Keyboard hooking 방지를 위한 패스워드 입력 방법 연구

강승구* 곽진석* 이영실* 이훈재**

*동서대학교

**동서대학교 컴퓨터정보공학부

A study on Password Input Method to Protect Keyboard hooking

Seung-Gu Kang* Jin-Suk Kwak* Young Sil Lee** Hoon Jae Lee*

*Dongseo University

**Div. of Computer and Information Engineering, Dongseo University

E-mail : mintkang1105@gmail.com, monkeykjs@naver.com, attract35@hotmail.com, hjlee@dongseo.ac.kr

요 약

최근 인터넷 기술의 발전으로 인해 웹 서비스의 이용시간 및 장소에 대한 제약 없이 바로 접속할 수 있는 편리성이 제공되어 사용자가 급증하였다. 웹서비스에서는 일반적으로 ID/Password 인증방식을 사용하고 있으며, 사용자인증 후 웹서버에 저장된 사용자의 개인정보를 확인할 수 있다. 이를 보호하기 위해 웹 서비스 공급자는 다양한 보안 기법들을 제공하고 있다. 그러나 사용자가 키보드를 통해서 개인정보를 입력하는 순간에 공격자가 Keyboard hooking 을 이용하여 개인정보가 탈취되는 사건이 최근 발생되고 있다. 이에 본 논문에서는 Keyboard hooking 방지를 위해 패스워드 입력 시 CAPTCHA로 구성된 문자들이 특정 Map상 무작위로 배치되어 이를 마우스나 터치를 통해 입력되는 방법을 제안한다.

ABSTRACT

Recently, Due to development of Internet techniques, user suddenly increased that Used of Web services and with out constraints of place and time has been provided. typically, Web services used ID/Password authentication. User confirmed personal data Stored on Web servers after user authorized. web service provider is to provide variety security techniques for the protection personal information. However, recently accident has happened is the malicious attackers may capture user information such as users entered personal information through new keyboard hooking. In this paper, we propose a keyboard hooking protected password input method using CAPTCHA. The proposed password input method is based on entering the password using mouse click or touch pad on the CAPTCHA image. The mapping of CAPTCHA image pixels is random.

키워드

Keyboard hooking, Password input method, Keylog, CAPTCHA

Ⅰ. 서 론

최근 자주 발생되는 개인정보 유출 사고는 먼저 악의적인 공격자가 사용자의 PC에 바이러스, 악성코드, 기타 해킹 프로그램을 통해 사용자의 컴퓨터를 감염시켜 사용자의 ID, Password 등을 탈취, 이를 이용하여 2차적으로 개인 정보를 탈취하는 과정으로 이루어진다. 또한 탈취된 개인정보를 사용하여 신분 도용 등 추가적인 피해를 발생시키고 있다. 키보드 후킹 공격은 사용자가 PC에서 서비스 이용을 위한 ID, Password 입력 시 키보드의 입력된 값을 탈취하기 위해 많이 활용되고 있다. 또한, 키보드 후킹은 포트해킹, 드라이버 후킹, 메시지후킹 방법 등 다양한 방법으로 이루어진다[1][2].

이에 따라 이러한 공격들을 방어하기 위한 방어대책이 활발히 연구되고 있으며, 그 예로 2007

년 정보보안 논문지에 발표된 김인석 등의 "종단간 암호화(End-to-End Encryption)를 이용한 전자금유거래 정보보호 강화"방법이 제안되었다[3]. 이 방법은 보안 프로그램의 보안기능을 우회하는 해킹 툴을 이용한 데이터 절취 공격에 대한 대응 방안으로 PKI 응용 프로그램과 키보드 보안 프로그램의 연동 시 제공되는 종단간 암호화(End-to-End Encryption) 방안이다. 또한 KISA에서는 그래픽과 마우스를 이용한 입력방법인 SecurePass를 지난 2010년에 발표하였고, 2011년 정보보호학회 논문지에 발표된 맹영제 등의 "모바일 뱅킹에서 비밀퍼즐을 이용한 비밀증명방법과 거래승인방법"은 사용자 서명을 CAPTCHA 이미지로 생성하여 사용자 비밀정보를 보호하고 문서의 내용을 조작하는 공격에 대응하는 방법이다[4][5].

본 논문에서는 keyboard hooking 방지를 위한 새로운 패스워드 입력방법을 제안한다. 제안된 방법은 사용자 패스워드 입력 단계에서 화면에 무작위로 뿌려지는 특정 MAP 상의 문자를 CAPTCHA로 구성하며, 이를 마우스나 터치를 사용하여 패스워드 입력을 수행한다. 제안된 방법은 일반 PC뿐만 아니라 모바일 단말기에서도 적용이 가능하며, 일반 PC에서 사용 시 마우스를 이용하여 입력하고 Smart Phone등 터치스크린을 지원하는 기기에서는 터치를 통해 입력된다.

본 논문의 구성은 다음과 같다. 먼저 2장의 관련 연구에서 CAPTCHA[6-11]와 KISA에서 제안된 SecurePass 입력방식[4]에 대하여 서술하고, 최근 심각한 문제로 대두되고 있는 Keyboard hooking 공격 방법[2]에 대하여 살펴본다. 또한 3장에서 제안하는 입력 방법에 대하여 기술, 4장의 제안한 입력방법에 대한 보안성 분석 그리고 마지막 5장에서 결론을 맺도록 한다.

II. 관련 연구

2.1 CAPTCHA

"CAPTCHA(**Completely Automated Public Turing test to tell Computers and Humans Apart**)"는 컴퓨터와 사람을 구별 할 수 있는 튜링 테스트의 일종으로써, 주로 컴퓨터 소프트웨어에 의한 자동화된 공격을 차단할 때에 사용된다. 현재 CAPTCHA는 자동화된 소프트웨어 대리자에 의한 웹 서비스의 자동 계정생성, 카페 자동가입신청, 블로그 댓글의 스팸광고, 투표 봇, 게시판 글의 자동등록 등을 차단하는데 유용하게 쓰이고 있다[6][7].

자동화된 공격을 막기 위해서 사용되는 텍스트 기반 CAPTCHA는 Yahoo의 EZ-gimpy CAPTCHA, WindowsLive Hotmail CAPTCHA, Windows MSN CAPTCHA, Google의 Gmail CAPTCHA 등이 있다. 이러한 텍스트 기반 CAPTCHA의 경우 OCR(Optical Character Recognition)기술을 이용하여 변형된 글자를 인식할 수 있는 취약점들이 들어나면서 주된 공격 대상이 되었다. 이를 보완하기 위해 이미지 기반의 CAPTCHA와 문자의 색상을 다르게 하는 CAPTCHA, 텍스트와 이미지를 융합한 형태의 CAPTCHA등 다양한 방법들이 제안되고 있다[8][9][10]. 또한 최근에 움직이는 형태의 CAPTCHA가 소개되면서 기존의 정적인 텍스트/이미지 기반에서 벗어나 동적인 형태의 CAPTCHA로 발전해가고 있는 추세이다[11].

그림 1. CAPTCHA의 형태

2.2 KISA의 SecurePass

2010년 4월 발표된 KISA(Korea Internet Security Agency, 한국인터넷진흥원)의 SecurePassr기술은 키로깅(Key Logging) 및 숄더 서핑(Shoulder Surfing) 공격에 취약한 키보드 입력 방식을 대체하기 위한 기술로써, 그래픽과 마우스를 이용해 패스워드를 입력하는 방식이다.

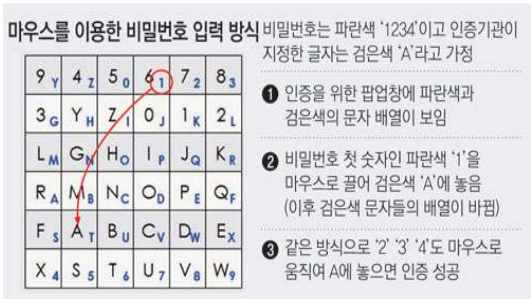

그림 2. KISA의 SecurePass 입력방식

그림 2과 같이 KISA의 SecurePass기술은 그래픽을 이용한 패스워드 입력판상에서 각각 검정색 상층 문자와 파란색 하층문자가 랜덤하게 배열된다. 이때 사용자의 패스워드가 '1234' 이고 인증기관이 지정한 글자는 검은색 'A'라고 한다면, 파란색 '1'에 해당하는 Pixel을 마우스로 드래그 하여 지정된 글자의 위치로 이동시켜 입력하게 된다. 이후 패스워드 입력판은 무작위로 재배치되며 남

은 패스워드 입력도 같은 방식으로 움직여 입력하게 되고, 마우스 입력이 종료되면 사용자 인증이 이루어진다. 하지만 패스워드 입력 시 마다 Graphic Map은 재배치되어야 하며, 이것은 연산과정의 증가로 인한 연산속도의 저하와 필요 메모리공간의 증가로 이어 질 수 있다.

2.3 키보드 후킹 공격기법

키보드 후킹 공격기법은 포트해킹, 드라이버후킹, 메시지후킹 등이 있다. 이중 키보드 포트 해킹은 MCU의 키보드 포트를 여러번 읽을 수 있는 취약점을 이용한 공격으로 키보드포트를 모니터링 하여 사용자의 입력정보를 가로챌 수 있다. 그리고 키보드 드라이버 후킹은 키보드 드라이버 필터에 호출되는 함수를 후킹 하는 방법이며, 키보드 메시지 후킹은 시스템의 Hook 테이블의 필터함수를 변경하는 방법이다.

III. 제안하는 입력 방법

본 논문에서 제안하는 Keyboard Hooking 방지 방법은 CAPTCHA를 사용하여 Ramdom 배치된 Image map에 마우스 또는 터치를 통하여 입력하는 방법이다. 그리고 사용자의 패스워드 전송 시 서버에서 발급된 소수 P를 이용하여 전송되는 데이터를 보호한다.

3.1 CAPTCHA를 이용한 입력 방법

사용자의 패스워드는 서버에서 전송된 웹 브라우저 상의 CAPTCHA Image Map에 마우스 입력으로 받아지는 좌표 값을 가지고 입력된다. 그림 3과 같이 CAPTCHA Image Map의 각각의 pixel은 CAPTCHA로 만들어지며 6×6 ~ 8×8의 원소를 가지는 하나의 Image Map으로 형성된다. 그리고 매 순간마다 pixel의 자리는 무작위로 배치되며, 더미 pixel도 무작위로 포함된다.

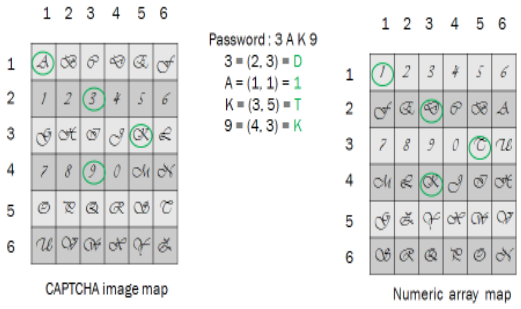

그림 3. 임의의 배열 속성값 치환 과정

사용자 패스워드인 '3', 'A', 'K', '9' 값은 소수 P를 seed로 가지는 임의의 숫자배열의 속성값 'D', '1', 'T', 'K'로 치환되고, 이 값은 $Ps = g^{D1\,TK} \bmod P$ 연산 후 서버로 전송되어진다. 아래 표 1은 사용되는 System factor이고, 그림 4는 System Data flow이다.

목록	내 용
ID	사용자 ID
PW	사용자 패스워드
Sp	숫자배열로 변경된 패스워드
P_n	맵 설정 seed 값
g	원시다항식의 유한체 원소
Ps	클라이언트에서 생성된 패스워드
Ps*	서버에서 생성된 패스워드
mod	논리연산 □
C_{map}	CAPTCHA 이미지 맵
N_{map}	숫자 배열 맵
Cd	입력된 좌표값

표 1. System factor

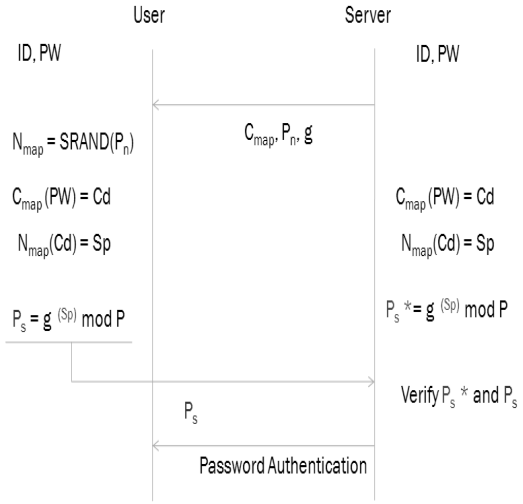

그림 4. System Data flow

IV. 보안성 분석

4.1 Keyboard Hooking

Keyboard Hooking은 사용자의 키보드를 통하여 입력되는 Data를 System과 사용자 사이에서 가로채어 사용자의 중요한 정보를 해킹하는 방식이다. 이런 Keyboard Hooking을 방지하기 위해서 우리는 CAPTCHA Image Map에 마우스(또는

터치)입력방식을 사용하여 사용자의 패스워드를 입력하는 방안을 제안 하였다. 이것은 사용자의 패스워드가 입력되는 과정에서 CAPTCHA로 변경된 Image를 사용하여 사용자 패스워드의 노출을 막고, 실제 사용되는 값은 마우스(또는 터치)를 통하여 입력되는 좌표값을 임의의 배열 속성값으로 치환하여 사용한다. 치환된 값은 전송에 사용될 Ps값 생성에 사용되며 사용자 패스워드의 노출을 최소화 시킬 수 있다. 따라서 제안된 방법은 사용자의 패스워드를 Keyboard Hooking하여 탈취하는 것을 방지할 수 있다.

4.2 재사용 공격

사용자 인증에 사용되는 Ps*는 서버에서 전송된 CAPTCHA Image Map과 소수 P를 사용하여 생성된다. CAPTCHA Image Map이 6×6배열이라고 가정하고 각 Pixel은 중복되지 않는 숫자 0~9와 영문 A~Z를 무작위 배치가 된다면, Map의 개수는 36!가 된다. 여기에 더미블록을 추가하게 되면 더 많은 Map의 종류가 생성 가능하며, CAPTCHA Image Map을 통해 입력된 좌표값은 소수 P에 의해 생성된 임의의 배열값으로 치환되어서 암호화에 사용함으로 P의 변화에 임의의 배열은 변화되어 이전 사용된 Ps*를 가지고 사용자 인증에 사용하기 어려우며, 이전 과정에서 탈취한 정보는 다음 공격에 사용하기 힘들다.

Ⅴ. 결론 및 향후방향

최근 일반적으로 사용되는 ID/Password 인증방식은 다양한 후킹 기법을 통하여 탈취되고 있으며, 탈취된 정보를 통하여 사용자의 개인정보가 2차적으로 노출되는 사건이 발생하고 있다. 2차적으로 노출된 개인신상정보를 이용하여 새로운 이메일계정을 생성한 후 공격대상자의 주소록에 등록된 주소로 스팸메일, Pshishing 사이트 유도메일, 금융사기 메일발송을 이용한 금전적인 피해사건이 발생 되고 있어 이를 방지하기 위한 방안이 필요하다. 이에 본 논문에서는 CAPTCHA를 이용한 마우스(또는 터치)를 입력방법을 제안하였다. 제안된 방법은 사용자가 개인정보를 입력하는 순간 공격자의 Keyboard Hooking에 의해 탈취되는 공격방법을 방지할 수 있음을 보여 주었다.

본 논문에서 제안한 CAPTCHA를 이용한 입력방법은 ID/Password인증방법에 국한되지 않고, 향후 공인인증서 및 기타인증부분에서도 적용이 가능함으로써 보다 높은 보안성을 가지는 시스템 설계에 활용이 가능할 것으로 기대된다.

참고문헌

[1] 김선종, 권정옥, “금융 보안 서버의 개인키 유출 사고에 안전한 키 교환 프로토콜”, 한국정보보호학회, 정보보호학회논문지, 제19권, 제3호, p119-131, 2009.6

[2] 성재모, 이수미, 노봉남, 안승호, “이용자의 금융거래정보 보호를 위한 확장 종단간(End-to-End) 암호화 기술과 보안고려사항”, 한국정보보호학회, 정보보호학회논문지, 제20권, 제4호, p145-154, 2011.8

[3] 김인석, 이수미, 임종인, “종단간 암호화(End-to-End Encryption)를 이용한 전자금융거래 정보보호 강화”, 정보보안 논문지, 제7권 제2호, p65-71, 2007.6

[4] KISA, "SecurePass", "http://news.donga.com/3/all/20100415/27578455/1", 2010.4

[5] 맹영재. 양대현, 이경희, “모바일 뱅킹에서 비밀퍼즐을 이용한 비밀증명방법과 거래승인방법”, 한국정보보호학회, 정보보호학회논문지, 제21권, 제1호, p187-199, 2011.2

[6] Carnegie Mellon University, “The Official CAPTCHA Site,” http://www.captcha.net/

[7] 김성호, 양대헌, 이경희, “색상 정보를 이용한 문자 기반 CAPTCHA의 무력화”, 정보보호학회 논문지 19권, 6호, 2009. 12

[8] 강전일, 맹영재, 김군순, 양대헌, 이경희, “복수의 이미지를 합성하여 사용하는 이미지기반의 캡차와 이를 위한 안전한 운용 방법” 정보보호학회 논문지 18(4), pp.153-165, 2008년8월

[9] 김남수, 문광호, 안연찬, 김유성, “영문 텍스트-이미지 융합 캡차”, 한국멀티미디어학회 2010 추계학술발표대회, 13권 2호, 2010.

[10] Eli Bunbury-Blanchette, “An image-based CAPTCHA that Exploits the difficulties in Computer Vision”

[11] KOFST NEWS "움직이는 이미지를 이용한 새로운 형태의 캡차(captcha) 보안 기법 개발“, http://online.kofst.or.kr/Board/?acts=BoardView&bbid=1005&page=29&nums=7543&sfl=&stx=, 2010.1.2