Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.559

BadUSB의 취약성 및 대응방안

최 준†‡
국방보안연구소

Countermeasures for BadUSB Vulnerability

Jun Choi†‡
Defense Security Institute

요 약

USB 메모리에 의한 정보유출・악성코드 유입 등에 대한 방어를 위해 다양한 복사방지・장치제어와 같은 보안기술들이 지속적으로 연구・개발 되고 있다. 하지만, 지난 2014년 Black Hat Security Conference에서 USB의 새로운 취약성으로 제시된 BadUSB에 대해서는 치명적 보안결함으로 인식되고 있음에도 불구하고 대응책이 미흡한 실정이다. 이를 개선하기 위해, BadUSB로 인한 취약성을 대상으로, 기술적・제도적・관리적 측면의 대응방안을 제시하고자 한다.

ABSTRACT

To defend against information leakage or malware inflow by USB memory, security technologies such as copy protection and device control have being researched and developed. However, countermeasure are insufficient despite being recognized as a fatal security-hole for BadUSB presented at the Black Hat Security Conference 2014. To solve this problem, the countermeasures for BadUSB vulnerability are proposed.

Keywords: BadUSB, Secure USB, Firmware Hacking

I. 서 론

USB(Universal Serial Bus)는 컴퓨터와 주변기기를 연결하는 기술 표준 가운데 하나로서, 자료의 저장 혹은 파일 이동에 사용되는 플래시메모리 기반 USB 저장장치 뿐만 아니라, 키보드 및 마우스 등 다양한 곳에서 활용도가 증대되고 있다[1].

하지만, 지난 2014년 Black Hat Security Conference에서 독일 'Security Research Labs'의 Karsten Nohl과 Jakob Lell에 의해, 일반적으로 위조와 변조가 쉽지 않다고 알려진 USB 펌웨어 영역 대상, 악성소프트웨어 멀웨어(malware)를 감염시킬 수 있는 공격 'BadUSB'가 발표되었다[2].

본 논문에서는, 이 공격으로 인해 USB 메모리 뿐만 아니라, USB 포트에 삽입되는 모든 주변 장치들까지 해킹 도구로 악용되거나, 멀웨어 전염의 매개체로 작동될 수 있는 보안 취약성을 알아보고, 이에 대한 대응방안을 제시해보고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 BadUSB 개념 및 관련 연구 동향에 대해 살펴보고, Ⅲ장에서는 BadUSB로 인한 취약사례를 제시하며, Ⅳ장에서는 BadUSB에 대한 기술적・제도적・관리적 측면의 대응방안을 제안하고, 끝으로 Ⅴ장에서는 결론을 맺는다.

접수일(2015년 3월 12일), 게재확정일(2015년 4월 7일)
† 주저자, choijun1014@hotmail.com
‡ 교신저자, choijun1014@hotmail.com(Corresponding author)

II. BadUSB 개념 및 관련 동향

2.1 개 념

일반적으로 USB 메모리는 Fig.1.에서 보는 바와 같이, USB 외부에는 USB 포트와 연결 할 수 있는 커넥터가 있으며, 내부는 데이터를 저장하는 플래시 메모리 기반 대용량 저장장치 및 커넥터와 플래시 메모리 칩 사이에서 데이터 전송을 제어하는 컨트롤러 펌웨어로 구성되어 있다.

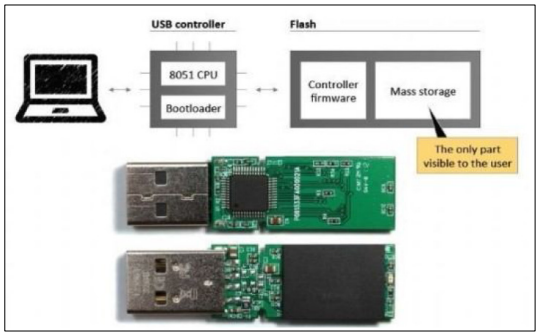


Fig. 1. Structure for USB flash memory[3]

기존에 USB 메모리를 이용하여 악의적 목적의 자료 유출 및 위·변조 공격시 대상 타겟은 대용량 저장장치에 국한되어 있었던 반면, 일반적 기술로는 접근이 용이하지 않다고 인식되었던 펌웨어에 대해서는 특별한 공격기술이 제시되지는 않았다.

하지만, 2014년 Black Hat에서 역공학을 통해 USB 펌웨어를 조작하여 해킹용 도구 혹은 시스템 공격 목적으로 악용 가능한 USB 메모리의 보안 취약성이 제시되었으며, 이후 USB 커넥터를 갖는 장치들을 대상으로 컨트롤러 펌웨어 영역이 악의적으로 훼손된 경우, BadUSB 라고 명명하고 있다.

사실, USB 펌웨어 영역은 업데이트 혹은 패치 목적상 수정이 가능하기 때문에[4], 이러한 수정 기능이 악용될 때 발생 가능한 위·변조 취약점은, 90년대 중반이후 USB 기술이 소개되었던 시점부터 예상되었던 사안이다. BadUSB의 근본적인 원인은, 일반적 운영체제들이 USB 펌웨어 대상 무결성 검증 목적의 펌웨어 코드 검증과 같은 기능을 수행하고 있지 않음으로 인해, USB 포트에 삽입되는 다양한 장치들에 대해 운영체제가 무조건적으로 승인하는 방식 때문이다. 이것은 USB의 최초 설계사상에 기인한 것으로서, 현재 운용되고 있는 USB 장치의 단순 보안패치에 의해서는 대응이 제한된다고 볼 수 있다.

2.2 관련 동향

2014년 8월 미국에서 개최된 Black Hat Security Conference에서 독일 Karsten Nohl과 Jakob Lell(이하 Nohl)은, 'BadUSB - On Accessories that Turn Evil' 이라는 주제로, BadUSB로 인한 보안취약성에 대해 발표를 하였다.

이 발표에서 Nohl은 USB 기반 장치류의 컨트롤러 펌웨어 영역에 대한 조작을 통해 멀웨어가 유입될 수 있다는 점을 최초로 제시하였고, 멀웨어가 심어진 USB 장치는 컴퓨터의 제어권, 데이터탈취 등의 목적으로 악용될 수 있다는 연구결과와 함께, 기존 바이러스 방어 P/G으로는 이와 같은 공격에 대해 대응하기 어렵다는 점을 강조하였다.

하지만, Nohl은 발표 시점 기준으로 연구 결과에 대해 대응책이 없고, 기존 사용중인 USB에 미치는 부정적 파급효과가 매우 크다는 이유로, 본인들이 멀웨어 삽입을 위해 사용한 코드는 구체적으로 공개하지 않았다.

이 후, 2014년 9월 Derbycon Security Conference에서 Adam Caudill과 Brandon Wilson(이하 Caudill)[5]은 Nohl의 방법과 유사하게 USB 펌웨어내 멀웨어를 삽입함으로써 BadUSB를 제작할 수 있음을 시연하였다. 또한, Nohl이 BadUSB 제작 코드를 공개하지 않은 것과 달리, Caudill은 취약성을 갖고 있는 BadUSB에 관한 모든 것이 공개되어야 하고, 공개된 취약성에 대해 USB 기술 기반의 장치를 제작하는 업체 혹은 여러 사람들이 대응할 필요가 있다고 판단하여, BadUSB 제작에 사용된 소스코드를 오픈소스 코드 저장소인 GitHub에 공개하였다.

Nohl과 Caudill 등에 의해, BadUSB로 인한 취약성이 입증되고, 누구나 BadUSB를 제작할 수 있다는 문제점으로 인해, USB 기술이 적용된 장치 제조사·주변기기 제작업체에게는 USB 펌웨어 영역을 대상으로 하는 멀웨어 삽입 및 악의적 위·변조 등에 대해 대응책 마련이 시급한 과제로 인식되는 추세이다.

III. BadUSB 보안 취약성

보안 분야의 취약성 발표는 일반적으로 악의적 목적을 가진 해커들에 의해 특정 피해가 발생된 이후

발표되는 반면, BadUSB는 보안 기술 연구 그룹에 의해 최초로 알려졌다. 따라서, Ⅲ장에서 제시되는 BadUSB 보안 취약성들은, 기존에 피해가 발생한 경우를 토대로 제시하는 것이 아니라, 2014년 Black Hat과 Derbycon에서 BadUSB 기술이 발표됨에 따라, 이를 토대로 예상해 볼 수 있는 보안 취약성들로 구성되었다.

3.1 'Phison'社 Controller 제품군

Caudill은 Derbycon Conference에서 BadUSB 관련 발표 및 시연시, 세계적으로 상위 수준의 USB 제조회사인 Taiwan Phison Electronics의 컨트롤러(Fig. 2.)를 타겟으로 하였다. Phison社 Controller에 대한 취약성이 발표된 이후, Phison社 Controller가 탑재되어 있어 BadUSB로 전용 가능성이 있다고 공개된 제품은 다음과 같다[6].

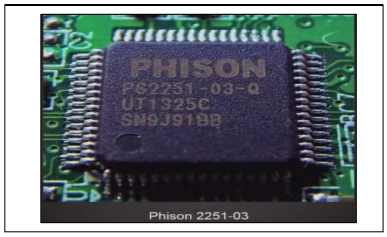


Fig. 2. Phison社 Controller 2251-03

- Patriot 8GB Supersonic Xpress(with PS2251-03(2303) controller)
- Kingston DataTraveler 3.0 T111 8GB
- Silicon power marvel M60 64GB
- Patriot Stellar 64 Gb Phison
- Toshiba TransMemory-MX USB 3.0 16GB
- Toshiba TransMemory-MX USB 3.0 8GB
- Kingston DataTraveler G4 64 GB
- Patriot PSF16GXPUSB Supersonic Xpress 16GB
- Silicon Power 32GB Blaze B30 (SP032GBUF3B30V1K)
- Kingston Digital 8GB USB 3.0 DataTraveler (DT100G3/8GB) - Using PS2251-03
- SanDisk Ultra 16Gb USB 3.0 SDCZ48-016G

상기 제품들은 BadUSB로 악용될 가능성이 있는 Phison社 Controller를 대상으로 하고 있지만, BadUSB를 제작하는 기술은 타업체 컨트롤러에 대해서도 적용이 가능한 기술이므로, USB 장치류 펌웨어 대상 잠금 기능이 적용되지 않았거나, 무결성 검증 과정이 없는 컨트롤러들은 BadUSB로 사용될 수 있는 취약 가능성이 있다고 볼 수 있다.

3.2 BadUSB로 인해 발생 가능한 취약성

펌웨어 로드는 장치 드라이버에서 구현된다. 많은 장치들의 펌웨어는 추가적 하드웨어 설치 없이 제조사나 판매회사 설계 요구사항에 의해 갱신 혹은 수정이 가능하다. 하지만 이런 가능성으로 인해 의도하지 않은 펌웨어 위·변조가 가능한 것이며, 이를 기반으로 BadUSB로 악용될 수 있다.

USB 포트와 연동되는 다양한 장치들의 컨트롤러 펌웨어가 멀웨어에 의해 감염되어 예상되는 피해는 다음과 같이 매우 다양하다[2,5,7].

- 키보드 자판 입력 조정 권한 획득
- 파일 관리자 비밀번호 등 중요정보 획득
- 파일 열람, 파일 변경 및 파일 추출
- 인터넷 접속시 악성 웹사이트로 유도
- USB 포트에 접속되는 주변 장치들 감염
- 네트워크 카드 스푸핑, 컴퓨터 DNS 경로 조작
- PC 부트로더(boot loader) 감염
- USB 드라이브내 hidden partition 생성

BadUSB에 의해 발생 가능한 상기 취약성들은, 멀웨어가 펌웨어에 유입되었다는 특성으로 인해, 펌웨어 영역까지는 스캔하지 않는 대부분 백신 프로그램으로 탐지하기 어려우며, 펌웨어가 감염된 BadUSB는 포맷 등의 방법으로는 대응이 될 수 없기에, 심각한 보안 위협으로 작용할 수 있다.

Ⅳ. BadUSB에 대한 대응방안

앞에서 살펴본 바와 같이, 사용 편의성으로 인해 활용도가 다양한 USB 기반 장치들(메모리, 키보드,

마우스 등)의 컨트롤러 펌웨어 영역으로의 멀웨어 유입으로 인한 취약성은 매우 다양하고, BadUSB로 변형된 장치들은 단순 보안패치 혹은 기존 멀웨어 탐지(백신) 프로그램 등으로는 대응되지 않는 이유로 이해, 심각성이 매우 크다고 볼 수 있다.

이 장에서는 이러한 현실태/문제점을 고려하여, BadUSB에 대해 기술적 대응방안 뿐만 아니라, 국가적 차원에서 BadUSB로 인해 발생 가능한 위협을 예방하기 위해, 현재 우리나라 국가(공공)기관에서 적용중인 보안 관련 지침의 수정·보완 사항을 포함하여 제시하고자 한다.

제시되는 방안들에 대한 선택 및 적용 여부는, USB 장치별 달성하고자 하는 보안수준 목표, USB 장치별 마이크로컨트롤러의 성능, 갱신·패치 소요 여부, 대응방안 적용에 따른 비용 증가량 대비 효율성 등이 종합적으로 고려되어 결정되어야 한다고 본다.

따라서, USB 장치들의 설계 단계부터 고려가 되어야 적용 가능한 이상적 보안위협 대응방안 제시뿐만 아니라, 이미 배포된 USB 장치들이 BadUSB로 악용될 수 있는 가능성을 제조사 및 사용자 입장에서 일정부분 감소시킬 수 있는 방안들에 대해 장·단점을 고려하여 제시한다.

4.1 코드 서명(Code Signing)

USB 기반 장치들이 BadUSB로 제작 가능한 근본 원인은 펌웨어 영역에 대한 갱신 혹은 수정 목적의 코드 유입이 가능하도록 펌웨어 잠금 설정이 되어있지 않은 점도 있지만, 근본적인 원인은 펌웨어 영역에 유입되는 코드들에 대해 무결성 검증 기능이 구현되어 있지 않으며, 코드 생성자에 대한 인증 기능이 없다는 점에 기인한다. 따라서, 가장 원천적인 대응방안으로서 USB 장치 설계단계부터 펌웨어에 대한 코드 서명 기술 적용을 고려해 볼 수 있다.

코드 서명 기술은, 소프트웨어·펌웨어 구현을 위해 사용되는 코드가 정당한 사용자에 의해 작성되었으며, 위·변조가 되지 않았다는 것(무결성 보장)을 증명하기 위한 기술로서, 적용 사례는 운영체제에서 갱신 혹은 패치 목적의 코드 배포시 활용되는 경우를 들 수 있다.

일반적인 코드 서명 기술은, 코드 생성자의 정당성 인증과 무결성을 증명하기 위한 코드 생성이 요구되며, 그 과정은 Fig. 3.에서 보는 바와 같이 해쉬함수·비대칭키(공개키) 암호기술 들을 적용하여 이루어진다[8].

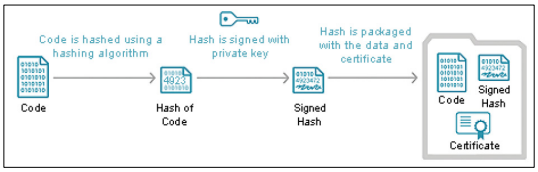
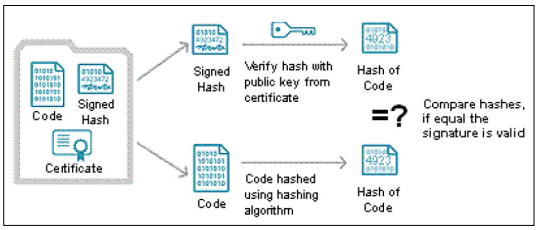


Fig. 3. Creating the code signing certificate

생성된 코드에 대해서는 Fig. 4.에서 보는바와 같이, 전자서명에 대한 검증 절차(해쉬함수가 적용된 코드를 대상으로, 서명 생성자의 개인키로 암호화된 데이터에 대해, 서명 검증자는 서명 생성자의 공개키로 복호화 하여 데이터 무결성 체크)와 유사하게 검증을 수행할 수 있다[8].



Fig, 4. Verifying Code Authenticity

하지만, 코드 서명 기술 적용시 간과하지 않아야 할 점은, 안전한 암호화 알고리즘의 선택과 구현의 정확성, 암호키와 같이 중요 정보에 대한 보호대책 강구 등이 고려되어야 한다는 점이다.

이에 대해, 4.2.절에서는 암호기술 관련 美 표준 기술에 기반하여, 코드 서명 기술 적용 관련, 추가적 보안 요구사항들을 언급하고자 한다.

4.2 FIPS 140-2 Level 3 이상 요구조건 충족

美 FIPS(Federal Information Processing Standards Publication) 140-2는 암호모듈 관련 보안수준(Security Level 1 ~ Level 4)별 요구사항을 제시하고 있다[9].

FIPS 140-2 Level 3 이상에서는, Level 1·2 충족 조건과 더불어, 몇 가지 추가 요구사항들(Identitiy 기반 인증, Physical 보안 강화 등)이 있지만, 이 중 BadUSB 대응방안과 관련하여 주의깊게 볼 사항은 '신뢰 경로(모듈 혹은 장치들에서 사

용되는 데이터 입·출력 포트는, 보호하고자 하는 대상과 논리적 혹은 물리적으로 격리될 수 있도록 설정된 경로)' 구현을 통해, 신뢰 할 수 없는 CSP[1]·소프트웨어·펌웨어 등이 시스템 상에서 실행되는 것을 방어한다는 것이다. 즉, 펌웨어 Protection 기능의 구현이 필수적으로 요구된다는 것이다.

따라서, USB 장치 제작시 4.1에서 제시한 코드 서명 기법과 4.2에서 제시하는 FIPS 140-2 Level 3 요구조건을 동시에 충족한다면, 멀웨어 코드가 USB 펌웨어 영역으로 유입됨에 따른 문제점을 개선할 수 있다.

4.3 펌웨어 갱신·패치 기능 잠금

잠금 기능을 이용한 대응방안은, USB 장치들에 사용되는 프로세서의 성능과 경제성(제작/판매 단가) 등을 고려시, 4.1에서 제시한 코드 서명 기술 구현이 현실적으로 제한되는 경우에 대체 방법이 될 수 있다.

즉, 이 방법은 USB 장치들의 펌웨어 대상 잠금 기능 활성화를 통해, 펌웨어 영역으로 멀웨어 뿐만 아니라, 임의의 코드 유입을 차단 함으로써 BadUSB 제작 가능성을 제한하는 것이다.

BadUSB 취약성을 최초 발표한 Nohl은 BadUSB에 대한 대응방안으로서, 'Whitelist USB devices, Block critical device classes, Use code signing for firmware updates, Disable firmware updates in hardware' 등 여러 가지를 제시하였지만, 그 중 펌웨어 갱신(업데이트)을 차단하는 것이 단순하고 효율적이라고 제안하였다[2,3].

하지만, 대부분의 USB 장치들이 컨트롤러 펌웨어 영역에 대한 갱신·패치를 위해 잠금 기능이 해제된 상태로, 공급이 되고 이용되어 왔다는 점을 고려하면, 이 방안의 경우 제품 출시시 최초 설정된 펌웨어 영역에 대해 기능 수정과 보완이 제한됨으로 인해 발생될 수 있는 제한사항과 문제점들은 감내해야 할 것이다.

1) Critical security parameter : security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs)

4.4 검사합 기반 펌웨어 Readable 기능 활용

4.3.에서 펌웨어 갱신·패치 기능을 차단하는 방법과 상이한 개념으로서. 펌웨어 갱신·패치 기능은 유지하되, 펌웨어에 대해 제조사가 배포하는 펌웨어 검사합(checksum) 값을, 사용자들이 주기적으로 확인 가능하도록 하는 방법이다[10].

이 경우, 일정 부분 펌웨어의 무결성 여부를 사용자가 직접 확인해 볼 수 있다는 장점은 있지만, 제조사는 신뢰할 수 있는 경로를 이용하여 사용자에게 검사합을 제공하여야 한다는 전제 조건과 함께, 사용자들이 주기적으로 검사합 값을 확인해야 한다는 불편함의 감내가 필요하다.

4.5 정보보호 관련 규정 개정 필요성 검토 요망

4.5절에서 제시하고자 하는 내용은, 기존 정보보호 관련 규정의 문제점을 제시하고자 하는 것이 아니다. 단, 새롭게 등장한 보안취약성에 대해서는 기존 규정들에서 고려되지 않은 사항이 있고, 현재 규정상으로는 대응 측면의 제한사항이 있으므로, 향후 관련 규정 제·개정시 BadUSB로 인해 발생 가능한 취약성도 고려가 되야 한다는 필요성에 대해 공감대를 형성하는데 목적이 있다고 볼 수 있다.

국가 정보보안을 위하여 각급 기관이 수행하여야 할 기본활동을 규정한 '국가정보보안기본지침(국가정보원, '14.4.1.)에 의거하여, 주요 정부기관들은 정보통신망·휴대용 저장매체 등에 대해 다양한 정보보호 대책을 수립하여 운용중이며, 상기 지침에 준하여 기관별 지침이 유사하게 수립되므로, 법제처[2]에 공지된 '미래창조과학부 정보보안 기본지침(미래창조과학부훈령 제25호, 2013.6.5.)'을 사례로 활용하여, 신규 보안 취약성인 BadUSB와 연계될 수 있는 관련 규정의 개정 필요성을 제시하고자 한다.

미래창조과학부 정보보안 기본지침 3조에서는 휴대용 저장매체 범주에 외장형 하드디스크·USB 메모리 등 정보를 저장할 수 있는 기억장치를 언급하고 있으며, 동 지침 32조에서는 휴대용 저장매체 관리의 방안으로, 국가정보보안기본지침의 'USB 메모리 등 휴대용저장매체 보안관리 지침' 준수를 요구하고 있다.

'USB 메모리 등 휴대용저장매체 보안관리 지침'

2) http://www.moleg.go.kr/main.html

4조에서는 USB 메모리가 충족해야 할 보안기능(지정데이터 암·복호화, 저장 자료의 임의 복제 방지기능, 분실시 저장데이터 보호를 위한 삭제 기능 등)에 대해 언급하고 있으며, 특히, USB 메모리 내부 데이터 기밀성 보호 측면에 주안점을 두고 있는 것을 알 수 있다.

하지만, 지금까지 살펴보았듯이, USB 메모리 뿐만 아니라, USB 포트에 접속 가능한 외장형 하드·키보드·마우스·웹캠 등이 BadUSB로 전환되어, 멀웨어의 유포 근원으로 활용될 수 있는 가능성을 고려시, USB 기반 제품 중 자료 저장을 위한 메모리 영역(Fig. 1. Mass storage)의 자료 누출 방지 측면에서 수립되었던 보안 정책들이, 향후에는 USB 기술을 이용하는 다양한 장치들의 펌웨어 영역으로의 멀웨어 유입까지 동시에 고려함으로써, 이들 장치들의 임의 사용시 발생 가능한 문제점을 예방할 수 있도록 보완되어야 할 것이다.

국가기관에서 이러한 BadUSB 예방 활동의 일례로서 코드 서명과 연계된 암호 기법 활용시, 4.2.절에서 언급된 美 FIPS 140-2 검증 기준에 준하여, 우리나라 국가정보원 산하 국가사이버안전센터[3]에서 시행중인 KCMVP(Korea Cryptographic Module Validation Program)의 보안수준별 요구조건을 고려해 볼 수 있다. 국가기관이 사용하는 상용 암호모듈의 시험 및 검증 등에 필요한 사항은 "암호모듈 시험 및 검증지침(행자부고시, 제2004-45호)에 규정하고 있고[11], KS X ISO/IEC 19790[12]을 검증기준으로 하며, KS X ISO/IEC 24759[13]를 시험기준으로 하고 있다.

4.6 기 타

저장 기능이 없음에도 불구하고, USB 포트를 이용하는 주변기기(키보드·마우스·카메라 등)들 또한 BadUSB 관점에서 심각한 보안 위협이 될 수 있다는 것은 앞에서도 언급하였다. 이에 대한 대응방안의 예로서, Linux Kernel의 경우, 이기종간 USB 장치들을 서로 구별할 수 있다는 점을 이용하여, 인가되지 않은 USB 주변기기들에 대해 Kernel Level에서 차단한다면, 일정부분 USB 기반 주변기기들로 인한 보안 취약성 확대 가능성을 예방할 수 있을 것이다.

3) http://service1.nis.go.kr/

관리적 대응방안의 일환으로서, 강조하고자 하는 사항은, 일반적으로 데이터 저장 기능이 없는 USB 포트 기반 키보드·마우스·카메라 등은 보안에 취약하지 않다고 인식되어, 별도의 통제 대책 없이 사용되고 있지만, BadUSB 제작 기술과 접목시, 보안의 위협요소로 작용할 수 있다는 심각성이 사용자들에게 인식될 수 있는 보안교육이 필요하다고 본다.

또한, BadUSB로 악용될 가능성이 있다고 발표되는 컨트롤러 탑재 제품의 사용 금지(주의), 백신 P/G 최신화 등이 있다(현재 백신 P/G으로는 BadUSB 펌웨어 영역 감염여부를 탐지 가능한 것은 아니지만, BadUSB로 인해 악성 소프트웨어가 실행 될 때 일정부분 예방 효과 기대).

Ⅴ. 결 론

2014년 Black Hat Security Conference를 통해 USB 기반 장치들의 컨트롤러 펌웨어 영역 대상 악성코드 유입에 따른 취약성이 발표된 후, 국내·외 다양한 언론 혹은 보안전문가들에 의해 BadUSB 위협에 대해서는 지속적으로 논의가 되어 왔으며, 최근에는 '산업 제어 시스템(Industrial Control Systems)'까지 확대되어 적용될 수 있는 위협 가능성들이 제시되고 있다[14,15].

하지만, 대부분의 USB 컨트롤러 펌웨어 관련 제조사에서는, 위험성을 인지하고 있음에도 신속한 대응방안을 제시하지 못하고 있는 실정이며, 직접적 피해 사례가 발표된 적이 없다보니, 향후 매우 심각한 보안 위협으로 대두될 BadUSB 기술이 많은 일반인들에게는 인지되지 못하고 있다.

이에 대해 이 논문에서는 BadUSB 개념 및 발생 원인, 예상되는 보안 취약 사례, 대응방안 등을 종합적으로 제시하고자 하였으며, 이 논문의 결과가 보안 전문가 및 제조사 뿐만 아니라 일반 사용자의 보안 인식 제고에도 활용되기를 기대한다.

References

[1] Simson L. Garfinkel. "USB deserves more support," Boston Globe Online, Dec. 1995.
[2] Karsten Nohl and Jakob Lell, "BadUSB - on accessories that turn evil," Black Hat USA, Aug. 2014.
[3] Security Research Labs, "BadUSB - on

accessories that turn evil," https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-Black Hat-v1.pdf, pp. 4, Aug. 2014.
〔4〕 Trenton Henry, David Rivenburg, and Dan Stirling, "Universal serial bus device class specification for devie firmware upgrade," USB Implementers Forum, pp. 7-9, May 1999.
〔5〕 Adam Caudill and Brandon Wilson, "Making BadUSB work for you," Derbycon, Sep. 1994.
〔6〕 https://github.com/adamcaudill/Psychson/wiki/Known-Supported-Devices
〔7〕 Karsten Nohl, "BadUSB – on accessories that turn evil," POC, Nov. 2014.
〔8〕 Certificate Authority Security Council, "Code singning," https://casecurity.org/wp-content/uploads/2013/10/CASC-Code-Signing.pdf, pp. 1-6, Oct. 2013.
〔9〕 NIST, "Security requirements for cryptographic modules," FIPS PUB 140-2, May 2001.
〔10〕 http://www.wired.com/2015/02/firmware-vulnerable-hacking-can-done/
〔11〕 Choi Myeonggil and Jeong Jaehun, "A study on the policy of cryptographic module verification program," Journal of academia-industrial technology, 12(1), pp. 257, Jan. 2011.
〔12〕 Korean Agency for Technology and Standards, "Information technology - Security techniques - Security requirements for cryptographic modules," KS X ISO/IEC 19790, Dec. 2007.
〔13〕 Korean Agency for Technology and Standards, "Information technology－Security techniques－Test requirements for cryptographic modules," KS X ISO/IEC 24759, Dec. 2007.
〔14〕 http://www.scmagazineuk.com/badusb-malware-could-be-used-to-infect-icss/article/399275/
〔15〕 http://securityaffairs.co/wordpress/33765/hacking/badusb-attack-ics.html

〈저자소개〉

최 준 (Jun Choi) 정회원
2001년 2월: 경희대학교 이학부(수학) 이학사
2003년 2월: 고려대학교 정보보호대학원 공학석사
2008년 2월: 고려대학교 정보보호대학원 공학박사
2014년 11월~현재: 국방보안연구소 선임연구원
〈관심분야〉 암호알고리즘, 암호키관리, 정보보호프로토콜