Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.5, Oct. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.5.1101

모바일 Anti-Virus 성능 시험을 위한 평가 기준 수립 연구*

이 정 호,[1†] 신 강 식,[2] 유 영 락,[2] 정 동 재,[1] 조 호 묵[3‡]
[1,2,3]KAIST 사이버보안연구센터 (선임연구원, 연구원, 책임연구원)

A Study on Establishment of Evaluation Criteria for Mobile Anti-Birus Performance Test*

Jeongho Lee,[1†] Kangsik Shin,[2] Youngrak Ryu,[2] Dong-Jae Jung,[1] Ho-Mook Cho[3‡]
[1,2,3]KAIST Cyber Security Research Center
(Senior Researcher, Researcher, Principal Researcher)

요 약

최근 스마트폰을 대상으로 하는 해킹 피해가 증가하는 가운데 이로 인한 사용자들의 스마트폰 보안에 대한 불안감이 커지고 있는 실정이다. 이러한 불안을 낮추기 위한 방안으로 모바일 안티 바이러스를 사용하는 것은 좋은 방법 중의 하나이다. 하지만 사용자들은 모바일 안티바이러스 성능과 기능에 대해 알 수 있는 방법이 많지 않다. 매년 모바일 안티바이러스 제품에 대한 성능평가를 진행하여 이를 공개해 주는 인증 기관이 존재하나 이런 기관들은 테스트 방법에 대한 세부 시험평가 항목과 자세한 결과를 공개하지 않는다. 그리고 이전 품질평가 연구들은 모바일 안티바이러스 제품 평가에는 적합하지 않은 평가 기준이 존재하거나 검증이 미흡하여 최신 모바일 안티바이러스 평가에는 적절하지 않다. 그래서 본 논문에서는 최신 모바일 안티바이러스 평가에 적합한 세부적인 모바일 안티바이러스 평가지표를 수립하고 이를 국내외 10종의 모바일 안티바이러스 제품에 적용하여 수립한 평가지표의 유효성을 검증하였다.

ABSTRACT

With the recent increase in hacks targeting smartphones, users are becoming increasingly anxious about the security of their smartphones. Using a mobile anti-virus is one of the best ways to reduce this anxiety. However, there aren't many ways for users to learn about mobile anti-virus performance and features. While there are certification organizations that conduct annual performance evaluations of mobile anti-virus products and make them publicly available, they don't disclose the specifics of their testing methods and detailed results. In addition, previous quality evaluation studies are not suitable for evaluating modern mobile anti-viruses due to the existence of evaluation criteria that are not suitable for mobile anti-virus product evaluation or lack of validation. Therefore, this paper establishes detailed mobile anti-virus evaluation metrics suitable for the evaluation of modern mobile anti-viruses and applies them to 10 domestic and international mobile anti-virus products to verify the validity of the established evaluation metrics.

Keywords: Anti-Virus, Malware, Performance Evaluation

Received(05. 31. 2024), Modified(07. 22. 2024), Accepted(08. 02. 2024)

* 본 논문은 과학기술정보통신부 글로벌사이버보안기술연구(과제 고유번호: 1711202451) 사업의 지원을 받아 수행된 연구임.

† 주저자, ddanzit@gmail.com
‡ 교신저자, chmook79@kaist.ac.kr(Corresponding author)

I. 서 론

최근 은행을 사칭한 가짜 앱으로 국내 약 4만대의 스마트폰이 해킹을 당하고 대북관계자 및 언론인 등을 노린 사이버공격에 국내의 한 국회의원의 스마트폰이 해킹을 당하였으며 스페인 총리, 국방장관 등 스페인 정부 고위 관료들의 스마트폰이 이스라엘산 스파이웨어 페가수스의 해킹 공격으로 상당한 양의 정보가 유출 당하는 등 스마트폰에 대한 해킹 피해가 증가하고 있으며 이로 인한 사용자들의 스마트폰 보안에 대한 불안감이 갈수록 커지고 있는 실정이다. 특히 전 국민의 95%가 스마트폰을 사용하면서 스마트폰 보급률 세계 1위를 자랑하는 우리나라는 스마트폰 보안에 대한 불안감이 더욱더 커지고 있다[1][2][3].

이렇듯 모바일 환경에서의 보안관련 문제들이 이슈화됨에 따라 모바일 스마트폰의 보안을 위해서는 조기 탐지 및 예방이 매우 중요하다. 이중 모바일 안티 바이러스 소프트웨어를 사용하여 악성 앱을 탐지하는 것은 가장 좋은 방법 중 하나로 꼽히고 있다. 하지만 사용자들은 모바일 안티 바이러스 성능과 기능에 대해 알 수 있는 방법이 많지 않다. 모바일 안티바이러스 제품에 대하여 매년 성능평가를 진행하여 이를 공개해주는 인증 기관이 존재하나 테스트 방법에 대한 세부 시험평가 항목에 대해서는 공개하지 않고 있다. 또한 이전 연구들은 모바일 안티바이러스 제품 평가에는 맞지 않는 보안 소프트웨어에 대한 평가이거나 오래된 연구들로 최신 모바일 안티바이러스 제품에는 다소 미흡한 평가 기준이다. 본 논문에서는 최신 모바일 안티바이러스 제품 평가에 적합한 세부적인 평가지표를 수립하였으며 이를 국내외 안드로이드 모바일 안티바이러스 10개를 선정하여 모바일 안티바이러스 제품에 적용하여 평가지표의 적합성을 평가하고자 한다. 안드로이드 OS는 2024년 3월 기준 전 세계 모바일 운영체제 점유율이 70.78%에 이를 정도로 가장 많은 사용자를 보유하고 있다[4]. 이렇기에 우리는 많은 사용자를 보유하고 있는 안드로이드 기기의 안티바이러스 제품을 대상으로 실험을 진행하였다.

본 논문의 구성은 다음과 같다. 2장은 관련된 연구에 대해 기술하였으며, 3장은 모바일 안티바이러스 평가 기준을 수립하여 이에 대한 검증을 진행하였으며 4장에서는 결론과 향후 연구 방향에 대하여 논하겠다.

II. 관련연구

2.1 모바일 안티바이러스 성능테스트 기관

2.1.1 AV-Comparatives[5]

오스트리아에 본사를 두고 인스브루크 대학과 협력하여 정기적으로 보안 제품 테스트를 진행하는 기관으로 테스트를 통과한 제품은 표준 인증을 부여하고 실패한 제품은 단순히 테스트한 것으로 지정된다.

파일 탐지 테스트, 성능 테스트, 전체 테스트의 3가지 테스트를 수행하며 파일 탐지 테스트는 100,000개의 악성코드 샘플에 대하여 각 안티 바이러스 제품을 검사하는 정적 테스트이며 성능 테스트는 시스템 성능에 미치는 영향을 측정하고 마지막으로 전체 테스트는 실제 사용자 경험과 최대한 유사하게 시뮬레이션하여 보안 제품의 모든 구성 요소가 악성코드를 처리하는지 테스트한다.

2.1.2 AV-TEST[6]

독일 마그데부르크에 본사를 두고 있으며 다양한 안티바이러스 제품을 테스트하는 글로벌 보안제품 성능을 평가하는 기관이며, 보호, 성능, 유용성 3가지 항목에 대해 테스트를 진행하여 최대 6점을 각각 부여하고 인증을 받으려면 제품이 총 10점 이상을 획득해야 하고 모든 카테고리에서 0점이 없어야 한다. 최고의 제품은 이 테스트에서 18점 만점을 획득하였다. 테스트를 위하여 각 제품을 100,000개가 넘는 샘플로 구성된 AV-TEST 테스트 세트를 이용하여 보호 테스트를 진행하고 12가지(파일 다운로드, 네트워크 파일 복사, 일반 프로그램 실행 등) 이상의 일반적인 시스템 작업을 수행하는 데 필요한 시간 차이를 측정하여 성능을 테스트한다. 사용성 테스트는 사용 편의성이나 사용자 인터페이스 디자인과는 관련 없이 안티 바이러스 프로그램이 정상 프로그램, 악성 웹사이트, 의심스러운 내용 등을 표시할 때 발생하는 사용성 문제를 측정한다.

2.1.3 MRT Effitas[7]

영국 런던에 본사를 둔 독립적인 성능 평가기관으로 초기에는 PC기반 뱅킹용 악성 위협에 초점을 맞추었지만 2017년부터 안드로이드 모바일 보안 앱에

대한 평가도 진행하고 있다. 악성앱 샘플을 활용해 SD카드 검사와 실시간 검사, 시뮬레이터 검사로 테스트를 진행하며 SD카드 검사는 악성 앱 설치가 완료되기 전 초기단계 탐지율을 평가하며 실시간 검사는 앱이 설치된 이후의 탐지율을 평가하며 시뮬레이터 검사는 최신 멀웨어 동향을 반영한 악성 앱을 직접 제작해 평가에 활용하는 것으로 신변종 악성앱을 얼마나 잘 찾아내는지를 평가한다. 또한 과잉탐지 검사는 정상 앱 샘플을 악성 앱으로 오판하는 경우가 얼마나 적은지 확인하고 우수한 성적으로 통과해야 인증을 획득할 수 있다.

2.1.4 SKDlabs[8]

CNAS(중국 합격평정국가인가 위원회)가 인증한 정보보안 평가 및 인증기관으로 중국에서 매우 공신력 높은 평가 기관으로 AMTSO(AntiMalware Testing Standards Organization), AVAR(Association of Anti Virus Asia Researchers) 멤버로 가입되어 있다.

중국의 실제 네트워크 환경에서 제품의 성능과 기능을 평가하는 것이 목적이며 안티바이러스 제품뿐 아니라 방화벽, 호스트 보호, APP, UTM, 클라우드, 네트워크 모니터링, VPN 등 다양한 분야 테스트를 진행하고 있다. 안티바이러스 제품의 경우 악성코드 탐지율 98.5%이상이어야 하며 동시에 별도의 과잉탐지(과탐) 기준을 충족해야 하는데 시스템 앱에서 단 1개의 과탐도 발생해서는 안되고 일반 정상 앱으로 오인하는 경우도 0.05%이하 이어야 한다는 매우 엄격한 기준을 가지고 있다.

실시간 보호기능의 경우 중국에 널리 퍼져 있는 6,000개의 샘플을 사용하며 스마트폰 보안 소프트웨어를 사용하여 바이러스 샘플을 완전히 검사하고 제거한 다음 발견되지 않은 샘플을 설치 및 실행하는 방식으로 테스트를 진행한다.

2.2 기존 평가기준 연구

맹두열 등은 국제표준 ISO/IEC 9126을 기반으로 계층적 분석 방법을 이용하여 다수의 평가 요인을 범주화하고 가중치 정보를 마련하고 평가 항목을 기능성, 성능성, 편의성의 3가지 큰 항목과 25가지 세부 평가 항목으로 선정하고 포털 사이트에서 공개 안티바이러스 소프트웨어 70여종을 수집한 후 실제 테스트 환경에서 품질 평가를 수행하였다[9]. 하지만 세부 평가 항목이 25개로 비교적 적고 PC용 안티바이러스 소프트웨어를 대상으로 평가 항목을 선정함으로써 모바일 안티바이러스 제품에는 일부 평가 항목이 적용되지 못하는 단점이 존재한다.

Table 1. Comparison of Evaluation Criteria

Evaluation Criteria	Number of evaluation items	Evaluation Target Type	Number of evaluation targets	Main Quantitative evaluation items
Doo-lyel Maeng	25	PC Anti-Virus	70	Detection Accuracy
Suk-Jo Shin	21	Mobile Anti-Virus	2	Scan Speed
Yong-Man Han	8	Mobile Software	-	Response Time
Jee-Hoon Suh	13	Mobile Application	2	Time Efficiency, Resource Utilization
Proposed Evaluation Criteria	50	Mobile Anti-Virus	10	Detection Accuracy, Scan Speed, Resource Efficiency

신석조 등은 ISO/IEC 9126을 기반으로 스마트폰 안티바이러스 제품에 대한 기능성, 신뢰성, 유용성, 이식성, 효율성의 5가지 항목과 21가지 세부 항목을 가지는 효과적인 평가 항목을 개발하고 테스트 환경을 구성하여 스마트폰 안티바이러스 제품을 테스트하였다[10]. 하지만 세부 평가 항목이 21개로 적고 안티바이러스 제품 2개(V3 Mobile, Virobot Mobile)에 대해서만 평가가 이루어졌으면 2개의 안티바이러스 제품을 서로 다른 테스트 장비와 안드로이드 버전으로 테스트를 진행하였으며 평가 항목 중 효율성 부분에서 악성코드 검사 시간을 제외한 악성코드 탐지율, 오탐율 등은 평가를 하지 못하는 문제점이 존재한다.

한용만 등은 ISO/IEC 25000을 기반으로 AHP 기법을 적용하여 모바일 소프트웨어에 대한 보안성, 상호운용성, 이식성, 유지보수성, 효율성, 사용성, 신뢰성, 기능성의 8가지 항목의 품질 특성을 도출하고 이중 4개의 특성에 대하여 품질 측정 항목을 제시하였다[11]. 하지만 4가지 특성에 대해서만 평가 방법을 제시하였고 세부 평가 결과에 대한 상세 내용을 공개하지 않아서 품질 특성에 대한 검증이 제대로 이루어졌다고 보기 어렵다.

서지훈 등은 모바일 애플리케이션의 특성을 성능에 대한 효율성, 호환성, 사용성, 신뢰성, 보안성,

Table 2. Version for each Mobile Anti-Virus

Mobile Anti-Virus	Version
V3 Mobile Security	3.8.0.9
Alyac M	3.0.4.7
ESET Mobile Security	8.2.15.0
SK Shielders Mobile Guard	23.1.2
Avast Mobile Security	23.24.0
Norton 360	5.76.0.231201002
Avira Antivirus Security	7.22.0
Bitdefender Mobile Security	3.3.224.2368
Kaspersky Standard	11.109.4.11153
Malwarebytes Mobile Security	5.3.4

이식성의 6가지 주특성과 시간 효율성, 공존성, 운영성 등 13가지 부특성으로 분류하고 메트릭을 만들어 6개의 애플리케이션에 적용하여 품질 평가를 검증하였다[12]. 하지만 애플리케이션에 대한 품질 평가 항목을 기준으로 평가를 진행하여 모바일 안티바이러스 제품 평가에는 적합하지 못한 단점이 존재한다.

III. 평가 기준 수립 및 검증

이전 연구들에서 제시한 품질평가 기준은 PC용 안티바이러스 제품에 대한 품질평가 방법이거나 일부 세부 평가 항목만 있어 항목수가 적고 제대로 된 검증이 이루어지지 못하는 등의 한계가 존재한다. 이렇게 모바일 안티바이러스 제품 평가 방법을 개선하기 위하여 본 논문에서는 국내외 다양한 품질 평가 표준과 각 모바일 안티바이러스 매뉴얼을 바탕으로 공통 평가 항목 및 기능을 도출하고, 불필요한 평가 항목을 삭제 및 단순화하여 평가 기준을 수립하였다. 참고한 품질 평가 표준은 다음과 같다. ISO/IEC 25000[13][14], ISO/IEC 25010[15], ISO/IEC 25020[16], 과학기술정보통신부 고시 "소프트웨어 기술성 평가 기준 지침"[17].

평가 기준은 악성 앱을 얼마나 정확하고 빠르게 탐지하는지와 같은 성능을 평가하기 위한 ***기능성***, 모바일 장치의 자원인 배터리를 얼마나 효율적으로 사용하고 온도가 과도하게 발생하는지를 확인하기 위한 ***자원 효율성***, 사용자가 얼마나 편리하게 사용할 수 있는지를 평가하기 위한 ***사용성***, 악성코드를 탐지하는 기능 외에 추가적인 보안기능을 평가하기 위한 ***부가 기능***, 신속한 업데이트 및 지원을 확인하기 위한 ***공급업체 지원*** 등 크게 5가지로 분류하여 수립하였다.

Table 3. Specifications of the Device used for evaluation

PC	
CPU	i5-12400
Memory	16GB
Storage	SSD 500GB
OS	Windows10 Pro(64bit)
Mobile Device	
Product	Samsung Galaxy Tab A7 Lite
Internal Memory	32GB
External Memory	SD Card 128GB
OS	Android 13

평가 결과는 모바일 안티바이러스의 제품명을 표기하지 않고 순서를 무작위로 알파벳 A-J로 표기하였다.

3.1 평가 기준 검증을 위한 테스트 환경

기존 성능테스트 기관과 이전 연구들에서는 테스트 환경을 공개하지 않거나 상이한 장치와 안드로이드 버전으로 환경을 구성하거나, 테스트에 사용한 안티바이러스 제품군이 적어 제대로 된 평가가 이루어지기 어려운 부분들이 존재하였다. 본 논문에서는 각각의 모바일 안티바이러스가 설치된 모바일 장치를 동일한 사양의 PC에 연결하고 중앙에서 제어가 가능하도록 구성하고 테스트를 진행함으로써 사용자의 개입없이 동시에 동일하게 성능테스트를 할 수 있도록 평가 기준에 적합한 검증 환경을 구축하였다.

수립한 평가 기준을 검증하기 위한 모바일 안티바이러스는 국내의 경우 V3 Mobile Security, 알약 M, SK쉴더스 Mobile Guard 제품을 선정하고 국외에는 ESET Mobile Security, Avast Mobile Security, Norton 360, Avira Antivirus Security 등의 제품을 선정하여 총 10종의 모바일 안티바이러스 제품을 선정하고 평가를 진행하였다. 모바일 안티바이러스 선정 기준은 다음과 같다.

(기준1) Google Play 내 국내 인지도 및 다운로드 수가 높은 모바일 안티바이러스 제품

(기준2) 별점 3.5 이상의 신뢰성 있는 제품

Table 4. Overall Evaluation Table(Functionality)

	Good	Average	Bad
A	9	1	1
B	10	1	0
C	10	1	0
D	7	4	0
E	1	0	0
F	5	3	3
G	7	4	0
H	9	2	0
I	2	1	0
J	4	1	6

(기준3) 안드로이드 운영체제 및 태블릿 설치가 가능한 제품

성능 평가에 사용할 악성 앱은 연구 목적으로 금융 관련 기관과 보안 관련 기관에서 제공 받거나 자체 크롤링 시스템에서 수집한 악성 앱을 총 6개의 샘플 그룹으로 구성하여 평가하였다.

(샘플1) 피싱, 스파이웨어, 금융 등 악성 유형별 악성 앱 1,000개

(샘플2) 랜덤 샘플링하여 선정한 최근 3년내 발생한 악성 앱 10,000개

(샘플3) 최근 1년 이내 발생한 악성 앱 1,000개

(샘플4) 최근 3년간 발생한 금융 피싱 관련 악성 앱 5,000개

(샘플5) 3개월 이내 발생한 금융 관련 악성 앱 100개

(샘플6) 1개월 이내 발생한 악성 앱 140개

평가는 동일한 환경에서 동시에 명령 수행 및 악성 앱이 모바일 장치에 설치되도록 Controller와 Agent를 자체 개발하여 수행하였으며 수행된 내용에 대한 로그는 데이터베이스에 저장하여 수행여부를 추후 확인할 수 있도록 구성하였다.

성능평가에 사용된 Mobile 기기는 성능 평가시 하드웨어 성능에 따른 평가 성능에 미치는 영향도를 쉽게 확인하기 위하여 저사양의 기기를 선택하였다. PC 및 Mobile 기기의 사양은 〔표 3〕에서 보는 바와 같다.

Table 5. Overall Evaluation Table(Resource Efficiency)

	Good	Average	Bad
A	1	2	0
B	2	0	1
C	0	2	1
D	0	3	0
E	2	0	1
F	2	1	0
G	1	2	0
H	3	0	0
I	1	2	0
J	2	1	0

3.2 평가 기준 및 검증

3.2.1 기능성

기능성 평가 항목은 정확성 및 신속성을 평가하는 항목으로 모바일 안티바이러스 제품이 모바일 기기에 악성 앱이 설치되거나 SD카드 수동검사 시 얼마나 빠르게 탐지하고 올바르게 탐지하는지를 확인하는 평가 항목이다. 정확성의 대표적인 평가 기준은 악성 앱 1,000개를 PC를 통하여 모바일 장치에 설치했을 때 모바일 안티바이러스 제품이 실시간으로 얼마나 정확하게 악성 앱을 탐지하는지를 확인하는 것이 목적이다. 정확성은 85%이상 정확히 탐지하였을 경우 Good, 75%이상 85%미만일 경우 Average, 75% 미만일 경우 Bad로 평가하였다.

신속성은 SD카드 검사시 얼마나 빠르게 악성 앱을 검사하는지를 확인하는 것이 목적이다. 신속성은 악성 앱이 많아질수록 검사시간이 증가하는 것을 고려하여 악성 앱의 수에 따라 나누어 평가 기준을 세분화하였다. 악성 앱이 200개 미만일 경우 검사 시간이 2분 이하일 경우 Good, 6분 미하일 경우 Average, 6분 초과일 경우 Bad로 평가하였고, 악성 앱이 1,000개일 경우 검사시간이 10분이하일 경우 Good, 30분 이하일 경우 Average, 30분 초과일 경우 Bad로 평가하였다. 자세한 신속성 평가 기준은 Appendix A에 자세히 표기하였다.

이 평가 기준은 다른 평가 기관의 기준값과 실험을 통해 나온 평균 결과값을 기반으로 보정하여 설정

Table 6. Overall Evaluation Table(Usability)

	Good	Average	Bad
A	4	2	3
B	5	1	3
C	3	2	4
D	3	2	4
E	3	1	5
F	5	1	3
G	3	1	5
H	3	2	4
I	4	1	4
J	4	0	5

하였다.

기능성 평가의 총 11개의 세부 평가 항목 중 B와 C 모바일 안티바이러스 제품이 우수 10개, 평균 1개를 받아 가장 좋은 결과가 나왔다. 기능성에서 E의 경우 SD카드 검사 기능이 없어 SD카드 검사가 이루어지지 못하였으며 I의 경우는 SD카드 검사중 내부 메모리 부족 등의 이유로 일부 오류가 발생하여 몇가지 항목에서는 제외되었다.

각 악성앱 샘플별 기능성에 관한 평가 결과는 Appendix B에 표기하였으며 기능성 관련 평가 항목은 Appendix D에서 찾아볼 수 있다.

3.2.2 자원 효율성

자원 효율성 평가 항목은 모바일 안티바이러스가 악성 앱 검사시 모바일 장치의 자원이 얼마나 변화하는지를 평가하는 항목이다. 이 항목은 배터리 및 온도 변화량이 낮을수록 좋은 성능을 나타낸다고 할 수 있다. 배터리 사용률의 평가 기준은 모바일 안티바이러스 미검사시와 3분간 악성 앱 5,000개 검사후의 배터리 잔량 차이를 평가하며 안티바이러스의 백그라운드 사용률을 확인하기 위하여 배터리를 100% 충전후 72시간 경과후 배터리 잔량을 확인하여 평가한다. 3분간 배터리 사용률은 0.3% 이하이면 Good, 0.3% 초과 1%이하이면 Average, 1%초과일 경우 Bad로 평가하였다. 72시간 경과후 배터리 사용률은 30% 이하이면 Good, 30%초과 50%이하이면 Average, 50%초과이면 Bad로 평가하였다.

온도 평가 기준은 3분간 악성 앱 5,000개에 대한 안티바이러스 검사를 수행했을 때 온도 변화량을 체크하는 방식으로 평가를 진행하였다. 온도차가 2℃ 이하이면 Good, 4℃이하이면 Average, 4℃초과이면 Bad로 평가하였다.

Table 7. Overall Evaluation Table(Add-Ons)

	Good	Average	Bad
A	12	0	10
B	13	0	9
C	9	1	12
D	9	1	12
E	2	1	19
F	12	0	10
G	6	1	15
H	6	1	15
I	12	0	10
J	6	1	15

자원 효율성 평가항목 총 3개의 세부 평가 항목 중 H 제품이 우수 3개를 받아 가장 좋은 결과를 보여주었다. 세부항목 중 72시간후 배터리 변화율에서 E 제품의 경우 배터리가 방전이 되어 백그라운드에서 배터리 소모량이 많은 것을 알 수 있었다.

자원 효율성과 관련된 평가 결과는 Appendix C, 평가 항목은 Appendix E에 첨부하였다.

3.2.3 사용성

사용성 평가 항목은 제품에서 사용자 편의성을 얼마나 제공하는지에 대한 평가항목이며, 사용자 학습 용이성은 얼마나 다양한 언어를 제공하는지 제품내에 사용자 메뉴얼을 제공하는지에 대해 평가한다. 입력 데이터지원 항목은 간편 및 정밀 검사시 사용자가 원하는 검사 대상을 지정할 수 있는지에 대해 평가하며 설치제거 용이성은 제품을 오류없이 정상적으로 제품을 제거할 수 있는지에 대해 평가하는 항목이다. 지원 여부만 묻는 항목은 지원하는 경우 Good, 미지원인 경우 Bad로 평가하였으며 지원 가능 개수인 경우 미지원인 경우 Bad, 1개~2개인 경우 Average, 3개 이상인 경우 Good으로 평가하였다.

사용성은 총 9개의 세부항목이 있으며 모바일 안티바이러스 B와 F가 가장 우수한 결과를 얻었다. J의 경우 10개가 넘는 언어를 지원하고 있었다.

사용성에 대한 자세한 평가 항목은 Appendix F에 첨부하였다.

Table 8. Overall Evaluation Table(Vendor Support)

	Good	Bad
A	5	0
B	5	0
C	5	0
D	4	1
E	5	0
F	4	1
G	4	1
H	4	1
I	5	0
J	3	2

3.2.4 부가 기능

부가 기능은 실시간 탐지 및 수동검사인 기본검사를 제외하고 추가적인 보안 기능을 제공하는지 평가하는 항목이다. 예약검사 기능이 있는지 VPN, Wifi 관리 기능이 있는지, 루팅 여부 확인 기능이 있는지 등 다양한 평가 항목이 있으며 총 22개의 세부 평가 항목으로 이루어져 있다.

모바일 안티바이러스 B 제품이 가장 우수한 결과를 나타내었으며 A 제품의 경우 다양한 수동검사 방식을 제공하고 있었다.

부가 기능에 대한 자세한 평가 항목은 Appendix G에 첨부하였다.

3.2.5 공급업체 지원

이 항목은 기능 추가 및 지속적인 업데이트가 이루어지고 있는지 문제 발생시 업체가 지원을 신속하게 제공하는지를 평가하는 항목이다.

총 5개의 세부항목이 있으며 A, B, C, E, I의 항목이 우수한 결과를 얻었으며 비교적 모든 제품들이 양호한 결과를 얻었다.

공급업체 지원에 대한 자세한 평가 항목은 Appendix H에 첨부하였다.

IV. 결 론

본 논문에서는 기존 품질평가 기준과 이전 연구들에서 불필요한 항목을 제거하고 단순화 및 그룹화하여 기능성, 자원효율성, 사용성, 부가기능, 공급업체 지원 등 크게 5가지 평가항목으로 분류하고, 총 50개의 세부적인 평가기준을 수립함으로써 최신 모바일 안티바이러스 제품을 평가하기 위한 객관적이고 정량적인 기준을 제시하였다. 이렇게 제시한 평가 기준을 바탕으로 10종의 모바일 안티바이러스 제품에 대한 품질평가를 진행함으로써 평가기준에 대한 유효성을 검증하였다. 또한 저사양의 모바일 기기를 기준으로 평가를 진행함으로써 하드웨어 성능에 따라 평가지표에 미치는 영향이 미비함을 확인하였다.

향후 연구에서는 점차 증가하고 있는 iOS에 대한 평가를 진행하여 OS에 따른 평가 기준의 유효성을 검증하고 수립된 평가 기준을 바탕으로 매년 새로운 모바일 안티바이러스 제품을 평가하고 새로운 유형의 악성 앱을 평가함으로써 평가 기준에 대한 신뢰성을 향상하고 평가 기준을 보완해 나갈 예정이다.

Appendix

A. Evaluation Criteria

Evaluation Items			Good	Average	Bad
Detection Accuracy			85%〈=	75%〈=, 〈85%	〈75%
Scan Speed	Number of Malwares	〈 200	〈=2min.	2min.〈, 〈=6min.	6min.〈
		1,000	〈=10min.	10min.〈, 〈=30min.	30min.〈
		5,000	〈=50min.	50min.〈, 〈=2.5hour.	2.5hour.〈
		10,000	〈=1.6hour.	1.6hour.〈, 〈=5hour	5hour.〈
Battery Usage		3min.	〈=0.3%	0.3%〈, 〈=1%	1%〈
		72hour.	〈=30%	30%〈, 〈=50%	50%〈
Temperature			〈=2℃	2℃〈, 〈=4℃	4℃〈

B. Functionality Evaluation Results

Evaluation Criteria	A	B	C	D	E	F	G	H	I	J
(1)	75.28%	98.04%	94.75%	95.57%	97.22%	96.29%	97.01%	96.81%	96.6%	78.48%
(2)	86.23%	99.67%	96.85%	99.9%	-	93.02%	98.99%	99.98%	-	93.08%
(3)	55.8%	94.9%	88.8%	91.3%	-	75.1%	87.6%	91.2%	-	86.3%
(4)	100%	99.98%	99.98%	99.8%	-	90.58%	99.62%	99.98%	-	90.74%
(5)	100%	100%	100%	100%	-	100%	100%	100%	100%	100%
(6)	87.86%	90.71%	91.43%	85.71%	-	90%	91.43%	90.71%	-	32.86%
(7)	00:00:29	03:23:11	01:00:36	01:26:00	-	01:47:40	01:29:45	00:40:51	-	07:09:05
(8)	00:02:09	00:02:35	00:06:47	00:15:31	-	00:33:05	00:18:18	00:06:24	-	01:40:16
(9)	00:04:11	00:31:25	00:56:44	00:53:57	-	02:52:03	01:10:36	00:51:12	-	05:22:50
(10)	00:00:16	00:00:48	00:00:59	00:03:18	-	00:05:04	00:02:48	00:01:28	00:03:09	00:12:10
(11)	00:00:21	00:01:21	00:01:47	00:04:12	-	00:07:24	00:04:39	00:02:13	-	00:19:51

C. Resource Efficiency Evaluation Results

Evaluation Criteria	A	B	C	D~	E	F	G	H	I	J
(12)	0%	0%	1%	1%	0%	0%	1%	0%	1%	0%
(13)	32%	52%	46%	33%	100%	36%	27%	20%	24%	45%
(14)	3℃	2℃	5℃	3℃	0℃	2℃	4℃	2℃	4℃	1℃

D. Evaluation Category 1: Functionality

Evaluation Category	Evaluation Item	Evaluation Criteria
Functionality	Accuracy	(1) Real-time detection accuracy with malware app installations (1,000)
		(2) Manual scan detection accuracy test of 10,000 malware apps (last 3 years)
		(3) Detection accuracy test of malware apps (1,000) from the past year (since Jul 2022)
		(4) Detection accuracy test of finance phishing malware apps (5,000) over 3 years
		(5) Detection accuracy test of finance malware apps (100) occurring within 3 months (Aug 2023)
		(6) Detection accuracy test of malware apps (140) that occurred within 1 month (Nov 2023)
	Speed	(7) Test speed for the manual scan of 10,000 malware apps (Test 2)
		(8) Test speed for recent malware apps (1,000) within 1 year (Test 3)
		(9) Test speed for financial phishing-related malware apps (5,000) over 3 years (Test 4)
		(10) Test speed for financially related malware apps (100) within 3 months (Aug 2023) (Test 5)
		(11) Test speed for malware apps (140) within 1 month (Nov 2023) (Test 6)

E. Evaluation Category 2: Resource Efficiency

Evaluation Category	Evaluation Item	Evaluation Criteria
Resource Efficiency	Battery Usage	(12) Check the battery level during the Test 4 scan. Method: Check the battery remaining after running an antivirus scan for 5,000 malware for 3 minutes from a 100% charge
		(13) Antivirus background mode battery level Method: Check the battery level after 72 hours from 100% charge
	Temperature	(14) Temperature check during the Test 4 scan Method: Check the temperature change when running an antivirus scan for 5,000 malware for 3 minutes

F. Evaluation Category 3: Usability

Evaluation Category	Evaluation Item	Evaluation Criteria
Usability	Users' ease of operation	(15) How many languages do products support?
		(16) Does the product offer manuals?
	Input data support	(17) How many ways (or additional options) do the Quick and Deep Scans offer to specify what to scan?
	Ease of understanding progress	(18) Does it provide a UI/UX that makes it easy to understand the scan's progress being performed?
	Installation environment suitability	(19) Does the product installation process not prompt you to install other external programs?
	Ease of uninstallation	(20) Is the product easy to install and uninstall?
	Report Generation	(21) Does it provide detection and quarantine result reports in a file?
	Custom detections and scans	(22) Can users exclude certain conditions (folder, filename, extension, detection name, etc.) from detection and inspection?
	Real-time detection	(23) Is it possible to specify a specific location for real-time detection?

G. Evaluation Category 4: Add-ons

Evaluation Category	Evaluation Item	Evaluation Criteria
Add-ons	Manual Scanning	(24) After real-time detection, can the AV set actions for detected malware?
		(25) How many manual scanning methods does the AV offer?
		(26) Can the AV allow specific locations (files, drives, specific folders, etc.) to be scanned during a manual scan?
		(27) Does it have a scheduled scan feature?
	Network Security	(28) Block harmful sites or manage user-defined sites?
		(29) Ability to prevent or detect specific network-based intrusions?
		(30) VPN or proxy capabilities?
		(31) WiFi management capabilities?
	System Security	(32) Is it possible to see a history of recently installed apps?
		(33) Does it have phishing-specific detection or blocking capabilities (URL, SMS, Email)?
		(34) Does it have the ability to clean up and block old (unused) apps?
		(35) Does it have the ability to manage app permissions (location, mic, contacts, call logs, messages, etc.)?

Evaluation Category	Evaluation Item	Evaluation Criteria
Add-ons	System Security	(36) Does it have an app lock feature?
		(37) Does it have the ability to tamper with the OS and check for rooting?
	Privacy	(38) Does it have a junk file deletion feature?
		(39) Does it allow you to delete your browsing history?
		(40) Does it have the ability to delete user history (recently opened files, list of running documents, etc.)?
		(41) Does it have the ability to manage internet banking (check for banking app fraud)?
		(42) Does it have the ability to manage payment information (e.g., PayPal)?
	Others	(43) Does it have a QR scanner scan function?
		(44) Does it have the ability to handle exceptions in detection?
		(45) Does it have a function to clean smartphone memory?

H. Evaluation Category 5: Vendor Support

Evaluation Category	Evaluation Item	Evaluation Criteria
Vendor Support	Maintenance	(46) Does the product continue to receive regular product updates and feature additions?
	Schedule updates	(47) Does it allow users to control engine (DB) updates automatically or manually?
	Troubleshooting and support	(48) Does the product have a Q&A or FAQ on the homepage or within the AV product?
		(49) Does it provide technical support in the Korean language on the homepage?
		(50) Does the provider have a contact support or service (such as a chatbot) that can respond quickly in case of a problem?

References

[1] MBC News, https://imnews.imbc.com/news/2021/politics/article/6110348_34866.html, Apr. 2024.

[2] Kyunghyang shinmun, https://www.khan.co.kr/world/europe-russia/article/202205031513001, Apr. 2024.

[3] Hankyoreh, https://www.hani.co.kr/arti/politics/defense/733857.html, Apr. 2024.

[4] Statcounter, https://gs.statcounter.com/os-market-share/mobile/worldwide, Apr. 2024.

[5] AV-Comparatives, https://www.av-comparatives.org/, Apr. 2024.

[6] AV-Test, https://www.av-test.org/, Apr. 2024.

[7] MRG-Effitas, https://www.mrg-effitas.com/, Apr. 2024.

[8] SKD LABS, https://www.skdlabs.com/html/english/, Apr. 2024.

[9] Doo-lyel Maeng, Jong-kae Park, and Sung-joo Kim, "A study on quality evaluation methodology establishment of anti-virus software based on the real test environment," The Journal of Korean Institute of Communications and Information Sciences, 35(3), pp. 450-451, Mar. 2010.

[10] Suk-Jo Shin, Seon-Joo Kim, Chun-Yan Jiang, and In-Jun Jo, "Effective evaluation about the antivirus solution for smart phone," Journal of information and communication convergence engineering, 9(6), pp. 697-699, Dec. 2011.

[11] Yong-Man Han, Gwangyeul Yun, Seonhg-Cheol Kim, Jong-Moo Chioi, and HaeYoung Yoo, "Design of quality evaluation for mobile software," Proceedings of ther Korean Information Science Society Conference, 39(1), pp. 200-201, Jun. 2012.

[12] Jee-Hoon Suh, Jae-Hyun Choi, and Jong-Bae Kim, Jea-Won Park, "Design of quality evaluation model for mobile application," 18(10), pp. 2454-2458, Oct. 2014.

[13] ISO/IEC 25000, "Systems and software engineering: systems and software quality requirements and evaluation," 2014.

[14] Hye-jeong Jeong, "Trends in standardizing software quality measurement," TTA Journal, No. 128, p. 104, Jan. 2010

[15] ISO/IEC 25010, "Systems and software engineering: systems and software quality requirements and evaluation - system and software quality models," 2011.

[16] ISO/IEC 25020, "Systems and software engineering: Systems and software Quality Requirements and Evaluation - Quality measurement framework," 2019.

[17] "Software technical evaluation criteria guidelines," Ministry of Science and ICT notice, No 2021-98, Dec. 2021

〈저자소개〉

이 정 호 (Jeongho Lee) 정회원
2002년: 한남대학교 컴퓨터공학과 학사
2004년: 경희대학교 정보통신대학원 통신망관리공학과 석사
2017년~현재: 한국과학기술원 사이버보안연구센터 선임연구원
〈관심분야〉 웹보안, 시스템보안, 악성코드 분석

신 강 식 (Kangsik Shin) 정회원
2016년 2월: 충남대학교 컴퓨터공학과 학사
2018년 2월: 충남대학교 컴퓨터공학과 석사
2020년~현재: 한국과학기술원 사이버보안연구센터 연구원
〈관심분야〉 악성코드 분석, 사이버보안, 딥러닝 보안

유 영 락 (Youngrak Ryu) 정회원
2011년: 한밭대학교 컴퓨터공학과 학사
2021년: Technische Universität Berlin Computer Science 베를린공대 컴퓨터 사이언스 석사
2022년~현재: 한국과학기술원 사이버보안연구센터 연구원
〈관심분야〉 사이버보안, 악성코드 분석, 난독화

정 동 재 (Dong-Jae Jung) 종신회원
2011년: 아주대학교 정보 및 컴퓨터공학부
2013년: 한국과학기술원 정보보호대학원 석사
2020년: 한국과학기술원 정보보호대학원 박사
2020년~현재: 한국과학기술원 사이버보안연구센터 선임연구원
〈관심분야〉 악성코드 분석, 시스템보안, 흐름 분석

조 호 묵 (Ho-Mook Cho) 종신회원
2006년: 아주대학교 정보통신공학과 정보보호학 (공학석사)
2018년: 전남대학교 정보보안협동과정 (이학박사)
2014년~현재: 한국과학기술원 사이버보안연구센터 책임연구원/실장
〈관심분야〉 사이버보안, 악성코드 분석, XAI 보안