PC 보안 강화를 위한 취약점 점검 항목의 개선 방안 연구

이승혁*, 유도진**, 이용준**
*극동대학교 인공지능보안학과
**극동대학교 해킹보안학과 교수
201763021@kdu.ac.kr

A Study on Improvement Measures for Vulnerability Inspection Items to Enhance PC Security

Seung-Hyuk Lee*, Do-Jin Yoo**, Yong-Jun Lee**
*Department of Hacking & Security, Far East University
**Dept. professor of Hacking Security, Far East University

요 약

본 연구는 기존 PC 보안 점검 도구의 한계를 보완하고 최신 사이버 위협에 대응할 수 있는 새로운 보안 점검 항목을 제안하였다. 제안된 항목인 사용 메신저 금지, PC 시작 프로그램 제어, Windows 서비스 점검을 통해 정보 유출 방지, 시스템 자원 최적화, 보안 취약점 감소 효과를 확인하였다. 이러한 추가 항목들은 기존 보안 도구의 부족한 점을 보완하여, 더욱 포괄적이고 강화된 보안 체계를 구축하는 데 기여할 수 있음을 입증하였다.

1. 서론

최근 정보통신기술(ICT)의 발전에 따라 사이버 위협의 양상은 더욱 복잡하고 정교해지며 그 빈도 또한 빠르게 증가하고 있다. 특히 COVID-19 팬데믹 이후 원격 근무와 재택근무가 일상화되면서 개인용 컴퓨터(PC)가 업무의 핵심 도구로 자리 잡았다. 이는 PC가 단순히 개인 작업을 위한 기기를 넘어, 중요한 데이터와 민감한 정보를 저장하고 처리하는 핵심 자원으로 변모했음을 의미한다. 이러한 변화 속에서 PC 보안은 선택이 아닌 필수 요소가 되었으며, PC의 보안성이 확보되지 않을 경우, 이는 곧 전체 시스템의 안전성에 심각한 영향을 미치게 된다 [1].

그러나 현재 널리 사용되고 있는 대부분의 보안 점검 도구들은 여전히 기존의 표준 보안 항목에만 초점을 맞추고 있어, 다변화된 최신 사이버 위협에 효과적으로 대응하지 못하는 한계를 보이고 있다. 예를 들어, USB 자동 실행 차단, 바이러스 백신 설치 여부, 기본적인 보안 패치 적용과 같은 항목들은 여전히 중요한 요소이지만, 지능형 지속 위협(APT), 랜섬웨어, 피싱 공격 등 최신의 복합적인 사이버 공격을 충분히 반영하고 대응하는 데는 부족함이 있다. 이러한 상황에서 최신 위협에 대비하지 못한 보안 체계는 기업과 개인 정보 자산을 보호하는 데 있어 큰 취약점을 남길 수 있다 [2].

따라서 본 연구는 이러한 기존 보안 점검 도구의 한계를 분석하고, 이를 보완할 수 있는 보다 강화된 보안 점검 체계를 마련하기 위해 새로운 취약점 점검 항목을 제안하고자 한다.

2. 관련 연구

최근 정보통신기술의 발전과 COVID-19 팬데믹 이후 원격 근무가 활성화되면서 PC 보안 위협이 증가하고 있다. PC는 중요한 데이터가 저장된 핵심 자원으로, 보안 위협에 취약할 경우 시스템 전체에 영향을 미칠 수 있다. 현재 사용되는 보안 점검 도구들은 기본적인 보안 항목(예: USB 자동 실행 차단, 바이러스 백신 설치, 보안 패치 적용)에 초점을 맞추고 있으나, 최신 사이버 위협을 충분히 반영하지 못하는 한계가 있다. 주요 PC 보안 점검 도구로는 ESTsoft의 알약과 이스트소프트의 보안 점검 도구가 있다. 이들 도구는 USB 자동 실행 차단, 바이러스 백신 설치 여부 확인, 보안 패치 적용 상태 점검 등 기본적인 보안 항목을 점검하는 데 중점을 둔다.

[표 1] 2023년 상반기 사이버 위협 동향 보고서

구분 \ 연도		2022	비율	2022	비율	2023	비율
침해사고 신고	DDoS 공격	48	10.1	74	11.1	124	18.7
	악성코드	125	26.4	222	33.2	156	23.5
	랜섬웨어	118	24.9	207	30.9	134	20.2
	서버 해킹	275	58.1	310	46.3	320	48.2
	기타	25	5.3	63	9.4	64	9.6
합계				669		664	

위 [표 1]은 2022년 상반기부터 2023년 상반기까지 주요 PC 침해사고 유형과 발생 빈도를 보여준다. 이 데이터에 따르면,

서버 해킹이 가장 빈번한 사고 유형이며, 악성코드 감염(랜섬웨어 포함)과 DDoS 공격 역시 증가 추세를 보이고 있다. 특히 악성코드 중 랜섬웨어가 큰 비중을 차지하고 있어 보안 위협의 심각성을 강조하고 있다. 이는 기업과 개인 사용자 모두에게 중요한 경고를 제공하며, 기존 보안 체계를 강화할 필요성을 뒷받침한다 [3].

[그림 1] 알약과 ESTsoft 취약점 점검도구

위 [그림 1]는 알약과 이스트소프트 보안 점검 도구의 화면을 나타내고 있다. 알약은 47개의 점검 항목이 있으며, 이스트소프트 보안 도구 역시 기본적인 보안 점검 항목을 제공하여 바이러스 백신 설치 여부, 보안 패치 적용 여부 등을 확인할 수 있다. 그러나 이들 도구는 다변화된 최신 사이버 위협을 충분히 반영하지 못하고 있으며, 복합적인 위협 요소에 대한 대응이 미흡한 상태이다. 이러한 배경에서 본 연구는 기존 보안 도구의 한계를 보완할 수 있는 새로운 점검 항목을 제안하고자 한다. 제안된 점검 항목들은 다양한 최신 보안 위협에 대응할 수 있는 포괄적인 보안 점검 체계를 마련함으로써, 개인과 기업 환경 모두에서 보안성을 높이는 데 기여할 수 있을 것으로 기대된다 [4].

3. 제안 내용

본 연구는 기존 PC 보안 점검 항목의 한계를 보완하기 위해 추가적인 보안 항목을 제안한다. 구체적으로 사용 메신저 금지, PC 시작 프로그램 제어, Windows 서비스 점검, 운영체제 사용자 계정별 권한 설정 점검, 시스템 복원 설정 확인을 추가하였다. 이들은 각각 보안을 강화하는 다양한 역할을 수행한다. 사용 메신저 금지는 메신저를 통한 정보 유출을 방지하며, PC 시작 프로그램 제어는 불필요한 프로그램의 자동 실행을 막아 시스템 자원을 절약한다. Windows 서비스 점검은 불필요한 서비스 비활성화로 보안 취약점을 줄이고, 사용자 계정별 권한 설정은 최소 권한 원칙을 통해 불필요한 권한 남용을 방지한다. 마지막으로, 시스템 복원 설정 확인은 보안 사고 발생 시 빠른 복구를 돕는다 [5].

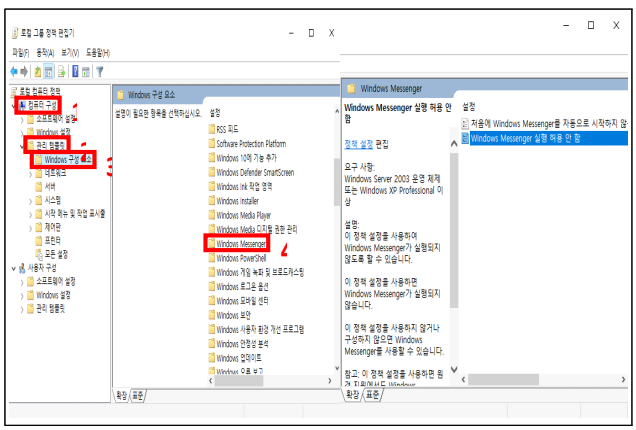
[표 2] 취약점 점검제안 항목

번호	제안된 점검 항목	설명
1	사용 메신저 금지	메신저 프로그램을 통한 정보 유출 및 피싱 공격을 방지하기 위해 주요 메신저 사용을 차단하여 보안성을 강화함.
2	PC 시작 프로그램 제어	PC 부팅 시 자동으로 실행되는 프로그램 중 불필요하거나 잠재적 보안 위협이 될 수 있는 프로그램을 차단하여 보안성을 높이고 시스템 자원 낭비를 줄임.
3	Windows 서비스 점검	불필요한 Windows 서비스를 비활성화하여 시스템 자원을 절약하고, 보안 취약점을 줄이며, 악성 코드의 비인가 서비스 실행을 방지함.

위 [표 2]에서 제안된 항목들은 기존 보안 점검 항목을 넘어서는 추가적인 보호를 제공한다. 특히, 정보 유출 방지, 시스템 자원 관리, 악성 코드 예방 등의 측면에서 실질적인 보안 강화 효과를 기대할 수 있습니다. 이러한 점검 항목들은 최신 보안 위협에 대한 대응 능력을 높여, PC 보안의 전반적인 수준을 향상시키는 데 기여한다.

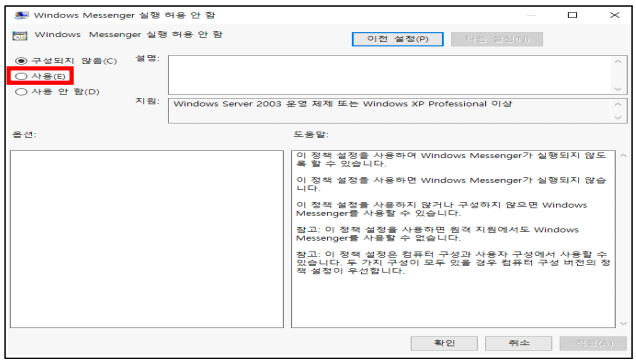
4. 실험 결과

본 연구에서는 Hyper-V 가상화 기술을 이용하여 Windows 10 운영체제를 기반으로 실험을 구성하였으며, ESTsoft의 알약과 ESTsoft 보안 점검 도구를 비교 분석하였다. 각 도구는 각각 47개와 62개의 취약점 점검 항목을 제공하며, 바이러스 백신 설치 여부, USB 자동 실행 차단, 보안 패치 적용 여부 등 기본적인 보안 항목을 점검하는 데 중점을 두고 있었다. 실험 결과, 기존 보안 도구들은 주로 기본적인 보안 요구 사항에 초점을 맞추고 있으며, 본 연구에서 제안한 3가지 추가 취약점(사용 메신저 금지, PC 시작 프로그램 제어, Windows 서비스 점검)은 포함되지 않은 것으로 확인되었다. 이는 기존 도구들이 최신 사이버 위협에 대응하는 데 한계가 있음을 보여주며, 본 연구에서 제안한 보안 항목들이 이를 보완할 수 있음을 시사한다.



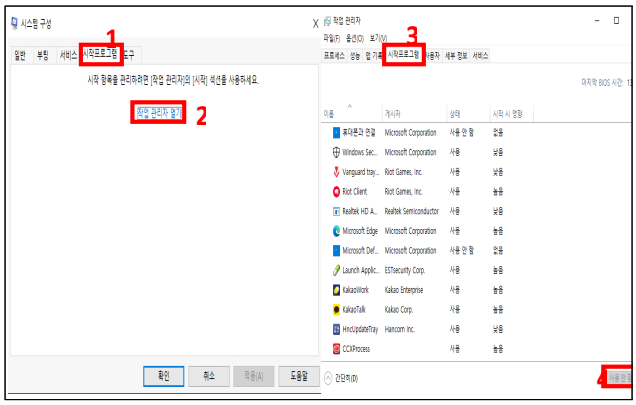
[그림 2] 사용 메신저 금지1

위 [그림2]와 같이 로컬 그룹 정책 편집기 창이 열리면, 먼저 '시스템 구성'을 선택하고, 그 다음으로 '관리 템플릿'을 클릭한다. 이후 'Windows 구성 요소' 섹션에서 'Windows Messenger' 항목을 찾아 선택한다.



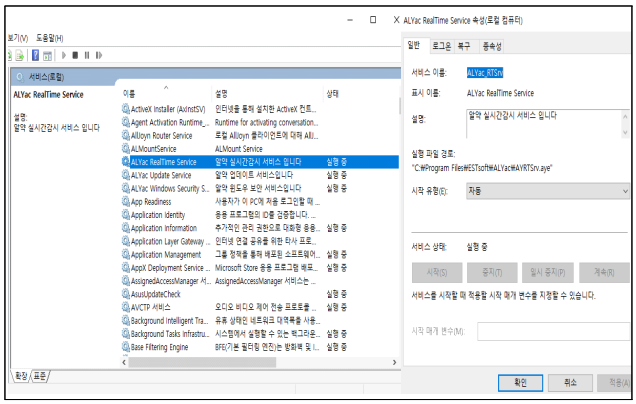
[그림 3] 사용 메신저 금지2

위 [그림 3]와 같이 Windows Messenger 설정을 비활성화하여 메신저 사용을 차단한다. 해당 점검항목을 추가함으로써 메신저 프로그램을 통한 정보 유출 및 피싱 공격을 예방하여, 조직 내 중요한 정보의 유출 위험을 줄일 수 있다.



[그림 4] PC 시작 프로그램 제어

위 [그림 4]와 PC 시작 프로그램 제어: msconfig 명령어로 스템 구성 창이 열리면 '시작 프로그램' 탭으로 이동한 후 '작업 관리자 열기'를 클릭한다. 작업 관리자가 열리면 다시 '시작 프로그램' 탭으로 이동하여, 비활성화할 프로그램을 선택한 후 '사용 안 함' 옵션을 클릭한다. 이를 통해 해당 프로그램이 시스템 부팅 시 자동으로 실행되지 않도록 설정할 수 있으며, 이 과정은 불필요한 프로그램의 실행을 차단하여 시스템 성능을 최적화하고 부팅 속도를 개선하는 데 도움이 된다. PC 부팅 시 자동으로 시작되는 프로그램을 비활성화하면 시스템 자원의 효율적인 활용과 부팅 속도의 향상이 가능하다. 또한, 불필요한 프로그램의 실행을 차단함으로써 보안 취약점을 줄일 수 있으며, 외부 공격자가 시스템에 접근할 수 있는 경로를 최소화하는 데 도움이 된다.



[그림 5] Windows 서비스 점검

위 [그림 5]와 같이 Windows 서비스 점검: services.msc 명령어로 Windows 서비스 관리자를 열어 불필요한 서비스를 비활성화하여 시스템 자원을 절약하고 보안을 강화한다. 해당 점검항목을 추가함으로써 불필요한 서비스로 인한 자원 낭비를 줄이고, 서비스의 비인가 실행을 차단함으로써 시스템 보안을 강화한다. 본 연구의 실험 결과는 기존 보안 도구에서 다루지 않는 추가 보안 항목들이 PC 보안을 보다 강화할 수 있음을 보여준다. 각 추가 항목은 시스템 성능을 최적화하고, 최신 사이버 위협에 효과적으로 대응할 수 있는 중요한 역할을 한다.

본 연구의 실험 결과는 기존 보안 도구들이 주로 기본적인 보안 요구 사항에 중점을 두고 있음을 확인시켜 주었으며, 최신 사이버 위협에 대한 대응력에서는 보완이 필요함을 보여줬다 . 본 연구에서 제안한 추가 보안 항목인 사용 메신저 금지, PC 시작 프로그램 제어, Windows 서비스 점검은 기존 도구들이 다루지 않는 영역을 보완하여 보안 체계를 강화하는 효과가 있었다. 이와 같은 추가 항목을 통해 메신저를 통한 정보 유출 방지, 부팅 속도 최적화와 시스템 자원 절약, 그리고 불필요한 서비스 비활성화로 인한 보안 강화가 가능해졌다. 이는 단순한 취약점 점검을 넘어, PC의 전반적인 보안성을 크게 향상시킬 수 있는 가능성을 보여준다. 결론적으로, 본 연구는 기존 보안 도구의 한계를 분석하고, 최신 사이버 위협을 고려한 보안 항목의 추가가 PC 보안에 실질적으로 기여할 수 있음을 입증하였다. 향후 이러한 추가 보안 항목들은 기존 도구의 한계를 보완하여, 더욱 포괄적이고 효율적인 보안 관리 체계를 구축하는 데 기여할 것으로 기대된다. 이를 통해 최신 사이버 위협에 대응하고, 보안 수준을 한층 강화할 수 있을 것이다.

4. 결론

본 연구는 기존 보안 점검 도구들이 충분히 다루지 못했던 취약점들을 보완하고자 새로운 보안 점검 항목을 제안하여 PC 보안성을 전반적으로 향상시키는 방안을 제시하였다. 특히, 사용 메신저 금지, PC 시작 프로그램 제어, Windows 서비스 점검과 같은 제안된 항목들은 최신 사이버 위협에 대한 대비력을 높이는 데 중요한 역할을 하며, 가상 환경에서의 실험을 통해 그 효과가 입증되었다. 이들 항목을 통한 보안 점검의 확대는 정보 유출 방지, 불필요한 서비스의 자원 소모 최소화, 시스템 자원 관리 효율성 제고에 기여하여 더욱 포괄적인 보안성을 실현하였다. 또한, 본 연구는 보안 점검 항목의 강화를 통해 기존 보안 도구의 한계를 보완하고, 보안 도구 개발과 보안 정책 수립에 참고할 수 있는 구체적 방향을 제시하였다. 이는 다양한 환경에서의 보안 요구 사항을 충족하고, 최신 위협에 대한 대응력을 강화하는 데 유용한 자료가 될 수 있다. 향후 연구에서는 본 연구에서 제안된 항목을 실제 환경에 적용하여 성능을 최적화하는 연구가 필요하며, 추가적으로 다양한 운영체제와 네트워크 환경에서의 실험을 통해 보안성을 더욱 강화할 수 있을 것이다. 아울러, 최신 사이버 위협에 신속히 대응할 수 있도록 보안 도구의 지속적인 업데이트가 요구되며, 사용자 인식 제고를 위한 보안 교육과 정책 수립이 병행된다면 더욱 안전한 디지털 환경 구축에 기여할 수 있을 것이다.

참고문헌

[1] 최영훈, 김두현 and 신영진. (2020). ICT기반 원격근무의 현황분석 및 개선방안에 관한 연구: 코로나-19사태에서의 팬데믹 관점을 중심으로. 융합사회와 공공정책, 14(2), 33-74.

[2] 이선재, 이일구, 안예린, 박소영, 윤지희, 정유진, 최유림, 윤선우, 장다은. (2019). 사이버보안 위협 분석 및 개선 방안에 대한 연구. 한국산업보안연구, 9(1), 69-97.

[3] 한국인터넷진흥원(KISA). (2023). 2023년 상반기 사이버 위협 동향 보고서. 한국인터넷진흥원.

[4] Vasani, V.; Bairwa, A.K.; Joshi, S.; Pljonkin, A.; Kaur, M.; Amoon, M. Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. Electronics 2023, 12, 4299. https://doi.org/10.3390/electronics12204299

[5] 조진근. (2019). PC보안 강화를 위한 기술적 취약점 진단 항목 개선 연구. 융합정보논문지, 9(3), 1-7.