안전한 상거래를 위한 가상 비밀번호 입력 시스템

권만준, 이원호
아주자동차대학
e-mail: mjkwon@motor.ac.kr

Virtual Password Input System for the secure Electronic Transactions

Mann Jun Kwon, Won Ho Lee
Ajou Motor College

요 약

본 논문에서는 사용자의 원천 비밀정보의 직접적인 유출을 근본적으로 방지하고자, 사용자 스스로가 원천 비밀정보를 이용해 일회성의 가상 비밀정보를 생성, 키보드입력 및 화면 훔쳐보기와 리플레이 공격, 그리고 피싱 등의 공격으로부터 안전성을 보장할 수 있는 가상 비밀번호 입력 시스템을 제안한다.

1. 서 론

인터넷 환경이 디지털 경제의 신경망으로 인식되기 시작하면서 인터넷뱅킹, 전자상거래가 신 경제의 핵심으로 자리 잡게 되었다. 이러한 디지털 경제의 출현은 우리생활에 풍요롭고 편리한 구조를 제공하지만 해킹에 의한 개인정보(아이디, 비밀번호, 주민번호 등)의 유출로 인하여 사용자에게 치명적인 손해를 입힐 수 있는 양면성을 가지고 있다. 해커들이 과거에는 시스템을 마비시키는 불특정 다수에 대한 공격을 했다면 근래에는 피싱, 백도어, 악성코드 등 특정인의 정보를 수집하여 해킹하는 방식으로 바뀌고 있으며 이러한 공격에 의한 사고가 현실화 되어 다가오고 있다.

이에 따라 다양한 보안 강화책을 수립하여 대처해 나가고 있지만 잔존하고 있는 문제점들을 살펴보면 나날이 발전하여 생성되는 해킹 프로그램에 대한 수집, 분석 능력에 한계가 있으며, 특히 상용 키로그 프로그램 및 원격접속 프로그램에 대해서는 탐지가 곤란한 실정이다. 공인인증서의 경우도 PC 해킹을 통한 가로채기 및 키로그 프로그램 등을 통한 훔쳐보기로 안전함을 보장하는데 무리가 있다. 인감도장처럼 사용되는 사용자의 서명용 키를 단순히 PC나 일반 저장매체 등에 손쉽게 관리하는 것이 일반화 되었으며 이런 상황에서는 해커가 사용자의 ID 및 비밀번호(Password)와 함께 전자서명용 키를 탈취하는 것은 어렵지 않으며 PKI 시스템을 사용하더라도 현재와 같은 사이버 범죄가 발생할 위험성은 존재한다고 볼 수 있다. 즉, PKI 기반의 서비스는 키 관리와 전자서명 행위가 독립적인 보호 장치 속에서 이루어져야만 만족할만한 안전도를 갖춘다고 할 수 있을 것이다.

이를 보완하기 위해 또 다른 인증 솔루션으로 일부 일회성 암호생성기(OTP)를 사용하고는 있지만 하드웨어 토큰의 구입, 유지, 관리 등에 따르는 비용을 감수하더라도 개별 토큰에 PIN(Personal Identity Number) 형식의 비밀번호를 더 외워야 한다는 부담과 비밀번호, 계좌번호, 주민번호, 카드번호 등의 비밀정보에 대해서는 여전히 무방비 상태로 노출된다는 것이다. 아무리 강력한 PKI환경의 암호화 솔루션으로 보호한다고 해도 사용자의 중요한 비밀정보를 입력단에서 가로채기한다면 모든 것이 허사로 종결되고 만다는 것을 간과해서는 안 되는 것이다. 이와 같은 현상에서 가장 효율적인 해결책은 사용자의 원천 비밀정보인 인감도장에 대한 사용권한을 보호함으로써 이루어 질 수 있다.

본 논문에서는 이러한 사용자의 원천 비밀정보의 직접적인 유출을 근본적으로 방지하고자, 사용자 스스로가 원천 비밀정보를 이용해 일회성의 가상 비밀정보를 생성, 키보드입력 및 화면 훔쳐보기와 리플레이 공격, 그리고 피싱 등의 공격으로부터 안전성을 보장할 수 있는 가상 비밀번호 입력시스템을 제

안한다.

2. 시스템 개요 및 프로토타입

진정한 의미의 비밀정보는 사람의 머릿속에만 있고 그것이 어떠한 직접적인 행위로도 표출 되어서는 안 된다는 것이 가장 안전한 형태의 보안시스템이라 할 수 있다. 안전한 방식의 암호화 시스템이 사용된다 해도 원천적인 비밀정보가 노출되면 모든 것이 무의미하게 된다. 그러나 인터넷의 개방성 환경으로 인해 사용자 자신임을 인증받기 위해 수행되는 행위 절차상에 비밀번호가 해킹 위험에 노출이 될 수밖에 없는 환경이 되었다. 일회성 가상 비밀번호 입력시스템은 이러한 기반의 개념 하에 비밀정보(패스워드 등)를 사용자의 머릿속에서 밖으로 표출시키지 않고 단지 암호화 논리에 따른 키 값으로만 사용, 사람의 행위 자체를 암호화 연산의 도구로 활용하게 함으로써 다양한 공격으로부터 안전성을 보장하게 된다. 즉, 사용자의 간단한 연산 능력으로 생성되는 일회성 가상 비밀번호는 해커에게 해킹당하고 있다는 가정하에서도 더 이상의 가치성을 갖지 못하게 함으로써 사용자 머릿속에 있는 원천 비밀정보가 사용자 자신이 노출하지 않는 한 영원한 확률성을 가진 비밀정보로 유지하게 된다.

가상 비밀번호 입력 시스템은 가상 키 입력시스템의 가장 기본이 되는 방식으로 여러 사용자가 사용하는 자동화기기(CD/ATM), 디지털 도어록과 같은 출입통제 시스템 또는 은행 창구 등에서 쓰이는 비밀번호 키패드 입력시스템과 같이 주변사람이 쳐다볼 수 있고 지속적인 화면 캡처가 가능치 않은 곳에 적용되어 안전성을 보장할 수 있는 가상 비밀번호 입력을 통한 인증 시스템이다. 자동화기기의 예를 들어 그 과정 및 원리를 살펴보면 다음과 같다.

[표 1] 가상 비밀번호 입력시스템의 디스플레이 유니트

(P_1) 1	(P_2) 2	(P_3) 3	(P_4) 4	(P_5) 5	(P_6) 6	(P_7) 7	(P_8) 8	(P_9) 9	(P_0) 0
(pr_1) 9	(pr_2) 7	(pr_3) 3	(pr_4) 2	(pr_5) 4	(pr_6) 5	(pr_7) 6	(pr_8) 1	(pr_9) 0	(pr_0) 8

P_1 P_2 P_3 … : 디스플레이 유니트의 인덱스 값.

pr_1 pr_2 pr_3… : 디스플레이 유니트에 인증서버가 보내준 중복되지 않는 랜덤한 10개의 숫자 값.

① 사용자의 현금카드나 신용카드를 ATM 기에 넣으면 표 1.과 같은 디스플레이 유니트가 화면에 표시된다.

② 디스플레이 유니트 상단의 인덱스에서 사용자는 자신의 비밀번호에 해당하는 값을 찾고, 그 값과 매칭되는 아랫단의 숫자값을 알아낸다.

③ 사용자는 매 인증시마다 알파값(알파값 : 가상 비밀번호 생성을 위해사용자가 매번 임의로 지정하는 숫자)을 자신이 정해 ②의 결과 값에 동일하게 가감하여 일의 자리만 입력한다.

④ 원천 비밀번호의 자릿수만큼 ②~③단계를 반복한다.

사용자는 함수 $F_p(P_i)=pr_i$에 생성된 값에 임의의 값 R을 정하여 10진 모듈러 연산을 한 연산식 (식1)은 다음과 같이 표현한다.

$$\left.\begin{array}{l}(F_p(P_1) + (\pm R)) \bmod 10 = Z_1\\(F_p(P_2) + (\pm R)) \bmod 10 = Z_2\\\quad\cdot\quad\cdot\quad\cdot\\\cdots\cdots\cdots\cdots\text{(식1)}\\\quad\cdot\quad\cdot\quad\cdot\\(F_p(P_n) + (\pm R)) \bmod 10 = Z_n\end{array}\right\}$$

(식1)과 같이 수행되는 연산식에 따라 생성된 일회성 가상 비밀번호 Z_1 Z_2…Z_n를 인증서버에 전달한다.

인증시스템은 아래 연산식 (식2)에 따라 (식1)에서 $F_p(P_i)=pr_i$과 전달받은 일회성 가상 비밀번호 Z_1 Z_2…Z_n를 알고 있으므로, 일회성 가상 비밀번호 Z_1 Z_2…Z_n에 사용자가 정한 알파값 R이 가질 수 있는 숫자값인 0~9까지의 수를 개별 비밀번호 자리에 가감함으로써 원천 비밀번호에 매칭된 값인 pr_i의 집합을 구할 수 있다.

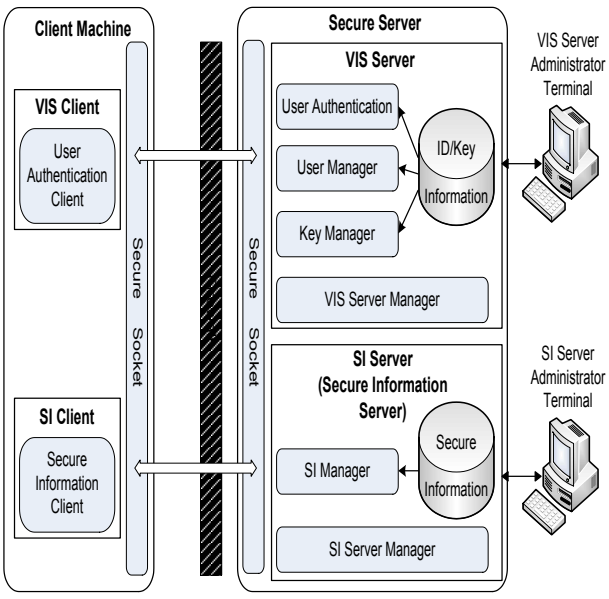
$$\left.\begin{array}{l}P_{1\{i\}} = F^{-1}(pr_i) = pr_i = (Z_i + (R_1)) \bmod 10 \quad (i = \text{비밀번호의 자릿수})\\P_{2\{i\}} = F^{-1}(pr_i) = pr_i = (Z_i + (R_2)) \bmod 10\\\quad\cdot\quad\cdot\quad\cdot\\\cdots\cdots\cdots\text{(식2)}\\\quad\cdot\quad\cdot\quad\cdot\\P_{0\{i\}} = F^{-1}(pr_i) = pr_i = (Z_i + (R_0)) \bmod 10\end{array}\right\}$$

(식2)로부터 10개의 $P_{j\{i\}}$(j= 1 to 10, i= 비밀번호의 자릿수)를 구하여 일치 여부를 판단한다.

여기서 R은 사용자가 일회성 가상 비밀번호 생성

을 위해 인증시마다 임의로 정하여 가감하는 알파값이며, F(x)=y는 x(=1 to 10)값을 인덱스로 해서 매칭값 y를 생성하는 함수이고 $F^{-1}(y)=x$는 y(=1 to 10)를 매칭값으로 해서 인덱스 값 x를 생성하는 역함수를 나타낸다.

위의 방식은 사용자가 일회성 가상 비밀번호를 한 자리씩 입력할 때마다 디스플레이 유니트의 매칭값이 변하게 됨으로 해서 지속적인 화면 캡처와 키로그 프로그램을 통한 입력값의 가로채기 없이는 원래의 비밀번호가 가지고 있는 확률성을 보장함으로 해서 안전성을 갖게 된다. 즉, <표 1>에서 사용자의 원천 비밀번호가 1234라고 할 때 첫 자리만 살펴보면, 사용자가 디스플레이 유니트의 인덱스 값 1에 해당하는 매칭값 9를 보게 될 것이고, 그 순간 알파값 R=3으로 정해 더하기로 결정했다면 일회성 가상 비밀번호 입력값은 10진 모듈러 연산을 하여 1 → 9 + 3 = 12 mod 10 = **2**가 될 것이다. 이때 해커가 화면을 보고 입력값을 가로채기 해킹을 했다 하더라도 사용자가 더한 알파값을 알 수 없음으로 해서 한 자리 숫자가 갖는 0~9까지의 가능성 있는 경우의 수로 추측할 수밖에 없을 것이다. 즉, 디스플레이 유니트의 열개의 인덱스에 해당하는 매칭값은 알파값에 의해 모두 일회성 가상 비밀번호 입력값 2가 될 수 있다는 것이다. 따라서 지속적인 화면 캡처와 입력값 기로채기를 통한 패턴의 파악 없이는 원천 비밀번호의 유추가 불가한 만큼 불특정 다수가 사용하는 자동화기기 등의 적용에는 안전성을 보장할 수 있는 방법이 된다.



[그림 1] 가상 비밀번호 입력시스템 구조도

금융기관의 인터넷 뱅킹시 사용될 가상 비밀번호 입력 시스템 구조도는 다음 [그림 1]와 같이 구성되며, 네트워크 통신망을 통하여 클라이언트-서버 환경시스템에서 인증이 이루어진다. 프로토타입은 [그림 1]와 같은 환경에서 디스플레이 유니트를 통해 구현한다.

3. 결 론

본 논문에서 제안한 가상 비밀번호 입력시스템은 해킹이 되고 있다는 전제하에서도 중요한 비밀정보의 노출을 원천적으로 차단할 수 있으며, 만족할 수 있는 보안의 강도를 보장한다. 또한 다른 일회성 비밀번호의 생성을 통한 인증 메커니즘에서 요구하는 별도 하드웨어의 구입, 분실 및 파손 등에 따른 대응이 필요 없고 온라인, 모바일 및 오프라인 환경의 다양한 응용분야에 적용될 수 있다.

이는 기존 일회성 암호생성기와 달리 개인의 원천 비밀정보가 가상 비밀정보를 생성하는 키값으로 쓰일 뿐 개인의 머릿속에서 노출되지 않으므로 강력한 보안강도를 갖게 된다. 제안 시스템은 이동 단말형 하드웨어로도 쉽게 구현이 될 수 있다.

4. 참고문헌

[1] A. J. Menezes, P. C. Oorschot & S. A. Vanstone,"Handbook of Applied Cryptography", CRC Press LLC, 1997.

[2] Jalal Feghhi, Jalil Feghhi & P. Williams, "Digital Certificates: Applied Internet Security", Addison Wesly, 1999.

[3] RSA Laboratories, "One-Time Password Specification", http://www.rsasecurity.com/rsalabs

[4] 정보통신부, "인터넷상의 개인정보보호 가이드라인(안), 2005년 9.

[5] PCT/kr2006/585 "Apparatus for Inputting Password and Method of Inputting and Decrypting Password"

'이 논문은 2010년 아주자동차대학(산학협력단)의 연구지원을 받아 수행된 연구임'