

임계 암호 기법에 기반한 개선된 야누스 시스템의 설계

심미선*, 양종필**, 이경현***

* 부경대학교 정보보호학과

** 부경대학교 전자계산학과

*** 부경대학교 컴퓨터정보통신공학부

Design of improved Janus system based on the threshold cryptographic scheme

Mi-Sun Shim*, Jong-Phil Yang **, Kyung-Hyune Rhee ***

* Dept. of Information Security, PuKyong Nat'l University

** Dept. of Computer Science, PuKyong Nat'l University

*** Devision of Electronic, Computer & Telecommunication Engineering, PuKyong Nat'l University

요약

지속적으로 증가하고 있는 웹사이트는 사용자마다 유일한 신분확인정보(ID, 패스워드)를 요구한다. 이 때 사용자는 웹사이트마다 별개의 계정을 만드는 것이 공격자의 위협으로부터 안전하지만, 현실적으로 사용자의 기억의 한계, 편의 추구로 인해 한 사용자가 사용하는 계정의 가짓수는 한정되기 마련이다. 따라서, 어느 공격자가 단일 사용자의 특정 웹사이트에 대한 ID와 패스워드를 알게되면, 그 공격자는 다른 웹사이트에 동일한 ID와 패스워드를 사용한 로그인 시도 공격이 성공할 확률이 매우 높다고 할 수 있다.

본 논문에서는 이러한 사용자 ID와 패스워드에 대한 문제점을 해결하기 위한 방안으로서 사용자는 로그인하려는 웹사이트에 상관없이 항상 동일한 ID와 패스워드를 사용하지만, 실질적으로는 사용자 머신내에 있는 내부 프록시(proxy)에 의해서 웹사이트마다 독립적이고 유일한 가명 ID와 가명 패스워드를 생성하는 방안을 제안한다. 또한 제안 방안에서는 임계 암호 기법을 이용하여 단일 사용자 ID와 패스워드로부터 가명 ID와 가명 패스워드를 생성하는 함수를 안전하게 구성한다.

1. 서론

최근 인터넷의 급속한 성장으로 인해 전 세계 수천 개의 네트워크와 수백 만대의 컴퓨터들이 인터넷이라는 매체를 통하여 하나로 연결되어 가고 있다. 한편, 인터넷을 이용하는 사용자는 여러 웹사이트에 접속하여 자신들이 필요로 하는 정보들을 검색하거나 서비스들을 이용하게 된다. 이 때 웹사이트들은 서비스를 제공할 때 사이트의 이용권한을 주기 위해 사용자들에게 계정 등록을 요구한다. 계정이 등록된 사용자의 웹사이트 이용은 웹사이트가 해당 사용자의 취향이나 기호를 파악할 수 있게 해주는 도구가 된다.

사용자가 여러 웹사이트에 계정 등록시 각각 별개의 계정을 등록하는 것은 매우 번거로울 뿐더러 기억

하기도 어렵기 때문에 동일한 계정 정보(ID, 패스워드)를 사용하게 된다. 따라서, 어느 공격자가 단일 사용자의 특정 웹사이트에 대한 ID와 패스워드를 알게되면, 그 공격자는 다른 웹사이트에 동일한 ID와 패스워드를 사용한 로그인 시도 공격이 성공할 확률이 매우 높다고 할 수 있다. 본 논문에서는 위와 같은 공격을 간략히 “웹사이트 연결 공격”이라고 언급하겠다.

E. Gabber[3]는 야누스 서버라고 하는 단일 프록시서버에서 단일 사용자 정보(ID와 패스워드)에 대한 다수의 웹사이트를 위한 가명 ID와 가명 패스워드를 생성함으로써 웹사이트 연결 공격을 방지하기 위한 시도를 하였다. 하지만, [3]의 야누스 서버는 시스템 자체가 신뢰되고 공격에 안전해야만 전체 시스템이

정상적으로 운용이 된다. 만약, 어느 공격자가 야누스 서버에 대한 공격을 성공하게 되면, 그 공격자는 야누스 서버를 사용하는 모든 사용자의 유일한 ID와 패스워드를 획득할 수 있을 뿐만 아니라, 각 사용자들의 ID와 패스워드로부터 각 사용자들의 특정 웹사이트를 위한 가명 ID와 가명 패스워드를 자유로이 생성할 수 있게 된다.

본 논문에서는 공격의 주요 목표가 되는 야누스 서버에서의 사용자 ID와 패스워드로부터 가명 ID와 가명 패스워드를 생성하기 위한 함수를 좀 더 안전하게 구성하고자 한다. 야누스 서버의 함수에 임계 암호 시스템(threshold cryptosystem)을 적용하여 좀 더 강건하고 안전한 시스템을 구성한다. 본 논문의 구성은, 2장에서는 관련 연구에 관하여 기술하고, 3장에서는 제안하는 시스템의 구성 요소에 대해서 설명한 뒤, 4장에서는 이 요소들간의 동작을 살펴본다. 그리고, 5장의 안전성 평가 후 결론을 맺는다.

2. 관련 연구

2.1. 야누스 시스템[3]

야누스 시스템에서는 단일 사용자와 여러 웹사이트 사이에 야누스 서버라는 단일 중계 프록시를 두어, 가명 ID와 가명 패스워드를 생성한다. 즉, 사용자가 야누스 서버에 입력하는 단일 사용자 정보로부터 야누스 서버는 다수의 웹사이트에 대한 가명 ID와 가명 패스워드를 생성함으로써 사용자 신원을 보호한다. 그리고, 사용자가 유일하게 기억하고 있는 야누스 서버에 대한 사용자 정보의 입력은 사용자와 야누스 서버 간의 세션을 성립시킨다. 성립된 세션이 유지되는 동안, 야누스 서버는 사용자가 접속하는 여러 사이트에 대한 가명계정을 만들어 전달함으로써, 사용자의 편의성을 추구한다.

하지만, 야누스 서버가 공격자에게 노출 당하면 공격자는 Jauns서버에 입력된 사용자들의 ID와 패스워드를 알게 되고, 이를 이용하여 공격자는 야누스 서버 내의 야누스 함수를 동작시킴으로써 필요한 가명계정들을 자유로이 생성할 수 있는 단점이 있다.

2.2. (t, n) 임계 암호 시스템[1][4][5][6][7][8]

(t, n) 임계 암호 시스템($n \geq 2t - 1$)이란 n 개로 구성된 서버 시스템의 비밀값(주로 공개키 암호 알고리즘을 위한 비밀키(secret key))을 n 개의 서버로 각각 분산(sharing)시켜, 자신의 비밀 분배값(private

shared key) s_i ($1 \leq i \leq n$)를 소유하게 하고 서버 시스템을 대상으로 암호적 연산이 요구될 시에 적어도 t 개의 서버의 협조가 있어야 암호적 연산이 가능한 방안이다. 예를 들어, 임계 서명 시스템에서는 요청된 메시지 m 를 서명하기 위해서는 최소 t 개의 서버가 자신의 비밀 분배값으로 계산한 부분 서명값(partial signature) $PS_{s_i}(m)$ ($1 \leq i \leq t$)이 모여서 서버 시스템의 비밀키로 서명한 유효한 전자 서명문을 생성하는 기법이다. 따라서, 공격자가 서명문 위조를 위해서는 최소한 t 개의 서버를 공격해야만 전체 서버 시스템을 가장하여 암호학적 연산을 수행할 수 있다.

3. 가명 생성 시스템 구성 요소

본 장에서는 제안하는 시스템을 이루는 요소들에 대해서 정의한다. 그림 1은 제안 시스템의 구성 요소들 간의 상호동작에 대해 표현한다.

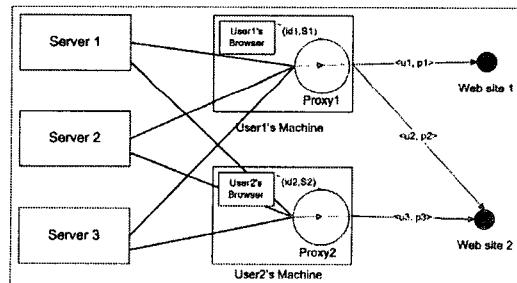


그림 1 전체 시스템

사용자 사용자는 자신의 머신 내에 위치한 웹 브라우저를 통하여 웹사이트와 메시지를 주고받는다. 여기서 사용자의 웹 브라우저는 프록시와 자동 연결되고, 프록시에 입력되는 사용자 정보(ID, 패스워드)는 서버들(그림 1에서의 Server1 - Server3)과 프록시로부터 가명계정(가명 ID, 가명 패스워드) 생성에 필요한 변수가 된다. 사용자는 프록시에게 가명계정의 생성과 웹사이트로의 전달을 위임한다.

서버 서버들은 각각 다른 머신에서 동작되는 하나의 템으로 구현되어진다. n 개로 구성된 서버들은 서로간의 통신이 없다. (t, n) 임계 암호 시스템에 입각한 n 개의 서버들에게는 공개키 암호 알고리즘을 위한 비밀키(secret key)가 [1]의 기법을 사용하여 분산(sharing)되어, 각 서버들은 자신의 비밀 분배값(private shared key)을 소유하게 된다. 프록시로부터 부분 서명값 요청이 있을 때 각 서버들은 자신의 비밀 분배값을 이용한 부분 서명값을 전달

한다.

프록시(Proxy) 프록시는 사용자 머신 내에 위치하며, 서버들과의 안전한 채널을 형성한다. 프록시는 같은 머신 내의 사용자의 정보를 입력받는다. 그 후, 특정 사이트로부터 가명계정의 요청이 있을 경우 서버들에게 해당 사용자 정보(ID, 패스워드)와 특정 웹사이트에 대한 정보를 전달하고, 그에 대한 부분 서명값을 요청한 뒤 (t, n) 임계 암호 방식에 따라서 t 개의 유효한 부분 서명값으로부터 서명값을 계산한다. 이 때 이 서명값은 가명계정의 생성 정보가 된다.

4. 가명 생성 시스템의 동작 방식

이 장에서는 3장에서 기술된 구성요소들 간의 상호 동작 방식에 대해 살펴본다.

4.1. 동작 시나리오

각 사용자의 브라우저는 같은 머신내의 프록시와 연결되어 있고, 웹 브라우저에서의 모든 메시지는 프록시를 거쳐가도록 설정된다. 그리고, 서버들과 프록시와의 모든 통신 메시지는 안전하게 전달되어 진다고 가정한다.

그림 1에서는 두 사용자의 경우를 예를 들어 전체 시스템을 구성하였다. $User_1$ 은 w_1 이라는 웹사이트에 접속을 시도한다고 가정한다. 이 때 $Proxy_1$ 은 자동 실행되어 $User_1$ 의 정보(id_1, SI)를 입력받은 후, w_1 으로 이동되게 한다. 여기서 id_1 은 $Proxy_1$ 에 대한 $User_1$ 의 ID를 나타내고, SI 은 해당 ID에 대한 일종의 패스워드를 나타낸다. 이렇게 $User_1$ 의 정보 입력은 $Proxy_1$ 을 가동시킨다. 그리고, 가동되는 동안 $Proxy_1$ 은 사용자의 요청에 따라 계속해서 가명계정($\langle u_i, p_i \rangle$)을 생성하게 된다.

$Proxy_1$ 의 동작은 $User_1$ 이 w_1 의 등록품이나 로그인 품에 입력하는 ID와 패스워드 값에 따라 다음과 같아야 한다.

- 실제로 사용하고자 하는 ID와 패스워드를 입력한다면, $Proxy_1$ 은 동작하지 않고 $User_1$ 은 자신이 입력한 계정으로 w_1 을 이용하게 된다.
- ID 입력 부분에는 “U”를, 패스워드 입력 부분에는 “P”를 입력한다면, $Proxy_1$ 은 그 문자에 반응하여 서버들로부터 $User_1$ 의 입력 정보(ID와 패스워드)와 해당 웹사이트 정보에 대한 부분 서명값들을

요청하게 되고, (t, n) 임계 암호 방식에 따라서 t 개의 유효한 부분 서명값으로부터 서명값을 계산한다. 이 때 이 서명값은 가명계정의 생성 정보가 된다.

그리고, $User_1$ 의 w_2 에 대해서는 w_1 과는 별개의 가명계정(그림1의 $\langle w_2, p_2 \rangle$)을 생성하게 된다. 세션이 종단된 뒤 새로 시작되더라도 특정 사용자의 특정 사이트에서의 가명계정은 항상 동일하다.

구체적인 가명계정 생성 프로토콜은 다음 절에 설명된다.

4.2. 가명계정 생성 프로토콜

이 절에서는 서버들과 프록시 사이에 가명계정이 어떻게 생성되는지에 대해 기술한다. 본 논문에서 사용되는 표기법은 다음과 같다.

- P_n : ID가 n 인 Proxy
- S_n : ID가 n 인 Server
- $SIG_X(\cdot)$: 통신개체 X 의 개인키를 사용한 전자서명
- I_X : 통신개체 X 의 인덱스(index)로 기본값은 0이며, 웹사이트로부터 계정 변경을 요청 받을 경우에 사용되는 변수

전제사항: P_1 과 서버들(S_n)간은 SSL을 통하여 키교환과 상호인증이 형성되어 있고, $User_1$ 은 P_1 에 대한 ID와 패스워드를 전송하여 P_1 을 활성화 시킨 상태이다.

과정1: 만약 $User_1$ 이 가명 ID와 가명 패스워드를 사용하고자 할 때, $User_1$ 은 웹브라우저를 통하여 w_1 의 ID입력부분에는 “U”, 패스워드 입력 부분에는 “P”의 입력으로, P_1 에게 가명계정 생성을 요청한다.

과정2: P_1 은 n 개의 서버들에게 $(id_1 \parallel SI_1 \parallel w_1 \parallel I_{w_1})$ 값을 전달하면서, 서명값($SIG_i, 1 \leq i \leq n$)를 요청한다.

과정3: 각 서버들($S_i, 1 \leq i \leq n$)은 자신의 비밀 분배값을 이용하여 아래와 같은 부분 서명값을 계산하여, P_1 에게 전달한다.

$$SIG_{S_i}(id_1 \parallel SI_1 \parallel w_1 \parallel I_{w_1})$$

과정4: P_1 은 n 개의 서버들로부터 받은 부분 서명값들을 (t, n) 임계 암호 시스템에 따르는 t 개의 유효한 부분 서명값으로부터 서명값을 생성한다. 예를 들어 (2, 3) 임계 암호 시스템인 경우,

$$\text{info} = \text{id1} \parallel \text{S1} \parallel \text{w1} \parallel \text{I}_{\text{w1}}$$

이라 하고, 임계 암호 기법에서의 결합(Combining) 연산을 *Com*로 나타낼 때, 다음과 같다.

$$\text{Com}(\text{SIG}_{\text{S2}}(\text{info}), \text{SIG}_{\text{S3}}(\text{info})) = \text{SIG}(\text{User1}, \text{w1})$$

여기서, *Com*은 적용되는 임계 암호 시스템 [1][4][5]에 의존적인 알고리즘이다.

과정5: 과정4에서 생성된 서명값을 실제 구현을 위해 서는 전자 서명과 같은 124비트 사이즈 정도로 만들어야 하므로 전자서명 값에 일방향 해쉬함수를 적용시킨 값을 사용하여 가명계정인 $\langle \text{u1}, \text{p1} \rangle$ 이 생성 가능하다.

$$H(\text{SIG}(\text{User1}, \text{w1})) = (\text{u1} \parallel \text{p1})$$

- 웹사이트로부터 계정 변경 요구가 있을 경우에 대한 방안

*User1*이 *w1*에서 사용하려는 가명계정이 등록되어 있는 경우 사용자는 *w1*으로부터 계정 변경 요청을 받게 되어, *P1*은 *User1*에 대한 *I_w1*의 값을 α 만큼 증가시킨 후, 변경된 *User1*의 정보로 새로운 부분 서명값을 서버들에게 재요청하여, 다른 사이트의 가명계정의 변경없이 해당 사이트의 새로운 가명계정을 생성받도록 한다. 하지만, *I*라는 변수로 인한 통신 정보량의 증가와 관리의 어려움이 있다는 단점이 있다.

5. 안전성 및 평가

제안 방안은 다음과 같은 암호학적 강도를 지닌다.

- **강건한 가명생성 함수:** 기존의 앤누스 서버를 통한 가명 생성 시스템에 임계 암호 기법을 적용하여 새로이 설계한 시스템으로, 시스템 자체가 신뢰되어야만 정상적인 운영이 가능한 기존 방식[3]과는 달리 $t-1$ 개까지의 서버들의 노출(compromise)을 허용함으로 좀 더 공격에 유연성이 있도록 설계하였다.
- **웹사이트 연결 공격 방지:** 가명 생성 정보가 프록시만으로 생성되어지는 것이 아니라 (t, n) 임계 암호 시스템에 근거한 서버들의 도움이 있어야만 하므로, 단지 사용자 자신의 공격을 통해 사용자 정보와 특정사이트에 대한 서명값을 획득하더라도, 다른 사이트에 대한 가명계정 생성에 필요한 정보들은 알 수 없으므로 웹사이트 연결 공격이 불가능해진다.

6. 결론

본 논문에서는 사용자 신원을 보호하기 위한 새로운 가명계정 생성 시스템을 제안하였다. 제안 방안은 기존 앤누스시스템과 임계 암호 시스템과의 결합으로 공격에 대한 유연성과 안전성을 지니는 새로운 가명계정 생성 방식이다. 향후 구현을 위해 구체적이고 세부적인 네트워크 및 시스템의 정상적인 운영 변수를 고려함으로써 다양한 공격에 대처 가능한 시스템의 개발이 적 할 것으로 판단된다.

[참고문헌]

- [1] A. Shamir. "How to share a secret", Communications of the ACM, 22:612-613, 1979.
- [2] D. Boneh, M. Franklin, "Building Intrusion Tolerant Applications", in Proceedings Crypto'97 pp. 425-439
- [3] Eran Gabber, Phillip B. Gibbons, Yossi Matias, Alain Mayer, "How to Make Personalized Web Browsing Simple, Secure, and Anonymous", In Proceedings of Financial Cryptography '97, 1997.
- [4] M. Malkin, T. Wu, D. Boneh, "Experimenting with Shared Generation of RSA keys", in Proceedings of the Internet Society's 1999 Symposium on Network and Distributed System Security(SNDSS), pp. 43-59
- [5] T.Rabin, "A simplified approach to threshold and proactive RSA", Proceedings of Crypto'98, pp. 89-104
- [6] Victor Shoup, "Practical Threshold Signatures", in Proceedings Eurocrypt 2000
- [7] Yvo Desmedt, "Some Recent Research Aspects of Threshold Cryptography", In information Security, First International Workshop ISW '97, volume 1196 of Lecture Notes in Computer Science, pp. 158-173, 1997.
- [8] 이경현, 김영인, 윤희영, "Pseudopia 함수를 이용한 각종 패스워드 관리방안", 한국멀티미디어학회 2000년도 춘계학술발표논문집, 제3권 제1호, pp71-75, 2000.