OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델

류연호
고려대학교 컴퓨터과학기술 대학원
yhryu@korea.ac.kr

Cross Authentication Model for Client-Sever by used OTP Concept

Yeon-Ho, Ryu
Graduate School of Computer Science and Technology, Korea University

요 약

패스워드를 이용한 사용자 인증은 인증을 요청한 사용자와 인증 서버간의 인증 자료의 흐름이 매우 중요하다. 사용자 또는 인증 서버의 단 방향에서의 인증이 갖는 한계는 사용자에 대한 비밀 정보를 인증 서버에서 모두 관리함으로써 인증 서버의 해킹에 무방비하다는 점과 단 방향으로의 인증으로 사용자 또는 인증 서버를 가장한 해킹에 취약하다는 단점을 지니고 있다. 그러므로, 본 논문은 사용자-인증 서버를 One Time Password를 이용하여 발생시킨 난수를 기반으로 상호 인증을 할 수 있는 효율적인 방안을 제시하였다.

제 1장 서 론

인증이란 어떤 사람이나 사물이 실제로 신고된 바로 그 사람(또는 바로 그 것)인지를 판단하는 과정이다.[1] 컴퓨터와 정보 통신 기술의 급속한 발달로 인터넷과 공중 전화망, 공중 데이터망과 같은 개방형 정보 통신망을 이용한 각종 정보의 교환 및 검색이 활발히 이루어지고 있는 과정에서, 인증은 개방형 정보통신망을 이용한 사이버 공간에서의 상대방과 직접 대면할 수 없는 특성으로 이용자의 신원을 확인하거나 정보 자원에 대한 진정성을 확보하기 위하여 매우 중요한 과정으로 인식될 수 있다.[2]

그러므로 본 논문은, 효과적인 인증을 제공하기 위하여 One Time Password(OTP) 개념을 이용한 사용자-인증 서버의 상호 인증 모델을 제안하였다. 이 방식은 공개키 알고리즘의 안전성을 기반으로 하고 있다.

본 논문의 제 1장에서는 인증의 중요성에 대하여 서술하였다.

제 2장에서는 논문의 목적과 사용자 인증 배경 연구로서 유닉스기반 패스워드 방식, 시간동기 OTP 방식, S-Key OTP 방식, Challenge-Response 방식, 영지식 증명방식의 특성과 문제점을 분석하였다.

제 3장에서는 제안된 OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델을 설명하였다.

제 4장에서는 본 논문에서 제안한 방식의 특징들을 요약 정리하고, 향후 연구 방향을 제시하였다.

제 2장 사용자 인증.

2.1 인증의 중요성.

인터넷이라는 불완전한 개방형 네트워크에서 사용자의 비밀 정보를 안전하게 보호하여 원하는 거래를 효율적으로 수행하기 위하여서는 물리적인 보안뿐 아니라 데이터, 통신 및 거래를 보호하기 위한 추가적인 전자적 수단이 필요하다. 특히 인터넷을 이용한 전자 상거래가 활성화됨에 따라, 인터넷의 개방성은 전자 상거래 이용자와 서비스 제공자 사이의 사용자 식별과 인증은 중요한 화두가 되었다.

2.2 사용자 인증.

2.2.1 유닉스 기반 패스워드 방식의 취약점.

1) 패스워드는 평문으로 전달된다.
2) 인증이 일방향으로 수행된다. 인증 시스템의 동작은 호스트 측에서 일방향으로 수행되어지기 때문에 호스트가 패스워드를 사용자에게 물어볼 수 있지만, 사용자는 그들이 정말로 정당한 호스트와 통신을 하는 지의 여부는 알 수 없다. 사용자가 패스워드를 제공하기 전에 어떠한 시험도 할 수가 없다.
3) 비밀 정보는 호스트에 보관된다. 사용자의 패스워드 관련 정보를 호스트에 보관하고 있음으로써 패스워드 파일이 누출되게 되면, 공격자는 이 패스워드 파일을 이용하여 사전 공격을 여러 대의 컴퓨터를 이용해서 쉽게 할 수 있다.

2.2.2 시간 동기 One Time Password(OTP) 방식.

시간 동기 OTP 방식은 매분마다 하나씩의 난수를 생성하기 위해 난수 발생 알고리즘과 64 비트 크기의 비밀키가 필요하다. 각각의 사용자에게는 특정키가 할당되어져 있는데, 이것은 지능형 토큰과 인증 서버의 데이터베이스에

저장되어진다.

이 방식의 단점은 양쪽에서 발생하는 난수를 일치시키기 위해 시간에 대한 동기가 보장되어야 한다는 점이다.
소위 시간 편차라 불리는 토큰이라는 것이 일회용이 아니고 일반적으로 수년간에 걸쳐 사용되어지는 장치이기 때문에, 하루에 몇 초 만이라도 늦어지거나 빨라진다면 토큰과 서버간의 동기는 또한 보장 될 수 없게 된다.
유효한 시간 간격과 관련된 문제가 있다. 토큰에서 생성된 난수가 여기서는 패스워드로 사용되어지는데, 이 패스워드에는 임의로 설정한 유효 시간이 있게 된다.

2.2.3 S/Key OTP 시스템.
S/Key OTP 시스템에 대한 상세한 설명은 국제 단체인 IETF(Internet Engineering Task Force) 표준 RFC1760에 나타나 있으며, 초기의 S/Key는 해쉬 알고리즘으로 DES를 사용하여 OTP 인증을 구현하였다. 하지만, 이 방식은 MD4 메시지 다이제스트 알고리즘을 기반으로 하는 시스템으로 다시 개발되어 RFC1320에 소개되었다.

S/Key OTP 시스템의 동작절차는 다음과 같다.
시스템 동작은 사용자 또는 클라이언트에서 적절한 OTP가 생성된 후, 시스템 또는 서버에서 검사되며, MD4 일방향 함수를 이용한다.S/Key OTP 시스템에는 두 가지 측면이 존재한다. 하나는 사용자 혹은 클라이언트 측면인데, 적절한 One-time password 가 생성되어져야 한다. 다른 하나는 시스템 혹은 서버 측면으로, One-time password가 검사되어져야 한다. One-time password는 MD4 One-way hash 함수를 이용해서 생성되고 검사되어진다. 이 시스템은 8바이트의 입력을 받아 8바이트의 출력을 얻도록 제작되었다. One-time password는 단방향 함수를 여러 번 적용함으로 계속해서 생성되어진다. 즉, 첫 번째 One-time password는 사용자의 비밀 패스워드(s)를 정해진 특정 수(n)만큼의 단 방향 함수를 수행함으로 생성되어진다. 즉, n=4라고 가정하면,

$$p(1) = f(f(f(f(s))))$$

다음 One-time password는 사용자의 패스워드를 단방향 함수에 n-1번 수행함으로 생성되어진다.

2.2.4 Challenge-response 방식.
사용자가 인증 요구와 함께 사용자 식별 번호(PIN)을 인증 서버에 전달하게 되면, 인증 서버는 난수를 생성하여 Challenge로 사용자에게 전달한다.
이와 동시에 인증 서버는 이용자의 사용자 식별 번호에 해당하는 패스워드를 키 데이타베이스에서 꺼내 이것을 이용하여 난수의 암호화를 시작한다. Challenge 를 받은 사용자는 그것을 자신의 패스워드로 암호화하여 response로 인증 서버에게 반환한다.

이 방식의 단점은 여러 번의 절차로 인해 다소 느린 점과 사용자의 PIN에 해당하는 비밀번호를 인증 서버에서 보관함으로써 서버가 해킹 될 경우, 사용자 인증에 취약 동기 방식에 비해 복잡성이 적고 안전성이 높기 때문에 이 방법을 적용한 인증 시스템이 국외에서 많이 개발되고 있다.

2.2.5 영지식 증명 방식.
영지식 증명 방식은 증명자와 검증자가 대화를 통해 증명을 하는 방식으로 증명자가 어떤 사실의 정당성에 관한 사실만을 검증자에게 전달하는 방식으로 그 이외의 어떠한 정보도 노출시키지 않는다는 의미를 갖고 있다. 즉, 증명자가 자신만이 아는 비밀 정보를 검증자에게 전송하지 않고, 자신의 비밀 정보가 아닌 어떤 다른 정보를 전송해 검증자에게 자신만이 비밀 정보를 갖고 있다는 사실을 증명할 수 있는 증명 방식이다.

확률적 튜닝기계를 M이라 할 때, 임의의 입력정보 X에 대해 확률 공간 M(X)를 생성하게 된다. 이때 확률 공간 M(X)를 확률 변수로 간주할 수 있으며, 입력 정보 X를 변화시켜 확률 변수들의 집합을 구할 수 있다.

대화형 증명 방식 (P,V)는 임의의 입력 정보 X에 대해 자신들이 가지고 있는 랜덤 테이프에 따라서 (P,V) [X]로 표시되는 확률공간을 생성한다. 이 확률공간의 특성에 의해 영지식 대화형 증명방식이 정의 된다.

즉, 임의의 다항식 계산 능력을 갖는 검증자 V에 대해 다항식 계산 능력을 갖는 확률적 튜닝기계 MV가 존재하고 {MV[X]}와 {(P, V)[X]}가 구별 불가능한 (P,V)를 영지식 증명 방식이라 한다.[3]

제 3장 OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델

가정1) 사용자-인증 서버간의 자료 교환은 공개키 알고리즘을 이용하고, 암호화된 자료는 공개키 알고리즘의 안정을 기반으로 보호된다.[4][5]
가정2) 사용자-인증 서버간의 토큰 발생을 위한 난수 발생은 인증 서비스의 요청에 따라 발생되며, 각 사용자-인증 서버에서 발생시킨 난수는 각각의 인증시에 유일한 값을 갖는다.

1) 문제 제기.
2장에서 고찰한 것과 마찬가지로 사용자 인증의 가장 큰 문제점은 사용자 인증이 인증 서버가 갖고 있는 사용자 비밀 정보를 활용한다는 점과 사용자-인증 서버간의 자료 교환을 할 때 평문을 이용할 경우에는 사전 공격이 허용된다는 점을 들 수 있다.[6]

위의 두 가지 문제점을 해결한 혁신적인 방식인 영지식 증명 방식의 경우, 사용자와 인증 서버의 인증 내용을 교환해야 하는 COMM.TAPE가 필요하며 COMM.TAPE가 정당한지 여부에 대하여는 검증이 되지 않은 상태에서 사용자 인증을 하게 된다.

할 수 밖에 없다는 점을 꼽을 수 있고, 장점으로는 시간

2) 제안 내용.

사용자	인증서버
인증 요청	
1.사용자난수 발생	3.인증서버난수 발생
2.사용자난수 암호화 (인증서버의 공개키)	4.인증서버난수 암호화 (사용자의 공개키)
5.사용자,인증서버난수교환	
6.인증서버난수 복호화 (사용자의 비밀키)	8.사용자난수 복호화 (인증서버의 비밀키)
7.인증서버난수암호화 (인증서버의 공개키)	9.사용자난수암호화 (사용자의공개키)
10.사용자,인증서버난수교환	
11.사용자난수복호화 (사용자의비밀키)	13.인증서버난수복호화 (인증서버의비밀키)
12.최초사용자난수와 검증한사용자난수비교	14.최초의인증서버난수와 검증한인증서버난수비교
15.결과가 일치할 경우 비밀번호 송부	16.결과가 일치할 경우 비밀번호 수령.

먼저, 사용자는 인증을 인증 서버에 요청한다.

1.2. 사용자는 인증 요청과 함께, 자신의 난수 발생기를 통하여 사용자 난수를 발생시킨다. 발생된 사용자 난수는 인증 서버의 공개키로 사용자 난수를 암호화시킨다.

3.4. 인증 서버의 경우, 같은 원리로 인증 서버의 난수를 발생시키고 사용자의 공개키로 난수를 암호화 시킨다.

5. 각각 발생시킨 암호화된 사용자 난수와 인증 서버의 난수를 각각 상호 교환한다.

6.7. 교환된 암호화된 인증 서버와 사용자 난수는 사용자와 인증 서버의 비밀키로 각각 복호화한다.

8.9.10. 복호화된 사용자와 인증 서버의 난수는 인증서버와 사용자의 공개키로 다시 암호화하여 상호 교환하게 된다.

11.12.13.14. 상호 교환된 검증된 사용자와 인증 서버의 난수는 사용자와 인증 서버의 비밀키로 각각 복호화하게 된다.

15.16. 최종 단계로써 최초에 생성한 사용자와 인증 서버의 난수와 검증을 받은 사용자와 인증 서버의 난수를 비교하여 난수의 값이 같으면 사용자와 인증 서버는 각각 인증을 확인할 수 있게 된다.

3) 제안 모델의 장점.

(1) 사용자와 인증 서버 양단에서 인증이 가능하다. 사용자와 인증 서버의 양단에서 각각 발생시킨 난수를 상호 교환하여 검증함으로써 사용자와 인증서버는 인증의 상대를 각각 인증할 수 있다.

(2) 인증 서버에서 사용자에 대한 비밀 정보를 보관하지 않는다.

(3) 사용자와 인증 서버의 자료 교환은 공개키 알고리즘에 의해 암호화된 자료가 전송된다.

제 4장 결 론.

본 논문에서 제시한 OTP 개념을 이용한 사용자-인증서버의 상호 인증 모델은 사용자와 인증 서버가 각각 발생시킨 난수를 인증 상대인 인증 서버와 사용자로부터 검증을 받아 적법한 사용자 또는 인증 서버인지를 확인하는 방법을 제시하였다.

인증 서버에서 인증과 관련된 사용자의 비밀 정보를 별도로 관리하지 않고도 사용자를 인증함으로써 인증 서버가 해킹 되었을 경우 사용자 인증에 대한 위험을 사전에 예비할 수 있다. 사용자-인증 서버간의 자료 교환을 공개키 알고리즘을 바탕으로 안전성을 확보함으로써 스니핑의 문제를 해결할 수 있는 방안을 제공한다.

향후에는 이 모델이 상호 인증을 위하여 사용자-인증서버의 난수를 사용자-인증서버에서 암호화/복호화가 공개키 알고리즘을 이용하여 2번 사용한다. 이 점은 사용자 인증을 위하여 인증 서버에서 발생시킨 난수에 대한 암호화와 복호화에 대한 검증 작업에서 많은 시스템 부하를 요구하게 된다. 그러므로, 향후 인증 서버의 암호화와 복호화를 위한 성능을 향상시킬 수 있는 방안이 추가로 연구되어야 할 것이다.

참 고 문 헌

[1] http://www.terms.co.kr

[2][3] 이홍섭, " 서명고리 OTP 인증과 보안 속성 RBAC 모델에 기반한 네트워크 접근 통제에 관한 연구" , 대전대학교 대학원 컴퓨터공학과 시스템소프트웨어 공학전공 박사학위 논문, pp 1 ~ 34 , 1998.

[4] R.L.Rivest, A.Shamir, and L.Adlemen, " A Method for obtaining Digital Signatures and Public-Key Cryptosystems" , p 8 ~ 13.

[5] Ahentication, Authorization and Accounting(aaa), http://www.ietf.org/html.charters/aaa-charter.html.

[6] 박윤주," 보안성을 고려한 패스워드기반 인증 컴포넌트의 설계 및 구현" , 고려대학교 대학원 컴퓨터학과 전산과 석사학위논문 , pp 5~25,2000