정 보 보 호 학 회 지
제24권 제1호, 2014. 2

사이버보안 위협 변화에 따른 취약점 분석 방안

민 병 길*, 안 우 근*, 서 정 택*

요 약

각종 악성코드와 취약점이 하루가 다르게 출현하고 있다. 주기적인 취약점 분석·평가는 새로운 사이버보안 위협에 신속하게 대응하고 지속적으로 사이버보안을 강화하는 중요한 활동이다. 그러나 최근 스마트폰 이용 확산에 따른 모바일 보안위협 증가와 기반시설 제어시스템에 대한 보안위협 증가는 기존 취약점 분석·평가 방법의 구조적인 변화를 요구하고 있다. 본 논문에서는 스마트폰 테더링과 같은 모바일 보안위협에 따른 취약점 분석·평가 시의 고려사항과 시스템 영향을 최소화 할 수 있는 분석 절차와 방안을 제시하고 있다. BYOD를 사용한 모바일 인터넷 사용은 내·외부 네트워크 구분을 무의미하게 만들고 있기 때문에 다양한 침입경로에 대한 분석이 필요하다. 또한 제어시스템과 같이 높은 가용성이 요구되는 시스템에 대해서는 유휴시간 점검, 백업 시스템 점검, 테스트 베드 등을 사용한 취약점 점검 방법의 도입이 필요하다.

Ⅰ. 서 론

취약점 분석은 구축, 운영되고 있는 정보시스템의 사이버보안 취약점을 찾아냄으로써, 이를 제거하거나 보안대책을 수립하도록 하여 지속적으로 사이버보안을 강화해 나가는 적극적이고 효과적인 보안활동이다. 따라서 미국은 FISMA(Federal Information System Management Act)를 제정하고, 정부기관의 정보시스템에 대하여 매년 취약점 분석·평가를 수행하고 보호계획을 작성토록 하고 있으며, 우리나라 또한 “정보통신기반보호법(법률 제11690호)”을 제정하고 “주요정보통신기반시설”을 지정하여 매년 취약점 분석·평가를 수행토록 하고 있다.

최근 정보통신 환경은 클라우드, 스마트폰 등의 BYOD (Bring Your Own Device) 활용이 확대되고, 사이버 공격 대상 또한 전통적인 정보통신시스템에서 기반시설 제어시스템으로 급변함에 따라 취약점 분석·평가 방법에 대한 구조적 변화가 요구되고 있다. 본 논문은 이러한 사이버보안 위협 변화에 따른 취약점 분석·평가 절차를 제시하였다.

Ⅱ. 사이버보안 위협 변화

2.1. 모바일 인터넷 증가에 따른 보안위협

스마트폰의 확산으로 모바일 인터넷 이용이 급격하게 증가하고 있으며, 이러한 모바일 기기를 업무에 활용하는 BYOD 흐름 또한 크게 증가하고 있다. 스마트폰과 태블릿을 업무에 이용하는 직원의 수는 2014년 전세계적으로 3억 5천만 명에 달할 것으로 전망되고 있으며[1], 국내 스마트폰 가입자 또한 2012년 3,200만 명에서, 2015년에는 4,200만 명에 이를 것으로 전망되고 있다. 이에 따라 모바일 보안 위협 또한 크게 증가하여 2012년 3/4분기 51,477개의 안드로이드 모바일 악성코드가 발견되었다[2]. 이는 직전 분기 대비 약 10배가 증가한 수치이다. 기업의 BYOD 허용 여부를 떠나 이미 많은 직원들이 업무에 스마트폰을 활용하고 있으며, 이에 따라 모바일 보안위협 또한 크게 증가하고 있다. 따라서 취약점 분석·평가 시, 모바일 보안위협에 대한 고려가 필수적으로 요구되고 있다.

본 연구는 2012년도 산업통상자원부 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 원자력융합원천기술개발 과제입니다. (No.20121510100030)
* ETRI 부설 연구소(bgmin@ensec.re.kr, wgahn@ensec.re.kr, seojt@ensec.re.kr)

2.2. 제어시스템에 대한 보안위협 증가

2011년 10월 발견된 Stuxnet은 제어시스템을 공격한 최초의 사이버 무기로 평가되고 있으며, 이란의 원자력 시설을 공격하였다[3]. 이후에도 Duqu(2011), Flame (2012)과 같은 기반시설 및 제어시스템을 공격 대상으로 하는 악성코드들이 지속적으로 발견되고 있다. 미국은 ICS-CERT(Industrial Control System -CERT)[4]를 운영하고 있으며, ICS-CERT Monthly Report에 따르면 매 회계연도(FY : Fiscal Year)별 제어시스템 사이버 사고(incident)는 [표 1]과 같이 2010년 40건에서 2011년에는 130건, 2012년에는 198건으로 급증하였다.

〔표 1〕 ICS Incident & Vulnerabilities

ICS-CERT Metrics	FY-10	FY-11	FY-12
ICS Incident	40	130	198
ICS Related Vulnerabilities	17	145	171

이렇게 기반시설 및 제어시스템에 대한 사이버보안 위협은 계속되고 있으며, 앞서 통계자료를 통하여 살펴본 바와 같이 앞으로 더욱 증가할 것으로 예상된다. 따라서 제어시스템에 대한 취약점 분석 · 평가를 주기적으로 수행하여 보안 취약점을 제거하고 보안대책을 수립하여 적용하는 노력이 필요하다.

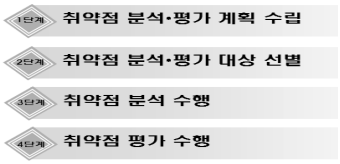
Ⅲ. 관련연구

3.1. KISA 취약점 분석 · 평가 모델

취약점 분석 · 평가는 수행 주체에 따라서 다양한 방식과 절차를 가지고 수행된다. 그러나 큰 틀에 있어 한국인터넷진흥원((舊)한국정보보호진흥원)의 취약점 분석 · 평가 모델[5]을 벗어나지 않는다. 이 모델은 현황분석, 취약점 분석, 위험 평가, 대책 권고의 4단계로 구성되며, 취약점 분석은 다시 자산 분석, 위협 분석과 취약점 분석으로 세분화되어 구성된다. 전체 모델과 세부 수행절차는 [그림 1]과 같다. 이 모델은 대부분의 취약점 분석 · 평가 시 적용되고 있으나, 제어시스템 취약점 분석과 같이 점검 대상 시스템의 가용성 보장이 필요한 경우에 대한 보다 세부적인 절차 수립이 필요하다.

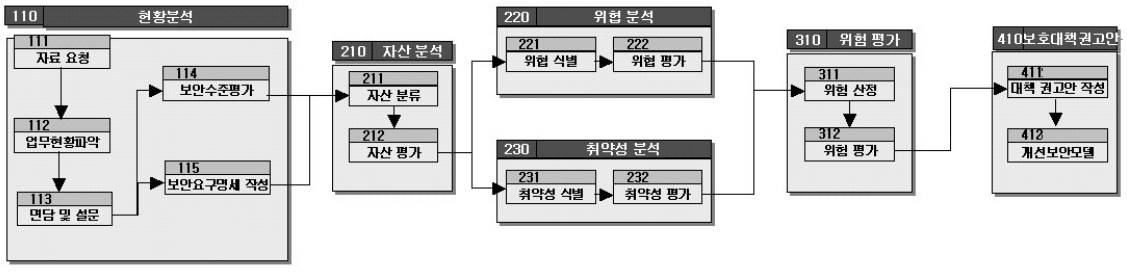
3.2. 취약점 분석 · 평가에 관한 기준 고시

우리나라는 정보통신기반보호법(법률 제11690호)에 의거 주요정보통신기반시설에 대해서 주기적으로 취약점 분석 · 평가를 수행하고, 이에 대한 보호대책을 수립하도록 하고 있다. 동법 제9조 4항은 미래창조과학부장관이 '취약점 분석 · 평가에 관한 기준'을 정하여 고시토록 하고 있으며, 동법 시행령 제18조 4항에는 고시되는 해당 기준은 취약점 분석 · 평가의 절차, 범위 및 항목, 평가방법을 포함 하도록 하고 있다.



〔그림 2〕 취약점 분석 · 평가 수행 절차

2013년 8월 고시된 미래창조과학부 고시 제2013-37호의 취약점 분석 · 평가 기준은 계획 수립, 평가 대상 선별, 취약점 분석, 취약점 평가의 4단계 절차를 제시하고, 관리적, 물리적, 기술적 취약점 분석을 수행토록 하

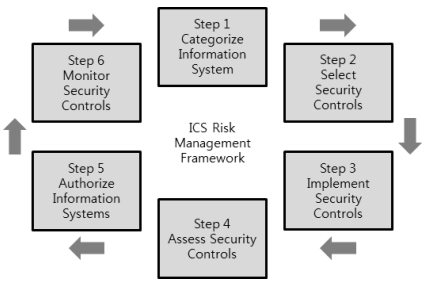


〔그림 1〕 (舊)한국정보보호진흥원 취약점 분석 · 평가 모델

고 있다. 고시의 취약점 분석 기준 항목은 2012년 12월, 제어시스템 22개 항목, PC 20개, 데이터베이스 24개 항목을 신설, 확대하여 제어시스템 보안위협 증가 등 새로운 사이버보안 위협 변화에 대한 점검이 가능하게 하였다. 그러나 사이버보안 위협 변화에 따른 취약점 분석 절차의 세부적 제시가 부족하다.

3.3. Guide to ICS Security

제어시스템에 대한 보안위협이 증가함에 따라, 美 NIST (National Institute of Standards and Technology)는 2011년 제어시스템 보안을 위한 프레임워크와 보안항목(security control)을 제시한 “Guide to Industrial Control System Security(NIST SP 800-82) [6] "를 발표하고, 2013년 이를 다시 개정하여 NIST SP 800-82 Rev. 1를 발표하였다. NIST SP 800-82는 위험관리 프레임워크와 관리, 운영, 기술적 측면의 보안항목을 제시하고 있다.

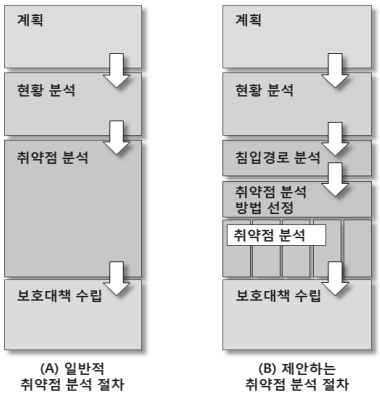


〔그림 3〕 ICS Risk Management Framework

그러나 제시된 프레임워크는 위험관리에 대한 큰 틀의 프레임워크로 세부적인 취약점 분석 절차의 제시는 부족하다.

Ⅳ. 사이버보안 위협 변화에 따른 취약점 분석 방안

모바일 및 제어시스템 보안위협 증가에 따른 취약점 분석을 수행하기 위해서는 보안항목 구성 외에 절차에 대한 구조적 개선도 필요하다. 일반적인 취약성 분석 절차는 계획 수립, 현황 분석 수행, 취약점 분석, 보호대책의 수립으로 이루어진다. 제안하는 취약점 분석 절차는 취약점 분석을 세분화하여 침입경로 분석, 취약점 분석 방법 선정, 취약점 분석으로 구성하여, 사이버보안 위협 변화에 대응토록 하고 있다.

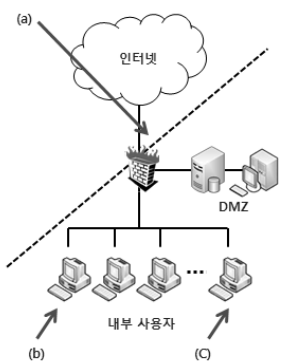


〔그림 4〕 제안하는 취약점 분석 절차

4.1. 침입경로 분석

[그림 5]는 일반적인 네트워크 구조를 간략화하여 표현하고 있다. 일반적으로 취약점 분석 시, [그림 5]의 점선 위쪽을 외부 네트워크로 보고, 외부로부터의 침입경로 (a)만 분석한다. 점선의 아래쪽은 내부 네트워크로 인식하고, USB 등을 통한 악성코드 감염 등에 대해서만 고려한다. 따라서 외부로부터의 접근통제, 보안대책은 방화벽 등의 유선네트워크 접점에서만 적용되게 된다. 그러나 모바일 인터넷, BYOD 사용의 증가는 이러한 전통적 내·외부 구분을 의미없게 만든다. 스마트폰 등을 사용한 테더링(tethering)은 내부 네트워크로 인식되던 사용자 단말에서 직접 모바일인터넷으로 연결할 수 있게 함으로써 방화벽을 무력화시키고, 외부로부터의 침입이 직접 내부로 이어질 수 있게 되었다.

따라서 일반적인 취약점 분석 시, 내부와 외부네트워크를 구분하고 연결 접점을 분석하는 기존의 방식은 새



〔그림 5〕 침입경로의 다양화

로운 사이버보안 위협 변화에 따라 의미가 없어졌다. 대신 [그림 5]의 (b), (c)와 같은 내부 사용자 영역에서도 외부로부터의 침입경로가 형성될 수 있음을 인식하고, 침입경로의 다양성에 대한 분석이 필요하며, 보안대책의 수립 시에도 기존의 내·외부 구분에 따른 심층적 방어 개념이 아닌 전방위적이고 입체적인 보안대책 수립이 필요하다.

4.2. 시스템 영향을 최소화하는 취약점 분석 방법 선정

제어시스템은 원격지의 장치를 모니터링 및 제어하는 특성으로 인해 일반 IT시스템과는 다른 특징이 있다.

[표 2]와 같은 특성으로 인하여, 제어시스템과 일반 IT 시스템의 가장 큰 차이점은 보안 목적의 우선순위가 다르다는 것이다. 전형적인 IT 시스템의 경우, 기밀성을 가장 중요하게 고려하고 있으며 다음으로 무결성, 가용성 순으로 우선순위 정하고 있다. 그러나 제어시스템의 경우, 보안 목적 우선순위가 IT 시스템과는 반대로 가용성이 가장 중요시된다. 중요 인프라를 모니터링 및 제어하는 시스템은 반드시 높은 가용성을 보장하며 작동해야 한다. 시스템 정지에 따른 여파는 단순 불편을 넘어, 막대한 물리적 파급효과로 이어지기 때문이다.

이와 같이 제어시스템은 높은 실시간성과 가용성을 요구하고 있어, 취약점 분석으로 인한 시스템 중단 또는 영향을 최소화해야 하며, 제어기기, 제어프로토콜 등 제

〔표 2〕 제어시스템과 정보(IT)시스템 비교

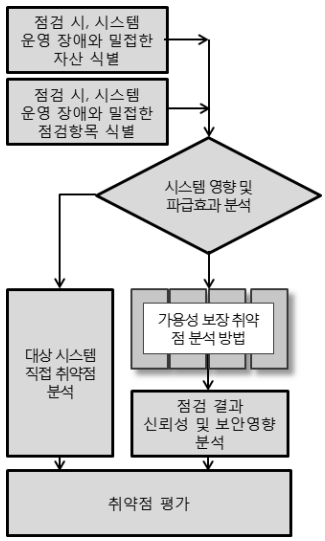
특징	제어시스템	정보(IT)시스템
성능 요구사항	기계적 수준의 실시간성 응답시간 (예:10ms)	사람이 기다릴 수 있는 수준 실시간 응답성 요구
가용성 요구사항	24시간 무중단 운영 (운영정지가 매우 제한적)	고장이나 장애가 일정수준 허용됨
구성	컴퓨터, 네트워크 현장 제어장치(PLC, IED, RTU 등)	컴퓨터, 네트워크 장비
생애주기 및 교체비용	긴 생애주기(15-20년) 고가의 구입 비용	짧은 생애주기(3-5년) 저렴한 구입 비용
소프트웨어	전용 응용프로그램 산업계에 적합한 전용 프로토콜	다양한 응용프로그램 공개 및 표준화된 통신 프로토콜
보안패치	패치 어려움	패치 용이

〔그림 6〕 일반 IT 시스템과 제어시스템 보안목적 우선순위 비교

어시스템에만 사용되는 시스템, 기기 등에 대한 취약점 점검도 수행해야 한다. 제어시스템에 대한 취약점 점검 기준은 미래창조과학부 고시(제2013-37호)에서 제시되고 있으며, ICS-CERT의 제어시스템 공통 취약점 보고서[7]를 참조할 수 있으므로, 본 논문에서는 제어시스템 취약점 분석·평가 시 적용할 수 취약점 분석 절차에 대하여 제시하였다.

제어시스템에 대한 취약성 분석 절차 역시 동일한 순서로 이루어지게 된다. 그러나 제어시스템 취약성 분석은 일반 IT 취약성 분석과 달리 제어시스템 특성 상, 취약점 분석으로 인한 시스템 영향을 최소화하도록 진행되어야 한다.

제안하는 취약점 분석 절차는 시스템 영향을 최소화할 수 있는 취약점 분석 방안을 제시하고 있으며, 취약점 분석 전, 취약점 분석 방법 선정 절차를 추가로 구성



〔그림 7〕 제안하는 취약점 분석 방법 선정 및 취약점 분석 절차

하고 있다. 취약점 분석 방법 선정과 점검 방법은 다음과 같다.

1) 시스템 운영, 물리적 피해 등에 밀접한 영향을 미치는 자산 식별
2) 1)의 해당 시스템을 대상으로 한 점검항목 중, 시스템 운영에 영향을 미칠 수 있는 항목 식별
3) 해당 자산과 점검항목이 시스템 운영에 미치는 영향과 파급효과 분석
4) 3)의 분석결과에 따라서 필요한 경우 다음과 같은 점검 방법으로 대체하여 점검 수행
   - 시스템 운영 유휴시간을 이용한 점검
     - 시스템이 운영하는 대상 시설을 사용하지 않거나, 영향이 적은 시간을 선정하여 취약점 분석 수행
   - 백업 시스템을 이용한 점검
     - 백업 시스템이 구성되어 있는 경우, 백업 시스템을 대상으로 취약점 점검 수행(단, 백업 시스템이 운영 시스템과 이기종으로 구성된 경우에는 적용할 수 없음)
   - 테스트베드를 이용한 점검
     - 점검 대상 시스템과 동일한 시스템, 환경으로 구성된 테스트베드 시스템이 구성되어 있는 경우, 테스트베드에서 취약점 분석 수행
   - 자산분석, 구성설정 점검을 통한 점검 또는 문서분석
     - 상기와 같은 점검이 불가능 한 경우, 자산분석, 구성설정 등을 점검하여 해당 취약점에 의한 보안 영향을 분석·평가
5) 4)의 과정을 통하여 분석된 취약점 분석 결과는 실제 운영되는 시스템(최초의 취약점 분석 대상 자산)에 대한 점검결과로서 활용하기 위하여, 실 운영시스템과 점검한 시스템과의 비교분석을 통하여 점검결과의 채택 여부 및 보안영향을 분석

각 방법은 실제 운영되는 시스템을 직접 대상으로 하고 있지 않기 때문에, 점검결과가 최초의 대상 시스템에 대하여 얼마나 정확한가 하는 것을 분석해야 한다. [표 3]은 각 분석 방법에 대하여 비교한 것으로, 구성설정, 문서 점검 방법은 시스템 영향성이 가장 낮은 반면, 점검결과 또한 실제 취약점을 정확하게 점검할 수 없다. 유휴 시간 점검방법은 점검결과의 신뢰성이 가장 높지만, 시스템에 대한 영향성 또한 가장 크기 때문에 시스템 영향에 대비한 비상대응, 복구 방안을 강구하고 점검을 수행해야 한다. 제안된 취약점 분석 방법은 운영 시스템 현황과 여건에 따라서 선택 적용되어 질 수 있다.

〔표 3〕 시스템 영향 최소화를 위한 취약점 분석 방법 비교

	유휴 시간 점검	백업시스템 점검	테스트베드 점검	자산, 구성설정, 문서 점검
시스템 영향	상	중	하	없음
점검결과 신뢰성	상	중	중	하
점검결과 신뢰성 검토방안	점검결과 활용	주 운영 시스템과 백업시스템 비교 분석	운영시스템과 테스트베드 비교분석	점검항목의 실현 요건 검토
비상대응 및 복구	데이터 백업, 복구 인력 대기	백업시스템 복구인력 대기	-	-

Ⅴ. 결론

스마트폰 등의 BYOD 사용 확산으로 모바일 보안위협이 크게 증가하였으며, 이에 따라 일반적인 취약점 분석·평가에서와 같은 내·외부 네트워크 구분과 분석은 의미가 없게 되었다. 또한 기반시설 제어시스템에 대한 보안위협 증가로 이에 대한 취약점 분석이 필수적으로 요구되고 있다. 본 논문에서는 이러한 사이버보안 위협 변화에 따른 취약점 분석 절차 개선 방안을 제시하였다. 제시된 방안은 테더링 등을 통한 모바일 보안위협에 대한 외부 침입경로 분석 절차를 제시하고, 높은 가용성과 시스템 안전성을 요구하는 제어시스템 분석을 위한 취약점 분석 방법 및 선정 절차를 제안하였다. 제안된 방안은 각 기업의 취약점 분석·평가 시 변형하여 적용함으로써, 취약점 분석 평가 시, 시스템 영향성을 최소화할 수 있을 것으로 기대된다. 향후 제안된 절차를 반영한 취약점 분석·평가 전체 모델을 연구하고, 이를 실제 점검에 적용하여 검토·개선하는 노력이 필요하다.

참고문헌

[1] "*Mobile Security: BYOD, mCommerce, Consumer & Enterprise 2013-2018*", Juniper research, 2013.

[2] "*국가정보보호백서 2013*", 국가정보원, 미래창조과학부, 방송통신위원회, 안전행정부, 2013.

[3] Nicolas Falliere, Liam O Murchu and Eric Chien, "*W32.Stuxnet Dossier*", Symantec Security Response Report, Feb. 2011.

[4] http://ics-cert.us-cert.gov

[5] "*취약점 분석 · 평가 모델*", KISA, Dec. 2002.

[6] "*Guide to Industrial Control Systems(ICS) Security*", NIST, Apr. 2013.

[7] "*Common Cybersecurity Vulnerabilities in Industrial Control Systems*", DHS, May 2011.

〈저자소개〉

민 병 길 (Byung-gil Min)
정회원

2002년 2월 : 충북대학교 컴퓨터공학과 졸업
2004년 2월 : 포항공과대학교 컴퓨터공학과 석사
2004년 2월~현재 : ETRI 부설 연구소 선임연구원/실장
<관심분야> 제어시스템 보안, 원자력 사이버 보안, 취약성 분석 · 평가

안 우 근 (Woogeun Ahn)
정회원

2011년 2월 : 고려대학교 컴퓨터통신공학과 졸업
2013년 2월 : 고려대학교 컴퓨터학과 석사
2013년 1월~현재 : ETRI 부설 연구소 연구원
<관심분야> 제어시스템 보안, 역공학, 위험관리

서 정 택 (Jungtaek Seo)
종신회원

1999년 2월 : 충주대학교 컴퓨터공학과 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사
2006년 2월 : 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월~현재 : ETRI 부설 연구소 선임연구원/부장
<관심분야> 제어시스템 보안, 취약성 분석 · 평가, 스마트그리드 보안, 원자력 사이버 보안, DDoS 공격 탐지 및 대응