디지털산업정보학회 논문지 제12권 제4호-2016년 12월
http://dx.doi.org/10.17662/ksdim.2016.12.4.089

사례 위주로 본 공급자망을 중심으로 한 IT제품 보안 위험*

최 웅 철**

Case studies : Security issues of IT products in terms of supply chain

Choi Woongchul

〈Abstract〉

Before an IT product is used, there is a sequence of the process such as the components supply-demand of the product, their assembly and production, their logistics and delivery, and then finally, the product can be used by a user. During this sequence of the process, there can be many security exposures and risks. In this paper, we show, by examining security cases of various IT products, that there are many security exposures in the process of IT products from their production to their delivery to end users and in their use, and also show how critical the security exposures are. Even though there are various security theories, technologies and security controls, there is still weak link from the production of an IT product to its use, and this weak link can lead to security vulnerabilities and risks. This paper tries to call attention to the importance of the execution of the security control and the control components. We examine the practical cases to find out how the security control is paralyzed, and to show how it is compromised by asymmetric security resources. Lastly, from the cases, we examine and review the possible domestic security issues and their countermeasures.

Key Words : Industrial Security, Security Control, Supply Chain

Ⅰ. 서론

오늘날 디지털 시대에 사용되는 IT제품들이 최종 완제품이 되기까지, 그리고 최종 사용자에게 인도되어 사용되기까지 과정을 보안 통제 관점에서 살펴보면, 여러 과정을 거치는 동안 보안 위협에 노출될 가능성이 매우 높다는 것을 알 수 있다. 제품 생산자의 입장에서는 좀 더 좋은 제품을 좀 더 낮은 가격으로 생산하기 위하여, 부품 수급에서부터 단위 모듈, 그리고 조립에 이르기까지 많은 과정에서 전 세계의 관련 업체들과 협력하게 되고, 따라서 이 과정에서 보안 위협이 보안 위험으로 될 가능성은 매우 높다고 하겠다. 이미 ISO에서는 이러한 공급자망의 보안 위협에 대한 보안 프레임워크로써 ISO 28000:2007 Specification for security management systems for

* 이 논문은 2014년도 광운대학교 교내학술연구비 지원에 의해 연구되었음.
** 광운대학교 컴퓨터소프트웨어학과 교수

the supply chain[1] 이라는 표준안을 오랜 검토 끝에 제정하였음에도 불구하고, 부품에서부터 완제품까지, 그리고 소비자에게 제품이 인도되어 사용될 때 까지 여러 단계에서 약한 연결고리(weak link)에 대한 보안 위협 및 위험들이 끊임없이 나타나고 있다. 본 논문은, 다양한 형태의 보안 위험을 가진 제품들이 시중에서 사용되었던 다수의 사례들을 살펴봄으로써, 공급자망을 통한 제품의 보안 위협에 대한 문제를 제기하고, 보안 통제가 어떤 식으로 무력화되는지에 대한 주의를 환기시키고자 한다. 또한 보안 통제의 각 요소의 중요성 및 비대칭 보안 위협과 관련한 심각한 문제들을 살펴봄으로써 보안 통제에 대한 주의를 제고하고자 한다.

Ⅱ. 연구배경

공급자망을 통한 보안위협은 광의적 의미의 보안 위협으로써, 네트워크에 접속되는 IT제품을 각종 보안 위협에 감염 시킨 채 공급하는 것을 의미한다. 이 위협이 가능한 이유는, 오늘날 대부분의 IT제품들이 제조될 때, 전 세계의 부품업체들로부터 가격대성능비가 좋은 부품을 구매하거나, 또는 생산을 아웃 소싱할 수 있다. 그리고 제품의 조립 또한 인건비가 저렴한 제 3국가에서 조립하여 공급하거나, 또는 물류 또한 아웃소싱함으로써, 생산에서부터 최종 소비자가 IT제품을 구매하여 사용할 때까지, 단일 보안 통제하가 아닌, 보안 통제가 결여된 여러 단계를 거침으로써, 보안 위협에 쉽게 노출될 가능성이 있다는 것이다. 이렇게 공급된 IT제품은 최종사용자가 IT제품을 사용하는 경우 보안 위협에 바로 노출될 수 있다. 만일 최종 사용자가, 정보기관이나 국방기관 또는 관련 기관에 근무하는 직원인 경우 문제의 심각성은 훨씬 커진다. 위와 같이 공급자망을 통한 IT제품의 보안 위협은, 보안 위협을 예방, 탐지가 단일 제품 생산, 공급인 경우보다 훨씬 어려우며, 책임 소재 또한 쉽게 결론내리기 힘든 구조로써, 보안 위협을 실행하고자 하는 공격자 측면에서는, 악성코드를 네트워크에 심어 보내는 것보다, 상대적으로 손쉬울 수 있고, 타겟의 범위를 한정 시킬 수 도 있으며, 공격 범위를 넓힐 수도 있는 등, 상대적으로 매우 효과적일 수 있다. 본 논문은, 이러한 공급자망을 통한 실제 사례를 살펴봄으로써, 보안 위협의 심각성과 이에 대한에 대한 경각심 및 보안 통제에 주의를 환기 시키며 이를 제고하고자 한다.

Ⅲ. 실제 보안 위험 사례들

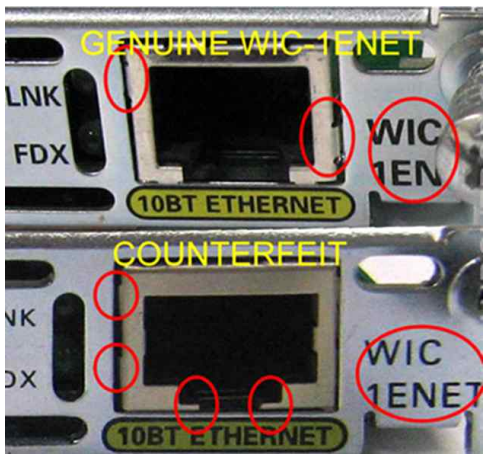
3.1 가짜 시스코 라우터 및 스위치 사건 (2008년)

2008년 미국에서는 FBI를 중심으로 미국 이민국, 세관국 등으로 특별반이 구성되어 미국 내에서 거래되고 있는 시스코 장비들 - 라우터, 스위치 등 400대 이상의, 당시 시가로 7600만달러 이상의 가짜 장비를 적발하는 사건이 발생하였다[2-4]. FBI는 이 사건에 대한 설명 자료를 ppt로 만들어 발표하였다. 이 사건은, 2001년 뉴욕 테러 이후 미 대통령 직속으로 Homeland security 라는 초정부적 기구[5]를 만들어 미국의 안전을 보호하기 위해 다방면에서 노력을 하고 있던 중, 물리적 안전 뿐만 아니라 사이버 공간의 안전에 대해 검토되고 기획되던 중에 발각된 사건으로 많은 주목과 우려를 낳게 되었다. [2]에 따르면, 각종 네트워크 장비들이 위조된 정황들에 대해 설명하고 있으며, 단순히 장비뿐 아니라, 위조 장비를 납품하는 과정에서도 다양한 위조품이 납품되고 또한 이를 실행한 납품 조직이 검거되었는데, 특히 미국 정부 산하 군 기관 등에 납품되어 사용됨으로써 충

격을 주었다. 이로 인하여 얼마나 많은 기밀 정보가 유출되었는지, 또한 어디로 유출되었는지에 대한 우려에 따라 광범위하고도 심도 있는 조사가 실시되었다. 장비들이 위조된 경우, 부품들이 미국 이외의 지역, 특히 특정 나라의 부품들이 주로 사용되었는 정황과, 체포된 범법자들의 국적 등에서, 사건의 심각성이 증폭되었다. 이에 납품된 정부 산하 기관들, 특히 국방 관련 기관들의 장비들을 전수 조사함으로써 400대 이상의 장비들이 모조품임을 알 수 있었고 이에 대한 상세한 자료들은 인터넷에서 확인할 수 있다. 이 사건을 통하여 보안 관련하여 여러 중요한 문제점들을 깊이 있게 검토하게 되었는데, 공급망에서의 보안 점검 통제, 납품 프로세스에서의 보안 통제, 그리고 납품된 장비의 보안 점검 통제 등 기존 보안 통제 제영역의 확대 필요성이 강력히 대두되었다.

<그림 1> 시스코사 제품의 정품과 위조품 사진 [3, 4]

<그림 2> 시스코사 제품의 정품과 위조품 사진 [3, 4]



<그림 3> 시스코사 제품의 정품과 위조품 사진 [3, 4]

아래는 가짜 제품이 발견된 시스코사의 라우터 및 스위치 장비들의 모델명들이다[2-4].

라우터 (Router)	1000 series, 2000 series	
스위치 (Switch)	WS-C2950-24, WS-X4418-GB	
인터페이스 카드 (Interface Card)	GigaBit Interface Card (GBIC)	WS-G5483, WS-G5487
	WAN Interface Card (WIC)	VWIC-1MFT-E1, VWIC-2MFT-G703, WIC-1DSU-T1-V2

3.2 바이러스에 감염된 디스크 드라이브

3.2.1 바이러스에 감염된 맥스터사의 하드디스크 드라이브 (2007년)

하드디스크 드라이브 제조사인 맥스터(Maxtor)사 제품 중, 스토리지 3200(Maxtor Basics Personal Storage 3200) 모델 일부가 바이러스에 감염된 채 전 세계에서 판매되는 사건이 2007년 가을 발생하였다[6].

<그림 4> 맥스터사의 외장 하드디스크 제품

이 드라이브는 전 세계 몇 개 지역에서 생산된 제품에서 바이러스에 감염된 제품이 판매되었는데, 감염된 드라이브를 설치하면, 그 시스템에 바이러스가 자동적으로 옮겨지도록 되었다. 이 제품은 제조사인 Seagate 사(Maxtor 사)가 직접 생산한 것이 아니고, 계약에 의해 하청 생산하였는데, 내부 조사 결과 하청 생산 과정에서 생산 회사 직원의 부주의에 의해 바이러스가 옮겨지게 된 것으로 알려졌다.

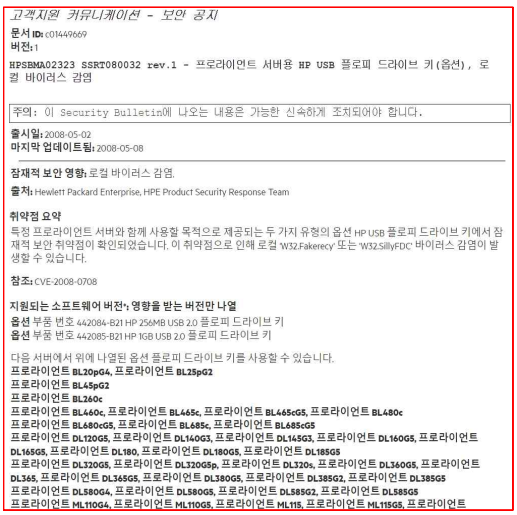
3.2.2 멜웨어에 감염된 디스크 드라이브 판매 (2011년)

할인판매 스토어 체인인 ALDI사의 호주 ALDI에서 판매된 Fisson 외장 형 4-in-1 디스크 드라이브가 멜웨어에 감염된 채 판매되었다[7, 8]. 호주 CERT (The Australian Computer Emergency Response Team, AusCERT)는 판매된 제품에 'Conficker'라는 웜바이러스(멜웨어)가 감염된 것을 발견하고 이를 공지하고 필요한 조치를 취하였다. 'Conficker'라는 웜바이러스(멜웨어)에 감염된 경우, 감염된 PC에서 보안 프로그램 업데이트, 인터넷 사이트 접근 불능 등의 증상이 나타나는 것으로 알려졌으며, 업무처리에 큰 피해를 줄 수 있다.

<그림 5> ALDI에서 판매된 Fisson 외장 형 4-in-1 디스크 드라이브

3.2.3 바이러스에 감염된 HP사의 USB 드라이브 (2008년)

HP사의 서버 모델 중 널리 알려진 모델인 ProLiant 서버 모델에 사용되는 USB 드라이브에서 바이러스에 감염된 제품이 발견되었다. 이 USB 드라이브를 사용하는 서버인 경우, 셋업과정에서 두 가지 종류의 바이러스에 감염이 되어 보안 위협에 노출되었다[9].



고객지원 커뮤니케이션 - 보안 공지

문서 ID: c01449669
버전: 1

HPSBMA02323 SSRT080032 rev.1 - 프로라이언트 서버용 HP USB 플로피 드라이브 키(옵션), 로컬 바이러스 감염

주의: 이 Security Bulletin에 나오는 내용은 가능한 신속하게 조치되어야 합니다.

출시일: 2008-05-02
마지막 업데이트됨: 2008-05-08

잠재적 보안 영향: 로컬 바이러스 감염.

출처: Hewlett Packard Enterprise, HPE Product Security Response Team

취약점 요약

특정 프로라이언트 서버와 함께 사용할 목적으로 제공되는 두 가지 유형의 옵션 HP USB 플로피 드라이브 키에서 잠재적 보안 취약점이 확인되었습니다. 이 취약점으로 인해 로컬 'W32.Fakerecy' 또는 'W32.SillyFDC' 바이러스 감염이 발생할 수 있습니다.

참조: CVE-2008-0708

지원되는 소프트웨어 버전: 영향을 받는 버전만 나열

옵션 부품 번호 442084-B21 HP 256MB USB 2.0 플로피 드라이브 키
옵션 부품 번호 442085-B21 HP 1GB USB 2.0 플로피 드라이브 키

다음 서버에서 위에 나열된 옵션 플로피 드라이브 키를 사용할 수 있습니다.
프로라이언트 BL20pG4, 프로라이언트 BL25pG2
프로라이언트 BL45pG2
프로라이언트 BL260c
프로라이언트 BL460c, 프로라이언트 BL465c, 프로라이언트 BL465cG5, 프로라이언트 BL480c
프로라이언트 BL680cG5, 프로라이언트 BL685c, 프로라이언트 BL685cG5
프로라이언트 DL120G5, 프로라이언트 DL140G3, 프로라이언트 DL145G3, 프로라이언트 DL160G5, 프로라이언트 DL165G5, 프로라이언트 DL180, 프로라이언트 DL180G5, 프로라이언트 DL185G5
프로라이언트 DL320G5, 프로라이언트 DL320G5p, 프로라이언트 DL320s, 프로라이언트 DL360G5, 프로라이언트 DL365, 프로라이언트 DL365G5, 프로라이언트 DL380G5, 프로라이언트 DL385G2, 프로라이언트 DL385G5
프로라이언트 DL580G4, 프로라이언트 DL580G5, 프로라이언트 DL585G2, 프로라이언트 DL585G5
프로라이언트 ML110G4, 프로라이언트 ML110G5, 프로라이언트 ML115, 프로라이언트 ML115G5, 프로라이언트

<그림 6> USB 드라이브 키가 감염되었다는 사실을 공지한 HP사 웹페이지 내용[10]

Ⅳ. 바이러스에 감염된 컴퓨터

4.1 바이러스에 감염된 Toshiba 신형 노트북 컴퓨터 (2008년)

2008년 도시바사의 노트북 모델중 저가 사양인 제품에서 바이러스에 감염된 제품이 판매된 경우가 보고되었다[11]. 알려진 모델은 Satellite 모델로, 판매될 당시 제품의 봉인은 뜯기지 않은 새제품이었는데, 당시 노트북에는 시만틱사의 안티바이러스 프로로램도 기설치된 상태였다고 하며, 제품 생산 제조 과정에서 'RavMon'이라는 바이러스가 감염된 것으로 알려졌다. 이 'RavMon'바이러스는 USB 자동실행(Autorun) 바이러스로, 이 자체가 action agent 역할을 수행할 수 있으므로, 보안에 심각한 위협이 될 수 있다.

4.2 바이러스에 감염된 신형 PC들(2012년)

마이크로소프트사가 중국에서 판매되고있는 신형 PC들과 노트북 컴퓨터 20대를 조사한 결과, 4대의 신형 PC들과 노트북 컴퓨터들에서 멜웨어가 사전에 설치된 것을 발견하였다고 2012년 발표하였다[12]. 마이크로소프트사가 발견한 멜웨어는 'Nitol'이라 불리는 것으로, 케이만 제도에 있는 서버로부터 통제되는 것으로 알려졌다. 마이크로소프트사는, 중국에서 자사 소프트웨어의 불법 사용에 대한 조사과정에서 위 사실을 발견하였고 이를 공지하였다. 마이크로소프트사는, 자사 운영체제인 Windows 운영체제가 인터넷에서 연결기반의 서비스를 제공한다는 점에서 본 사건의 심각성에 주목하였다. 즉, Windows 운영체제가 설치된 신형 PC를 사용할 경우, 인터넷 연결기반 서비스를 통하여 짧은 시간 내에 많은 PC들에게 멜웨어가 옮겨질 가능성이 매우 높은 상황이었으며, 신형 PC에서 바이러스에 감염된 것은 제조사 또는 제조사 협력 업체를 통하여 가능했을 것이라는 추측이 가능한 상황이었다.

Ⅴ. 비대칭 보안 위협의 효과성 및 보안 통제에 있어서 '사람'의 중요성 사례

5.1 정부 건물에서 발견된 주인 없는 USB 드라이브

미국 워싱턴 D.C. 의 보안부 소속의 연방 부장검사들이 근무하는 건물에서 주인 없이 놓여진 USB 메모리 2개가 발견되었다[13]. 그 중 하나의 USB 메모리는 남자화장실에서, 다른 하나는 팩스기 근처에서 놓여 진 것이 발견된 것으로 알려졌다. 이 USB들에는 악성 코드들이 담겨져 있었던 것으로 조사결과 밝혀졌다. 만약 이 메모리들이 습득된 후 아무런 의심 없이 PC에 연결되었을 경우, 보안부서 내 PC들이 쉽게 악성코드에 의해 감염되었을 것이고, 따라서 많은 보안 정보들이 유출되었을 것이다. 다행히 위 사건은, 화장실 청소원이 발견하여 즉시 신고함으로써, 보안 위협을 사전에 방지할 수 있었던 사건이었다. 이 사건은 보안 통제에 있어 몇 가지 중요한 시사점을 던져주고 있다. 첫째는, 정부기관 산하 주요 시설에 대한 비대칭적 보안 공격이다. 정부 기관 및 산하 기관들의 출입 및 시설에 대한 물리적 접근은 엄격히 통제되며, 물리적 접근 통제에 대한 비용은 상당히 큰 금액인 반면에, 이를 뚫을 수 있는, 상대적으로 저렴한 USB 메모리들 몇 개를 건물 이곳저곳에 뿌려두고, 그 중 하나라도 PC에 성공적으로 연결된다면, 값비싼 비용을 들여 구축한 물리적 보안 통제가 거의 무용지물화 되고 마는 결과를 가져 올 수 있다. 둘째, 보안 통제에 있어 인력의 중요성을 다시 한 번 상기 시키는 계기가

되었다. 즉, 분실된듯한 의심스러운 USB 메모리를 발견하고 신고한 청소원이 없었더라면, 정보 유출에 따른 보안 위험 및 그에 따른 손실은 상당했을 것이었는데, 이를 방지한 것이 결국 청소원이라는 인력이었던 것이다. 즉, 보안 통제를 위한 각종 장비 및 시스템도 중요하겠지만, 결국 인력에 대한 보안 교육 또한 중요하며, 더불어 인적 자원들의 대화 내용, 사무 작업 후의 쓰레기 처리 등 물리적 보안 시스템을 우회할 수 있는 위협 요소들이 많기 때문에, 인적 자원에 대한 보안 교육에도 소홀함이 없어야 할 것 이다.

5.2 군 해외 주둔지 부대 주변에서 판매되는 USB, CD 등의 악성 코드

미국에서는 2001년 911 사태이후 테러와의 전쟁을 통하여, 아프가니스탄, 이라크 등에서 전쟁과 전쟁을 이어가고 있었다. 미군 및 유엔 주둔지에서는 여러 단계의 물리적 보안 통제를 강화하기 위하여, 만일의 사태에도 방어할 수 있도록 많은 비용과 자원을 투입하여 보안을 강화하고자 하였다. 미군 주둔지 부대에서 군사 작전을 위해 기지 외부로 출병하는 경우, 출병 정보에 대한 보안 통제가 매우 심하였는데도 불구하고, 정보가 사전 누출되어 전투 시 인명 피해가 심한 경우도 있었는데, 사건 조사 결과, 출병 정보가 사전 누출된 정황도 있어서, 정보 유출 예방에 많은 노력을 하였고, 또한 기지 내외의 물리적 보안 및 정보 보안 강화에 많은 비용과 자원을 투입하였음에도 유사 경우가 발생하였는바, 보안 통제에 대한 검토 결과 중 한 가지 조사 결과에 주목하였다. 즉, 군사 기지 주변에는 현지인들이 군 병력을 대상으로 물건을 판매하는 경우가 다수였고, 이 경우 판매 물건에는 동영상 또는 각종 유틸리티가 포함된 불법 USB 메모리, CD/DVD 동영상 등이 포함되어 있었는데, 이들 중 99%이상이 각종 바이러스에 감염된 채 거래되고 있음이 밝혀졌다. 즉, 주둔지 경비를 위해 많은 비용과 자원을 투입하였음에도 불구하고, 외부의 비교적 값싼 USB 또는 CD/DVD를 기지 내로 들여보냄으로써, 상대적으로 매우 손쉽게 보안 정보 자원에 접근할 수 있었고, 출병과 같은 고급 정보를 획득할 수 있었다. 이런 경우에 있어서도 보안 통제에 있어 많은 시사점을 던져 주고 있다. 즉, 보안 통제를 위해 많은 비용 및 자원을 투입하고도, 비대칭적으로 USB, CD/DVD 등과 같은 값싼 자원을 이용하여 큰 어려움 없이 고급 정보에 접근 할 수 있다는 점, 그리고, USB 또는 CD/DVD를 이용할 때 불법 자료는 사용하지 말아야 한다든지, 또는 부득이 사용할 경우라도 보안 점검 후 사용한다든지 하는 기본적인 보안 통제에 대한 교육에 대한 강조는 아무리해도 지나치지 않고, 그런 보안 활동이야말로 자신과 부대원들의 생명을 지킨다는 점이다.

VI. 국내 시장 사례

6.1 휴대폰 백도어 사례

레노버, 화웨이, ZTE 등 중국제조사의 휴대폰들이 백도어를 사용하고 있다는 사실 및 정황이 계속 보도되었다[14]. 미국 정부는 이런 이유로 화웨이 제품을 시장에서 배제시키고, 화웨이사는 이에 불복하여 여러 절차를 밟았으나 결국 미국시장에서 철수하였다. 휴대폰 백도어 문제는 최근에도 끊임없이 제기되고 있는데, 최근 샤오미사의 휴대폰에 앱을 통한 백도어 문제가 보도되었다[15].

Ⅶ. 맺음말

각종 IT제품이 제조사에 의해 생산에서부터 완성되어 사용자에게 인도되어 사용될 때 까지, 여러 과정에서 보안 위협이 존재함을 다수의 실제 사례들로부터 볼 수 있었으며, 이러한 보안 위협과 위험은, 공급자망의 보안 위험에 대한 보안프레임워크로써 ISO 28000:2007 Specification for security management systems for the supply chain[1]와 같은 보안 프레임워크안이 없어서가 아니라, 보안 통제 각 요소들의 유기적인 협력이 없이는 무력화되기 쉬우며, 일단 보안 위험이 실제로 나타나는 경우 그 피해가 상당하다는 특징이 있다. 이 문제의 심각성은, 오늘날과 같이 해외 직접 구매가 가능한 시대에서, 한 국가의 보안 통제가 아무리 효과적이다 할지라도, 사용자가 제품을 해외에서 직접 구매를 함으로써, 사용자 국가의 보안 통제를 의도적이든 그렇지않든 우회할 수 있게 되고, 따라서 보안 통제 자체가 무력화하게 된다. 또한 많은 경우, IT 제품의 보안 위험은, 사전 예방이 최선임에도 불구하고, 본 논문의 여러 사례들에서 보는바와 같이, 보안 위험이 현실화 된 후에야 비로소 해당 제품의 수거 또는 방지 대책이 작동하게 되는, 사후 처리 형태의 보안 통제만이 동작하게 되는 문제가 있다. 이미 많은 기업에서 보안의 중요성을 인지하고 이 분야에 투자를 많이 하고 있으나 [16, 17], 이 문제의 보다 더 심각한 점은, 보안 위험을 가진 장비가 정보나 국방과 같은 민감한 정보를 다루는 부서에 납품되어 사용되는 경우로, 국가 존립 자체를 흔드는 문제로까지 비화될 수 있음을 인지하여, 보안 통제 각 요소 각각의 동작과 유기적 연동에 대한 시스템적인 모니터링 프로세스가 꼭 필요함을 알 수 있다.

참고문헌

[1] ISO 28000:2007, http://www.iso.org/iso/catalogue_detail?csnumber=44641, ISO

[2] Raul Roldan, http://www.zdnet.com/article/fbi-counterfeit-cisco-routers-risk-it-subversion/, ZDNET, 2008.

[3] Andover Test for Real/Fake Cisco, http://www.andovercg.com/services/cisco-counterfeit-wic-1dsu-t1.shtml, Andover.

[4] Zeriva Anti-Counterfeit Process, http://www.zeriva.com/cisco-refurb/refurb-process/zeriva-anti-counterfeit-process/, Zeriva.

[5] Dept. of Homeland Security. https://www.dhs.gov/, US Government.

[6] Robert McMillan, http://www.infoworld.com/article/2650800/security/seagate-ships-virus-laden-hard-drives.html, Infoworld, 2007.

[7] Michael Lee, http://www.zdnet.com/article/aldi-sells-hard-drives-with-malware-inside/, ZDNET, 2011.

[8] Darren Pauli, http://www.crn.com.au/news/aldi-recalls-conficker-infected-hard-drives-265264, CRN, 2011.

[9] Virus Bulletin, https://www.virusbulletin.com/blog/2008/04/hp-ships-infected-usb-keys, Virus Bulletin, 2008.

[10] HP 고객지원센터, http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c01404119, HP, 2008.

[11] Anonymous, http://blog.irreverence.co.uk/?p=509, 2008.

[12] Associated Press, https://www.theguardian.com/technology/2012/sep/14/malware-install

ed-computers-factories-microsoft, TheGuardian, 2012.
[13] Robert Charette, http://spectrum.ieee.org/riskfactor/computing/it/thumb_drive_security_peril_at, IEEE Spectrum, 2008.
[14] 성상훈, http://www.ittoday.co.kr/news/articleView.html?idxno=58403, 아이티투데이, 2015.
[15] Swati Khandelwal, http://thehackernews.com/2016/09/xiaomi-android-backdoor.html, The Hacker News, 2016.
[16] 정병호, "기밀정보 유출 경험을 가진 기업들의 정보사고 대응역량 강화에 관한 연구," 디지털산업정보학회 논문지, 제12권, 제2호, pp. 73-86.
[17] 김정은, 김성준, "정보보호관리체계(ISMS)를 이용한 중소기업 기술보호 개선방안 연구," 디지털 산업정보학회 논문지, 제12권, 제3호, pp. 33-54.

■ 저자소개 ■

최 웅 철
Choi Woongchul

2002년 9월~현재
광운대학교 컴퓨터소프트웨어학과 교수
2001년 5월 Univ. of Illinois, Ph.D., Computer Science
1991년 2월 서울대학교 컴퓨터공학과(공학석사)
1989년 2월 서울대학교 컴퓨터공학과(공학사)

관심분야 : 데이터네트워크, 보안
E-mail : wchoi@kw.ac.kr

논문접수일 : 2016년 11월 20일
수 정 일 : 2016년 12월 13일
게재확정일 : 2016년 12월 14일