WM_INPUT 메시지를 활용한 이미지 기반 인증 보호방안 연구

이경률°, 임강빈*
°순천향대학교 보안안전융합기술사업화센터
*순천향대학교 정보보호학과
e-mail: carpedm@sch.ac.kr°, yim@sch.ac.kr*

A Protection Technique for Screen Image-based Authentication Utilizing the WM_INPUT message

Kyungroul Lee°, Kangbin Yim*
°R&BD Center for Security and Safety Industries (SSI), Soonchunhyang University
*Dept. of Information Security Engineering, Soonchunhyang University

● 요 약 ●

키보드 정보가 노출되는 취약점이 발견되면서 키보드를 통하여 아이디 및 비밀번호를 입력하는 인증의 보안성 결여 문제가 대두되었다. 이를 대응하기 위하여 마우스를 통하여 비밀번호를 입력하는 이미지 기반 인증이 등장하였으며, 이 인증방식은 인터넷 뱅킹 및 결제 서비스와 같이 중요도가 높은 서비스에 도입되어 사용자가 입력하는 비밀번호를 안전하게 보호한다. 하지만 키보드와 동일하게 사용자가 입력하는 마우스 데이터가 노출되는 취약점이 발견되고 있으며, 본 논문에서는 WM_INPUT 메시지를 활용하여 노출되는 마우스 데이터를 보호하는 방안을 제시한다. 제시하는 방안은 WM_INPUT 메시지를 활용하는 공격을 효과적으로 방지하며, 이를 통하여 이미지 기반 인증방식의 안전성을 강화할 수 있을 것으로 사료된다.

키워드: 마우스 (mouse), 이미지 기반 인증 (image-based authentication), WM_INPUT 메시지 (WM_INPUT message), 마우스 데이터 보호 기술 (protection technique for mouse data)

I. Introduction

키보드 정보가 노출되는 취약점이 발견되면서 키보드를 통하여 아이디 및 비밀번호를 입력하는 인증의 보안성 결여 문제가 대두되었고, 이를 대응하기 위하여 마우스를 통하여 비밀번호를 입력하는 이미지 기반 인증이 등장하였다. 이 인증방식은 인터넷 뱅킹 및 결제 서비스와 같이 중요도가 높은 서비스에 도입되어 사용자가 입력하는 비밀번호를 안전하게 보호하지만, 키보드와 마찬가지로 마우스 데이터가 노출되어 사용자의 비밀번호가 탈취되는 문제점이 발견되고 있다.

마우스 데이터를 탈취하는 공격기술을 살펴보면, 온라인으로 쉽게 구할 수 있는 마우스 로거를 사용하여 마우스 데이터를 탈취하는 공격[1]과 윈도우즈 운영체제에서 제공하는 API를 활용하여 마우스 데이터를 추적하는 공격[2], WM_INPUT 메시지를 활용하여 입력되는 마우스 데이터를 탈취하는 공격[3]이 연구되었다.

따라서 본 논문에서는 WM_INPUT 메시지를 활용하여 입력되는 마우스 데이터를 탈취하는 공격에 대응하기 위하여 WM_INPUT 메시지를 활용하여 임의의 마우스 데이터를 무작위로 발생시킴으로써 마우스 데이터를 보호하는 방안을 제안한다.

II. Related works

최근 WM_INPUT 메시지를 활용하여 입력되는 마우스 데이터를 탈취하는 공격이 연구되었다. 이 공격은 WM_INPUT 메시지로부터 전달되는 마우스 데이터를 토대로 사용자가 입력하는 마우스의 위치를 추적한다. 따라서 그림 1과 같이 실제 결제 사이트에서 사용자가 입력하는 비밀번호가 노출되는 문제점이 존재한다[3].

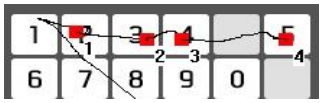

Fig. 1. Mouse data exposure result using WM_INPUT message

III. The proposed protection technique

WM_INPUT 메시지를 활용하는 공격자는 WM_INPUT 메시지로부터 전달되는 정보를 신뢰하며, 해당 정보를 주기적으로 수집함으로써 마우스 움직임을 추적한다. 따라서 본 논문에서는 공격자로 하여금 WM_INPUT 메시지에 포함된 실제 마우스 데이터를 탈취하지 못하도록 임의의 마우스 데이터를 무작위로 발생시킴으로써 마우스 데이터를 보호하는 방안을 제안한다. 그림 2와 같이 공격자는 사용자가 입력하는 실제 마우스 데이터뿐만 아니라 무작위로 발생된 마우스 데이터도 함께 수집하게 되며, 이로 인하여 무작위로 발생된 데이터를 구분하지 못하는 공격자는 사용자가 입력하는 실제 마우스 데이터를 탈취하지 못한다.

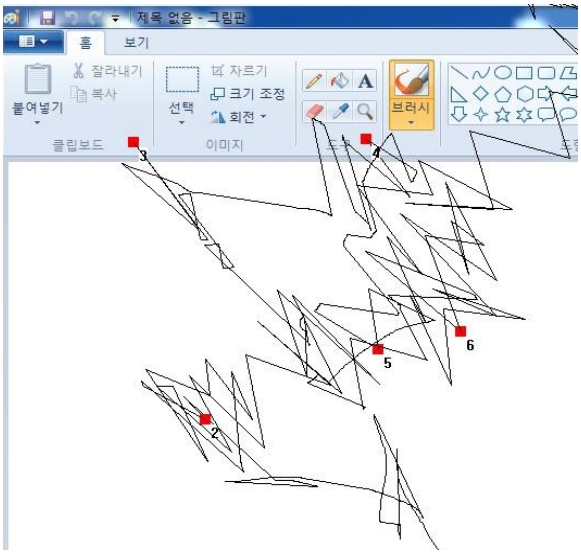

Fig. 2. Mouse data tracing result using WM_INPUT message attack with proposed technique

결과를 살펴보면, 보호 프로그램을 실행하기 위한 첫 번째 클릭을 제외하고, 2번부터 6번까지의 클릭 정보와 그 과정에서의 마우스 정보를 수집하였다. 하지만, 그림 1과 같이 일반적으로 사용자에 의한 마우스 움직임이 아니라, 그 주위에 무작위로 생성된 좌표에 의함 움직임도 함께 수집되었으며, 정확하지 않은 마우스 움직임 및 실제 클릭 위치로 인하여 실제 입력하는 마우스 데이터를 유추하기에는 한계가 존재한다.

반면, 보호 프로그램의 경우에는 자신이 생성한 무작위의 마우스 데이터를 확보하기 때문에 이를 필터링함으로써 사용자가 입력한 마우스 데이터만 수집하는 것이 가능하며, 그림 3과 같이 마우스 움직임 및 클릭 정보를 토대로 입력하는 비밀번호를 안전하게 보호하는 것이 가능하다.

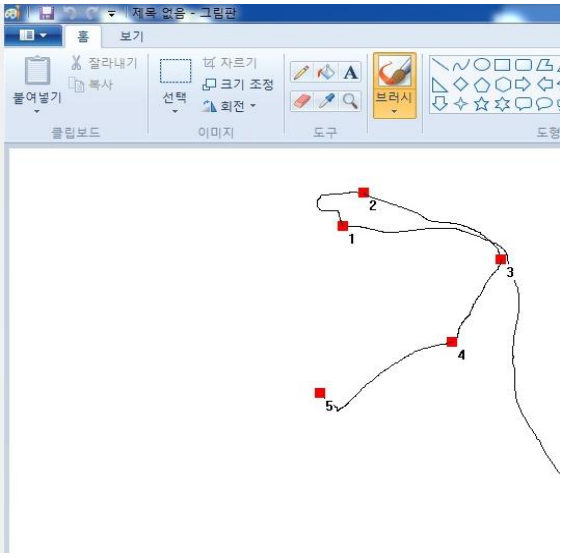

Fig. 3. Protected mouse data using proposed technique

IV. Conclusions

본 논문에서는 이미지 기반 인증에서 마우스 데이터의 노출을 방지하기 위하여 WM_INPUT 메시지를 활용한 마우스 데이터 보호 방안을 제안하였다. 제안하는 방안은 무작위의 마우스 데이터를 사용자가 입력하는 실제 데이터와 혼합함으로써 공격자에 의한 마우스 데이터의 노출을 효과적으로 방지한다.

REFERENCES

[1] Hyeji Lee, Yeunsu Lee, Kyungroul Lee, and Kangbin Yim, “Security Assessment on the Mouse Data using Mouse Loggers”, Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), pp.387-393, Nov. 2016.

[2] Kyungroul Lee, Insu Oh, and Kangbin Yim, “A Protection Technique for Screen Image-based Authentication Protocols Utilizing the SetCursorPos function”, Proceedings of the World conference on Information Security Applications (WISA), Aug. 2017.

[3] Kyungroul Lee and KangbinYim, “Vulnerability Analysis on the Image-based Authentication: through the WM_INPUT message”, Proceedings of the International Workshop on Convergence Information Technology (IWCIT), Dec. 2017.