한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

기계 인지 기반 BAD USB 탐지 방안 연구

오인수[O], 임하빈[**], 이경률[***], 임강빈[*]
[*O]순천향대학교 정보보호학과
[**]고려대학교 정보보호대학원
[***]순천향대학교 보안안전융합기술사업화센터
e-mail: catalyst32@sch.ac.kr[O], habin103@korea.ac.kr[**], carpedm@sch.ac.kr[***], yim@sch.ac.kr[*]

Countermeasure for Detecting BAD USB based on Machine Recognition

Insu Oh[O], Habin Yim[**], Kyungroul Lee[***], Kangbin Yim[*]
[*O]Dept. of Information Security Engineering, Soonchunhyang University
[**]Center for Information Security Technologies (CIST), Korea University
[***]R&BD Center for Security and Safety Industries, Soonchunhyang University

● 요 약 ●

본 논문은 사람에 의하여 발생하는 패턴과 기계적으로 발생하는 패턴과의 차이점을 인지함으로써 BAD USB 탐지하는 방안을 제안한다. BAD USB는 펌웨어를 조작하여 악의적인 행위를 수행하는 공격으로, BAD USB를 탐지하기 위한 많은 연구가 진행되었지만, 펌웨어 내부에 존재하는 악성코드를 효과적으로 탐지하기에는 어려움이 존재한다. 따라서 본 논문에서는 사람에 의하여 나타나는 행위에 대한 패턴과 기계적으로 발생하는 패턴을 구분하여 악의적인 행위를 인지함으로써 BAD USB를 탐지하는 방안을 제안한다.

키워드: 배드 유에스비(BAD USB), 패턴 기반(pattern-based), 기계 인지(machine recognition)

Ⅰ. Introduction

BAD USB는 쉽게 접근하기 어려운 영역인 USB 컨트롤러 내의 펌웨어를 조작하여 악의적인 행위를 수행하는 공격으로, 2014년 Black Hat security conference에서 최초로 공개되었다[1]. 일반적으로 USB 컨트롤러 내의 펌웨어는 위/변조가 어려워 공격에 주로 활용되지는 않았지만, 장치 및 컨트롤러에 새로운 기능을 추가하거나 버그와 같은 오류를 정정하기 위하여 업데이트 기능을 제공함으로써 이를 통한 악의적인 코드를 삽입하는 공격이 가능함을 검증하였다. 공격 방법으로는 업데이트를 위한 펌웨어 파일을 수정하여 공격 코드를 삽입하고, 해당 공격 코드를 실행하기 위한 후킹 코드를 덮어씀으로써 후킹을 통하여 공격 코드를 수행하는 방법이며, 공격 코드의 구성에 따라 다양한 공격이 가능한 특징을 가진다. 그 일례로 키보드나 마우스와 같은 입력장치로 위장함으로써 사용자가 입력하는 비밀번호와 같은 인증정보를 탈취하거나, 네트워크 카드로 위장함으로써 공격자가 준비한 악의적인 서버로 접속하도록 유도하는 등의 공격 시나리오가 존재한다[1, 2, 3].

이와 같은 BAD USB는 실제 악성코드가 저장된 공간이 컨트롤러 내부이기 때문에 일반적인 방법으로는 접근하기 어려운 문제점이 있다. 이를 대응하기 위한 기존의 방안으로 블랙리스트 및 화이트리스트 기반 탐지방안과 펌웨어 및 부트로더를 수정하지 못하도록 방지하는 방안 등이 제안되었지만[2], 실질적으로 공격에 활용되는 코드 및 행위를 탐지하기에는 현실성이 부족하다. 따라서 본 논문에서는 BAD USB가 공격을 위하여 미리 준비된 명령 및 행위를 수행할 때 사람이 아닌 기계적인 특성이 발생한다는 특징에 기인하여 BAD USB를 탐지하는 방안을 제안한다.

Ⅱ. Preliminaries

상기와 같이 BAD USB는 알려지지 않은 공격기술을 활용하며, 이를 탐지하기 위한 대응이 시급히 요구된다. 따라서 BAD USB를 탐지하고 대응하기 위한 방안이 연구되었으며, 대표적으로 리스트 기반 접근제어와 펌웨어 잠금 방안이 연구되었다.

1. 리스트 기반 접근제어

이 방안은 BAD USB로 탐지된 장치 정보를 블랙리스트에 추가하여 차후 해당 정보를 가진 장치가 연결되는 경우에는 차단하는 방안과

사용자에 의하여 올바른 장치로 선택된 정보를 화이트리스트에 추가하여 차후 해당 정보를 가진 장치가 연결되는 경우에는 허용하는 방안이었다. 따라서 BAD USB로 탐지된 장치는 차단되고, 사용자가 올바른 장치로 선택하지 않은 장치를 차단함으로써 BAD USB가 호스트로 연결되는 것을 방지한다. 리스트에 추가하기 위한 장치 정보로 흔히 PID (Product ID)와 VID (Vendor ID) 등을 활용하며, 이를 기반으로 리스트를 작성하여 탐지한다[2].

2. 펌웨어 잠금

이 방안은 BAD USB가 공격 코드를 저장하기 위하여 반드시 펌웨어를 조작하기 때문에 하드웨어적인 방법으로 펌웨어가 수정되는 것을 방지하는 방안이다. 따라서 공격자가 펌웨어를 수정하지 못하기 때문에 효과적으로 BAD USB를 방지하는 것이 가능한 장점이 있지만, 펌웨어에 기능을 추가하거나 오류 등을 정정하지 못하는 단점도 존재한다[4].

III. The Proposed Scheme

상기와 같이 기존의 다양한 BAD USB 대응방안이 연구되었음에도 불구하고 효과적으로 공격 코드 및 행위를 탐지하는 것은 한계가 있으며, 이는 공격 코드가 저장된 펌웨어에 접근하는 것이 일반적이지 않은 방법으로 이루어지기 때문이다. 따라서 본 논문에서는 공격 코드를 직접적으로 탐지하는 것이 아닌, 공격 행위를 탐지함으로써 BAD USB를 대응하는 방안을 제안한다.

BAD USB는 펌웨어를 조작한 후, 공격 코드를 실행함으로써 악의적인 행위를 수행한다. 예를 들면, 피해자의 시스템을 파괴할 목적으로 키보드나 마우스와 같은 입력장치로 위장한 경우, 사용자가 자리를 비우거나 시스템을 사용하지 않는 시간을 이용하여 미리 준비된 코드를 수행하는 공격이 가능하다. 이러한 공격 시나리오로는 탐색기를 실행하고 파괴할 드라이브를 선택한 후, del 키 및 포맷, 삭제 등의 기능을 실행하는 명령을 추가적으로 전송하여 시스템을 파괴하는 공격이 가능하다. 이를 위하여 특정 행위를 수행하기 위한 키보드의 스캔코드를 미리 정의하여 전달하는 과정이 반드시 필요하다. 하지만 이러한 과정에서 사람에 의하여 행위를 수행하는 패턴이 나타나는 것이 아니라, 기계 기반의 패턴이 나타난다. 따라서 본 논문에서는 이러한 행위를 사람 및 기계임을 판단함으로써 BAD USB를 효과적으로 탐지하는 방안을 제안한다.

또한 기계 기반의 행위를 수행할 경우에는 사람에 의하여 발생하는 무작위적, 혹은 비정규화된 시퀀스가 발생하는 것이 아니라 주기적, 혹은 정규화된 시퀀스가 발생하기 때문에 이러한 정보도 함께 활용함으로써 BAD USB를 탐지하는 것이 가능할 것으로 사료된다.

탐지방안의 일례를 살펴보면, 일정 기간 동안 사용자의 키 입력 패턴을 분석한 후, 해당 패턴에 위배되는 입력이 있을 경우, 혹은 기계적으로 발생하는 일정한 입력이 있을 경우에는 기계적으로 명령을 수행하는 것으로 판단하여 BAD USB를 탐지한다. 하지만 이러한 경우 오탐이 발생할 확률이 높기 때문에 사용자가 입력하는 키의 시퀀스를 분석하여 동시에 적용함으로써 오탐을 보다 적게 발생하도록 향상시키는 것이 가능할 것으로 사료된다.

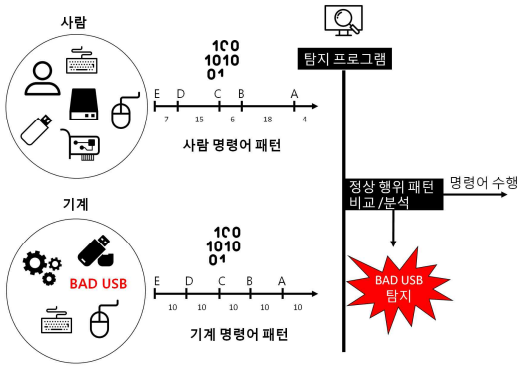

Fig. 79. The proposed BAD USB detection technique

IV. Conclusions

본 논문에서는 사람과 기계에서 발생하는 특성이 다른 점을 이용하여 BAD USB의 악성행위를 탐지하는 방안을 제안하였다. 기존의 BAD USB 탐지방안은 취약한 기능을 원천적으로 제거하거나 장치에 대한 목록을 생성하는 방법이므로 효과적으로 탐지하기에는 한계가 있다. 하지만 제안한 방안은 BAD USB가 악의적인 행위를 수행할 때 발생하는 기계적인 특성을 탐지함으로써 기존의 방안보다 효과적으로 탐지하는 것이 가능하다.

Acknowledgments

이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01057300).

References

[1] K. Nohl and J. Lell, “BadUSB – on accessories that turn evil”, Black Hat USA, Aug. 2014.

[2] S. Neuner, “Marshall Plan Scholarship Final Report: Security of the Universal Serial Bus”, Dec. 2014.

[3] D. J. Tian, A. Bates, K. Butler, “Defending Against Malicious USB Firmware with GoodUSB”, Proceedings of the Annual Computer Security Applications Conference (ACSAC), pp.261-270, 2015.

[4] Soyeon Nam, Insu Oh, Kyungroul Lee, Kangbin Yim. (2016.07). Study on BAD USB Detection Technique based on User Cognition. Proceedings of the Korean Society of Computer Information Conference , 24(2), 93-94.