$
$k_1 \| k_2 = k$
$c = E_{k_1}(m)$
$r = KH_{k_2}(m)$
$R = g^r \bmod p$
$s = x/(r+x_a) \bmod q$

[정보전달]
A $\Rightarrow$ B : (c,R,s)

[B(singcryption 확인]
$k = hash((y_a R)^{s \cdot x_b} \bmod p)$
$k_1 \| k_2 = k$
$m = D_{k_1}(c)$
accept m only if
$R = g^{KH_{k_1}(m)} \bmod p$

위의 알고리즘은 $(y_a \cdot g^r)^{s \cdot x_b} = (y_b^{x_a+r})^s$의 수행으로 Forward Secrecy를 제공하지 못하므로 [2]에서 수행하는 것처럼 r를 보내는 것이 아니고 B에서 수행할 때는 g^r를 이용하여서 알고리즘을 완성하므로 이를 A에서 계산하여서 B에게 보내주는 형식이다. 결과적으로 이러한 변환은 프로토콜에 Forward Secrecy를 제공하게 된다. 이를 이용하여서 패스워드 기반의 프로토콜 설계를 수행한다.

3. 패스워드 기반의 Signcryption

[4]와 같은 프로토콜을 살펴보면 A는 패스워드를 위수가 q인 Z_p^*의 원소 중에서 선택된 공개값 g의 지수로 계산하여서 수행한다. 이것만으로는 Dictionary Attack에 대해서 취약성을 가지므로 이를 극복하기 위해서 랜덤한 수를 선택하여서 지수로 사용하여 계산하고 있다. 이러한 정보를 B에게 전달하여서 패스워드와 랜덤 수에 대한 정보 등을 이용하여서 동일한 키를 설정한다.

A와 B는 동일한 패스워드를 가지고 있다고 가정한다.

[비밀변수]

P : 패스워드(A와 B가 사전에 합의에 의해서 가지고 있는 인간이 기억할 수 있는 짧은 패스워드)

[공개변수]

p : 큰 소수

q : $p-1$을 나누는 큰 소수

g : 위수가 q인 Z_p^*의 원소

$hash$: 일방향 해쉬함수

KH : keyed-일방향 해쉬함수

[A(Signcryption)]

$x \in_R [1,2,\cdots,q-1]$

$k = hash(g^{x+P} \bmod p)$

$k_1 \| k_2 = k$

$c = E_{k_1}(m)$

$r = KH_{k_2}(m)$

$R = g^r \bmod p$

$s = x/(r+P) \bmod q$

[정보 전달]

A $\Rightarrow$ B : (c,R,s)

[B(Unsigncryption)]

$k = hash(g^s * R * g^{2P} \bmod p)$

$k_1 \| k_2 = k$

$m = D_{k_1}(c)$

accept m only if

$R = g^{KH_{k_2}(m)} \bmod p$

위와 같은 프로토콜은 짧은 패스워드를 가진 A와 B가 Signcryption을 수행하는 프로토콜이다. 여기서, A는 랜덤 수 x를 선택할 때 큰 소수를 선택해야 한다. g^{x+P}를 계산하는데 짧은 패스워드와 짧은 x를 선택하여서 계산한다면 Dictionary Attack에 취약점이 노출될 수도 있다.

4. 짧은 패스워드 기반의 키 교환 Signcryption 기법

[비밀변수]

P : 패스워드(A와 B가 사전에 합의에 의해서 가지고 있는 인간이 기억할 수 있는 짧은 패스워드)

[공개변수]

p : 큰 소수

q : $p-1$을 나누는 큰 소수

g : 위수가 q인 Z_p^*의 원소

$hash$: 일방향 해쉬함수

KH : keyed-일방향 해쉬함수

[A]

$x \in_R [1,2,\cdots,q-1]$

$k = hash(g^{x+P} \bmod p)$

$r = KH_k(P)$

$R = g^r \bmod p$

$s = x/(r+P) \bmod q$

[정보 전달]

A $\Rightarrow$ B : (R,s)

[B]

$k = hash(g^s * R * g^{2P} \bmod p)$

위와 같이 키교환을 위한 간단한 프로토콜을 구성할 수 있다. DLP에 대한 안전성을 가정하고 랜덤값 x가 큰 수를 선택하여서 계산되어진다면 계

산상에서 안전하게 된다.

짧은 패스워드를 가지고 계산되어지면 Dictionary Attack에 안전하지 않게 된다. 따라서, 랜덤수를 이용하여서 Dictionary Attack에 강하게 만들게 된다. 또한 일방향 해쉬함수의 특성상 결과값을 가지고 원래의 정보를 추측한다는 것은 불가능하므로 이를 이용한 프로토콜이다.

향상된 프로토콜을 위해서는 r의 생성시에 A와 B 둘만이 알고 있는 비밀정보를 이용하여서 암호학적 비도를 향상할 수도 있다. 즉, r은 서로간의 비밀정보를 이용한 x와P의 관계식을 풀기 위한 정보값이다. 또한 인증과 여러 가지 공격에 대해서 추가적인 정보를 이용해서 r을 계산하여서 이용할 수도 있다.

Ⅲ. 결론

본 논문에서는 2가지를 제안하고 있다. 즉, 패스워드 기반의 Signcryption과 짧은 패스워드를 이용한 키교환 프로토콜이다. 일부 논문에서는 패스워드를 이용하기 위해서 패스워드와 안전한 통신로를 통해서 송신자와 수신자가 합의한 랜덤값을 이용해서 해쉬값을 취한 후 이용되는 방법이 언급되기도 하였다. 그러나, 규모가 큰 인프라에서는 현실적으로 불가능하고 그 랜덤값을 교환하는 문제에 직면하게 되었었다. 일반적인 알고리즘에서는 짧은 패스워드의 취약성을 극복하지 못하고 긴 패스워드를 이용하고 있고 이를 위해서 스마트카드를 이용한 방법이 대두되고 있다. 또한, 현실에서 짧은 패스워드와 부가적인 랜덤값을 선택하여서 금융업무에 적용되고 있다.

본 연구 결과를 토대로 여러 가지 시스템에 패스워드 기반의 안전한 프로토콜 설계에 적용될 것으로 기대된다. 즉, TLS 및 IPSec 등 최근 활발한 연구가 진행되고 있는 부분에서 본 연구를 이용한 안전한 프로토콜을 적용하여서 많은 부분에 이용될 수 있을 것으로 기대된다.

또한, 본 연구는 Signcryption에 대한 이론을 이용하였으며, Zero-Knowledge에 대한 연구 결과를 이용한 향상된 짧은 패스워드를 이용한 키교환이 가능하다고 생각된다.

참고문헌

[1] S. Bellovin and M. Merritt, "Encrypted Key Exchange : Password-Based Protocols Secure against Dictionary Attacks," IEEE Symposium on Security on Security and Privacy, 1992.

[2] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) << cost(signature)+cost(encryption),"In Advances in Cryptology-CRYPTO'97, vol.1294 of LNCS, pp.165 - 179 (1997).

[3] Hee Yun Jung, Dong Hoon Lee, Jong In Lim and Ki Sik Chang, "Signcryption Schemes with Forward Secrecy," WISA 2001.

[4] Jonathan Katz, Rafail Ostrovsky and Moti Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memoriable Passwords" 2001.