Asia-pacific Journal of Convergent Research Interchange
Vol.9, No.5, May 31 (2023), pp.1-11
http://dx.doi.org/10.47116/apjcri.2023.05.01

Development of Automation Program for Windows PC System Vulnerability Check

Windows PC 시스템 취약점 점검을 위한 자동화 프로그램 개발

Hyeong-Ju Sun[1], Dong-Hak Kim[2], Jin-Hyung Park[3], Jong-Won Kim[4]

선형주[1], 김동학[2], 박진형[3], 김종원[4]

[1] Researcher, Korea Institute of Science and Technology Information, gilnyangyi@kisti.re.kr
[2] Researcher, Korea Institute of Science and Technology Information, dhkim@kisti.re.kr
[3] Principal Researcher, Korea Institute of Science and Technology Information, ntoskr@kisti.re.kr
[4] Senior Researcher, Korea Institute of Science and Technology Information, kjw@kisti.re.kr

Corresponding author: Jong-Won Kim

Abstract: With the development of information and communication technology, attack techniques of information and communication systems are gradually developing, and cyber attacks damage such as viruses, hacking, and information leakage are increasing. Accordingly, the 'Ministry of Science and ICT' and the 'Korea Internet & Security Agency' have published 「A Guide for the analysis and evaluation method of technical weaknesses of major information communication infrastructure」 and 「A Guide for Cloud Vulnerability Check」encouraging users to take measures for vulnerabilities. Computers in the company are checking vulnerabilities according to guide and in-company security policies, but personal computers are poorly checked due to lack of user awareness or budget and manpower, and security threats targeting to individual users are rapidly increasing. In this paper, we would like to propose program, a program that streamlines vulnerability checks, compares and analyzes guidelines, related instrcutions, and vulnerability check software to check vulnerabilities in Windows PC systems. This program simplified the operation procedure of the vulnerability check program to improve user convenience, and unlike other vulnerability check software, it automated the process of taking action after vulnerability check. In addition, computer security could be improved by including additional vulnerability check items in addition to the items checked by the existing vulnerability check software.

Keywords: Computer Security, Automation Program, Windows PC System, Computer Vulnerability

요약: 정보통신기술의 발전과 함께 정보통신시스템의 공격기법도 점차 발전하게 되어 바이러스, 해킹, 정보 유출 등의 사이버공격 피해가 증가하고 있다. 이에 과학기술정보통신부와 한국인터넷진흥원에서는 정보통신시스템 취약점을 점검하기 위해 「주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드 」와 「클라우드 취약점 점검 가이드」 등을 발간하여 사용자들에게 취약점 조치를 권장하고 있다. 기업 내에 있는 컴퓨터는 사내 보안 정책이나 가이드에 맞게 취약점 점검을 수행하고 있지만, 개인용 컴퓨터는 사용자의 인지 부족 또는 예산 및 인력 부족 등의 이유로 취약점 점검이 부실한 상황이며, 개인 사용자를 노리는 보안 위협

Received: January 22, 2023; 1st Review Result: March 09, 2023; 2nd Review Result: April 04, 2023
Accepted: April 30, 2023

이 빠르게 증가하고 있다. 이에 본 논문은 취약점 점검을 효율화하고, 가이드라인과 관련 지침, 취약점 점검 소프트웨어의 점검 항목을 비교·분석하여 Windows PC 시스템의 취약점 점검을 하는 프로그램을 제안하고자 한다. 본 프로그램은 사용자의 편의성을 제고하기 위해 취약점 점검 프로그램 동작 절차를 간소화하였고, 타 취약점 점검 소프트웨어와 달리 취약점 점검 후 조치 과정을 자동화하였다. 또한, 기존 취약점 점검 소프트웨어에서 점검하는 항목들과 더불어 추가 취약점 점검 항목들을 포함하여 점검함으로써 컴퓨터 보안성을 향상할 수 있었다.

핵심어: 컴퓨터 보안, 자동화 프로그램, 윈도우 컴퓨터 시스템, 컴퓨터 취약점

1. 서론

정보통신기술의 발전으로 금융·의료·교육·교통 등의 데이터와 서비스를 언제 어디서나 제공받을 수 있게 되었다. 반면, 정보통신시스템의 공격기법 또한 같이 발전하게 되어 바이러스, 해킹, 정보 유출 등의 사이버공격 피해가 증가하였다. 최근에는 컴퓨터의 랜섬웨어 감염으로 인해 상수도·통신 등 주요 분야에 대한 피해가 발생하였고, APT(Advanced Persistent Threat) 공격그룹이 가상자산을 탈취하기 위해 거래소를 공격한 사례도 확인되었다. 또한 북한의 해킹조직에 의해 이메일 기반의 스피어 피싱 공격기법을 구사한 APT공격이 증가하고 있다. 이러한 공격은 개인정보 유출 등의 문제가 발생하기 때문에 컴퓨터의 취약점을 점검해야 한다[1-3]. 이에 과학기술정보통신부와 한국인터넷진흥원에서는 이러한 취약점을 점검하기 위해 「주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드」[4]와 「클라우드 취약점 점검 가이드」[5] 등을 발간하여 사용자들에게 취약점 조치를 권장하고 있다[6][7]. 앞서 언급한 가이드에서는 서버, 보안, 네트워크, 제어시스템, 데이터베이스, 웹, 클라우드 등의 장비에 대한 취약점 분석·평가 방법을 제시한다. 보고서에 의하면 기업 내에 있는 컴퓨터는 사내 보안 정책에 맞게 취약점 점검을 수행하고 있지만, 개인용 컴퓨터는 사용자의 인지 부족 또는 예산 및 인력 부족 등의 이유로 취약점 점검이 부실한 상황이며[8-10], 이글루 시큐리티에서는 개인 사용자를 노리는 보안 위협이 빠르게 확산한다고 보고하였다[11]. 컴퓨터의 취약점 점검을 위한 소프트웨어는 일부 존재하지만, 대다수 상업용으로 개발된 상용 소프트웨어이거나, 취약점 점검 항목들이 최신화되지 않아 점검 항목들이 한정적인 소프트웨어들이다. 심지어 수동으로 취약점 점검·조치를 수행해야 하는 소프트웨어도 존재하여 개인이 취약점 점검을 하기 위해선 여러모로 어려운 상황이다. 그러므로 가이드라인을 준수하기 어렵거나 최신 보안 정책을 적용할 수 없는 개인용 컴퓨터는 여러 취약점에 노출되어 있는 환경이다. 본 논문은 취약점 점검의 작업 시간을 효율화하고 가이드라인과 관련 지침, 취약점 점검 소프트웨어의 점검 항목을 비교 · 분석하여 취약점 점검을 하는 프로그램을 제안하고자 한다. 본 프로그램은 사용자의 편의성을 제고하기 위해 취약점 점검 프로그램 동작 절차를 간소화하였고, 타 취약점 점검 소프트웨어와 달리 취약점 점검 후 조치를 자동화하였다. 또한, 기존 취약점 점검 소프트웨어에서 점검하는 항목들과 더불어 추가 취약점 점검 항목들을 포함하여 점검함으로써 컴퓨터 보안성을 향상할 수 있었다.

2. 관련 연구

2.1 Windows PC 취약점 점검 가이드

Windows PC 시스템은 Microsoft사에서 개발한 운영체제로 MultiTasking과 GUI(Graphical User Interface) 환경을 제공하기 위해 개발된 운영체제이다. 이 운영체제는 현재까지도 가장 많은 사용률을 보이고 있으며[12], 그중에서는 Windows 10 버전이 가장 많이 사용되고 있다[13]. 이에 여러 기관에서는 Windows PC 운영체제 환경에서의 취약점 점검 항목을 분석하여 규정·지침을 개정하거나 가이드라인을 작성하였다. 대표적으로 정보보호·디지털 전문 준정부기관인 한국인터넷진흥원에서 정보통신시스템의 취약점 점검을 위해 「주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드」와 「클라우드 취약점 점검 가이드」 등을 발간하였다. 여러 취약점 점검 소프트웨어들은 해당 가이드를 참고하여 취약점 항목을 점검한다.

분류	점검항목	중요도	항목코드
1. 계정 관리	패스워드의 주기적 변경	상	PC-01
	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	PC-02
	복구 콘솔에서 자동 로그온을 금지하도록 설정	중	PC-15
2. 서비스 관리	공유 폴더 제거	상	PC-03
	항목의 불필요한 서비스 제거	상	PC-04
	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지	상	PC-05
	파일 시스템이 NTFS 포맷으로 설정	중	PC-16
	대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정	중	PC-17
	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정	하	PC-18
3. 패치 관리	HOT FIX 등 최신 보안패치 적용	상	PC-06
	최신 서비스팩 적용	상	PC-07
	MS-Office, 훈글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안패치 및 벤더 권고사항 적용	상	PC-08
4. 보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	PC-09
	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	PC-10
	OS에서 제공하는 침입차단 기능 활성화	상	PC-11
	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	PC-12
	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지등 이동식 미디어에 대한 보안대책 수립	상	PC-13
	PC 내부의 미사용(3개월) ActiveX 제거	상	PC-14
	원격 지원을 금지하도록 정책이 설정	중	PC-19

[그림 1] 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드, PC취약점 분석·평가 항목

[Fig. 1] A Guide for the Analysis and Evaluation Method of Technical Weaknesses of Major Information Communication Infrastructure, PC Vulnerability Analysis and Evaluation Items

두 가이드라인은 구성의 큰 차이를 보이지 않지만, 「클라우드 취약점 점검 가이드」 Windows PC 항목인 '비인가 무선랜 사용 제한 (PC-13)'항목은 위 가이드라인에는 포함되지 않는 항목이다. 이는 클라우드 환경의 보안 수준 향상을 위해 '클라우드 보안 인증제 심사' 내 취약점 점검 항목으로 포함된 것으로 판단되며, 공공-WiFi 등의 사용으로 인한 취약점이 존재하기에 본 논문에서 제안하는 프로그램에서는 해당 항목을 PC-20으로 취약점 점검 항목을 추가한다.

2.2 Windows PC 취약점 점검 소프트웨어

Windows PC 시스템의 취약점 점검 소프트웨어는 내PC돌보미(KISA)와 같은 무료 소프트웨어와 내PC지키미(AhnLab) 와 ComVoy(지인소프트)와 같은 상용 소프트웨어들이 있다. 이러한 취약점 점검 소프트웨어들의 취약점 점검 항목은「주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드」를 참고한 항목이거나 사내 보안 정책, 관련 관리지침에 의해 변경·추가된 항목이다. 내PC지키미(AhnLab)는 2022년 12월 31일에 무료서비스를 종료하여 현재는 개인적인 목적으로 사용할 수 없으며, 내PC지키미를 포함한 대다수의 취약점 점검 소프트웨어가 기업에서 활용할 목적으로 출시된 소프트웨어이므로 일반 사용자들이 이용하기엔 많은 어려움이 있다. 내PC돌보미(KISA)의 경우 한국인터넷진흥원에서 무료로 배포하는 취약점 점검 소프트웨어로 이스트시큐리티와 잉카인터넷 컨소시엄에서 점검 수행·원격서비스를 지원한다. 그러나 내PC돌보미(KISA)는 취약점 항목별 조치 방법에 대해서만 언급되어 있어 수동으로 조치해야 하며, 타 소프트웨어에 비해 점검 항목이 상대적으로 적은 탓에 보안 위협에 쉽게 노출될 수 있다는 문제가 존재한다.

2.3 취약점 점검 기술 및 언어

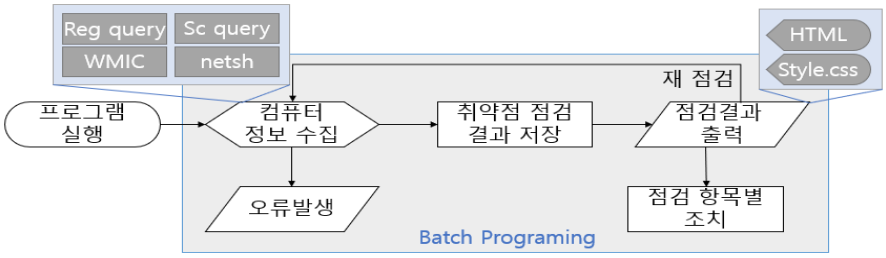
Windows PC 시스템 작업을 수행하기 위해선 GUI를 통해 단순 클릭만으로 수행하거나 명령 프롬프트(Command Prompt)의 명령 창을 통해 명령을 입력하며, 배치(Batch)는 명령어들이 나열되어 있는 텍스트 파일로 명령 프롬프트에서 작동한다. 명령 프롬프트의 발전 형태인 확장 가능한 명령줄 인터페이스 파워셸(PowerShell)이 존재하며, 명령 프롬프트와 파워셸은 서로 호환되어 있으므로 명령 프롬프트에서 파워셸 사용이 가능하다. Windows PC 시스템 내에서 동작하는 일련의 작업은 명령어 기반으로 배치 프로그래밍을 통해 스크립트(script) 작성 · 실행하여 자동으로 처리할 수 있다. 대표적으로 레지스트리에 지정된 하위 키의 항목을 반환하는 reg query 명령어, 로컬 또는 원격 구성의 네트워크 설정을 변경하는 netsh 명령어, 지정된 서비스, 드라이버 종류에 대한 정보를 표시하는 sc query 명령어 등을 사용해서 취약점을 점검할 수 있다.

3. 프로그램 설계

3.1 프로그램 구조

Windows PC 시스템의 GUI환경은 입출력과 같은 기본적인 기능들을 사용자가 편리하게 사용할 수 있도록 도와주는 환경이지만, 명령 프롬프트와 배치 프로그래밍을 사용하여 명령줄을 통해 자동으로 취약점 점검·조치를 수행하면 수동으로 점검·조치하는 시간을

단축할 수 있다. 본 논문에서 제안하는 프로그램은 Windows 스크립트로 조치할 수 있는 취약점에 대해 자동으로 취약점 점검·조치를 수행하는 프로그램으로 설계하였다. 아래 [그림 2]를 통해 본 논문의 프로그램 구조를 확인할 수 있다.



[그림 2] 프로그램 구조

[Fig. 2] Program Structure

프로그램이 실행되면 컴퓨터의 레지스트리 및 환경변수와 같은 정보들을 Windows의 관리 도구인 WMI(Windows Management Instrumentation) 등의 명령어로 확인하여 변수로 저장하고, 앞서 관련 연구에서 제시한 각 취약점 항목의 점검을 수행한다. 점검 수행 후 점검 결과를 변수로 저장하여 HTML(Hypertext Markup Language)과 CSS(Cascading Style Sheets)를 사용해서 웹 페이지로 결과를 출력하고 항목별로 조치할 수 있는 기능과 재점검을 할 수 있는 기능을 수행할 수 있게 한다. 컴퓨터 정보를 수집하는 과정 중 오류가 발생할 시 화면에 관련 오류 내용을 출력한다. 최신화된 취약점 점검 목록을 주기적으로 업데이트하는 기능이 필요하지만, 현재는 내부 연구용으로 개발된 시범 프로그램이므로 취약점 점검 목록이 최신화되면 정기적으로 업데이트를 수행할 수 있는 기능을 고려하고 있다.

3.2 설계 구현

3.2.1 취약점 점검 구현

Windows 운영체제는 버전에 구애받지 않고 동일한 명령어 방식을 사용하기에 시스템 환경이 변경되어도 Windows라는 동일 운영체제 범주 내에선 범용적으로 사용할 수 있다. 본 논문의 프로그램은 Windows 운영체제 기반으로 동작할 수 있도록 명령 프롬프트와 파워셸 인터프리터로 설계하고, 결과 화면 출력은 HTML/CSS를 통해 설계하였다.

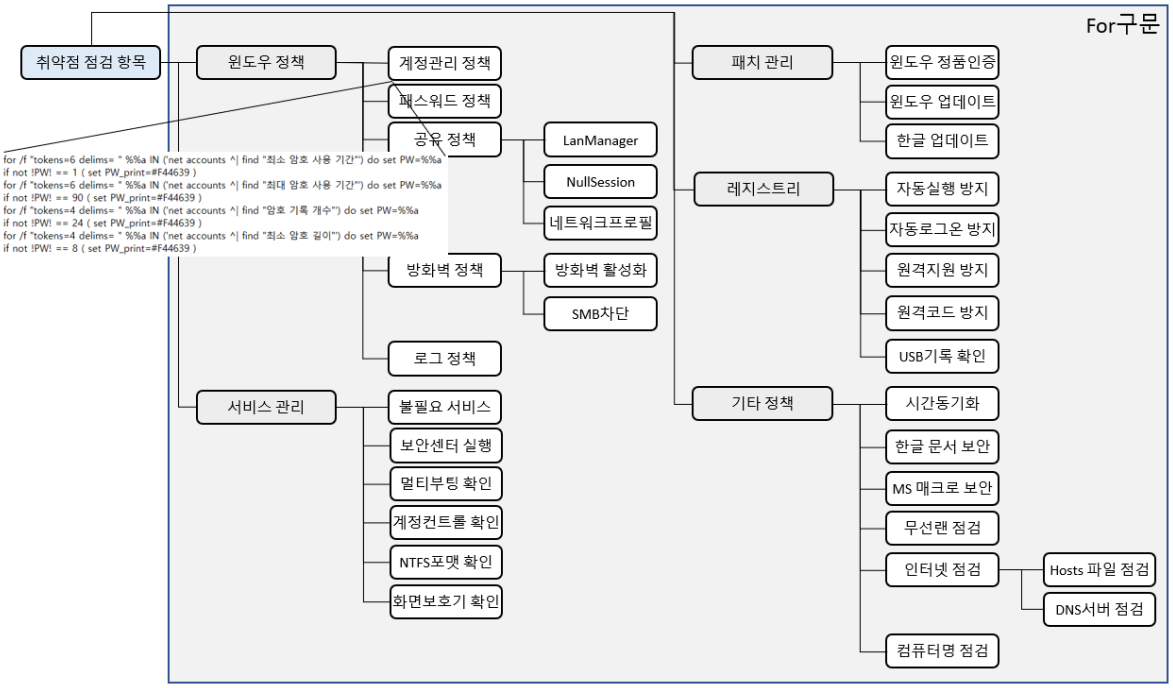
[표 1] 취약점 이슈에 의한 변경·추가 점검 항목

[Table 1] Change and Additional Check Items Due to Vulnerability Issues

항목	근거	중요도
PC-20 추가	「클라우드 취약점 점검 가이드」 ,‘비인가 무선랜 사용제한’ 항목 추가	중
PC-09, PC-10 대체	AntiVirus 테스트 보고서[14][15], Protection기능 비교에 따른 대체	중
PC-14, PC-18 제외	Microsoft사의 IE브라우저 지원 종료 및 사용 종료 발표에 의한 제외	하
USB 접근기록 점검	「방송통신위원회 정보보호 관리지침」 제45조, 보조기억매체 관리	중
MS 매크로 보안 점검	PC취약점점검 분석·평가 PC-08항목, ‘벤더 권고사항 적용’, CVE-2021-40444 ‘PC보안 강화를 위한 취약점 점검항목 개선연구’ 설문조사 의견[16]	상
한글 문서 보안 점검	PC취약점점검 분석·평가 PC-08항목, ‘벤더 권고사항 적용’, CVE-2018-15982	상

컴퓨터명/그룹명 변경	「방송통신위원회 정보보호 관리지침」 제35조, PC보안관리 CVE-2021-42278, CVE-2021-42287	하
정품인증 점검	악성코드 설치 차단 및 보안 인식 강화 목적[17][18] HackTool/Win32.KMSAuto.C2922905, Misc.HackTool.AutoKMS 등	중

위에서 언급된 가이드라인 외에 취약점 이슈 및 지침에 의해 변경·추가된 점검 항목이 존재한다. 이는 작성된 소프트웨어의 보안 취약점(Common Vulnerabilities and Exposures) 목록과 시스템 발전 등의 이유로 변경된 취약점 목록, 정보보호 관리지침에 의해 추가된 항목이다. Windows PC 시스템을 보호하고자 취약점 이슈에 의한 변경·추가 점검 항목을 위 [표 1]을 통해 확인할 수 있다. 가이드라인의 취약점 점검 항목과 위 [표 1]항목을 포함하여 본 프로그램에서 점검한다. 점검하고자 하는 취약점 점검 항목은 아래 [그림 3]과 같다.



[그림 3] 프로그램의 취약점 점검 항목 구현

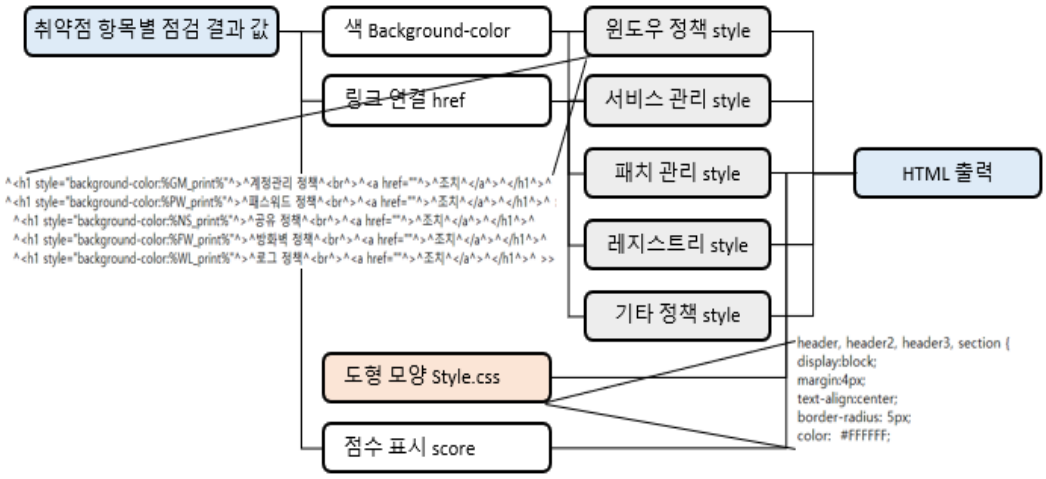
[Fig. 3] Implementation of Vulnerability Check Items in Program

본 논문의 프로그램은 취약점 점검 항목은 취약점 점검 가이드·지침과 추가 취약점 이슈에 대한 항목을 구현한다. 윈도우 정책, 서비스 관리, 패치 관리, 레지스트리, 기타 정책의 5개의 카테고리로 나누고 29개의 취약점 점검 항목을 구현한다. 또한 프로그램 동작 중 비정상 종료 상황에 대비하여 각 항목별로 오류코드를 작성하였다. 사용자 단에서 강제 종료를 하였을 때와 각 명령어를 사용하였을 때, 결과를 출력할 때 발생할 수 있는 에러 등에 대해서 프로그램 실행 시 오류가 발생하면 오류코드를 화면에 출력하도록 설계하였다.

3.2.2 결과 화면 구현

본 논문의 프로그램을 사용해 나온 각 취약점별 결과 값을 토대로 아래 [그림 4]의

절차를 통해 웹 페이지로 출력되는 기능을 구현하였다.



[그림 4] 프로그램의 결과 표시 절차

[Fig. 4] Procedure for Displaying Results of Program

[그림 4]는 취약점 항목별 점검 결괏값에 따라 웹 페이지로 표시되는 절차를 간소화한 그림이다. 저장되는 결괏값을 토대로 스타일을 설정하고, 해당 취약점 항목의 조치를 링크로 연결하여 웹 페이지를 구현한다.

4. 실험 및 평가

4.1 실행 환경 및 구성

본 논문에서 제안한 프로그램을 평가하기 위해 타 취약점 점검 소프트웨어와 동일한 시스템 환경에서 실험을 진행하였다. 실행 환경은 Windows PC 시스템 환경에서 본 프로그램과 내PC돌보미(KISA)와 내PC지키미(AhnLab)를 통해 모든 취약점 항목을 점검할 수 있도록 응용 프로그램 설치, USB연결, 무선랜 사용 등의 조건을 설정한다.

4.2 프로그램 평가

본 논문에서 제안한 프로그램의 평가를 위해서 취약점 점검 항목이 적절하게 구현되어 있는지 확인하고 각 취약점 점검 소프트웨어와 비교·분석하여 각 취약점별 전·후 조치사항 확인하고 프로그램 사용 중 특이사항에 대해 평가하였다. 각 취약점 항목에 대한 결과를 웹 페이지로 표시되고, 취약점에 대한 보안 조치기능과 재점검 기능을 수행할 수 있었다. 프로그램 실행 결과 화면 상단에는 취약점 점검 상태에 따른 점수를 표시하고, 하단에서 점검을 수행한 항목이 빨간색으로 표시된다면 해당 취약점은 조치되지 않은 상태임을 의미하며, 파란색으로 표시된다면 조치되어 있는 상태임을 의미한다. 프로그램의 <조치 전> 화면과 <조치 후>의 결과 화면은 아래 [표 2]의 화면으로 나타난다.

[표 2] 프로그램 조치 전·후 화면

[Table 2] Program Action Before and After Screen

<조치 전>

<조치 후>

각 점검 항목을 색으로 표시하여 직관적으로 확인하기 용이하다. 전체 설정 기능을 통해 모든 취약점 점검 항목을 자동으로 조치함으로써 <조치 후>와 같은 결과 화면을 출력하였다. 단, 일부 항목의 경우 수동으로 조치해야 하는 항목(멀티 부팅 확인, 인터넷 점검 등)이 존재해 해당 항목은 조치 방법에 대한 설명을 출력하였다. 취약점 점검 소프트웨어의 취약점 점검 항목은 가이드·지침·추가 취약점 항목을 포함하여 [표 3]과 같이 비교하였다. 본 논문의 프로그램은 다른 취약점 점검 소프트웨어에 없는 취약점에 대해 점검을 수행하였다.

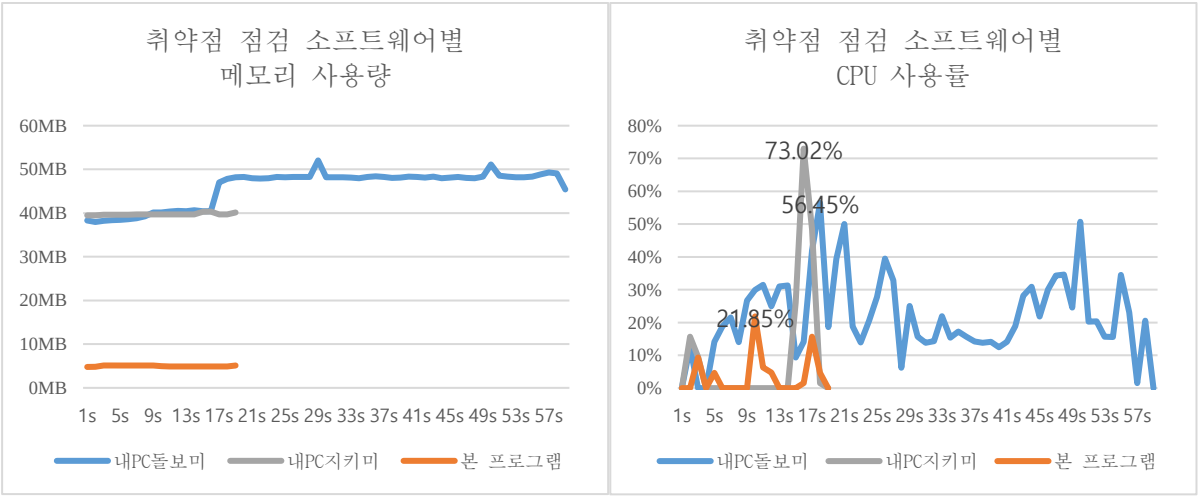
각 취약점 점검 소프트웨어별 메모리·CPU 사용량 등을 알 수 있는 성능 모니터의 Working Set과 % Processor Time을 1초 간격으로 성능을 비교한다. 아래 [그림 5]는

성능모니터를 사용한 각 취약점 점검 소프트웨어별 메모리 사용량과 CPU 사용률을 나타낸 그림이다.

[표 3] 취약점 점검 소프트웨어별 점검 항목 비교

[Table 3] Compare Check Items by Vulnerability Check Software

	PC-01 ~ PC-15	PC-16 ~ PC-17	PC-18 ~ PC-19	PC-20	Null Session 차단	보안 센터 실행	UAC 설정	SMB 포트 차단	계정 관리 정책	로그 정책	인터넷 점검	시간 동기화	LanManager 인증 수준	USB 접근 기록 확인	한글 문서 보안	MS 매크로 보안	컴퓨터 그룹명 변경	정품 인증 점검
내PC돌보미 (KISA)	√		√		√	√	√	√	√	√								
내PC지키미 (AhnLab)	√	√	√	√	√	√	√	√	√	√	√	√	√					
본 논문의 프로그램	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√



[그림 5] 취약점 점검 소프트웨어별 메모리·CPU 사용량

[Fig. 5] Memory·Cpu Usage by Vulnerability Check Software

본 논문의 프로그램은 점검 진행 상황을 명령줄로 표시하기 때문에 내PC돌보미(KISA)나 내PC지키미(AhnLab)에 비해 메모리와 CPU 사용량이 낮은 것으로 확인되었다. 내PC돌보미는 점검 후 결과 내용을 다시 점검프로그램 내 결과창으로 출력하고, 원격서비스를 위한 로그 기록 등으로 인해 지연시간이 발생하여 소요되는 시간이 길어지는 것으로 판단된다. 내PC지키미(AhnLab)는 내PC돌보미와 결과를 출력하는 절차가 유사하지만 많은 CPU 사용률로 인해 비교적 점검 시간이 적게 소요된 것으로 판단된다. 반면, 본 프로그램은 위와 같은 절차가 불필요하여 빠른 시간 내에 점검이 수행된 것을 확인할 수 있었다. 성능 모니터에서 1% 미만의 수치는 기록되지 않아 내PC지키미(AhnLab)와 본 프로그램은 CPU 사용률이 0%로 기록된 수치가 있는데, 이 부분을 제외하여 CPU 사용률의 평균을 계산하였다. 아래 [표 4]는 취약점 점검 소프트웨어별 성능 비교표이다.

[표 4] 취약점 점검 소프트웨어별 성능 비교

[Table 4] Performance Comparison by Vulnerability Check Software

	내PC돌보미 (KISA)	내PC지키미 (AhnLab)	본 논문의 프로그램
점검 시간	59sec	19sec	19sec
메모리 사용량 평균	45.91MB	39.74MB	4.97MB
CPU 사용률 평균	23.26%	29.06%	8.61%

취약점 조치 시간의 경우 내PC돌보미(KISA)는 수동으로 조치해야 하므로 오랜 시간이 걸리고 내PC지키미(AhnLab)는 각 점검 항목별 조치 절차를 간소화할 수 있었지만, 전체 점검 항목을 조치하는 기능은 없었다. 반면, 본 프로그램은 취약점 항목별 조치 절차를 자동화하여 단시간 내에 조치할 수 있었다. 본 논문의 프로그램은 다른 취약점 점검 소프트웨어에 비해 더 많은 취약점 점검 항목으로 보안성을 향상했고, 단축된 점검·조치 시간과 동작 절차 간소화로 효율성을 높였으며, 무료로 프로그램을 사용할 수 있는 장점이 있었다. 그러나, 타 취약점 점검 소프트웨어에 비해 GUI로 구성되지 않은 점검 화면, 각 점검 항목별 세부 내용에 대한 설명이 미흡하다는 점과 내부 연구용으로 개발된 시범 프로그램이므로 수동으로 업데이트해야 하는 한계가 존재하였다. 더불어, 일부 소수 컴퓨터에서는 WMI 명령어가 실행되지 않는 원인불명의 오류가 발생한다. 위 사항은 Microsoft 공식적인 문서인 Learn에서 제시하는 방안으로도 해결되지 않았다[19]. 따라서 위 사항들은 향후 지속적인 프로그램 유지관리를 통해 보완할 예정이다.

5. 결론

코로나19로 인한 재택근무자들의 개인 컴퓨터는 기업에서 배포하는 여러 프로그램에 의해 보안 관리가 되고 있지만 취약점을 점검하는 프로그램은 부실하다는 의견들이 지속적으로 제기되고 있다[8][20]. 2019년 대국민 보안관리 실태조사에 의하면 약 90%의 컴퓨터에는 백신이 설치되어 있지만 그 외 기타 보안 점검 항목들에 대해서는 부실한 것으로 확인되어 사용자들의 컴퓨터 보안 인식과 취약점 점검은 부족한 실정이다[9]. 따라서 본 논문에서는 Windows PC 시스템의 여러 최신 취약점에 대해서 분석 및 점검을 수행하고, 이에 따른 결과를 도출하여 사용자가 편리하게 취약점 점검을 할 수 있는 프로그램을 개발하였다. 본 프로그램은 무료로 사용할 수 있기에 관련 파일을 특정 웹사이트를 통해 배포 받을 수 있다. 취약점 점검 소프트웨어가 없는 개인 사용자나 소규모 사업자가 Windows PC 시스템의 취약점을 점검할 수 있으며, 사용자 편의성을 제고하기 위해 취약점 점검 프로그램 동작 절차를 간소화하였다. 또한, 타 취약점 점검 소프트웨어와 달리 취약점 점검 후 조치 과정을 자동화하였으며, 위 2절 관련 연구 [그림 1]에서 제시한 취약점 점검 항목들과 더불어 [표 1]에서 제시한 항목들도 추가로 점검함으로써 컴퓨터 보안성을 향상할 수 있었다. 향후 파워셸의 발전 형태인 윈도우 터미널을 이용한 방법이나 맥, 리눅스 등의 다른 운영체제에서도 취약점 점검을 수행할 수 있도록 프로그램을 지속적으로 개발하여 향후 제기될 최신 취약점 항목들에 대해 주기적으로 점검 항목 범위를 확장하여 컴퓨터 보안성 제고에 기여할 예정이다.

6. Acknowledgments

이 논문은 2023년도 한국과학기술정보연구원(KISTI) 기본사업으로 수행한 것입니다.

References

[1] Cyber Threat Trend Report for the Second Half of 2022, Korea Internet & Security Agency, (2022)
Available from: https://www.kisa.or.kr/20205/form?postSeq=1022&lang_type=KO&page=1

[2] K. H. Han, APT attacks and Countermeasures, Journal of Convergence for Information Technology, (2015), Vol.5, No.1, pp.25-30.
Available from: https://www.earticle.net/Article/A250789

[3] J. K. Cho, Study on Improvement of Vulnerability Diagnosis Items for PC Security Enhancement, Journal of Convergence for Information Technology, (2019), Vol.9, No.3, pp.1-7.
DOI: https://doi.org/10.22156/CS4SMB.2019.9.3.001

[4] Detailed Guide for Analysis and Evaluation of Major Information and Communication Infrastructure Technology Vulnerabilities, Korea Internet & Security Agency, (2021)
Available from: https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=35988

[5] Cloud Vulnerability Check Guide, Korea Internet & Security Agency, (2020)
Available from: https://isms.kisa.or.kr/main/csap/notice/?boardId=bbs_0000000000000004&mode=view&cntId=45

[6] H. C. Jung, Development of PC security automatic diagnosis system modeling technique for safe use of PC, Konkuk University, Master Thesis, (2020)

[7] S. Y. Min, C. S. Jung, K. H. Lee, E. S. Cho, T. B. Yoon, S. H. You, Design of Comprehensive Security Vulnerability Analysis System through Efficient Inspection Method according to Necessity of Upgrading System Vulnerability, Journal of Korea Academia-Industrial cooperation Society, (2017), Vol.18, No.7, pp.1-8.
DOI: https://doi.org/10.5762/KAIS.2017.18.7.1

[8] C. K. Park, Security status and countermeasures in the increasing telecommuting environment after COVID-19, SoongSil University, Master Thesis, (2021)

[9] https://blog.alyac.co.kr/44, Jul 30 (2019)

[10] K. H. Han, I. S. Kim, A Study on Threat Analysis of PC Security and Countermeasures in Financial Sector, The journal of the institute of internet, broadcasting and communication, (2015), Vol.15, No.6, pp.283-290.
DOI: https://doi.org/10.7236/JIIBC.2015.15.6.283

[11] IGLOO SECURITY_2016 Security Predictions Report, IGLOO SECURITY, (2016)
Available from: https://www.igloo.co.kr/newsroom/reference/

[12] https://www.statista.com/statistics/218089/global-market-share-of-windows-7/, Jul 27 (2022)

[13] https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide, Nov (2022)

[14]https://www.av-test.org/en/antivirus/home-windows/windows-10/october-2022/microsoft-defender-4.18-221514/, Sep-Oct (2022)

[15] https://www.av-comparatives.org/tests/advanced-threat-protection-test-2022-consumer/, Nov 10 (2022)

[16] S. H. Kim, A Study on the Improvement of Vulnerability Checklist for Enhanced PC Security, Konkuk University, Master Thesis, (2019)

[17] K. P. Ma, Software Genuine Scheme for responding to the online activation vulnerability, ChonNam National University, Master Thesis, (2015)

[18] https://asec.ahnlab.com/ko/32612/, Mar 16 (2022)

[19] https://learn.microsoft.com/en-us/previous-versions/tn-archive/ff406382(v=msdn.10)?redirectedfrom=MSDN, Mar 9 (2010)

[20] B. Y. Park, J. W. Yang, C. H. Seo, System Design and Implementation for Security Policy Management of Windows Based PC and Weakness Inspection, Journal of the Korea Institute of Information Security & Cryptology, (2008), Vol.18, No.1, pp.23-30.

