(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월18일
(11) 등록번호 10-2046262
(24) 등록일자 2019년11월12일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 21/56* (2013.01)
(52) CPC특허분류
G06F 21/577 (2013.01)
G06F 21/56 (2013.01)
(21) 출원번호 10-2018-0123949
(22) 출원일자 2018년10월17일
심사청구일자 2018년10월17일
(65) 공개번호 10-2019-0073255
(43) 공개일자 2019년06월26일
(30) 우선권주장
1020170174459 2017년12월18일 대한민국(KR)
(56) 선행기술조사문헌
KR101803889 B1*
KR1020130071617 A*
KR1020150084123 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이경호
서울특별시 강남구 선릉로 222, 105동 501호 (대치동, 대치아이파크아파트)
최다희
서울특별시 동대문구 홍릉로 13, 101동 702호 (현대코아아파트)
(뒷면에 계속)
(74) 대리인
윤귀상

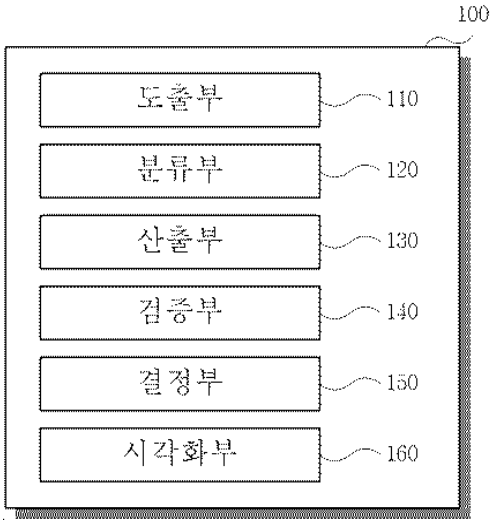
전체 청구항 수 : 총 8 항 심사관 : 구대성

(54) 발명의 명칭 **모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치 및 방법, 이 방법을 수행하기 위한 기록 매체**

(57) 요 약

본 발명은 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치에 있어서, 모바일 악성 코드 데이터에 대해 정적 분석 및 가상 환경 하에서 동적 분석을 수행한 결과에 대해 기존 모바일 악성 코드에서 활용된 블랙 리스트를 이용하여 악성 코드의 특성을 도출한 후, 도출한 특성들 중에서 모바일 악성 코드 데이터와 관련성이 높은 특성을 선정하는 도출부, 분석부에서 선정된 특성들을 이용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류하는 분류부, 분류된 악성 행위에 대해 자산, 위협 및 취약성을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출하는 산출부 및 산출부의 결과에 대해 모바일 악성 코드 탐지과정의 효율을 검증하고, 검증 결과를 데이터베이스에 저장하는 검증부;를 포함하는 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치를 개시하고 있다.

대 표 도 - 도1



(72) 발명자

박원

서울특별시 노원구 화랑로 564, 202동 114호 (공릉동, 육사아파트)

오준형

서울특별시 서초구 신반포로 270, 116동 1801호(반포동, 반포자이아파트)

이주현

서울특별시 동대문구 이문로3길 73-9

김창연

서울특별시 중랑구 신내로21길 16, 504동 204호(대림아파트)

유영인

서울특별시 성북구 삼선교로22길 25-6(삼선동5가)

이 발명을 지원한 국가연구개발사업

과제고유번호	20170018530012003
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발
연구과제명	머신러닝 기반 지능형 악성코드 분석 통합 플랫폼
기 여 율	1/1
주관기관	주식회사 엔에스에이치씨
연구기간	2017.09.01 ~ 2017.12.31

명 세 서

청구범위

청구항 1

모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치에 있어서,

모바일 악성 코드 데이터에 대해 정적 분석 및 가상 환경 하에서 동적 분석을 수행한 결과에 대해 기존 모바일 악성 코드에서 활용된 블랙 리스트(Black List)를 이용하여 악성 코드의 특성을 도출한 후, 상기 도출한 특성들 중에서 모바일 악성 코드 데이터와 관련성이 높은 특성을 선정하는 도출부;

상기 도출부에서 선정된 특성들을 이용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류하는 분류부;

상기 분류된 악성 행위에 대해 자산(Asset Value), 위협(Threat) 및 취약성(Vulnerability)을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출하는 산출부;

상기 산출부의 결과에 대해 모바일 악성 코드 탐지과정의 효율을 검증하고, 상기 검증 결과를 데이터베이스에 저장하는 검증부; 및

기준이 다른 조합 가능한 모든 모바일 데이터 셋(set)에 대한 상기 검증부의 검증결과를 기초로, 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정하는 결정부;를 포함하는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치.

청구항 2

삭제

청구항 3

제 1 항에 있어서, 상기 산출부의 자산(Asset Value)은,

악성 코드가 실행할 수 있는 도메인의 중요도로 침해 지표(IOC)에서 정의하고 있는 공격 대상인 사용자(user), 애플리케이션(application) 및 시스템(system) 중 적어도 하나를 포함하는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치.

청구항 4

제 1 항에 있어서, 상기 산출부의 위협(Threat)은,

기계학습으로 가중치가 부여된 악성 코드 행위 정보로 자산에 대해 발생 가능한 공격자로부터의 설치(Installation), 활성화(Activation), 악성 페이로드(Malicious Payloads) 및 오버 뷰(Over view) 중 적어도 하나를 포함하는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치.

청구항 5

제 1 항에 있어서, 상기 산출부의 취약점(Vulnerability)은,

자산의 구체적 행위에 대한 분류 정보로, 자산에서 분류한 침해 지표(IOC)의 기준들에 대한 세부 항목인 쿠키(cookie) 정보, 이-메일(E-mail) 정보 및 시스템(system) 정보 중 적어도 하나를 포함하는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치.

청구항 6

제 1 항에 있어서,

상기 위험도에 따라 비율, 색상 및 도표 중 적어도 어느 하나로 표현하는 시각화부;를 더 포함하는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치.

청구항 7

모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 방법에 있어서,

모바일 악성 코드 데이터에 대해 정적 분석 및 가상 환경 하에서 동적 분석을 수행한 결과에 대해 기존 모바일 악성 코드에서 활용된 블랙 리스트(Black List)를 이용하여 악성 코드의 특성을 도출한 후, 상기 도출한 특성들 중에서 모바일 악성 코드 데이터와 관련성이 높은 특성을 선정하는 단계;

선정된 특성들을 이용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류하는 단계;

상기 분류된 악성 행위에 대해 자산(Asset Value), 위협(Threat) 및 취약성(Vulnerability)을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출하는 단계;

상기 산출 결과에 대해 모바일 악성 코드 탐지과정의 효율을 검증하고, 상기 검증 결과를 데이터베이스에 저장하는 단계; 및

기준이 다른 조합 가능한 모든 모바일 데이터 셋(set)에 대한 검증결과를 기초로, 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정하는 단계;를 포함하는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 방법.

청구항 8

삭제

청구항 9

제 7 항에 있어서,

상기 위험도에 따라 비율, 색상 및 도표 중 적어도 어느 하나로 표현하는 단계;를 더 포함하는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 방법.

청구항 10

제7항 및 제9항 중 어느 한 항에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 방법을 실행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치 및 방법, 이 방법을 수행하기 위한 기록 매체에 관한 것으로, 더욱 상세하게는 알려지지 않은 새로운 모바일 악성 코드의 공격에 대비할 수 있도록 구현한 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 방법에 관한 것이다.

배 경 기 술

[0003] 기계 학습 또는 머신 러닝(machine learning)은 인공 지능의 한 분야로, 컴퓨터가 학습할 수 있도록 하는 알고리즘과 기술을 개발하는 분야를 말한다. 가령, 기계 학습(machine learning)을 통해서 수신한 이 메일(E-mail)이 스팸 메일(Spam mail)인지 아닌지를 분류할 수 있도록 훈련할 수 있다.

[0004] 모바일 환경에서의 악성 코드의 유입은 빠르게 증가하는 추세이며 이에 따라 금전적 피해를 야기할 수 있는 모바일 환경 하에서의 악성 행위의 탐지와 예측이 중요해지고 있다.

[0005] 악성 코드 탐지 방법으로는 특허출원 제10-2015-0188697호를 참조하면, 외부에서 수신 받은 데이터의 악성 코드 여부를 검사하여 검사 결과를 서버에 전송하고, 서버의 블랙리스트 데이터와 접속권한 결정정보를 바탕으로 허용 여부를 결정한 후 사용자 모바일 단말기로 전송한다. 사용자 단말기에서는 서버로부터 수신된 데이터를 바탕으로 외부에서 수신 받은 데이터를 허용 또는 차단한다.

[0006] 또한, 특허출원 제10-2014-0102287호를 참조하면, 가상 머신 기반 애플리케이션 동적 분석 시 모바일 애플리케이션 행위에 대한 사용자 인지 회피도를 측정하는 방법에 관한 것으로서, 더욱 상세하게는 애플리케이션 실행에 대한 사용자 인지율에 따라 악성 행위를 탐지할 수 있는 가상 머신 기반 애플리케이션 동적 분석 시 모바일 애플리케이션 행위에 대한 사용자 인지 회피도를 측정하는 방법을 제안한다.

[0007] 또한, 특허출원 US8782792B1을 참조하면, 모바일 플랫폼 상에서 악성 코드를 탐지하기 위한 컴퓨터 구현 방법에 관한 것으로서, 에뮬레이션 정보를 이용하여 보안 서버를 포함하는 악성 코드 평가 결과를 수신하는 단계를 포함하여, 악성 코드 평가 결과를 기반으로 보안 조치를 수행하는 것 등이 있을 수 있으며, 이는 다양한 다른 방법 및 시스템, 컴퓨터에서 판독 가능한 매체 등에 반영될 수 있다.

[0008] 또한, 특허출원 제10-2011-0131093호를 참조하면, 모바일 악성 행위 어플리케이션의 API(Application Programming Interface) 목록 및 API 호출 순서를 패턴화하여 악성 행위 패턴을 생성하는 악성 행위 패턴 생성부 및 악성 행위 패턴에 기초하여 분석 대상 어플리케이션의 악성 행위 여부를 분석하는 악성 행위 분석부를 포함하는 장치를 제안한다.

[0009] 그러나 기존의 모바일 악성 코드 탐지 방법은 규칙 기반(Rule-based)이나 블랙리스트(Blacklist) 기반이기 때문에 알려진 공격에 대한 탐지만 가능하므로 알려지지 않은 새로운 모바일 공격에 대비할 수 있는 분류 기술이 요구된다.

선행기술문헌

특허문헌

[0011] (특허문헌 0001) 한국공개특허 제 10-2015-0188697 호

(특허문헌 0002) 한국공개특허 제 10-2014-0102287 호

(특허문헌 0003) 미국공개특허 제 US8782792B1 호

발명의 내용

해결하려는 과제

[0012] 이에, 본 발명의 기술적 과제는 이러한 점에서 착안된 것으로 본 발명의 목적은, 알려지지 않은 새로운 모바일 악성 코드의 공격에 대비하기 위해 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치 및 방법, 이 방법을 수행하기 위한 기록 매체를 제공하는 것이다.

[0013] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0015] 상기한 본 발명의 목적을 실현하기 위한 일 실시 예에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치에 있어서, 모바일 악성 코드 데이터에 대해 정적 분석 및 가상 환경 하에서 동적 분석을 수행한 결과에 대해 기존 모바일 악성 코드에서 활용된 블랙 리스트(Black List)를 이용하여 악성 코드의 특성을 도출한 후, 상기 도출한 특성들 중에서 모바일 악성 코드 데이터와 관련성이 높은 특성을 선정하는 도출부; 상기 분석부에서 선정된 특성들을 이용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류하는 분류부; 상기 분류된 악성 행위에 대해 자산(Asset Value), 위협(Threat) 및 취약성(Vulnerability)을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출하는 산출부; 및 상기 산출부의 결과

에 대해 모바일 악성 코드 탐지과정의 효율을 검증하고, 상기 검증 결과를 데이터베이스에 저장하는 검증부;를 포함한다.

[0016] 본 발명의 실시 예에서, 기준이 다른 조합 가능한 모든 모바일 데이터 셋(set)에 대한 상기 검증부의 검증결과를 기초로, 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정하는 결정부;를 더 포함할 수 있다.

[0017] 본 발명의 실시 예에서, 상기 산출부의 자산(Asset Value)은 악성 코드가 실행할 수 있는 도메인의 중요도로 침해 지표(IOC)에서 정의하고 있는 공격 대상인 사용자(user), 애플리케이션(application) 및 시스템(system) 중 적어도 하나를 포함할 수 있다.

[0018] 본 발명의 실시 예에서, 상기 산출부의 위협(Threat)은 기계학습으로 가중치가 부여된 악성 코드 행위 정보로 자산에 대해 발생 가능한 공격자로부터의 설치(Installation), 활성화(Activation), 악성 페이로드(Malicious Payloads) 및 오버 뷰(Over view) 중 적어도 하나를 포함할 수 있다.

[0019] 본 발명의 실시 예에서, 상기 산출부의 취약점(Vulnerability)은 자산의 구체적 행위에 대한 분류 정보로, 자산에서 분류한 침해 지표(IOC)의 기준들에 대한 세부 항목인 쿠키(cookie) 정보, 이-메일(E-mail) 정보 및 시스템(system) 정보 중 적어도 하나를 포함할 수 있다.

[0020] 본 발명의 실시 예에서, 상기 위험도에 따라 비율, 색상 및 도표 중 적어도 어느 하나로 표현하는 시각화부;를 더 포함할 수 있다.

[0021] 상기한 본 발명의 목적을 실현하기 위한 일 실시 예에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 방법에 있어서, 모바일 악성 코드 데이터에 대해 정적 분석 및 가상 환경 하에서 동적 분석을 수행한 결과에 대해 기존 모바일 악성 코드에서 활용된 블랙 리스트(Black List)를 이용하여 악성 코드의 특성을 도출한 후, 상기 도출한 특성들 중에서 모바일 악성 코드 데이터와 관련성이 높은 특성을 선정하는 단계; 선정된 특성들을 이용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류하는 단계; 상기 분류된 악성 행위에 대해 자산(Asset Value), 위협(Threat) 및 취약성(Vulnerability)을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출하는 단계; 및 상기 산출 결과에 대해 모바일 악성 코드 탐지과정의 효율을 검증하고, 상기 검증 결과를 데이터베이스에 저장하는 단계;를 포함한다.

[0022] 본 발명의 실시 예에서, 기준이 다른 조합 가능한 모든 모바일 데이터 셋(set)에 대한 상기 검증부의 검증결과를 기초로, 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정하는 단계;를 더 포함할 수 있다.

[0023] 본 발명의 실시 예에서, 상기 위험도에 따라 비율, 색상 및 도표 중 적어도 어느 하나로 표현하는 단계;를 더 포함할 수 있다.

[0024] 상기한 본 발명의 목적을 실현하기 위한 다른 실시 예에 따른 컴퓨터로 판독 가능한 저장 매체에는, 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 방법을 실행하기 위한 컴퓨터 프로그램이 기록되어 있다.

발명의 효과

[0026] 상술한 본 발명의 일 측면에 따르면, 모바일 운영체재에서의 데이터의 특성을 반영하여 악성 코드를 탐지하며, 알려지지 않은 새로운 모바일 악성 코드인 경우 악성 행위의 유무를 판단할 수 없는 잠재된 악성 코드의 탐지를 할 수 있는 유리한 효과가 있다.

[0027] 또한, 조합 가능한 모든 데이터 셋과 기준에 대한 검증으로 탐지율이 가장 높은 조합을 탐지 프로세스로 결정할 수 있어 이후에는 보다 빠르고 정확한 탐지를 할 수 있는 효과가 있다.

[0028] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0030] 도 1은 본 발명의 일 실시 예에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치의 구성

이 도시된 블록도이다.

도 2는 본 발명에 따른 모바일 악성 코드의 자산에 대한 특성을 분류하는 일 예를 나타내는 도면이다.

도 3은 본 발명에 따른 모바일 악성 코드의 악성 행위에 대해 자산, 위협, 취약점의 수준에 따라 위험도를 산출하기 위해 분류한 일 예를 나타내는 도면이다.

도 4 내지 도 5는 본 발명에 따라 산출된 위험도를 표시하는 일 예를 나타내는 도면이다.

도 6은 본 발명의 일 실시 예에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 방법의 순서도이다.

도 7은 도 6의 측정 방법에서 모바일 데이터 셋에 대한 검증 프로세스 수행 과정(S100)을 세분화한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시 예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시 예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시 예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시 예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시 예로 구현될 수 있다. 또한, 각각의 개시된 실시 예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0032] 이하, 도면들을 참조하여 본 발명의 바람직한 실시 예들을 보다 상세하게 설명하기로 한다.

[0033] 도 1은 본 발명의 일 실시 예에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치의 구성이 도시된 블록도이다.

[0034] 도 1을 참조하면, 본 발명의 일 실시 예에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치(100)는 도출부(110), 분류부(120), 산출부(130) 및 검증부(140)를 포함할 수 있고, 결정부(150) 및 시각화부(160) 중 적어도 하나의 구성을 더 포함할 수 있다. 본 발명의 위험 관리 장치(100)는 별도의 단말이거나 또는 단말의 일부 모듈일 수 있다. 도 1에 도시된 도출부(110), 분류부(120), 산출부(130), 검증부(140), 결정부(150) 및 시각화부(160)의 구성은 통합 모듈로 형성되거나, 하나 이상의 모듈로 이루어질 수 있다. 그러나, 이와 반대로 각 구성은 별도의 모듈로 이루어질 수도 있다.

[0035] 본 발명의 위험 관리 장치(100)는 작업 기억 능력 측정을 수행하기 위한 소프트웨어(어플리케이션)가 설치되어 실행될 수 있으며, 도출부(110), 분류부(120), 산출부(130), 검증부(140), 결정부(150) 및 시각화부(160)의 구성은 장치(100)에서 실행되는 소프트웨어에 의해 제어될 수 있다.

[0036] 도출부(110)는 모바일 악성 코드 데이터에 대해 정적 분석 및 가상 환경 하에서 동적 분석을 수행하고, 수행 결과를 바탕으로 기존 모바일 악성 코드에서 활용된 침해 지표(IOC, Indicator Of Compromise) 등의 블랙 리스트(Black List)기반으로 하여 모바일 악성 코드의 특성을 도출해 낸다. 도출된 모바일 악성 코드 데이터에서 기존의 모바일 악성 코드와 관련성이 높은 특성을 선정한다.

[0037] 분류부(120)는 도출부(110)에 의해 선정된 특성들을 활용하여 모바일 데이터에 기계학습 알고리즘(machine learning algorithm)을 적용하여 악성 행위를 분류한다. 이에 따른 분류 방법은 도 2를 참조하여 후술하기로 한다.

[0038] 산출부(130)는 분류부(120)에 의해 분류된 악성 행위에 대해 자산(Asset Value), 위협(Threat) 및 취약성(Vulnerability)을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출한다. 이에 따른 산출 방법은 도 3을 참조하여 후술하기로 한다.

[0039] 자산(Asset Value)은 악성 코드가 실행할 수 있는 도메인의 중요도를 의미하고, 분류 방법은 침해 지표(IOC)에서 정의하고 있는 공격 대상에 따라 크게 사용자(User), 애플리케이션(Application) 및 시스템(System)으로 구분할 수 있다.

[0040] 이 중 애플리케이션(Application)은 인터넷 주소(URL, Uniform Resource Locator), 이-메일 서비스(E-mail

Service) 및 파일 다운로드(File Download) 등을 의미하고, 시스템(System)은 네트워크(Network), 드라이버(Driver), 레지스트리(Registry), 프로세스(Process), 파일(File) 및 디스크(Disk) 등을 의미한다.

[0041] 위협(Threat)은 기계학습으로 가중치가 부여 된 악성 코드 행위 정보를 의미하고, 분류 방법은 자산에 대해 발생 가능한 공격자로부터의 위협을 설치(Installation), 활성화(Activation), 악성 페이로드(Malicious Payload) 및 오버 뷰(Over View) 등의 행위에 따라 구분할 수 있다.

[0042] 설치(Installation)는 특정 프로그램을 설치하는 방식으로 자산에 위협을 발생시키며, 리패키징(Repackaging), 업데이트(Update), 드라이브-바이-다운로드(Drive-by-Download) 및 독립형 프로그램(Standalone) 등을 의미한다.

[0043] 활성화(Activation)는 미리 설치된 특정 프로그램의 기능을 활성화하는 방식으로 자산에 위협을 발생시키며, 문자 메시지(SMS, Short Message Service), USB(Universal Serial Bus, 배터리(BAT, Battery), 시스템(SYS, System) 및 부트(BOOT) 등을 의미한다.

[0044] 악성 페이로드(Malicious Payloads)는 사용자가 주로 이용하는 서비스와 관련된 악성행위를 통해 자산에 위협을 발생시키며, 분류 방법은 권한 상승(Privilege Escalation), 원격 제어(Remote Control), 과금 결제(Financial Charges) 및 개인정보 탈취(Personal Information Stealing) 등으로 구분된다.

[0045] 이 중 권한 상승(Privilege Escalation)은 익스플로잇(Exploit), 암호화(Encrypted) 등을 의미하고, 원격 제어(Remote Control)는 네트워크(Network), 문자 메시지(SMS, short message service) 등의 의미한다. 과금 결제(Financial Charges)는 전화 통화, 문자 메시지를 이용하고, 개인정보 탈취(Personal Information Stealing) 문자 메시지, 전화번호 등을 이용한다.

[0046] 오버 뷰(Over view)는 특정 단말기 수준 이상의 네트워크, 시스템 등에 대한 악성행위를 통해 자산에 위협을 발생시키며, 사용자 계정(User Account), 암호화(Encrypted), 내장된 파일(RATC, Rage Against The Cage)을 포함하는 루트 익스플로잇(Root Exploit), 명령 및 제어(Command & Control) 및 악성 컴포넌트(Malicious Component) 등으로 구분된다.

[0047] 취약점(Vulnerability)에는 자산의 구체적 행위에 대한 분류 정보들로 자산에서 분류한 침해 지표의 기준들에 대한 일어날 수 있는 약 500개의 모든 행위의 경우의 수를 기준으로 세부 항목을 선정한다.

[0048] 예를 들어 쿠키(Cookie)는 히스토리 탐색기 이름, 히스토리 탐색기 버전, 히스토리 쿠키 이름, 히스토리 파일명 등을 의미하고, 이-메일(E-mail)은 첨부파일 정보, 첨부파일의 전자 우편 표준(MIME), 참조, 발신자, 수신자 주소(IP) 정보 등을 의미하며, 시스템(system)은 매체 접근 제어 일련번호(MAC address), 바이오스 날짜(BIOS Date), 바이오스 버전(BIOS Version), 네트워크 어댑터(Network Adaptor), 네트워크 주소(Network internet protocol address) 정보 등을 의미한다.

[0049] 예를 들어 DroidKungFu는 악성 코드를 포함하도록 불법 복제되어 트로이 목마가 숨겨진 채 다시 패키지(repackage)된 애플리케이션 형식의 안드로이드 악성 코드로 ① 루트 익스플로잇을 활용하여 감염된 장비에 대한 루트 액세스 권한을 사용자 몰래 획득하고, ② 루트 권한을 얻은 후, 장비 정보(IMEI 번호, 장비 모델, 안드로이드 버전)를 수집한 후, ③ 장비 정보를 수집한 후에는 사용자의 동의 없이 백그라운드에서 추가 패키지를 설치한다. ④ 추가 패키지는 감염된 장비를 봇(bot)으로 바꾸는 명령과 지시를 수신하기 위해 원격 서버에 연결하는 백 도어(back door)이다.

[0050] 도 2는 본 발명에 따른 모바일 악성 코드의 자산에 대한 특성을 분류하는 일부를 나타내는 도면이다.

[0051] 도 2를 참조하면 선정된 모바일 악성 코드 특성이 ① 리패키징(repackaging), ② 권한 상승(Privilege Escalation), ③ 설치(Installation), ④ 백 도어(Back door)가 되므로 도 2에 있어서는 DroidKungFu행에 설치(Installation) - 리패키징(Repackaging)으로 분류가 된다.

[0052] 도 3은 본 발명에 따른 모바일 악성 코드의 악성 행위에 대해 자산, 위협, 취약점의 수준에 따라 위험도를 산출하기 위해 분류한 일 예를 나타내는 도면이다.

[0053] 분석 결과 도출된 특성으로부터 분류된 악성 행위가 모바일 장치의 네트워크 서브넷(Network Subnet)을 매우 자주 공격하는 악성 코드 A인 경우에 위험도 산출하는 경우를 예를 들어 본다.

[0054] ① 악성 코드A는 네트워크 서브넷(Network Subnet)은 시스템(system)에 포함되므로 높은 위험도를 가지므로 자산 수준(Asset Value)를 Very High로 선정된다.

[0055] ② 악성 코드A는 매우 자주 식별되므로 위협 수준(Threat)을 High로 선정된다.

[0056] ③ 네트워크 서브넷(Network Subnet)의 경우 모바일 장치가 사용하는 IP(Internet Protocol)중 상대적으로 중요도가 낮으므로 취약점(Vulnerability)은 L(Low)로 선정된다.

[0057] ④ 자산 수준(Asset Value), 위협 수준(Threat), 취약점(Vulnerability)세 가지 정보를 나타내는 도 3에 따르면 6의 위험도가 산출된다.

[0058] 검증부(140)는 도출부(110), 분류부(120) 및 산출부(130)에서 작업을 수행하는데 소모된 시간, 사용된 리소스, 탐지율 등을 고려하여 모바일 악성 코드 탐지과정의 효율을 검증하고, 데이터베이스에 저장한다.

[0059] 결정부(150)는 조합 가능한 모든 모바일 데이터 셋(set)과 기준들에 대한 상기 검증부(140)의 검증결과를 기초로, 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정한다.

[0060] 시각화부(160)는 자산(Asset Value), 위협 수준(Threat) 및 취약점(Vulnerability)을 모바일 악성 코드의 위험군 분류를 위한 위험관리 방법론 중 위험도는 직관적으로 인식할 수 있도록 비율에 따른 분류, 색상에 따른 분류 및 도표 등으로 나타낸다. 표시 방법은 도 4 내지 도 5를 참조하여 상세히 설명하기로 한다.

[0061] 도 4 내지 도 5는 본 발명에 따라 산출된 위험도를 표시하는 일 예를 나타내는 도면이다.

[0062] 도 4를 참조하면 위협 수준(Threat)와 취약점(Vulnerability)만을 대상으로 하여 색상에 의한 위험도 분류를 나타내고, 각 위험도에 따라 지정된 색상을 보여주어 종합적인 위험성을 직관적으로 인식할 수 있게 한다. 앞서 산출된 위험도가 6인 경우, 위협 수준(TEF, Threat)이 High이고, 취약점(Vulnerability)이 Low이므로 M(Moderate)으로 위험성을 알리게 된다.

[0063] 도 5를 참조하면 탐지율에 의한 위험도 분류를 표시하고 있다. 탐지율이 40%인 경우 30% ~ 70% 범위에 속하므로 M(Moderate)이 되고, 탐지율이 87%인 경우에는 70% ~ 90% 범위에 속하므로 H(High)로 위험성을 알리게 된다.

[0064] 도 6는 본 발명의 일 실시 예에 따른 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 방법의 순서도이고, 도 7은 도 6의 측정 방법에서 모바일 데이터 셋에 대한 검증 프로세스 수행 과정(S100)을 세분화한 순서도이다.

[0065] 도 6과 7을 참조하면, 모바일 악성 코드 데이터 셋에 대해 탐지 과정의 효율을 검증하기 위한 프로세스(S100)이며, 검증 과정은 분석 및 특성 도출(S110) - 특성 선정(S120) - 행위 분류(S130) - 위험도 산출(S140) - 효율 검증(S150)의 단계로 구성된다.

[0066] 분석 과정 및 특성 도출 단계(S110)는 모바일 악성 코드 데이터 셋에 대해 정적 분석 및 가상 환경하에서 동적 분석을 수행하고, 분석 결과를 바탕으로 기존 모바일 악성 코드에서 도출된 침해 지표(IOC, Indicator Of Compromise) 등의 블랙 리스트(Black List)기반으로 하여 모바일 악성 코드의 특성을 도출해 낸다(S110). 도출된 모바일 악성 코드 데이터에서 기존의 모바일 악성 코드와 관련성이 높은 특성을 선정하고(S120), 이 때 선정된 특성들을 활용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류한다(S130).

[0067] 상기 분류된 악성 행위에 대해 자산(Asset Value), 위협(Threat) 및 취약성(Vulnerability)을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출하고(S140), 산출 결과를 기초로 일련의 작업을 수행하는데 소모된 시간, 사용된 리소스, 탐지율 등을 고려하여 모바일 악성 코드 탐지과정의 효율을 검증하고, 데이터베이스에 저장한다(S150).

[0068] 도 7을 참조하면, 검증 프로세스 수행 과정(S100)은 조합 가능한 모든 모바일 데이터 셋(set)과 기준들에 대해 수행하며(S200), 모든 검증 결과를 기초로 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정한다(S300).

[0069] 마지막으로, 자산(Asset Value), 위협 수준(Threat) 및 취약점(Vulnerability)을 모바일 악성 코드의 위험군 분류를 위한 위험관리 방법론 중 위험도는 직관적으로 인식할 수 있도록 비율에 따른 분류, 색상에 따른 분류 및 도표 등으로 나타낸다(S400).

[0070] 이와 같은 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 방법은, 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구

조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0071] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거니와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0072] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CDROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0073] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0074] 이상에서는 실시 예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0076] 100: 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치

110: 도출부

120: 분류부

130: 산출부

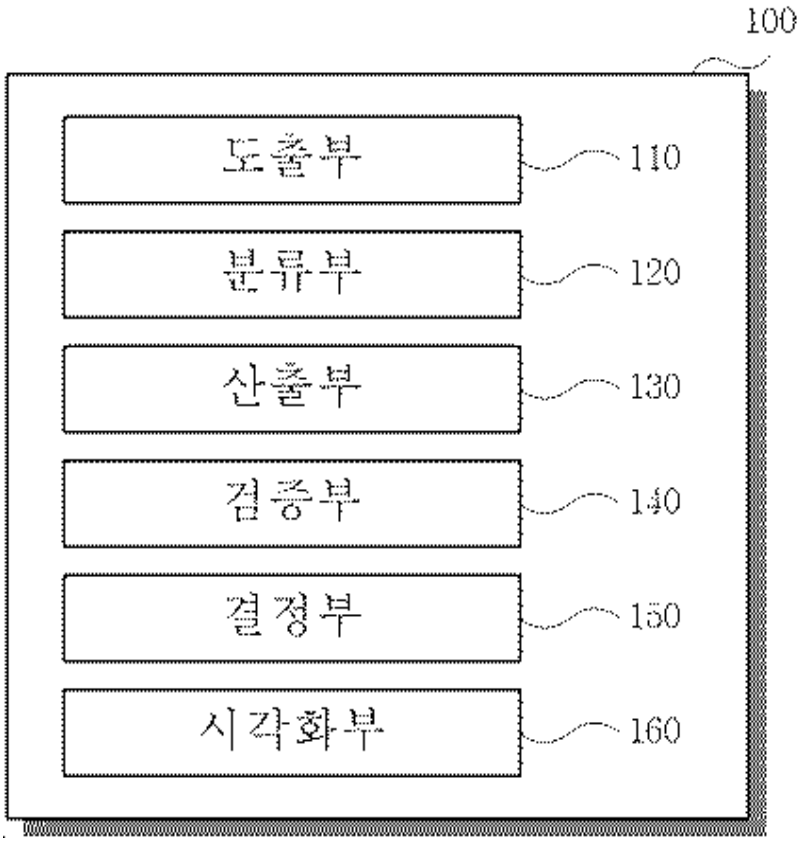
140: 검증부

150: 결정부

160: 시각화부

도면

도면1



도면2

항목	Installation				Activation								
	Repackaging	Update	ive-byDownlo	Standalone	BOOT	SMS	NET	CALL	USB	PKG	BATT	SYS	MAIN
악성코드 이름(예시)													
AnserverBot													
Asroot													
BaseBridge													
BeanBot													
BgServ													
ConPirate													
Crusewin													
DogWars													
DroidCoupon													
DroidDeluxe													
DroidDream													
DroidDreamLight													
DroidKungFu1													
DroidKungFu2													

도면3

① Asset Value (자산 수준)	② Treat (위협 수준)								
	Low			Medium			**High**		
Very Low	0	1	2	1	2	3	2	3	4
Low	1	2	3	2	3	4	3	4	5
Medium	2	3	4	3	4	5	4	5	6
High	3	4	5	4	5	6	5	6	7
Very High	4	5	6	5	6	7	**6**	7	8
	L	M	H	L	M	H	**L**	M	H
	③ Vulnerability (취약점)								

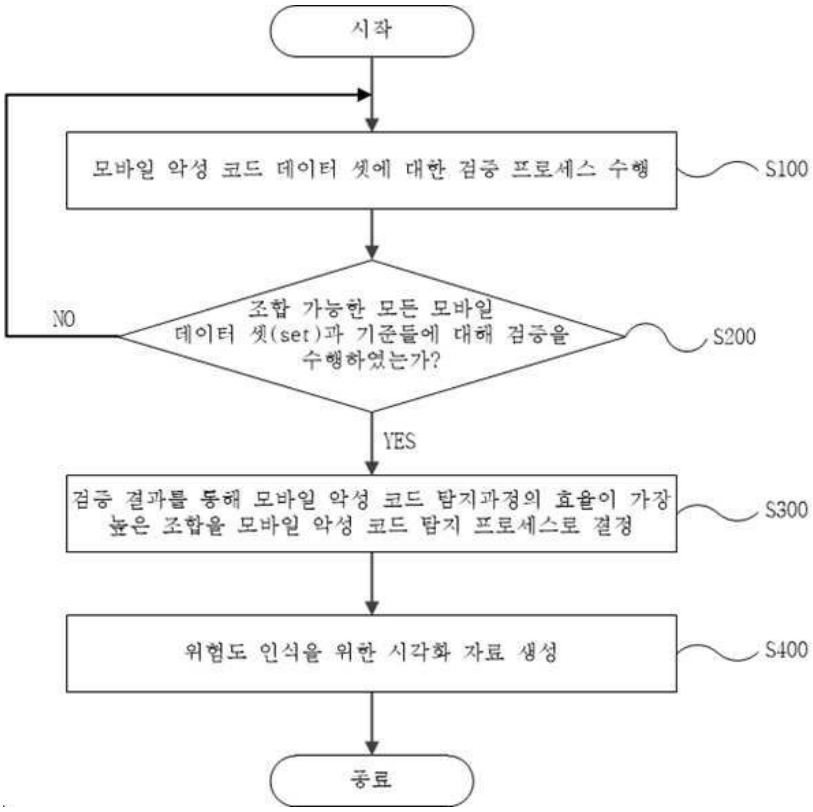
도면4

TEF	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
Loss Event Frequency		VL	L	M	H	VH
		Vulnerability				

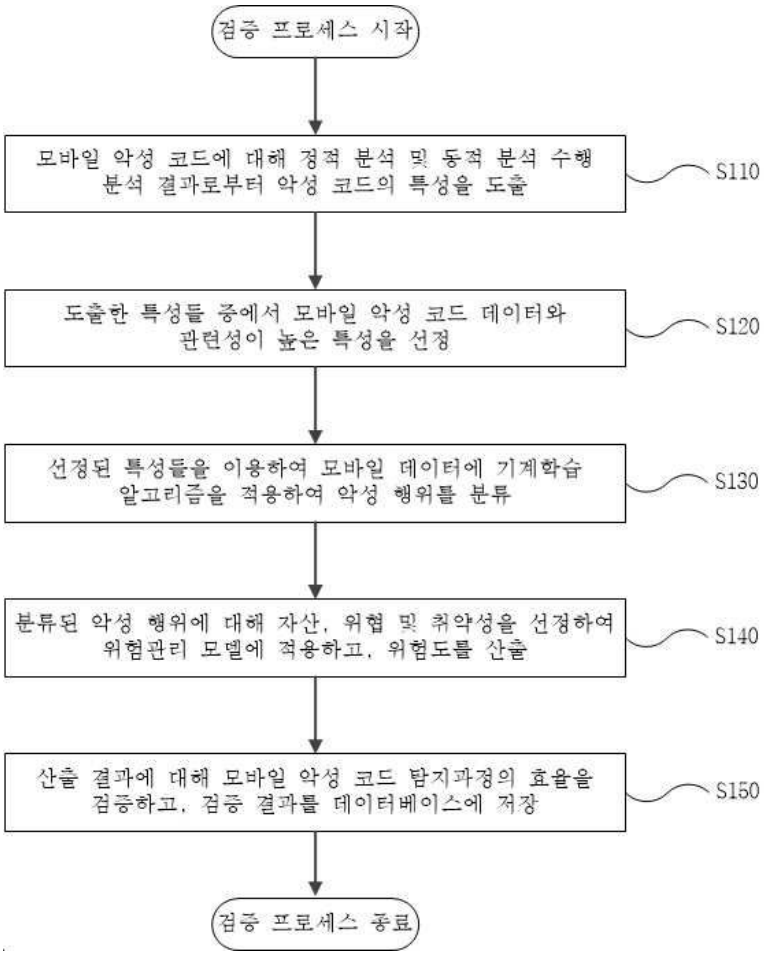
도면5

Rating	Range Low End	Range High End
Very High (VH)	90%	100%
High (H)	70%	90%
Moderate (M)	30%	70%
Low (L)	10%	30%
Very Low (VL)	0%	10%

도면6


시작
모바일 악성 코드 데이터 셋에 대한 검증 프로세스 수행
S100
조합 가능한 모든 모바일 데이터 셋(set)과 기준들에 대해 검증을 수행하였는가?
S200
NO
YES
검증 결과를 통해 모바일 악성 코드 탐지과정의 효율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정
S300
위험도 인식을 위한 시각화 자료 생성
S400
종료

도면7


검증 프로세스 시작
모바일 악성 코드에 대해 정적 분석 및 동적 분석 수행
분석 결과로부터 악성 코드의 특성을 도출
S110
도출한 특성들 중에서 모바일 악성 코드 데이터와
관련성이 높은 특성을 선정
S120
선정된 특성들을 이용하여 모바일 데이터에 기계학습
알고리즘을 적용하여 악성 행위를 분류
S130
분류된 악성 행위에 대해 자산, 위협 및 취약성을 선정하여
위험관리 모델에 적용하고, 위험도를 산출
S140
산출 결과에 대해 모바일 악성 코드 탐지과정의 효율을
검증하고, 검증 결과를 데이터베이스에 저장
S150
검증 프로세스 종료