셀룰러 오토마타를 이용한 일회용 패스워드 인증[1)]

윤희정° 전준철 김기원 유기영
경북대학교 컴퓨터공학과
{dude93°, jcjeon33, nirvana}@infosec.knu.ac.kr yook@knu.ac.kr

One-time password Authentication Using Cellular Automata

Hee-Jung Yoon° Jun-Cheol Jeon Kee-Won Kim Kee-Young Yoo
Dept. of Computer Engineering, Kyungpook National University

요 약

사용자의 ID와 패스워드를 인증 기반으로 하고 있는 현재의 컴퓨터 시스템들은 스니퍼나 IP 스푸핑 등을 통해 패스워드 누출에 대한 많은 위험성을 내포하고 있다. 이처럼 패스워드 도용을 이용한 불법 접속 시도 등 각종 위협에서 전산망을 안전하게 운용하기 위해 안전한 사용자 인증 기술의 확보가 필요한데, 이러한 대책들 가운데 주목 받는 기술이 일회용 패스워드이다. 본 논문에서는 병렬성을 가짐으로써 연산 속도가 빠른 셀룰러 오토마타(Cellular Automata, CA)를 이용해 일회용 패스워드를 생성한다. 그리고 사용자와 서버의 상호인증을 위한 인증인자를 생성하는데 CA를 적용하여 효율적인 인증 방식을 제안한다. 또한 제안된 방식이 여러 보안 요구사항에 안전함을 보인다.

1. 서 론

최근 컴퓨터의 급성장으로 인해 정보 자원을 유지 관리하는 중·대형 서버급 컴퓨터의 사용이 증가하고 있다. 하지만 불법적인 사람들로 부터의 사용, 정보의 노출, 수정, 파괴와 같은 비합법적인 행위로부터 시스템을 보호하기 위해 사용자의 정당성을 확인하는 사용자 인증 기술에 관심이 높아졌다. 현재 가장 일반적으로 사용되는 인증 방법은 패스워드 기반의 사용자 인증 방식이다. 그러나 사용자의 ID와 패스워드를 인증 기반으로 하고 있는 현재의 컴퓨터 시스템들은 스니퍼 등을 통한 패스워드 누출로 인해 재전송 공격과 같은 위협이 존재 한다. 사용자는 쉽게 기억할 수 있는 단순한 패스워드를 선택하는 경향이 있어 공격자의 사전 공격에 취약하다는 문제점이 있다. 또한 대부분의 패스워드 기반 인증방식이 사용자만 인증하기 때문에 서버 스푸핑 공격의 가능성이 있다. 이와 같은 문제점들을 해결하기 위한 안전한 패스워드 기반의 인증방식에 대한 많은 연구들이 이루어져왔다[1-4].

특히, Lamport는 일방향 해시 함수를 이용한 일회용 패스워드 개념을 제안하였으며[1], 이 방식을 기반으로 Haller는 S/KEY 일회용 패스워드 시스템을 제안하였다[5]. 그러나 사전공격과 재전송 공격의 특별한 경우인 재시도 공격에 안전하지 못함이 지적되어[6-7] 이를 보안한 일회용 패스워드 시스템을 제안하였고 현재 IETF RFC 2289에 표준화 되었다[8]. 하지만 일회용 패스워드 시스템 역시 사용자만 인증하고, 사용횟수를 제한하는 단점을 가지고 있다.

Von Neumann에 의해 소개된 셀룰러 오토마타는 임의의 시점에서 유한개의 상태를 가진 임의의 개체 셀이 셀 공간상에서 이웃한 cell들과 정해진 규칙에 따라 다음 시점의 상태로 변화하는 연산을 반복적으로 수행한다. 하드웨어 구현에도 적합하며 연산 속도가 빠른 셀룰러 오토마타는 자기재생 모델, 언어 인식, 의사난수 생성, 암호기술 등 많은 응용 분야에 활용되고 있다[9-11].

본 논문에서는 병렬성을 가짐으로써 연산속도가 빠른 셀룰러 오토마타를 이용하여 일회용 패스워드를 생성하여 효율성을 높인다. 뿐만 아니라 사용자와 서버의 상호인증을 위한 인증인자 생성에도 적용하여 보다 안전한 인증방식을 제안한다. 이를 위해 2절에서는 대표적인 일회용 패스워드 인증 방식인 일회용 패스워드 시스템과 셀룰러 오토마타에 대해 살펴보고, 3절에서 제안하는 인증 방식을 기술하고, 제안된 방식에 대한 안전성을 분석한다. 마지막으로 4절에서 결론을 맺는다.

2. 관련 연구

본 절에서는 S/KEY 일회용 패스워드 시스템의 결점을 보완한 RFC 2289 표준방식에 대해 살펴보고, 제안하는 인증방식에서 일회용 패스워드와 인증 인자 생성에 이용되는 셀룰러 오토마타의 기본 개념을 기술한다.

2.1 RFC 2289 일회용 패스워드 시스템

RFC 2289 방식은 S/KEY 방식인 RFC 1760의 체제를 보완시켜 표준화한 것이다. 이 방식에서는 일회용 패스워드 시스템의 운용을 위하여 두 개의 실체인 생성기와 서버를 가진다. 생성기는 사용자의 비밀 패스워드와 서버로부터 수신한 시도에 포함된 정보 즉 종자 값 (seed)을 함께 해시함수에 입력시켜 반복연산을 통해 하나의 일회용 패스워드를 생성한다. 매번 인증을 성공한 후에

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

는 해시함수의 반복 횟수를 하나씩 감소하여야 한다. 서버는 종자 값을 생성하여 해당 생성기로 보내야 하고, 수신한 일회용 패스워드를 검증하며, 수신한 바로 이전의 일회용 패스워드와 순차번호를 저장해야 한다. 일회용 패스워드의 검증은 생성기로부터 수신한 일회용 패스워드를 해시함수에 한번 적용시켜 연산한 후 그 결과를 이전에 접수한 일회용 패스워드와 비교함으로써 이루어진다. 구조가 단순하고 패스워드 노출이나 재전송 공격에 안전하지만, 초기에 사용횟수를 제한하고 사용자에 대한 인증만 이루어져서 위장공격에 취약한 문제점을 가진다. 또한 수백회 이상의 해시연산을 반복함으로써 연산 복잡도가 높은 단점이 있다.

2.2 셀룰러 오토마타

규칙성을 가지고 서로 연결된 여러 셀들로 구성된 CA는 상태갱신에 적용되는 규칙과 이웃 셀의 개수, 상태의 수와 경계조건 등의 요소들로 특징지어 진다. 각 셀들의 값은 규칙 R에 의해 이산 시간 단계에서 병렬적으로 갱신되고, 전체 셀들의 값이 갱신되는 것을 진화라 한다. S_i^t는 t 단계에서의 i 번째 셀의 상태이고, r은 이웃(neighborhood)의 반경 이라 할 때, 규칙 R은 다음과 같이 나타낸다.

$$S_i^{t+1} = R(S_{i-r}^t, \cdots, S_{i-1}^t, S_i^t, S_{i+1}^t, \cdots, S_{i+r}^t)$$

이웃은 $m = 2\times r + 1$ 개의 셀로 구성되고, 이웃의 상태는 2^m개 존재한다. 이는 규칙이 2^{2^m}개가 존재함을 의미한다. 예를 들어, 이웃의 반경 r이 1인 CA는 256개의 규칙을 가진다. 규칙은 일반적으로 규칙번호로 나타내고, 규칙번호는 셀의 다음상태를 진리표 형태로 표현했을 때, 출력 열의 10진 표현이다. 그림 1은 이웃 반경이 1인 CA의 규칙번호 표기방식을 나타낸다.

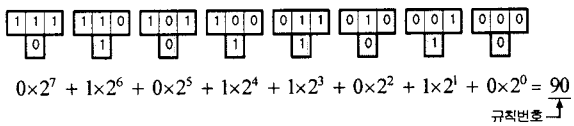

그림 1 규칙 90

경계조건이란 CA를 구성하는 셀들 중 가장 오른쪽 셀의 오른쪽 이웃이 존재하지 않기 때문에 이를 처리하는 조건을 말한다. 양쪽 끝 셀의 값을 '0'으로 간주하는 것을 null 경계조건이라 하고, 가장 왼쪽 셀과 가장 오른쪽 셀이 이웃한 것으로 간주하는 것을 periodic 경계조건이라 한다.

3. 제안한 인증 방식

본 절에서는 제안된 인증방식을 등록단계, 서버 인증단계, 그리고 사용자 인증단계로 나누어 설명하고, 기존의 방식과 비교, 분석한다.

3.1 용어 정의

제안된 방식에서 사용되는 시스템 계수를 다음과 같이 정의한다.

- CA_p : 일회용 패스워드를 생성하기 위한 CA
- CA_v : 인증인자를 생성하기 위한 CA
- R_p, R_v : CA_p, CA_v의 진화연산 규칙
- SEED : 일회용 패스워드 설정 초기 값
- ID_U : 사용자 U의 계정
- PW_U : 사용자 U의 비밀 패스워드
- $H(\cdot)$: 안전한 일방향 해시 함수
- X_n : CA를 n번 진화 연산하여 생성된 일회용 패스워드
- E : CA를 이용한 진화연산 횟수 or CA에 규칙을 적용한 진화연산 횟수
- N_U, N_S : 사용자 또는 서버가 생성한 nonce
- V_U, V_S : 사용자 또는 서버의 인증인자

3.2 제안된 인증 방식

제안하는 인증방식은 등록, 서버 인증, 그리고 사용자 인증의 3단계로 구성되며 각각의 단계는 다음과 같다.

(1) 등록 단계

이 단계는 오프라인 또는 안전한 채널 상에서 이루어진다. 서버는 일회용 패스워드를 생성하기 위한 CA 규칙 R_p와 사용자와 서버의 상호 인증 인자를 생성하기 위한 CA 규칙 R_v, 그리고 SEED를 생성하여 사용자에게 전달한다. 사용자는 SEED와 함께 자신의 비밀 패스워드를 연접해 해시 함수 H()를 수행하여 해시값 X_0를 만들어 서버에 안전하게 전송한다. 서버는 사용자의 계정 ID_U와 함께 초기 패스워드 X_0를 저장한다. 사용자와 서버는 각각 CA_p, CA_v를 가지고, X_0는 CA_p의 초기 상태가 된다. 그림2는 등록단계를 나타낸다.

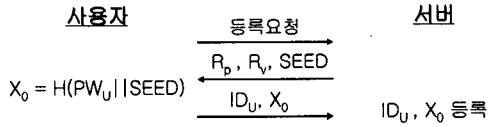

그림 2 등록 단계

(2) 서버 인증 단계

사용자는 서버에 로그인하기 위해 N_U를 생성하여 ID_U와 함께 전송한다. 서버는 수신된 N_U를 CA_v의 초기상태로 두고 등록단계에서 결정된 R_v를 적용하여 서버 인증인자 V_S를 생성한다. Nonce N_s를 생성하고, 사용자가 일회용 패스워드를 생성하기 위해 규칙 R_p를 사용하는 CA_p의 진화연산 횟수인 E를 랜덤한 값으로 생성한다. 생성된 세 인자를 사용자에게 전송한다. 사용자는 자신이 생성한 N_U를 CA_v의 초기상태로 두고 진화연산 시킨 값과 전송된 V_S이 동일한지 확인하고, 동일하다면 정당한 서버로 인증된다.

(3)사용자 인증 단계

서버 인증 과정을 거쳐 정당한 서버임이 확인되면 사용자는 전송된 N_s를 CA_v의 초기상태로 두고 진화연산 시켜 사용자 인증인자 V_U를 생성한다. 초기 패스워드 X_0를 CA_p의 초기상태로 두고 E번 진화연산 시킨 값, 즉 일회용 패스워드 X_E를 V_U와 함께 서버에 전송한다. 서버는 먼저 N_s를 CA_v의 초기상태로 두고 진화연산 시킨 값과 전송된 V_U를 비교한다. 그 결과 두 값이 동일하다면 등록 단계에 저장된 X_0를 CA_p의 초기상태로 두고 E번 진

화연산 시킨 값이 X_E와 같은지 확인하고, 만약 동일하다면 정당한 사용자로 인증한다. 그림3은 서버 인증과 사용자 인증 단계의 흐름도이다.

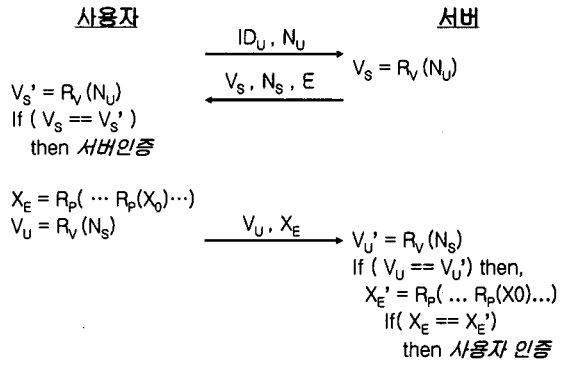

그림 3. 제안 방식의 흐름도

3.3 제안 방식 분석

제안된 인증 방식에서는 패스워드를 평문으로 전송하지 않으므로 패스워드 노출에 대한 염려가 없다. 초기 패스워드 생성과정에 사용자의 비밀 패스워드뿐만 아니라 서버가 생성한 큰 랜덤수 SEED를 함께 해시함수에 적용함으로써 오프라인 사전공격에 안전하다. 또한, 서버는 사용자가 접속 요구 시 매번 진화연산 횟수를 랜덤하게 생성하여 전송하므로 재전송 공격을 수행할 수 없다. 그리고 사용자와 서버가 생성한 nonce를 CA의 진화연산을 통해 인증인자를 생성하여 상호인증 하므로 공격자의 서버 스푸핑 공격을 방지할 수 있다. 또한 동시에 인증 세션을 개시하지 않도록 함으로써 레이스 공격을 막고, 타임아웃 옵션을 둔다면 서비스 거부 공격 역시 막을 수 있다[8]. 뿐만 아니라 제안 방식은 패스워드 사용 횟수에 대한 제한이 없다. CA의 진화연산은 비트연산자로만 이루어져 있으므로 연산속도가 해시함수보다 빠르며 구현이 용이하다. 표1은 기존의 일회용 패스워드 인증 방식과 제안한 인증 방식의 안전성 및 효율성을 비교 분석한 결과이다.

표. 1 제안 방식의 안전성 및 효율성 비교

	S/KEY 방식	RFC 2289	제안 방식
사용 횟수	n회	n회	제한 없음
패스워드 노출 방어	O	O	O
재전송 공격 방어	O	O	O
사전공격 방어	X	O	O
서버 스푸핑 공격 방어	X	X	O
상호 인증	X	X	O

4. 결 론

본 논문에서 셀룰러 오토마타를 이용하여 일회용 패스워드를 생성하고 상호 인증인자를 생성하여 안전하고 효율적인 상호인증을 가능하게 하는 인증 방식을 제안하였다. 제안한 방식은 병렬성을 가짐으로써 연산 속도가 빠르고 구현이 용이한 CA를 이용하여 효율성을 높이고, 패스워드의 사용횟수에 제한이 없다. 재전송 공격, 오프라인 사전공격에 안전하고, 사용자에 대한 인증뿐만 아니라 서버에 대한 인증과정을 통해 서버 스푸핑 공격을 막을 수 있다. 따라서 제안된 방식은 효과적인 일회용 패스워드 인증방식으로 사용될 수 있을 것으로 기대한다.

참고문헌

[1] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, Vol. 24, pp. 770-772, 1981.

[2] T. Kwon, "Authentication and key agreement via memorable password," *Proc. 2001 Internet Society Network and Distributed System Security Symposium*, San Diego, CA, Feb. 2001.

[3] T. Wu, "The Secure remote password protocol," Proc. *1998 Internet Society Network and Distributed System Security Symposium*, San Diego, CA, March 1998.

[4] S. M. Bellovin and M. Merritt, "Augmented encrypted key exchange: A Password-based protocols secure against dictionary attacks and password file compromise," *Proc. the First ACM Conference on Computer and Communications Security*, pp. 244-250, Dec. 1993.

[5] N. Haller, "The S/KEY One-Time Password System," RFC 1760, Feb. 1995.

[6] S. M. Yen and K. H. Liao, "Share authentication token secure against replay and weak key attacks," Information Processing Letters, Vol. 62, pp. 77-80, 1997.

[7] C. J. Mitchell and L. Chen, "Comments on the S/KEY user authentication scheme," ACM Operation Systems Review, Vol. 30, No. 4, pp. 12-16, Oct. 1996.

[8] N. Haller, C. Metz, P. Nesser, and M. Straw, "A One-Time Password System," RFC 2289[std61], Feb. 1998.

[9] J. Von Neumann, A. W. Burks, *Theory of Self-Reproducing Automata*, University of Illinois Press, Champaign, IL, 1966.

[10] A. Smith, "Real-time language recognition by one-dimensional cellular automata," *J. Comput. Syst. Sci.*, Vol. 6, pp. 233-253, 1972.

[11] G. Sheng-Uei and L. Syn Kiat, "Pseudorandom Number Generation with SelfProgrammable Cellular Automata," *IEEE Trans. on Computer Aided Design of Integrated Circuits and System*, Vol. 23, No. 7, pp. 1095-1101, 2004.