PingPong-128 키 수열 발생기를 이용한 모바일 보안 토큰에 관한 연구

김낙현*· 조상일* · 김태용** · 장원태** · 이훈재**

*동서대학교 유비쿼터스 IT학과

**동서대학교 컴퓨터 정보공학부

On a mobile security token using the PingPong-128 Generator

Nack Hyun Kim* · Sang Il Cho* · Tae Yong Kim** · Won Tae Jang** · Hoon Jae Lee**

*Dept. of Ubiquitous IT, DongSeo University

**Div. of Computer & Information, DongSeo University

E-mail : redroopang@hotmail.com

요 약

인터넷상에서 본인 고유의 서비스를 받기 위해서 본인인증 절차는 필수 요소이다. 본인인증 방법 중 가장 보편적으로 아이디/패스워드 방식이 사용되고 있다. 그러나 아이디/패스워드방식이 사용자 인증방법으로서 보안적 문제점이 발견되어, 추가적인 인증방법이 사용되고 있다. 그 예로, 공인 인증서, 보안카드, OTP(One Time Password)등이 있다. 이러한 추가적인 인증 방법들도 사용자의 부주의와 해킹 툴 등으로 인하여 완벽한 인증 방법이 아니라는 것이 확인 되었다.

본 논문에서는 기존에 사용되고 있는 인증 방법들에 대한 문제점들을 분석 후 PingPong-128 키 수열 발생기를 이용하여 보안 토큰을 생성 하여 서비스 제공자와 서비스 이용자 상호간의 안전한 인증방안을 제안한다.

ABSTRACT

In the internet communication technology, authentication of the user is main task. So far, very popular researches have been proposed for user authentications based on user_id and password. These existing methods have some merits as well as demerits also.

In this paper, we analyzed the existing authentication method problems and implement a secure PingPong -128 based key generator for internet technology. In our new scheme, we are using one time password and security card numbers to generate the secure tokens for the user and internet service provider.

키워드

Security, PingPong128 Generator, 보안토큰, 보안카드, OTP

Ⅰ. 서 론

정보통신 기술이 발달함에 따라 웹 서비스를 통한 생활이 보편화 되어 있다. 대부분의 웹 서비스들은 아이디/패스워드 방식을 사용하여 사용자에 대한 인증을 실시한다. 그러나 아이디/패스워드 방식으로만 사용자 인증을 할 경우 상당히 많은 보안 위협을 가진다.

이에 따른 피해를 막고자, 추가적인 인증 방법들이 제시되고 있다. 그 예로 공인인증서, 보안카드, OTP(One Time Password)토큰 등이 있다. 그

러나 사용자의 부주의와 해킹 툴 등으로 인해 안전하지 못하다는 것이 확인되었다. 공인인증서의 경우 포렌식 툴을 이용하여 삭제된 공인인증서를 복구가 가능하고 개인키 암호화 패스워드 또한 검출및 검증이 가능 하다. 그리고 보안카드는 키보드 후킹(Keyboard hooking)이나 파밍(Pharming)과 같은 방법으로 보안카드 숫자의 탈취가 가능하여 보안카드의 숫자를 알아낸다. OTP의 경우 피싱(Phishing) 공격으로 탈취한 OTP값으로 악의적인 사용이 가능하다.

본 논문에서는 기존에 사용되고 있는 사용자 인증 방법들의 각각의 문제점을 살펴본다. 그리고 그에 따른 문제점을 보완 하고자 PingPong128 키 수열 발생기를 이용하여 매번 새로운 숫자를 생성하는 보안카드 형태의 보안토큰을 제안한다.

II. 관 련 연 구

2.1 공인인증서

공인인증서는 공인인증기관에서 발행하는 전자적 정보로서, 전자서명의 검증 및 암호화에 필요한 공개키에 소유자 정보를 추가하여 만든 일종의 전자 신분증이다.

공인인증서에는 사용자가 공개키가 저장되며 개인키 저장 파일에는 사용자 개인키가 저장된다. 사용자의 개인키는 다른 사용자에게 노출되면 보안상의 위험이 있으므로 SEED블록 암호 알고리즘을 이용하여 암호화한다. SEED블록 암호 알고리즘에 사용되는 비밀키는 사용자의 개인키 암호화 패스워드를 이용하여 생성된다. 전자서명시스템에서 사용되는 공인인증서와 개인키 저장파일은 현재 X.509 v3의 기준에 따라 작성되며 “TTA, TTAS.KO-12.0012, 전자서명 인증서 프로파일 표준, 2002”와 “TTA, TTAS.KO-12.0013, 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준, 2001”에 국내 표준 및 규격이 명시되어 있다.[1]

공인인증서를 사용하기 위해서는 관련 파일들을 저장하여야 한다. 하드 디스크 드라이브와 USB드라이브를 주로 사용하게 되는데, 이러한 저장매체에 저장하여 사용 후 삭제를 하더라도 포렌식 툴을 이용하여 아무런 제약 없이 복구가 가능하다. 그리고 복구한 공인인증서의 개인키 암호화 패스워드 또한 검출과 검증이 가능하기 때문에 보안의 위협을 받고 있다. 그리고 공인인증서가 폐기 되더라도 사용자가 패스워드를 변경하지 않을시 상당한 위험을 초래한다.[2]

2.2 보안카드

인터넷뱅킹에서 안전성을 확보하기 위하여 30여개의 4자리 숫자 표로 구성된 카드이며, 비밀번호 생성에 870~1190개의 경우의 수를 가진 조합표이다. 그림1. 과같이 숫자 표상에서 임의적으로 두가지 번호에서 각각 그 번호에 속해있는 앞(a), 뒤(b) 두자리 숫자를 입력하는 방식이다.

일종의 일회성 비밀번호처럼 사용된다. 그러나 30여개로 구성된 번호와 4자리의 숫자는 변하지 않으므로 동일한 숫자를 재사용하는 경우가 빈번하여 일회성 비밀번호로서의 가치가 떨어진다. 그리고 파밍(Pharming)과같이 사용자의 도메인을 탈취하거나, 도메인 네임 서버(DNS) 또는 프록시 서버 주소를 변경하여 사용자가 정상 사이트 주소를 입력하더라도 위조 사이트로 접속되는 경우가 발생하면 보안카드는 경우의 수가 늘어나는 패스워드로 전락 하고 만다.

그림1. 보안 카드 견본

2.3 OTP(One Time Password)

OTP(One Time Password)는 사용자가 인증요구를 할 때 마다 새로운 비밀번호를 생성하여 사용하는 방식이다. 사용자와 인증기관과의 동기화 여부에 따라 동기화 방식과 비동기화 방식으로 나누어 진다[3].

OTP는 금융감독원의 전자거래 안전성 강화 종합대책에 의하여 거래금액이 일정액 이상일 경우 OTP사용을 의무화와 OTP 통합인증센터의 설립으로 인하여 인증 방법으로써 각광을 받고 있다.

그러나 OTP도 완벽한 보안 서비스를 제공하지는 않는다. 그 예로 피싱(Phishing) 공격[4]의 경우 공격자가 가상의 피싱 사이트를 만들어 인증에 사용되는 OTP값을 획득하여 인증 유효 시간 이전에 인증을 받을 수 있다. 이것은 2006년 7월 미국 씨티은행에서 발생한 해킹 사건으로 확인할 수 있다.

III. PingPong128 키 수열 발생기

PingPong128 키 수열 발생기[5]는 선형 귀환 이동 레지스터(LFSR, Linear Feedback Shift Registers)를 이용한 스트림 암호화 알고리즘 이다. LFSR은 선형성 때문에 출력 수열로부터 쉽게 예측이 가능하며, 길이가 L인 LFSR에 대하여 키 수열의 완전한 주기가 알려지면 수열의 연속 L항으로부터 구해지고, 알려져 있지 않다면 2L항으로부터 알 수 있다.[6] 그러나 조합 함수 또는 필터 함수를 이용한 비선형 부울 함수를 사용하거나, 불규칙한 클럭 제어 LFSR을 사용하는 방법으로 스트림 암호의 비선형성을 증가시킬 수 있다.

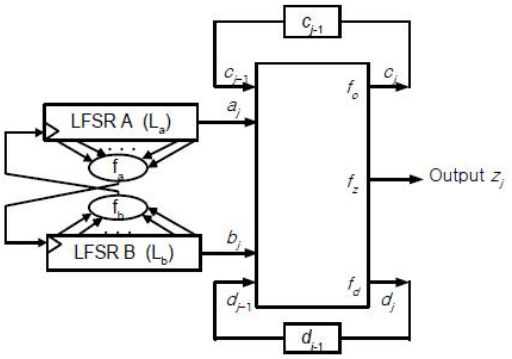

그림 2. PingPong128 키 수열 발생기

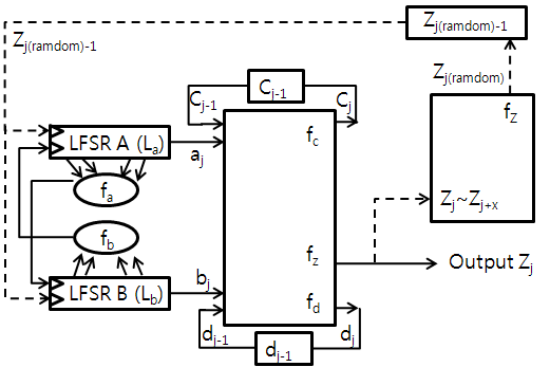

그림 3. 변형된 PingPong128 키 수열 발생기

PingPong128 키 수열 발생기는 기존의 LM합산 수열 발생기에서 상호 클럭 조절형 구조(Mutual clock-control Structure)를 추가하여 합산 수열발생기를 기초로 하여 그림 2. 와 같다. 상호 클럭 조절형 구조의 목적은 출력되는 키 수열에 비 선형성을 증가시켜 상관 공격 등의 암호해독을 어렵게 하는 것이다.

그림 2.에서 키 수열 발생기는 두 개의 LFSR로 구성되며, 다음 메모리 상태와 키 수열 비트를 생성하기 위해 LFSR의 출력 비트는 결합함수 f_z, 캐리함수 f_c 및 메모리 함수 f_d 에 각각 입력된다. LFSR은 불규칙한 클럭이 공급되며, 하나의 LFSR에 공급되는 불규칙 클럭수는 나머지 LFSR에서 생성된 비선형 필터함수(f_a 또는 f_b)로부터 얻어진다. 두 개의 LFSR 상태는 두 LFSR의 기억상태의 내용을 위해 정의되고, 시점 j에서 출력 z_j 는 f_z에 의해 생성된다. 캐리 상태는 c_j 는 f_c에 의해, 메모리 상태 d_j는 f_d에 의해 정의된다. 클럭 조절함수 f_a와 f_b는 두 LFSR의 현 상태에 의해 얻어지며, LFSR은 랜덤하게 클럭 조절된 후 캐리, 메모리 및 키 수열 출력을 생성한다. 또한, LFSR의 불규칙 클럭은 나머지 LFSR의 특정한 두 탭의 내용에 따라 클럭 수가 랜덤하게 결정된다. PingPong128 키 수열 발생기는 처음 초기화 과정에서 키(k)와 초기화 벡터(i, initial key)로부터 내부 상태가 채워지며, 내부 상태 길이가 키 길이보다 더 길기 때문에 내부 상태를 채우기 위한 키 확장 과정이 요구된다.

키 수열 발생기의 초개상태를 생성하는 과정은 발생기 자체를 두 번 사용하고 L_a의 시작 상태는 $L_a = (k \oplus iv) \bmod 2^{127}$ 같이 나타낸다. 그리고 L_b는 $L_b = (k<<1) \oplus (0 \mid iv)$로 나타낸다.

Ⅳ. PingPong128 키 수열 발생기를 이용한 보안 토큰

본 논문에서는 제안하는 PingPong128 키 수열 발생기는 기존의 PingPong128 키 수열 발생기에서 생성되는 비트 스트림을 배열하여 시점 j에서부터 추가 시점 x 까지의 비트들을 나열한다. 나열한 시점들 중에서 f_z를 이용하여 임의의 한 부분인 $Z_{j(ramdom)}$를 추출하고 키 수열 발생기의 초기화 과정에서 사용되는 초기화 백터와 exclusive OR 하여 새로운 비트 스트림의 생성을 가능하게 한다. 이러한 과정은 그림 3.을 통하여 확인 할 수 있다.

키 수열 발생기의 초기 상태는 $La = (PIN \oplus (iv \oplus Z_{j(random)-1}))$, $L_b = (k<<1) \oplus (0 \mid iv \oplus SN_{j(random)-1})$로 정의 할 수 있다.

그림 3.에서 나열된 시점들인 Z_j~Z_{j+x}를 보안토큰에서 구현되는 보안카드의 형태로 표기하고, $Z_{j(ramdom)}$를 인증에 사용된 패스워드로 가정을 하면 제안 하는 인증 구조에서 초기 등록 후 별도의 동기화 없이 지속적으로 새로운 키로 생성해 내는 일회용 보안카드가 생성 가능 하다.

전체적인 인증구조는 사용자가 로그인을 하면 웹 서버는 인증서버에게 사용자의 정보를 전송한다. 사용자 정보를 받은 인증서버는 사용자에 대한 정보를 확인 후 사용자 인증에 사용될 인증번호의 좌표와 웹 서버 체크 포인트를 웹 서버에게 전송 한다. 웹 서버 체크 포인트는 보안카드의 일정한 부분을 공개하여 사용자가 자신의 보안 토큰과 공개된 부분을 직접 확인하는 방식이다. 사용자는 인증번호 좌표와 웹 서버 체크 포인트를 확인 후 인증번호를 전송 한다. 인증 서버는 사용자 인증 번호를 확인하여 승인 여부를 결정한다.

그림 4.는 사용자와 인증기관 간의 초기 등록 과정을 타나낸다. 사용자는 자신의 고유 번호인 PIN Number와 임의 난수 R-N(Ramdom Number)를 인증기관의 공개키를 사용한 암호문으로 전송한다. 인증기관은 전송받은 메시지를 복호화하여 PIN과 R-N을 획득 한다. 그리고 사용자와 인증기관 모두가 PIN과 R-N를 키(k)와 초기 백터(iv)로 사용하여 PingPong128 키 수열을 발생시킨다. 사용자는 일정 길이의 키 수열을 인증기관에게 전송하고 인증기관은 자신의 키 수열과 비교하여 일치하면 초기 등록을 마친다.

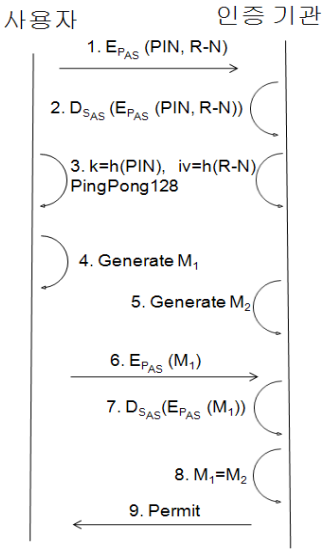

그림 4. 초기 등록 과정

초기등록이 완료가 되면, 그림 5.와 같이 제안하는 인증 방법에 따라서, 사용자는 웹을 통하여 로그인을 한다. 이때 웹 서버는 사용자 정보를 인증기관에게 전송하게 되고, 인증기관은 초기등록 시 저장되어 있는 PIN과 R-N을 키(k)와 초기화 백터(iv)로 사용하여 SC(Security Card)를 생성하게 된다. 그리고 사용자가 입력해야할 보안 카드의 좌표 SCC(Security Card Coordinate)와 웹 서버에서 공개할 보안카드 번호인 CP(Check Point)를 결정 하고 웹 서버에게 전송한다. 이때 사용자 또한 모바일 기기 상에서 PIN과 R-N을 사용하여 보안카드를 생성 한다. 그리고 사용자의 보안카드의 CP와 웹상에서 표시 되어 있는 CP의 동일 여부를 확인하고, 동일하다면 정당한 사이트로 판명할 수 있다.

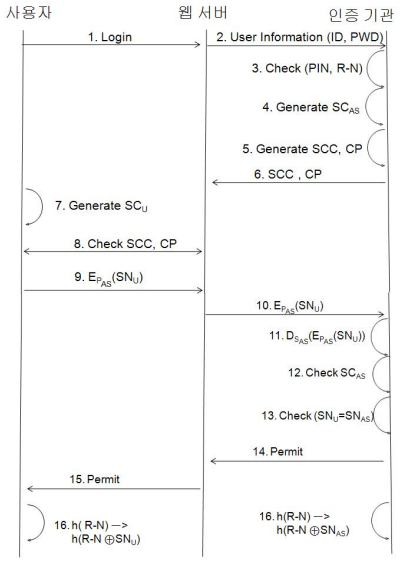

그림 5. 제안 하는 모바일 보안토큰 인증

현재의 사이트가 합당한 사이트라고 가정을 하면, 사용자는 자신의 인증에 사용될 SN(Security Number)을 입력하여, 인증기관의 공개키를 사용한 암호문으로 웹 서버를 통하여 인증기관에게 전송된다. 인증기관은 전송받은 SN을 비밀키로 복호화 하여, 자신의 SC에서 추출해낸 SN와 비교하여 승인 여부를 결정한다.

Ⅴ. 결 론

본 논문에서는 PingPong128 키 수열 발생기를 이용한 비트열에서 임의의 시점에서 출력된 비트를 초기화 벡터와 연산하여 새로운 비트열을 생성하도록 변형하고, 제안하는 방식에 이용하였다.

제안하는 모바일 보안토큰은 보안카드와 OTP의 혼합 방식으로, 기존에 사용하는 보안카드의 형태를 유지하고 있으며, 보안카드의 숫자는 OTP와 같이 지속적으로 변하는 구조 이다. 보안카드의 일회성으로 보안카드의 유출 또는 복제, 패스워드 추측, 키보드 후킹에 대한 보안성을 높이고, 웹 체크 포인트의 활용으로 피싱과 파밍 및 이에 유사한 공격 대한 보안성을 높일 수 있다.

추후 모바일과 인증기관간의 동기화를 위협하는 공격을 예방 하고, 시스템의 부하를 줄일 수 있는 방안을 연구하고자 한다.

참고문헌

[1] 한국 정보보호 진흥원, "공인인증서 표시를 위한 기술규격", Vol. 1.10, 2008.10

[2] 최윤성, 이영교, 이윤호, 박상준, 양형규, 김승주, 원동호, “삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출”, 한국정보보호학회, 정보보호학회논문지 제17권 제1호, pp 41-55, 2007.2

[3] 이장춘, 이훈재, 김태용, “스트림 알고리즘을 이용한 OTP 생성 및 동기화 인증 프로토콜”, 한국해양정보통신학회 추계종합학술대회, 2007

[4] Danesh Irani, Steve Webb, Jonathon Giffin,, Calton Pu, “Evolutionary Study of Phishing", eCrime Researchers Summit ,pp. 1-10, 15-16 Oct. 2008.

[5] 이훈재, 문상재, 박종욱, “PingPong-128 키 수열 발생기", 한국통신학회논문지, Vol. 31, No. 1C, pp. 80-87, 2006

[6] E. Dawson, "Cryptanalysis of Summation generator", Advances in Cryptology - ASICRYPT'92, Lecture Notes in Computer Science, Vol. 718, pp. 209-215, Springer-Verlag, 1993