한국컴퓨터정보학회 동계학술대회 논문집 제30권 제1호 (2022. 1)

이미지 기반 인증에서의 마우스 데이터 취약점 분석: 랜덤 마우스 데이터 생성 사이트를 기반으로

정원태[O], 이경률[*]
[O]대구가톨릭대학교 컴퓨터소프트웨어학과,
[*]대구가톨릭대학교 컴퓨터소프트웨어학부
e-mail: dnjsxo4354@cu.ac.kr[O], carpedm@cu.ac.kr[*]

Vulnerability Analysis of Mouse Data in Image-based Authentication: Based on Random Mouse Generation sites

Wontae Jung[O], Kyungroul Lee[*]
[O]Department of Computer Software, Daegu Catholic University,
[*]School of Computer Software, Daegu Catholic University

● 요 약 ●

비밀번호 인증 기술에서 키보드로부터 입력되는 데이터가 노출되는 문제점으로 인하여, 이미지 기반 인증 기술이 등장하였다. 이 기술은 주로 가상 키보드를 출력하고, 특정 위치에 클릭된 마우스 정보를 비밀번호로 활용한다. 마우스 데이터의 안전성 향상을 위하여 임의의 마우스 위치를 생성하는 랜덤 마우스 데이터 생성 기술이 등장하였지만, 해당 기술의 안전성 분석에 대한 연구가 미비한 실정이다. 따라서 본 논문에서는 GetCursorPos() 함수를 활용한 공격 기술과 WM_INPUT 메시지를 활용한 공격 기술을 기반으로 랜덤 마우스 데이터 생성 기술이 적용된 사이트에서의 마우스 데이터 취약점을 분석한다.

키워드: 이미지 기반 인증(image-based authentication), 마우스 로거(mouse logger), GetCursorPos 함수(GetCursorPos Function), WM_INPUT 메시지(WM_INPUT message)

I. 서론

한국지능정보사회진흥원의 인터넷 사용률에 따르면, COVID19로 인한 비대면 사회가 지속됨에 따라 인터넷 사용시간 및 사용률이 증가하고 있다[1]. 이에 따라, 비대면으로 사용자를 식별하기 위한 방안들이 과거부터 지속적으로 등장하였으며, 대표적인 사용자 인증 기술로는 비밀번호 인증, 이미지 기반 인증, 지문 인증, 홍채 인증 등이 있다. 일반적으로 구축이 용이한 장점으로 인하여 비밀번호 인증 기술이 주로 사용되며, 등록된 비밀번호와 입력한 비밀번호를 비교함으로써 사용자를 인증한다. 여기에서 비밀번호는 키보드로부터 입력되며, 키로거를 통하여 키보드로부터 입력되는 데이터가 탈취되는 취약점이 발견되었다.

이러한 키보드 데이터 노출 문제점을 해결하기 위하여, 이미지 기반 인증 기술이 등장하였으며, 모니터에 출력된 이미지에서 클릭된 특정 좌표를 비밀번호로 활용한다. 이 인증 기술에서의 중요한 정보는 출력된 이미지와 마우스 데이터이며, 더욱 안전하게 클릭하는 위치를 보호하기 위하여 임의의 위치에 마우스 커서를 생성하는 기술이 등장하였다. 하지만, 해당 기술의 안전성 분석에 대한 연구가 미비한 실정이다. 따라서 본 논문에서는 임의의 마우스 커서를 생성하는 랜덤 마우스 데이터 생성 기술이 적용된 사이트를 대상으로 이미지 기반 인증에서 마우스 데이터의 안전성을 분석한다.

II. 관련 연구

마우스 데이터를 보호하는 기술로는 랜덤 마우스 데이터 생성 기술과 마우스 위치 대칭이동 기술이 있다. 이 중 랜덤 마우스 데이터 생성 기술은 사용자로부터 입력되는 마우스 데이터의 노출을 방지하기 위하여, 무작위 위치에 마우스 커서를 생성하며, 공격자는 사용자가 어떠한 마우스 커서를 움직이는지 모르기 때문에 마우스 위치를 안전하게 보호한다.

공개된 마우스 데이터 공격 기술은 GetCursorPos() 함수를 활용한 공격 기술과 WM_INPUT 메시지를 활용한 공격 기술이 있다. GetCursorPos() 함수는 윈도우즈 운영체제에서 제공되는 API로, 스크린에서의 절대좌표를 반환한다. WM_INPUT 메시지는 해당 메시지에 대한 핸들러를 운영체제에 등록함으로써 메시지가 발생할 때 핸들러가 호출되며, 핸들러 내부에서 마우스 상대 좌표를 획득한다.

이러한 공격 기술을 통하여 마우스 좌표를 지속해서 추적함으로써 입력되는 비밀번호의 탈취가 가능하다.

III. 취약점 분석 결과

본 논문에서는 랜덤 마우스 데이터 생성 기술이 적용된 두 개의 사이트들을 대상으로, 마우스 데이터 공격 기술을 활용하여 마우스 데이터의 안전성을 분석한다. 이를 위하여 GetCursorPos() 함수를 활용한 공격 도구와 WM_INPUT 메시지를 활용한 공격 도구를 구현하였으며, 랜덤 마우스 데이터 생성 기술이 적용된 A 사이트에서 마우스 데이터의 탈취 결과를 그림 1에 나타내었다.

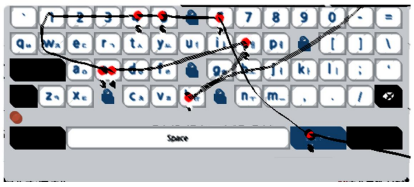

Fig. 1. A 사이트에서의 GetCursorPos() 함수를 활용한 공격 결과 일례

공격 결과, 임의의 위치에 마우스 커서가 생성되더라도 마우스 움직임과 클릭 위치를 성공적으로 탈취하였으며, 탈취한 비밀번호는 “boss456” 임을 확인할 수 있다. 이러한 실험 결과를 기반으로 두 개의 사이트에 대한 마우스 데이터 탈취 결과를 표 1에 나타내었다.

Table 1. 랜덤 마우스 데이터 생성 사이트 취약점 분석 결과

실험 환경	공격 기술	사이트	노출 여부
Windows10	GetCursorPos()	A	O
		B	O
	WM_INPUT 메시지	A	O
		B	O

결과를 살펴보면, 두 개의 사이트 모두 GetCursorPos() 함수와 WM_INPUT 메시지를 활용한 공격으로부터 마우스 데이터가 노출되는 것을 검증하였다.

IV. 결론

본 논문에서는 이미지 기반 인증에서 마우스 데이터를 보호하기 위하여 랜덤 마우스 데이터 생성 기술이 적용된 사이트의 안전성을 분석하였으며, 그 결과, GetCursorPos() 함수와 WM_INPUT 메시지를 활용한 공격으로부터 마우스 데이터를 보호하지 못하는 것을 검증하였다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1050542).

REFERENCES

[1] NIA, "2020 Survey on the Internet Usage," https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do;jsessionid=8297443C882037ECC0821396C30E6AD4.55820bfe7f7b06361509?cbIdx=99870&bcIdx=23213&parentSeq=23213, Mar. 2021.

[2] Kyungroul Lee, Insu Oh, and Kangbin Yim, "A Protection Technique for Screen Image-based Authentication Protocols Utilizing the SetCursorPos function," International Workshop on Information Security Applications (WISA), pp. 236-245, Aug. 2017.

[3] Kyungroul Lee and Kangbin Yim, "Vulnerability Analysis on the Image-based Authentication: through the WM_INPUT message," Concurrency and Computation: Practice and Experience, Vol. 32, Iss. 18, e5596, Sep. 2020.