(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년10월21일
(11) 등록번호 10-2017810
(24) 등록일자 2019년08월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) *G06F 11/30* (2006.01)
(21) 출원번호 10-2013-0043087
(22) 출원일자 2013년04월18일
심사청구일자 2018년01월23일
(65) 공개번호 10-2013-0117728
(43) 공개일자 2013년10월28일
(30) 우선권주장
61/625,700 2012년04월18일 미국(US)
(56) 선행기술조사문헌
US20090013407 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
짐페리엄 리미티드
이스라엘 텔아비브 메나헴 베긴 스트리트 23
(72) 발명자
아브라함 이츠하크
이스라엘 40300 크파르 요나 하라케펫 스트리트 25
카르타 야니브
이스라엘 52462 라메트-간 벤 호른 1/7
(74) 대리인
조의제

전체 청구항 수 : 총 24 항 심사관 : 문남두

(54) 발명의 명칭 **모바일 기기용 침입방지장치 및 방법**

(57) 요 약

모바일 컴퓨팅 플랫폼으로 기능하는 기업 사용자들의 말단 기기상에 위치한 파일 속으로의 해킹을 방지하도록 침입방지 시스템을 제공하기 위한 방법을 개시한다. 이 방법은 다수의 수신된 네트워크 패킷들의 각각을 위하여 저레벨 네트워크 패킷들을 필터링하고, 수신된 패킷들을 조사처리모듈로 오프로딩하며, 그리고 헤더 및 상기 수신된 패킷들의 각각의 패턴 중 적어도 하나에 기초된 의심스러운 패킷들을 표시하는 것을 포함한다. 이 방법은 또한 기기 및 네트워크의 보호를 보장하도록 시스템에 의해 방지대책을 취하고, 의심스러운 트래픽을 차단하도록 시스템에 의해 능동적 조치들을 취하며, 그리고 의심스러운 트래픽을 감지할 때 시스템에 의해 현재 접속을 끊는 것을 포함한다.

대 표 도 - 도1

명 세 서

청구범위

청구항 1

무선통신 네트워크에서 복수 개의 네트워크 패킷을 수신하는 통신기기상의 네트워크 공격을 방지하기 위한 컴퓨터화된 시스템에 있어서,

a) 실행 가능한 모듈들을 저장하는 비일시적 컴퓨터 판독가능한 저장매체, 상기 비일시적 컴퓨터 판독가능한 저장매체는,

상기 수신된 네트워크 패킷들의 결정론적 패턴 및 귀납적 패턴을 식별하도록 구성된 보안 인터페이스 모듈;

식별된 상기 결정론적 패턴 및 귀납적 패턴에 기초하여 상기 수신된 네트워크 패킷들을 필터링하고, 필터링된 패킷들을 출력하도록 구성된 패킷필터모듈;

상기 필터링된 네트워크 패킷들을 검사하고 상기 검사의 응답에 따라 상기 패킷필터모듈을 검사하고, 수신된 패킷들을 저장된 필터링 설정에 기초하여 의심스럽거나 정상적인 패킷으로 분류하도록 구성된 패턴감지기(Pattern Detector)모듈; 및

상기 필터링된 패킷들을 수신하고, 정상적으로 분류된 상기 패킷들의 패턴을 검출하고, 의심스러운 것으로 분류된 상기 패킷들을 더 검사하도록 구성된 커널 확장 모듈(kernel extension module)을 포함하며,

b) 상기 저장된 모듈들을 실행하도록 구성된 프로세서를 포함하는 컴퓨터화된 시스템.

청구항 2

제 1항에 있어서, 서드파티(3rd party) 애플리케이션에 의해 사용되도록 구성된 zCore Application Program Interface (API) 모듈을 더 포함하는 컴퓨터화된 시스템.

청구항 3

제 2항에 있어서, 서드파티 애플리케이션은 외부 파트너 애플리케이션 또는 개발자 애플리케이션인 컴퓨터화된 시스템.

청구항 4

제 1항에 있어서, 상기 패킷필터모듈에 통신 가능하게 결합된 서드파티(3rd party) 펌웨어 모듈을 더 포함하고, 상기 서드파티(3rd party) 펌웨어 모듈은 상기 네트워크 패킷들을 수신하도록 구성되는 것을 특징으로하는 시스템.

청구항 5

제 4항에 있어서, 상기 서드파티 펌웨어 모듈은 WiFi 펌웨어 모듈인 컴퓨터화된 시스템.

청구항 6

제 2항에 있어서, 상기 서드파티 애플리케이션은 보안 솔루션 벤더가 침입에 대한 통지를 수신하거나 새로운 침입이벤트를 등록할 수 있도록 구성된 컴퓨터화된 시스템.

청구항 7

제 1항에 있어서, 상기 필터링 설정은 패턴 매치 핸들링(pattern match handling), 패턴 조건, 패턴 제약(Cosntraints)으로 이루어진 그룹으로부터 선택되는 컴퓨터화된 시스템.

청구항 8

삭제

청구항 9

삭제

청구항 10

제 1항에 있어서, 공격을 나타내는 분류된 패킷의 패턴을 검출하는 것에 응답하여 취해질 하나 이상의 동작을 정의하는 위협 응답 모듈(threat response module)을 더 포함하는 컴퓨터화된 시스템.

청구항 11

제 10항에 있어서, 상기 위협 응답 모듈은 하나 이상의 통신기기프로토콜 상태 및 각 프로토콜 상태에 대한 확률을 이상(anomaly)과 연관시키도록 구성된 것을 특징으로 하는 컴퓨터화된 시스템.

청구항 12

삭제

청구항 13

적어도 하나의 프로세서를 구비하는 통신 기기상에 네트워크 공격을 방지하기 위한 방법에 있어서,

a. 상기 통신기기에서 복수의 네트워크패킷들을 수신하는 단계;

b. 상기 통신기기에서 수신된 패킷의 식별된 결정론적 패턴 및 귀납적 패턴에 기초하여 수신된 패킷을 필터링하고, 필터링된 패킷을 출력하는 단계;

c. 저장된 필터링 설정 규칙에 따라 필터링 패킷들을 "정상" 또는 "의심스러운" 패킷으로 분류하는 단계;

e. "정상"으로 분류된 패킷의 패턴을 검출하는 단계; 및

"의심스러운" 것으로 분류된 패킷을 더 검사하는 단계를 포함하는 통신 기기상에 네트워크 공격을 방지하기 위한 방법.

청구항 14

제 13항에 있어서, 상기 네트워크 패킷들은 상기 통신기기 상에 저장된 서드파티 펌웨어에 의해 수신되는 것을 특징으로 하는 방법.

청구항 15

제 14항에 있어서, 상기 서드파티 펌웨어는 WiFi 펌웨어인 방법.

청구항 16

제 13 항에있어서, 공격을 나타내는 분류된 패킷의 패턴을 검출하는 것에 응답하여 하나 이상의 동작을 취하는 단계를 더 포함하며, 상기 동작은 하나 이상의 통신기기프로토콜 상태 및 각각의 통신기기프로토콜 상태를 나타내기 위해 구성된 위협 응답 모듈(threat response module)과 각 프로토콜 상태가 이상(abnomaly)과 연관될 확률에 의해 특정되는 방법.

청구항 17

통신기기에 있어서,

실행 가능한 모듈들을 저장하는 비일시적(non-transitory) 컴퓨터 판독가능한 저장매체, 상기 비일시적 컴퓨터 판독가능한 저장매체는,

a) 복수 개의 네트워크 패킷들을 수신하도록 구성된 WiFi 펌웨어모듈;

b) 식별된 결정론적 패턴 및 귀납적 패턴에 기초하여 상기 수신된 네트워크 패킷들을 필터링하고, 필터링된 패킷들을 출력하도록 구성된 패킷필터모듈;

c) 저장된 필터링 설정에 따라 수신된 네트워크 패킷들의 패턴을 검출하도록 구성된 패턴감지기 모듈; 및

d) 상기 검출된 패턴이 하나의 공격을 나타내는 것에 응답하여 하나 이상의 교정 조치(corrective actions)를 취하도록 구성된 액션 모듈(action module)을 포함하고,

상기 저장된 모듈들을 실행하도록 구성된 프로세서를 포함하는 통신기기.

청구항 18

제 17항에 있어서, 상기 통신기기는 모바일폰, 스마트폰, 랩톱 및 태블릿을 포함하는 것을 특징으로 하는 통신기기.

청구항 19

제 17항에 있어서, 상기 통신기기는 호스트-기초된 및/또는 네트워크-기초인 것을 특징으로 하는 통신기기.

청구항 20

삭제

청구항 21

삭제

청구항 22

통신 네트워크에 정보를 전송하는 모바일 기기에 대한 공격을 방지하기 위한 침입방지시스템을 제공하기 위한 방법에 있어서,

복수의 네트워크 패킷을 수신하는 단계;

수신된 네트워크 패킷의 식별된 패턴에 기초하여 수신된 네트워크 패킷을 프로세서에 의해 필터링하는 단계;

상기 필터링된 네트워크 패킷의 임계 퍼센트보다 작은 것을 포함하는 상기 네트워크 패킷의 서브셋(subset)을 분류하도록 구성된 검사 처리 모듈(inspecting processing module)에 상기 필터링된 네트워크 패킷을 제공하는 단계;

상기 검사 처리 모듈(inspecting processing module)을 통해 상기 네트워크 패킷의 서브셋(subset)과 연관된 헤더 및 상기 네트워크 패킷의 서브셋(subset)의 패턴 중 적어도 하나에 기초하여 상기 네트워크 패킷의 서브셋(subset)을 분류하는 단계; 및

네트워크 패킷의 분류된 서브셋에 기초하여 상기 모바일 기기에서 상기 공격을 완화 또는 방지하기 위하여 하나 이상의 예방 조치를 취하는 단계를 포함하는 방법.

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

제 22항에 있어서, 상기 모바일 기기는 모바일 폰, 스마트폰, 랩톱 또는 태블릿 컴퓨터 중 하나를 포함하는 방법.

청구항 27

제 22항에 있어서, 침입방지시스템은 호스트-기초된 및/또는 네트워크-기초된 방법.

청구항 28

제 22항에 있어서, 상기 공격은 인증되지 않은 특권 상승(unauthorized privilege escalation)을 나타내는 분류된 내트워크 패킷의 패턴에 응답하여 검출되는 방법.

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

제 22항에 있어서, 침입방지시스템은 적어도 패킷필터, WiFi 소프트웨어 저장부 및 패턴인식기를 포함하는 방법.

청구항 33

제 32항에 있어서, 패턴인식기는 공격들을 인지하고 기록하기 위해 숙련된 방법.

청구항 34

제 22항에 있어서, 상기 하나 이상의 예방 조치는 의심스러운 트래픽을 차단하는 것을 포함하는 방법.

청구항 35

제 32항에 있어서, 상기 하나 이상의 예방 조치는 상기 모바일 기기를 상기 통신 네트워크로부터 접속을 끊는 단계를 포함하는 방법.

청구항 36

삭제

발명의 설명

기 술 분 야

[0001] 개시된 발명은 일반적으로 모바일 애플리케이션 보안분야에 관한 것으로서, 특히 모바일 처리 기기상에 효과적으로 작동할 수 있는 침입방지시스템에 관한 것이다.

배 경 기 술

[0002] 통신 네트워크 보안 시스템들에 있어서 두 알려진 보안 모델이 있는데, 침입방지 및 침입감지이다. 침입방지는 전형적으로 능동적인 반면, 침입감지는 예를 들면 보고에 사용되고 수동적이다. 네트워크에 근거한 그리고 호스트에 근거한 것을 포함하는 여러 종류의 침입방지 시스템들이 있다.

[0003] 침입감지시스템들은 일정하게 네트워크 내를 흐르는 통신들을 모니터하고, 이것은 그들이 의심스러운 네트워크 통신을 보호하고 차단 또는 드롭하며, 뿐만 아니라 네트워크 관리자에게 경고를 발생한다. 의심스러운 트래픽(traffic)을 차단 또는 드롭하는 과정은 네트워크의 보안을 보장한다.

[0004] 스마트폰, 더욱 인기가 있어지는, 태블릿 등, 및 더 보편화되고 있는 공중 무선 네트워크들을 포함하는 이동통신기기 처리와 함께, 모바일 기기들을 위한 보안의 문제가 더 높은 관심이 되고 있다. 현재로, 모바일 기기들을 위한 침입감지 또는 침입방지 시스템은 가능하지 않다.

[0005] 모바일 기기들에 대한 이 솔루션 부족의 숨겨진 이유는 침입감지 및 방지 시스템들이 매우 자원 집약적 - 즉,

그들은 애플리케이션레벨 프로토콜의 복잡한 처리 뿐만 아니라 패킷검사 과정을 수행하기 위하여 CPU로부터 집약적 연산을 요구한다는 사실이다. 이것은 또한 모바일 기기들의 배터리를 소모하고 더 일을 복잡하게 한다.

[0006] 부가하여, 공격자들이 그들의 공격 및 기술을 끊임없이 향상시키고 있고, 보안 산업에 있어서 따라잡기 위하여 일정한 경쟁으로 일정하게 발전하고 있다. 보편화되고 있는 새로운 형태의 공격들 중 하나는, 공격자와 동일한 네트워크에 연결된 모르는 사용자로부터 사용자 정보, 사용자 계정, 개인 정보 등을 훔치기 위하여 핫스팟(hotspot)을 사용하는 것이다. 정보가 도난당한 사용자는 이 정보 도난을 완전히 의식하지 못하고 있다.

[0007] 예를 들면, 기업 이용자(이하, 사용자라고 칭함)는 인터넷에 연결된 자신의 모바일 기기로 모바일 네트워크내에 있다. 라우터(router)와 다른 장치들은 네트워크에 연결될 수 있다. 동일한 네트워크상의 누군가는 네트워크을 통해 자신의 모바일 기기를 공격하는 것을 시도할 수도 있다. 양 기기가 네트워크 데이터를 얻으므로, 공격 장치는 사용자의 장치를 볼 수 있다. 공격자는 동일한 네트워크에서 모바일 기기 또는 컴퓨터를 가질 수 있다. 공격자는 사용자에게 네트워크 데이터 패킷을 전송함으로써 고의적인 무언가를 하고자 시도한다.

[0008] 사용자의 기기는 공격이 있었다고 이해하기 위하여, 네트워크 데이터를 실행할 필요가 있다.

[0009] 그러므로, 모바일 기기에 대한 침입감지 및/또는 방지를 제공하는 이점이 있게 된다.

발명의 내용

해결하려는 과제

[0010] 개시된 발명은 침입방지 및 감지 시스템을 제공하며, 이는 (모바일폰, 스마트폰 또는 태블릿 또는 당해 기술분야에서 알려진 그러한 모바일 컴퓨팅 플랫폼과 같은) 모바일 컴퓨팅 통신플랫폼 및 기기들에 배치될 수 있다.

[0011] 본 발명은 네트워크에 기초하고 호스트에 기초한 솔루션을 결합한다,

[0012] 본 발명의 한 실시예에 있어서, 침입방지시스템은 그 처리 요구사항들이 전문화된 펌웨어에 의해 오프로드되는 것을 개시한다.

[0013] 본 발명의 다른 실시예에 있어서, 침입방지시스템은 기기 및 네트워크의 보호를 보장하기 위하여 예방조치를 취한다.

[0014] 본 발명의 바람직한 한 실시예에 있어서, 침입방지시스템은 의심스러운 트래픽(traffice)을 차단하기 위하여 능동적인 조치를 취한다.

[0015] 본 발명의 또 다른 바람직한 실시예에 있어서, 의심스러운 트래픽을 감지할 때 침입방지시스템은 현재의 연결을 중단한다.

[0016] 본 발명의 또 다른 바람직한 실시예에 있어서, 침입방지시스템은 인증 등에 사용되는 키(key)를 획득함으로써 애플리케이션레벨보안을 수신하도록 서드파티(3rd party) 애플리케이션용 프레임워크를 제공함에 의해 모바일 컴퓨팅장치의 보안을 향상시킨다.

과제의 해결 수단

[0017] 모바일 컴퓨팅 플랫폼으로서 기능하는 기업 사용자의 말단(endpoint) 기기에 배치된 화일의 해킹을 방지하기 위해 침입방지시스템을 제공하는 방법을 개시한다. 그 방법은 수신된 복수 개의 네트워크패킷들 각각에 대해 저레벨의 네트워크패킷을 필터링하고, 수신된 데이터를 검사처리모듈로 오프로드하고, 전술한 수신된 패킷들의 각각의 헤더 및 패턴 중 적어도 하나에 기초하여 의심스러운 패킷들을 표시하는 단계를 포함한다. 그 방법은 또한 장치와 네트워크의 보호를 보장하기 위해 시스템이 예방조치를 취하고, 의심스러운 트래픽을 차단하기 위하여 시스템이 능동적인 조치를 취하고, 의심스러운 트래픽을 감지할 경우에 시스템이 현재의 연결을 중단시키는 단계를 포함한다.

[0018] 본 발명은 일반적으로 기업용 모바일 시장, 특히 기업 말단 사용자에 속하는 장치들과 같이 보안 목적을 위해 사용된다. 이 침입방지 및 감지기술은 저가의 애플리케이션에 대한 일반적인 특권으로 운영될 수도 있고, 자신의 기기를 휴대하는(Bring Your Own Device; BYOD) 솔루션으로 구성된다. BYOD는 직원들이 자신이 소유한 모바일 기기(랩탑, 태플릿, 및 스마트폰)를 자신들의 직장에 가져와서, 특권이 부여된 회사정보 및 애플리케이션에 액세스하도록 자신들의 기기를 사용하는 것을 허용하는 정책을 의미한다.

[0019] 본 발명의 일 실시예는 패킷 검사를 오프로드함으로써 구성될 있고, 그래서 배터리전원, CPU, 메모리와 같은 자

원을 훔치지 못하게 된다. 본 발명은 패킷검사, 펌웨어, 말단 기기에 대한 제품의 구성(architecture), 및 어느 층이 실행되는 가에 관한 것이다.

[0020] 본 발명은 위험과 공격을 식별하고 방지한다. 위험은 예상하지 못하거나 인증되지 않은 특권 상승(privilege escalation) 또는 네트워킹 목차이상(anomaly)을 통해 그 자체가 나타날 수도 있다. 무수한 공격은 특권 상승에 이르게 되고, 이는 인증되지 않은 채 식별가능하고, 다른 것들은 미묘하다. 일부 특권 상승은 예상되는 행동으로서 식별되는 반면에, 다른 것들은 예상하지 못하거나 인증되지 않은 대로 식별될 수 있다. 공격의 가 부정적 판단(false negatives) 위험의 수를 증가시키지 않으면서 가 긍정적 판단(false positives) 위험 또는 공격을 방지하기 위하여, 본 발명은 네트워크에 기초한 행동 분석을 제공한다.

[0021] 위험과 공격에 관해 수집된 데이터가 충분한 경우에, 컨버전스(convergence)가 발생하고, 연속된 데이터를 생성하면서 자동적으로 새로운 로직 베이스를 생성하고, 이는 공격과 데이터와의 관계를 나타낸다. 데이터를 네트워크로부터 수신하고, 검사받지 않고 정상적으로 처리한 후에, 이는 운영시스템 변수에 영향을 미치기도 하지만, 결정론적인 방식으로 변수들에게 영향을 주지는 않는다, 즉, 특정한 변수가 일정한 배열을 가지고 또 다른 변수가 일정한 배열을 가지면, 공격이 존재한다는 압도적인 가능성이 있게 된다.

[0022] 본 발명의 실시예의 양태에 따르면, 무선 통신 네트워크에서 복수 개의 네트워크패킷들을 수신하는 통신 기기에 대한 네트워크 공격을 방지하기 위해 컴퓨터화된 시스템을 제공하는 것이고, 그 시스템은, 수신된 패킷들을 검사하고 수신된 패킷들을 필터링 설정에 따라 의심스럽거나 정상적인 패킷으로 표시하도록 구성된 패턴감지기(Pattern Detector) 모듈, 및 커널 레벨(kernel level)에서 패킷들을 필터링하고, 수신된 패킷들을 패턴감지기 모듈로 전송하도록 구성된 패킷필터모듈을 포함하는 컴퓨터 판독가능한 펌웨어; 및 애플리케이션 레벨에서 펌웨어 모듈로부터 패킷들을 수신하고, 표시된 패킷들의 패턴을 감지하고, 패킷들이 표시되지 않았다면, 다음의 더 낮은 소프트웨어층에서 패킷들을 더 검사하는 컴퓨터 판독가능한 커널확장모듈 구성을 포함한다.

[0023] 본 발명의 실시예에 따르면, 시스템은 서드파티 애플리케이션에 의해 사용되도록 구성된 zCore Application Program Interface (API)를 포함한다.

[0024] 본 발명의 실시예에 따르면, 서드파티 애플리케이션은 외부 파트너 애플리케이션 또는 개발자 애플리케이션이다. 본 발명의 실시예에 따르면, 시스템은 패킷들을 수신하도록 구성된 패킷필터에 연결된 서드파티 펌웨어를 포함한다.

[0025] 본 발명의 실시예에 따르면, 통신 기기상에 네트워크 공격을 방지하기 위한 방법이 제공하고, 그 방법은, 상기 통신기기에 저장되어 있는 컴퓨터화된 판독가능한 펌웨어모듈에서 네트워크패킷을 수신하는 단계; 상기 펌웨어 모듈에서 수신된 패킷을 패킷필터모듈로 필터링하는 단계; 필터링 설정 규칙에 따라 수신된 패킷들을 패턴감지기로 "정상" 또는 "의심스러운" 패킷으로 표시하는 단계; 다음 소프트웨어층에서 수신된 패킷을 컴퓨터화된 판독가능한 zCore 커널확장모듈로 오프로드하는 단계; 상기 zCore 커널확장모듈에 의해 표시된 패킷들의 패턴을 감지하는 단계; 및 정상 패킷들을 다음 소프트웨어층으로 오프로드하는 단계를 포함한다.

[0026] 본 발명의 실시예에 따르면, 통신기기를 제공하고, 그 통신기기는, 기기 컴퓨팅 플랫폼으로의 해킹을 방지하도록 배열된 컴퓨터 판독가능한 침입방지 펌웨어를 포함하고,

[0027] 펌웨어는 복수 개의 네트워크 패킷들을 수신하도록 구성된 WiFi 펌웨어모듈; 상기 수신된 패킷들을 필터링하도록 구성된 패킷필터모듈;

[0028] 필터링 설정 규칙에 따라 상기 수신된 패킷들의 상기 패턴을 감지하도록 구성된 패턴감지기 모듈; 및 상기 필터링 설정 규칙을 저장하도록 구성된 보안저장모듈을 포함한다.

[0029] 본 발명에서 다음 용어들을 명료하게 한정한다:

[0030] 용어 "펌웨어(firmware)"는 모바일 기기의 전자회로보드에 저장된 본 발명의 보안프로그램 및 솔루션을 의미한다. 펌웨어는, 예를 들면, 모바일 기기 하드웨어 (예를 들면, 칩)상에 "플러쉬(flushed)"되고, 추출되어 모바일 기기 칩 상에 플래시된 이후에, 표준 WiFi 펌웨어의 대체물로서 실행될 수도 있다.

[0031] 용어 "커널(kernel)", "커널/하드웨어" 및 "커널확장"은 기본 하드웨어를 처리하는 운영체계의 일부를 의미한다.

[0032] 용어 "zCore 커널확장"은 물리적인 기기(예를 들면, 모바일 기기), 또는 가상기기 (예를 들면, 어떤 환경에서도 실행할 수 있는 소프트웨어 모방 기기)인 zcore.ko 커널 목적(kernel object)을 가르킨다.

[0033] 용어 "zCore API"는 네트워크 이벤트 또는 위험에 대한 표시자를 수신하기 위한 의도로 된 서드파티 애플리케이션(예를 들면, 다른 밴더(vendor)에 의해 운영되는 보안 애플리케이션)용 API 인터페이스를 의미하고, 본 발명 보안프로그램 및 솔루션을 알려준다.

[0034] 용어 "서드파티 WiFi 펌웨어"는, 802.11 또는 무선통신 약자에 대한 약자 프로토콜(802.11a,b,c,d,e,f, 등)을 실행하는 펌웨어 기기 또는 칩을 의미한다.

[0035] 용어 "서드파티 애플리케이션"은 서드파티 파트너 또는 개발자와 같이 외부 당사자에 의해 실행될 수 있는 애플리케이션을 지칭한다. 예를 들면, "zCore API"는 다른 보안 솔루션 벤더(vendor)에게 통보를 통합하여 수신하고 새로운 이벤트를 등록하는 능력을 공급한다.

[0036] 용어 "행동 속성(behavior attributes)"은 일반적인 행동을 결정하기 위해 검사되는 운영체계의 속성, 또는 일반적인 랜덤 변수로서 간주될 수 있는 다른 속성을 의미한다.

[0037] "행동 속성"에 관련한 용어 "이상(anomalies)"은, 네트워크 패킷 매개변수와같은 매개변수간의 이례적인 상관관계가 감지되거나, 프로토콜 결함의 정상적인 행동이 오작동하는 경우에, 이상이 발생하고 데이터(예를 들면, 패킷으로) 및 데이터에 의해 영향을 받은 운영체계의 속성에 대해 보여질 수 있는 개요를 의미한다.

[0038] 용어 "zConsole"은 모바일 기기와 같은 기기 및 대응하는 위험 및 리스크 수준의 가시화 및 관리에 사용되는 관리콘솔을 나타낸다. zConsole은 말단 기기의 구성, 및 위험방지 및 완화를 가능하게 한다. zConsole은 예를 들면, 모바일 기기를 사용하여 클라우드(cloud)상에 또는 조직 비무장지대(DMZ)내에 배치될 수 있다.

[0039] "이벤트 통보"는 유익한 이벤트(사용법 이벤트) 또는 데이터에 관련된 위험을 의미한다.

[0040] "위험응답 매트릭스 (Threat Response Matrix)" 및 "위험응답 매트릭스 구성"은 다수의 위험 유형에 대한 다수의 응답 옵션을 포함하는 매트릭스를 의미한다. 예를 들면, 네트워크에 대해 Rn 응답으로부터 위험×1 응답(Ri)이 선택된다.

[0041] 응답의 중대성은 또한 중시될 수도 있고, 모바일 기기가 연결된 네트워크의 최근 히스토리에 관해 결정된 위험 수위 요인에 따라 적응될 수 있다.

[0042] 용어 "zIPS" 또는 "zDefender"는 기업 및/또는 최종 사용자에게 제공되는 본 발명의 침입방지시스템(IPS) 제품을 의미한다.

[0043] 다르게 정의되지 않는다면, 여기서 사용되는 모든 기술 및/또는 과학용어는 본 발명이 속하는 기술에서 통상의 지식을 가진 자가 보편적으로 이해하는 동일한 의미를 갖는다. 여기에 기재된 유사하거나 동등한 방법 및 재료가 실제에서 또는 발명의 실시예를 검사하는 데 사용될 수 있다고 하더라도, 전형적인 방법 및/또는 재료를 이하에서 기술한다. 충돌의 경우에, 정의를 포함하는 특허명세서가 조정을 할 것이다. 부가적으로, 재료, 방법 및 실시예들은 단지 기술적인 것이고, 필연적으로 한정하고자 하는 것은 아니다.

[0044] 발명의 실시예의 방법 및/또는 시스템의 실행은 선택된 임무를 수동적으로, 자동적으로 또는 그 결합으로 수행하거나 완료하는 것을 수반한다. 더우기, 발명의 방법 및/또는 시스템의 실시예의 실제 기계류 및 설비에 따라, 몇몇 선택된 임무가 하드웨어, 소프트웨어 또는 펌웨어 또는 운영체계를 사용하는 그들의 결합으로 실행될 수 있었다.

[0045] 예를 들면, 발명의 실시예에 따라 선택된 임무를 수행하는 하드웨어는 칩 또는 회로로서 실행될 수 있었다. 소프트웨어로서, 발명의 실시예에 따라 선택된 임무는 적절한 운영체계를 사용하는 컴퓨터에 의해 수행되는 여러 개의 소프트웨어 지시대로 실행될 수 있었다. 발명의 전형적인 실시예에 있어서, 여기에 기재된 방법 및/또는 시스템의 전형적인 실시예에 따른 하나 이상의 임무는 복수 개의 지시를 수행하는 컴퓨팅 플랫폼과 같은 데이터 프로세서에 의해 수행된다. 선택적으로, 데이터 프로세서는 지시 및/또는 데이터를 저장하는 휘발성 메모리 및/또는 지시 및/또는 데이터를 저장하는 비휘발성 저장장치, 예를 들면, 자기 하드디스크 및/또는 제거가능한 매체를 포함한다. 선택적으로, 네트워크 연결이 또한 제공된다. 키보드 또는 마우스와 같은 표시 및/또는 사용자 입력기기도 제공된다.

[0046] 발명의 보다 중요한 특징들은 후술되는 발명의 상세한 설명에서 보다 더 이해될 수 있도록 광범위하기 보다는 개략적으로 기재되었다. 추가적인 발명의 세부사항 및 이점들은 상세한 설명에 기재될 것이고, 부분적으로는 설명으로부터 이해하고, 발명의 실시에 의해 습득하게 될 것이다.

발명의 효과

[0047] 본 발명은 모바일 컴퓨팅 통신 플랫폼 및 기기 등에 배치될 수 있는 침입 방지 및 감지시스템을 제공한다. 이 시스템은 네트워크에 기초하고 호스트에 기초한 솔루션을 결합하고, 전문화된 펌웨어에 의해 오프로드될 수 있다. 이 시스템은 또한 기기 및 네트워크의 보호를 보장하기 위한 예방조치를 취할 수 있으며, 의심스러운 트래픽을 차단하기 위하여 능동적인 조치를 취할 수 있다.

도면의 간단한 설명

[0048] 도 1은 본 발명의 원리에 따라 구성된 펌웨어의 모듈구조를 나타내고,

도 2는 본 발명의 원리에 따라 구성된 소프트웨어 관점으로부터 시스템의 계층적 구조를 나타내고,

도 3a는 본 발명의 원리에 따라 구성된 리코나이산스(reconnaissance) 공격 또는 TCP 내의 "SYN" 공격 식별 브랜치의 전 및 후의 단계들에 대한 흐름도이고,

도 3b는 본 발명의 원리에 따라 구성된 이용 경우들의 확장도이고,

도 4는 본 발명의 원리에 따라 구성된 퍼지상태기계의 흐름도이고,

도 5a는 본 발명의 원리에 따라 구성된 대시보드용 콘솔의 스크린숏(screenshot)이고,

도 5b는 본 발명의 원리에 따라 구성된 기기관리용 콘솔의 스크린숏이고,

도 5c는 안드로이드 기기상의 MITM 공격을 감지하는 zIPS의 스크린숏이고,

도 6은 본 발명의 원리에 따라 구성된 예시적 하드웨어 구성의 흐름도이고,

도 7a는 본 발명의 원리에 따라 구성된 오프로딩 조사처리모듈의 흐름도이고, 그리고

도 7b는 본 발명의 원리에 따라 구성된 오프로드된 패킷조작의 상세도에 대한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0049] 본 발명을 이해하고 실제에 있어서 어떻게 실행될 수 있는지를 알기 위하여, 도면들을 참조하여 이 예에 제한되는 것은 아니지만 바람직한 실시예를 통해 설명된다.

[0050] 본 발명의 다른 특징들 및 이점들은 뒤따르는 설명 및 제한되는 것은 아니지만 바람직한 실시예를 통해 더 이해될 수 있을 것이다.

[0051] 본 구성들은 네트워크 애플리케이션 보안에 관한 것이고, 특히 절대적인 것은 아니지만, 모바일 컴퓨팅 기기 및 플랫폼상에 효과적으로 작동할 수 있는 침입방지 시스템, 기기 및 방법에 관한 것이다.

[0052] 현재, 모바일 기기들을 위하여, 침입감지 또는 방지 시스템이 가능하지 않다. 모바일 기기들에 대한 솔루션의 부족에 숨겨진 이유는 이 침입감지 및 방지 시스템들이 매우 자원 집약적 - 즉, 그들은 애플리케이션레벨 프로토콜의 복잡한 처리 뿐만 아니라 패킷검사 과정을 수행하기 위하여 CPU로부터 집약적 연산을 요구한다는 사실이다. 이것은 또한 모바일 기기들의 배터리를 소모하고 더 일을 복잡하게 한다. 부가하여, 공격자들이 그들의 공격 및 기술을 일정하게 향상시키고 있고, 보안 산업에 있어서 따라잡기 위하여 일정한 경쟁으로 일정하게 발전하고 있다.

[0053] 본 실시예는 작동시스템의 프로토콜 스택을 사용하는 것보다 오히려 그것을 통해 모든 패킷 및 경로 이상의 조사를 회피함에 의해 프로토콜 분석을 위한 오버헤드를 줄이고 모바일 기기 OS 및 네트워크 자원의 극도의 사용을 피하는 솔루션을 제공하는 것이다. 이것은 소프트웨어 또는 하드웨어 층에 대한 의존성을 줄이기 위하여 논리 감지 엔진으로부터 물리적 패킷 모니터링 과정을 분리함에 의해 달성된다. 또한, 피캡(pcap), 네트필터(netfilter), nbf, 및 이 기술에서 알려진 기타 패킷 캡처링방법들과 같은 패킷 캡처링 라이브러리를 사용하는 모든 패킷들을 분석하는 대신, 본 발명은 조사를 위한 선택적 패턴들만 트리거하고 모바일 기기에 수신된 모든 패킷들을 깊게 조사할 필요가 없는 방법 및 시스템을 제공한다.

[0054] 본 발명에 따른 방법 및 기기의 원리 및 작동은 도면 및 뒤이은 설명으로부터 잘 이해될 수 있고, 전체를 통해 대응하는 요소들에 도면번호가 부여되며, 이것은 설명의 목적이지 권리의 범위를 한정하지 않는다는 것은 이해할 수 있을 것이다.

[0055] 도 1은 본 발명의 원리에 따라 구성된 펌웨어 모듈(100)의 예시적 모듈구조를 나타낸다. 펌웨어(100)는 다수의 서브-모듈들로 구성되고, 그들의 제1은 서드파티 WiFi 펌웨어(101)이다. 서드파티 WiFi 펌웨어(101)는 이 기술분야에서 알려진 바와 같은 다수의 WiFi 제조자들을 말한다는 것을 알아야만 한다. 각 판매자는 WiFi 펌웨어(101)에 대한 그 자신의 인터페이스 명세서(예를 들면, 하드웨어 및/또는 소프트웨어)를 갖고 있다. 본 발명의 일부 실시예들에 따르면, 서드파티 WiFi 펌웨어(101)는 통신에 있을 수도 있고 또는 패킷필터(102)에 접속될 수도 있다. 이 패킷필터(102) 책임은 WiFi 펌웨어(100)로부터 수신되는 저레벨 패킷들을 여과하고 이 패킷들을 수신된 패킷들을 조사하기 위한 패턴 감지기/인식기에 전송하는 것이다(도 3, 4 및 6에서 더 상세히 설명될 것이다). 이 패턴인식기 모듈(103)은 또한 WiFi 펌웨어(100) 및 패킷필터(102)와 통신하거나 접속될 수도 있다. 이 패턴인식기 모듈(103)은 펌웨어 레벨(예를 들어 도 6 및 7b에 보여주는 바와 같이)에서 깊은 패킷조사의 과정을 수행하기 위하여 구성된다. 보안저장부(104)는 패턴인식기(103) 및 패킷필터(102)의 여과설정기준(예를 들면, 패턴 매치 핸들러, 패턴 조건들, 패턴 규제) 그리고 개시된 발명에 의해 요구되는 부가적 정보를 저장하기 위하여 패턴인식기(103) 및 패킷필터(102)에 의해 사용된다. 본 발명의 일 실시예에 따르면, 예를 들어 도 5a, 5b 및 5c에 도시된 바와 같은 보안 애플리케이션 인터페이스(105)는 패킷필터(102)를 위하여 요구된 네트워크 패킷들의 결정론적 및 귀납적 패턴들을 특정하기 위하여 보안저장부(104)를 사용한다.

[0056] 도 2는 본 발명의 원리에 따라 구성된 소프트웨어 관점으로부터 시스템의 계층적 구조를 설명한다. 도 2는 본 발명의 소프트웨어 구조를 보여주고, 여기서 이 구조는 두 주 세그멘트로 즉 커널/하드웨어 레벨 및 애플리케이션레벨로 나누어진다.

[0057] 커널/하드웨어 레벨에 있어서, 상기에 언급한 함수를 갖는 WiFi 펌웨어(100), 하드웨어 제조자에 의해 제공된 표준 WiFi 기기 구동기인 WiFi 기기 구동기(201) 및 zCore Kernel 확장자(202)를 발견한다. 이 zCore Kernel 확장자(202)는 펌웨어(100)에 커널레벨 API(Application Program Interface)를 제공한다. 이것은 애플리케이션 레벨로부터 더 낮은 레벨들로, 즉 커널 및 하드웨어 레벨들로 기능(functions) 및 작동(operations)을 통과시키는데 사용된다.

[0058] zCore API(203)는 서드파티애플리케이션부(205)(즉, 외부 파트너 또는 개발자와 같은 "외부 당사자"에 의해 보강되어질 수 있는 애플리케이션들) 및 zDefender(204)에 의해 사용된다. 그것의 함수는 zCore Kernel 확장자(202)에 패킷들을 통과함에 의해, 그리고 서드파티 애플리케이션부(205) 또는 zDefender(204)에 의한 허락을 안전하게 고양시킴에 의해 그리고 처리를 위한 펌웨어(100)를 위하여 새로운 그리고 부가적인 논리를 제공함에 의해 펌웨어레벨에서 침입감지 오프로딩을 위한 공통 인터페이스를 제공하는 것이다.

[0059] 서드파티 애플리케이션부(205)는 표준 애플리케이션부이지만, 한편 zDefender(204)는 특정 공격에 대한 네트워크 보호를 제공하는 특정제품이다. zCore API(203)는, 펌웨어(100)에 의해 감지된 프로토콜 또는 애플리케이션 이상을 위한 고객활동을 등록하기 위하여, 마치 zDefender(204) 또는 서드파티 애플리케이션부(205)(이러한 애플리케이션부는 반-바이러스 및 다른 보안관련 애플리케이션들을 포함할 수 있다)와 같은, 다른 애플리케이션들을 위한 능력을 더 제공한다.

[0060] 본 발명은 각 프로토콜을 묘사하는 행동계통도를 자동적으로 발생하는 네트워크 프로토콜들을 분석한다. 이들 행동계통도는 프로토콜레벨 상에서 이상을 인식하고, 따라서 드릴 다운할 필요를 피하고 애플리케이션레벨 프로토콜들을 분석한다. 부가적으로, 행동계통도를 이용한 분석처리는 허위 긍정적 결과 및 네트워크와 사용자 기기 상의 오버헤드를 방지한다. 통과된 데이터는 체계화되고 일정할 필요가 있는 필드들이 분류되며 프로토콜의 세션 변동성에 비교된다.

[0061] 이것은 특징추출기술로서 인용될 수가 있다. 특징추출을 이론적으로 수행하는 많은 개방 자원제품들이 있지만, 그들은 스마트 기기들을 위하여 실질적 관련이 없고 스마트폰과 같은 모바일 기기를 위하여 최적화되지 않은 사용자 레벨 프로토콜들과 함께 불리하게 팽창된다. 본 발명은 프로토콜 분석을 위한 오버헤드를 줄이는 새로운 프레임워크를 제공한다. 예를 들어, 배터리 수명 및 처리파워를 보존하기 위하여, 네트워크 패킷이 불법구조, 옵션들, 변수들, 플래그들, 검사합계들, 등등의 관점에서 브레이킹 업(breaking up) 프로토콜이 아닌 Zcore 체크 및 증명을 제공한다. 본 발명은 네트워크 프로토콜 측 상의 애플리케이션레벨 패킷 조사를 제한하고, 호스트 침입방지 시스템(Intrusion Prevention System, IPS)으로부터 그것을 안전하게 한다. 코드상의 논리의 레이아웃은 입상레벨의 증가를 가능하게 하고 깊은 조사를 수행한다.

[0062] 시스템 및 네트워크 모니터링

[0063] 본 발명의 일부 실시예들에 따르면, 소프트웨어 또는 하드웨어 층에 대한 의존성을 줄이기 위하여 논리 감지 엔

진으로부터 물리적 패킷 모니터링이 분리된다. 한 예시적 솔루션이, 조사를 필요로 하는 관련 패킷/세션의 소프트웨어 층에 신호를 나타냄에 의해, 이것은, 도 6에 도시된 바와 같이, WiFi 기기 구동기에 일부변경을 요구해야만 하는 것으로서, 가속화된 HW일 수 있다. 부가적 방법들이 패킷 캡처링, 예를 들면 BSD 상에 /dev/bpfX로 이행된, 리눅스 또는 pcap 상의 네트필터 소켓에 의해, 네트워크 모니터링을 수행한다. 이 설계는, 대기 I/O를 사용하는 조사를 위해 표시된, 관련 패킷들을 갖는 소프트웨어 층을 신호하기 위한 하드웨어 논리를 허용한다. 이 소프트웨어 엔진은 상술한 결정논리를 사용하여 발생한 것이 정의 샘플인지 또는 부의 샘플인지를 알기 위하여 패킷 디퍼(deeper)를 조사한다.

[0064] 애플리케이션의 이상행동을 정의하고 수집하는 것

[0065] 위에서 설명한 바와 같이, 본 발명은 앞서 설명한 바와 같은 OS 행동 분석을 제공하고, 네트워크에 제공되는 두 애플리케이션 및 서비스를 망라한다.

[0066] 예를 들면, 마치 netd 서비스, 블루투스 인터페이스, 보이드 서비스, Webkit에 근거한 Browsers, NFC 서비스, 등과 같은 서비스 및 애플리케이션 내의 빌트(built)가 이상행동적 특성을 피하기 위하여 가깝게 모니터링 된다. 다른 애플리케이션들 및 처리들도, 특권이 확대되지 않는 것을 보장하기 위하여, 더 낮은 입상레벨 상에서 모니터링 된다. 악성애플리케이션들을 감지하기 위하여, 애플리케이션들 실행 그 자체는 추적되지 않지만, 애플리케이션에 의해 수행된 특권의 상승(Elevation of Privileges, EOP)을 캡처링하는데 초점이 맞춰지며, 이것은 악성애플리케이션들조차도 특권확대에 의해 명시된 악성행동을 수행하기 위하여 노력할 때 단지 악성으로 분류되는 것을 의미한다. 이와 같이, 컴퓨터 파괴 소프트웨어에 전통적인 신호에 근거한 접근을 사용함이 없이 행동분석을 통해 악성애플리케이션들을 찾아낼 수가 있다.

[0067] 한 콘텍스트에서 정상행동들이 다른 콘텍스트에서 이상행동들이 될 수 있다.

[0068] 본 발명의 분석은, 콘텍스트(context)분류 오류들을 피하기 위하여, k-0day 연구에 개시된 바와 같이 단일의 연산을 추적하지 않고 오히려 연산들의 세트를 추적하기 때문에, 콘텍스츄얼로 말하여도 좋다. 또한 오류율이 학습처리의 일부로 모니터링 된다: 테스트모드 상에서 한계값의 레벨이 증가하면, 기하급수적으로 오류율이 감소한다.

[0069] 공통 네트워크 패킷들 지식은 구성될 수 있는 프로토콜의 량이 특정애플리케이션인 것을 알려주고; 그러므로 선행기술 솔루션에 의해 제공된 바와 같이 깊은 패킷 조사가 불필요하다. 위험으로서 네트워크 패킷들의 분류는 "미확인" 탑재 또는 특정 애플리케이션 탑재를 감지하지 않고, 이것은 악성이고 앞서 특정되지 않은 위험이었다고 취급한다. 또한, 패킷들을 해독/디-오퍼스케이트 하기 위하여 막대한 자원이 소모되고, 그것은 비록 네트워킹 또는 애플리케이션 프로토콜에 순응할 수 있는 위험들을 모니터링 하는 것이 사실상으로 불가능하게 만들지만, 애플리케이션 층을 맹렬하게 추적하게 한다. 미확인 위험들을 조작하기 위한 호스트레벨보호 상에 초점을 맞추고, 성공적 공격을 위하여 사용된 기술들을 분석하며, 그리고 적절히 그들 스스로 실행으로부터 방법들을 방지하는 방어의 부가적 층이 부가되어졌고, 따라서 특권 및 실행을 높이는 이 위험을 허용하는 기술의 분류보다 오히려 위험의 특권분류 없이 위험을 경감한다.

[0070] 시스템 콜들(calls)의 차단을 우회하는 것을 목표로 한 공격들에 대한 방어(예를 들면, 복귀지향 프로그래밍(ROP))

[0071] 어드레스들이 이미 추출되었기 때문에 부가적 처리 없이, ASLR이 작동될 때 ROP는 가능하지 않다. 전체 ASLR 및 XN-비트 가능한 처리들은 "도구들(gadgets)"이 실행 흐름을 변경하기 위하여 유효한 스택-피벗 및 적절한 레지스터들을 갖도록 설비될 수 없기 때문에 복귀지향프로그래밍 기술을 완전히 차단한다.

[0072] 안드로이드 컴퓨터 파괴 소프트웨어를 사용하는 테스트: 샘플들의 수: 가-긍정적 판단 및 부정적 판단

[0073] 모든 구성들이 집적되고 현재 작동기기들로부터 통계적 데이터를 사용하여 테스트된 때 벤치마킹이 수행되었다. zConsole이 클라우드에 보내지는 데이터의 통계자료 및 포렌식들(forensics)을 모니터링하고, 데이터의 유효성을 단단히 모니터링한다. 가-긍정적 판단을 제거하기 위하여 분류되는 각 데이터 세트를 위하여 사용된 한계값 레벨의 동적 제어를 가능하게 하기 위하여 헷징(hedging) 기술이 사용된다.

[0074] 이행을 촉진하고 장애물을 제거하기 위하여 전 및 후에 측정하는 것이 중요하다.

[0075] 해커/컴퓨터 파괴 소프트웨어 공격으로부터 보호하기 위한 자체-탬퍼 감지

[0076] 본 발명은 처리들을 오퍼스케이트하고, 실행과 함께 탬퍼링을 방지한다. 만약 처리의 내용을 바꾼다면, 그것은

실행되지 않을 것이다. 예를 들면, 그것은 처리 상에서 안정적으로 수행할 것이고 실행 시간상에서 처리를 동적으로 디-오퍼스케이트하고 해독하며, 이것은 고정 뒤바꿈이 뒤바꿈 자들을 위하여 사소하지 않은 일이 된다는 것을 확실하게 한다.

[0077] 부가적으로, 본 발명은 디버거들이 영상의 섹션내용을 정확하게 파스할 수 없기 때문에 프로세스에 디버거들을 부착하는 것을 매우 어렵게 만든다. 이것은 이 기술분야에서 아직 알려지지 않은 반-디버깅 기술을 사용함에 의해 수행된다.

[0078] 도 3a는 본 발명의 원리에 따라 구성된 리코나이산스(reconnaissance) 공격 또는 전송제어프로토콜(Transmission Control Protocol, TCP) 내의 "SYN" 의 전 및 후의 단계들에 대한 흐름도이다. SYN 공격에 있어서, 발신자는 완전하게 될 수 없는 일정량의 커넥션들(connections)을 전송한다. 이것은 기입하기 위한 커넥션 대기들을 일으키고, 그것에 의해 TCP 사용자들을 합법화하는 서비스를 부정한다. 줄처진 의사결정 알고리즘의 예와 같이, 이하의 문단들은 TCP 프로토콜의 분석을 나타내는 행동트리의 브랜치를 논의한다. 결정노드들의 일부는 확률적이고 보안 소프트웨어를 위한 PASS/FAIL 결정을 일으킬 수 있다. 이들 PASS/FAIL 결정들은 기기를 위한 특정 정책에 의존하고 따라서 새로운 위험 및 잠정적 실행 중지의 신호를 주는 소프트웨어를 초래할 수가 있다.

[0079] 도 3a는, 소위 SYN 공격으로 불리는, 리코나이산스 공격을 발견하는 예를 통한 단계들이다. SYN 공격은 전송제어프로토콜(TCP) 내의 공격식별브랜치이다. 이 공격은 노드 51332를 통해 지정될 수 있고 이 공격을 식별하기까지 흐름독출은 다음과 같다:

[0080] 1. 5100 - TCP) NODE ->는 세션 진위(TCP 세션 산란 수집, 타이머 확인, 리코나이산스, seq. 공격, 등)를 모니터링 하기 위한 서브 노드들을 사용한다.

[0081] 2. 5110 - TCP-BASE-OPS ->는 패킷의 유효성을 체크하고, 기초 검사합계 계산과 같은 초기 프로토콜 검사를 수행한다.

[0082] 3. 51300 - TCP-FLAG-CHECK ->는 지향된 추가 세션인 플래그들/옵션들/변동들을 검사하고, 도시된 흐름에 있어서 그것은 51330으로 불리며, 이것은 확률적 노드들의 수집이고, 각각은 다른 한계값 변수들을 포함하고 있으며, 이것은 처리 최적화를 위한 병행 노드들로 반입하는 다른 위험들을 조사한다.

[0083] 4. 51331 - SYN FLOOD - 는 SYN 관련된 공격을 검사한다. 폭주처럼, 그것은 성공적 상태로 되고, 그리고 감지될 때 위험을 알린다.

[0084] 5. 51332 - SYN/ACK/FIN SCAN -은 검사하거나 또는 소스 인터넷 프로토콜(IP) 당 한계값을 정하고, 예를 들면 델타시간(dt) 시간주기를 넘는 (i)패킷들이 보내진 192.168.1.12(x), 이것은 단순한 계산 x(i)/dt=한계값으로 해석된다.

[0085] 6. 51333 - 스푸핑(spoofing) 감지 - 이 노드는 어떤 것이 SEQ/ACK 공격을 수행하기 위하여 노력하고 있다는 것을 검사한다.

[0086] 7. 51334 - 오르판/지속 타이머 공격 - 이 노드는 지속적인 TCP 타이머들에 있어서 취약성들을 이용하려는 어떤 시도, 또는 "오르판(orphans)"을 검사한다.

[0087] 노드들 스스로는 포맷 된 길에서 제약들 및 변경들을 조사한다. 각 노드들 세트는 동일한 데이터 세트들에 걸쳐 불필요한 반복 없이 미리 패킷분류를 진행한다. 노드들을 위한 '글루(glue)'는 트리(tree)를 상태기계에 옮길 수 있는 노드들 이내에서 보충된 트랜지션이다. 이 스테이트 머신(state machine)은 두 가지 이유들 때문에 한정된 지정기계로 되게할 수가 없다:

[0088] 1. 그것은 한정하지 않고, 그것은 복합적으로 적응할 수 있으며, 룰들을 재-발생할 수가 있다. 룰은 각 노드를 위한 소정레벨의 멤버십함수(이후 설명)과 함께 도 3에 도시된 표에 있어서 노드들의 '다발'이다.

[0089] 2. 룰들은 확률측정 및 함수들을 사용하는 퍼지일 수 있고, 그래서 존재하는 룰들로부터 룰들을 '유도'할 수 있다.

[0090] 도 3b는 본 발명의 원리에 따라 구성된 사용자 경우들의 확장 다이아그램이다. 기기사용자(320)에 속하는 사용자기기(310)는 행동속성(311)을 수집하고, 이상을 감지(312)하며, 그리고 zConsole(340)과 서로 조합하여 사실의 통보(313)를 제공한다. IT 관리자(330)는 기기관리(332) 및 정책집행(333)의 룰에 따라 명령(331)을 발부한

다.

[0091] 도 4는 본 발명의 원리에 따라 구성된 퍼지상태기계의 흐름도이다. 새로운 룰이 발생/'결정'될 때, 시스템의 상태 빌딩 알고리즘은 멤버십 함수(425)를 다시계산 한다. 패킷들은 데이터로 구성되어 있다. 데이터는 위험가능성발생기(420)에 의해 제공된다: 데이터_형태_패킷(411); 데이터_형태_프로세스(412); 및 데이터_형태_N(413). 이것은 zConsole 상에서 행하여지고, 멤버십 함수(425)의 동기요청 재계산을 통해 zCore(도 2의 참조블럭 202) 클라이언트에게 연재하여 보내진다.

[0092] 위험가능성발생기(420)는 또한 멤버십(Si) + 한계값/정상화(450), 및 그 다음 매치룰*이득/멤버십(Si)(460)을 업데이트 한다. 그 다음 세트 T(i,j) 내의 다음전송으로 점프(470) 및 다음 상태(Si + 1)의 제거-선택(480)을 업데이트 한다. 이 시스템은 집합이 달성될 때까지 멤버십(Si) + 한계값/정상화(450)를 업데이트 하기 위하여 반복적으로 순환함을 계속한다.

[0093] 이 기술은, 조작자들의 한정된 세트(비교, 부가, dec, mul, 등)로 변경들 및 제약들을 찾기 때문에, 소스 파일 내의 어떤 변화 없이 감지엔진의 논리를 변경하는 것을 허용한다.

[0094] 도 5a는 본 발명의 원리에 따라 구성된 대시보드(501)용 콘솔의 스크린숏이다. 다양한 시간 프레임들이, 이 경우 하루에, 보여질 수 있다(510). 공격 지리위치들이 지도상에 보여진다(520). 핀으로 찍힌 영역을 위한 공격의 수가 표시된다(530). 이벤트 로그(541)는 각 이벤트의 형태, 소스 및 시간을 보여준다. 보안상태(542)는 공격하의 기기의 수, 신용레벨 및 로드상태를 보여준다. 쓸모없는 기기들(543)은 더 이상 분석될 수 없는 기기들의 형태 및 수를 보여준다.

[0095] 도 5b는 본 발명의 원리에 따라 구성된 기기관리용(502) 콘솔의 스크린숏이다. 도 5b는 위험-응답-매트릭스 구조(550)의 zConsole의 실행을 보여준다. 이 위험응답매트릭스는 방어대책의 일부로서 공격의 경우에 있어서 취하여 지는 활동을 정의한다.

[0096] 도 5c는 본 발명의 원리에 따라 구성된 안드로이드 기기상의 중간(MITM) 공격 내의 사람을 감지하는 zIPS의 스크린숏이다. MITM 공격(551)은 두 시스템 사이의 통신을 가로챈다. 예를 들면, 목표는 클라이언트와 서버 사이의 TCP 접속이다. 공격자는 원래의 TCP 접속을 두 새로운 접속으로 분리하고, 하나는 클라이언트와 공격자 사이로 그리고 다른 하나는 공격자와 서버 사이로 한다. TCP 접속이 가로채 지자마자, 공격자는 독출가능하게 되는 프록시로서 활동하고, 가로챈 접속 내에 데이터를 삽입하고 변경한다. TCP 스캔(552)에 있어서, 포트 스캐너들은 작동시스템의 네트워크 함수를 이용한다. 만약 포트가 개방되면, 작동시스템은 TCP 3-자간 연결을 완전하게 하고, 포트 스캐너는 즉시 3 종류의 서비스거부공격을 수행하는 것을 피하기 위하여 접속을 폐쇄한다. 위험감지 메세지가 표시된다(560).

[0097] 도 6은 본 발명의 원리에 따라 구성된 예시적 하드웨어 구성의 흐름도이다. 단계(610)에서 새로운 패킷이 네트워크에 의해 수신된다. 펌웨어(201)는 헤더를 검사함(621)에 의해 시작되고 패턴들을 검사(622) 한다. 그 다음 WiFi 펌웨어가 패킷이 의심스러운지 여부를 결정한다(623). 만약 의심스러우면 패킷은 따라서 표시되고(624) 소프트웨어 층(202, 203)으로 통과된다. 우선 소프트웨어 층(202, 203)은 수신 버퍼 내에 새로운 패킷이 있다는 것을 감지한다(Rx)(631). 만약 패킷이 참조블록(624)에서 표시되었다면(632) 패턴 감지부(633)로 기여가 결정되고; 만약 아니면 다음 소프트웨어 층이 시험된다(634). 패킷이 의심스러운지 여부의 상세한 것은 도 3b 및 도 4와 관련하여 설명된다.

[0098] 도 7a는 본 발명의 원리에 따라 구성된 오프로딩 조사처리모듈의 상세에 대한 흐름도이다. 패턴감지기(710)는 행동통계(711)를 편집하고 의심스러운 패킷을 의심스러운 패킷 대기(715)로 양도함에 의해 패턴매치핸들러(712), 패턴조건(713) 및 패턴 제약(714)에 응답한다. SW 중단 핸들러(720)는 zCore.ko(721) 및 네트필터(732)를 포함하는 커널(730)과, 그리고 zCore 다이몬(741) 및 현 애플리케이션(742)을 포함하는 사용자 공간(740)과 함께 소통한다. 위험이 증명되자마자 패턴감지기(710)는 공통접속자(A)에 의해 표시된 바와 같이, 도 7b의 오프로더로 정보를 보낸다.

[0099] 패턴감지기(710)는 들어오는 트래픽을 필터링하고 헤더 시퀀스에 따라 현재수신된 패킷의 이상할 확률을 표시한다(도 1 및 도 6에 보여주는 바와 같이). 이 패턴감지기(710)는 깊은 패킷 조사를 피하기 위하여 조건들(713), 제약들(714) 및 매칭기준(712)을 이용하고, 단지 공격의 확률을 갖는 공격의 패턴들을 검사한다.

[0100] 본 발명의 일 실시예에 따르면, 데이터의 각 패킷은 프로토콜 상태 및 어드레스변수에 따른 실시간에 있어서의 이상을 가질 확률을 나타내는 확률매트릭스(711), 데이터 흐름 및 프로토콜 일관성 검사에 영향을 미친다. 의심

스러운 조작이 감지될 때, 패킷들은 의심스러운 패킷 대기(715)로 들어가고 소프트웨어는 그러한 요구들을 조작(720)하기 위하여 펌웨어(도 1에 도시)상에서 보강된 SW 중단을 사용하여 이들 패킷들을 액세스할 수 있다.

[0101] 본 발명의 일부 실시예들에 따르면, 소프트웨어 중단 모듈(720)은 정상 트래픽(패킷들의 예) 및 악성트래픽 사이를 구분하는 것이 제공되고, 통신기기 또는 네트워크 시스템에 위험할 수 있는 프로토콜을 안전하게 분석하기 위하여 악성트래픽을 다른 소프트웨어 층으로 전송한다.

[0102] 커널소프트웨어층(730)은 기기에 대한 간섭 및 요구를 하도록 구성되고, 기기 하드웨어와 함께 상호작용한다. 작동하는 시스템의 프로토콜 스택(732)은 네트워크에 걸쳐 수신된 프로토콜들 및 패킷들을 위한 커널공간에 실행된다. zCore.ko(721)는 모든 패킷들 및 작동하는 시스템의 프로토콜 스택 커널 확장부(732)를 사용하는 것보다 오히려 그것을 통해 단지 경로 이상들의 조사를 피하도록 구성된 커널확장부(도 2에 도시)이다. 그러므로, 비 의심스러운 프로토콜 스택 핸들러(721)에 도달하는 대신에, 패킷들은 노이즈를 필터링하고 결정을 얻기 위하여 완전히 각 이용 경우를 조사하는 zCore 애플리케이션(741)을 통해 완전히 조사되는데 처해진다. 이처럼, pcap, 네트필터, nbf, 및 이 기술에 알려져 있는 기타 패킷 캡처링방법들과 같은 패킷 캡처링 라이브러리를 사용하여 모든 패킷들을 분석하는 대신에, 본 발명 솔루션은 조사를 위한 선택 패턴들만 트리거하고 소프트웨어 상에서 모든 패들을 깊게 조사할 필요가 없다.

[0103] 도 7b는 본 발명의 원리에 따라 구성된 패킷형태로 네트워크에 걸쳐 전송된 데이터를 설명한다. 이 패킷은 이더넷(Ethernet) 헤더 데이터(770) 및 대응하는 데이터 페이로드(780)로 구성된다. 도 7b에서 알 수 있는 바와 같이, ARP형 패킷 및 IP 패킷이 수신되고 분석된다. 이 패킷은: 패킷 헤더 src(763) 어드레스, 목적지 어드레스(765) 및 ETH_P_ARP 또는 ETH_P_IP일 수 있는 프레임형 필드(761)를 포함한다.

[0104] 프레임 필드(761) 값에 따르면, 패턴감지기는 프로토콜 형태 및 정확한 오프세트를 인식할 수 있고, 이것은 공격패턴을 나타내는 값의 세트에 대하여 비교될 수 있다.

[0105] 데이터 페이로드(780)는 이 기술에 알려져 있는 바와 같은 ETH-P-ARP의 경우 및 ARP 프로토콜 헤더로 구성되고, HW 형(781), 프로토콜 형(782), 하드웨어 어드레스 크기(783), 프로토콜 크기(784), 조작부(785) 및 대응하는 필드: 하드웨어 어드레스 크기(783)로 알려진 길이를 갖는 HW SRC 어드레스(786)로 구성된다. (787)은 프로토콜 소스어드레스이고, 그것의 크기는 프로토콜 크기(784)에 알려진 바와 같으며, 목표 HW 어드레스(788)는 HW크기(783) 상에 알려진 길이에 대응하는 길이의 패킷요청을 기소한다. 프로토콜 목표어드레스(789)는 프로토콜 크기(784)와 같이 알려진 특정된 길이를 갖는 목표 프로토콜 어드레스이다.

[0106] 데이터 페이로드(780)는, 패킷헤더(761)를 위한 필드 값이 ETH_P_IP에 동일할 때, IP에 기초된 프로토콜을 포함할 수 있다. 이 페이로드는 IPv4에 기초된 데이터(751) 또는 헤더에 수신된 프로토콜에 따른 IPv6(752)패킷을 포함할 수 있다. IPv4패킷 및 IPv6패킷 둘 다 UDP, TCP, 또는 ICMP와 같은 프로토콜들로 놓일 수 있다.

[0107] 본 실시예들은 WiFi(802.11a,b,c,d,e,f, 등과 같은)를 포함하는 무선 네트워크에 적용하고 있지만, 여기에 한정되는 것은 아니다. 이 실시예들은 또한 코드분할다중접근(CDMA), CDMA-2000 및 대역확산신호를 수신하기 위한 광폭 CDMA(WCDMA) 휴대무선전화기 수신기, 모바일통신 휴대무선전화기용 글로벌 시스템(GSM), 일반 패킷무선서비스(GPRS), 확장된 GPRS(EGPRS), 3세대 휴대전화시스템(3G), 3GPP LTE 등과 관련한다. 단순화를 위하여, 비록 발명의 범위가 이것과 관련하여 한정되는 것은 아니지만, 기재된 발명의 실시예들은 CDMA, WCDMA, CDMA 2000 등을 포함할 수 있는 휴대무선전화기 시스템의 CDMA 가족에 관련되어도 좋다. 한편, 본 발명의 실시예들은 전기 및 전자 엔지니어 원(IEEE)에 의해 정의된 것들과 같은 무선데이터통신네트워크에 잘 실행되어도 좋다. 소정의 특정한 실시예들과 관련하여 본 발명을 개시하였지만, 또 다른 변경, 변조들이 이 기술분야의 통상의 지식을 가진자에 의해 그들 스스로 제안할 수 있기 때문에, 개시내용은 한정을 의미하지 않는다는 것을 이해할 수 있고, 그것은 첨부한 청구항들의 범위 이내에서 그러한 변경들을 포함할 의도임을 이해할 수 있을 것이다.

부호의 설명

[0108] 101: WiFi 펌웨어 102: 패킷 필터

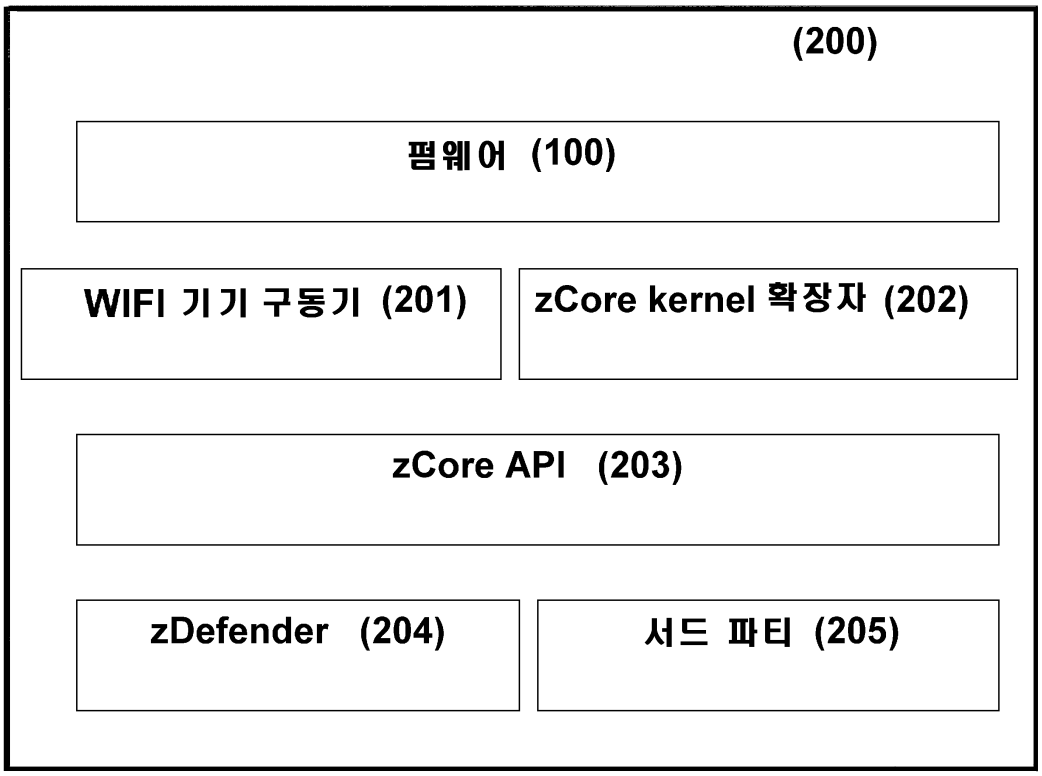
201: WiFi 기기 구동기 310: 사용자 기기

도면

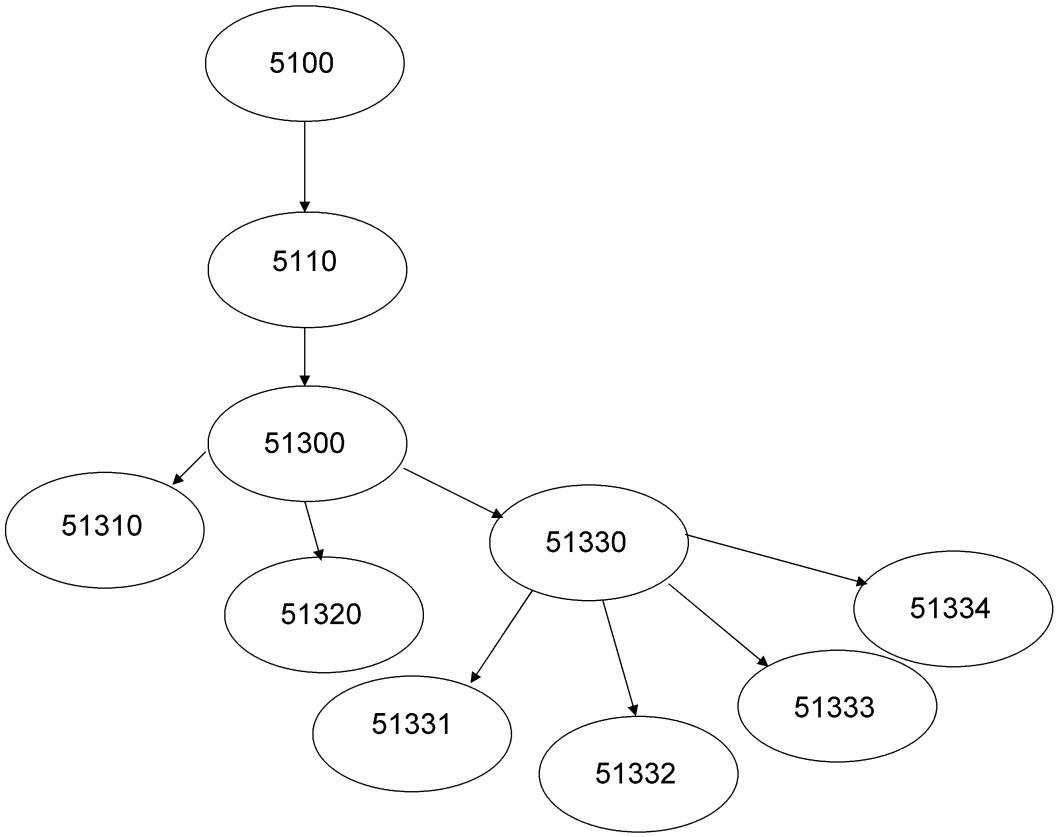
도면1


(100)
패킷
필터
(102)
WIFI
펌웨어
(101)
패턴
인식기
(103)
보안
저장부
(104)
보안 인터페이스 (105)

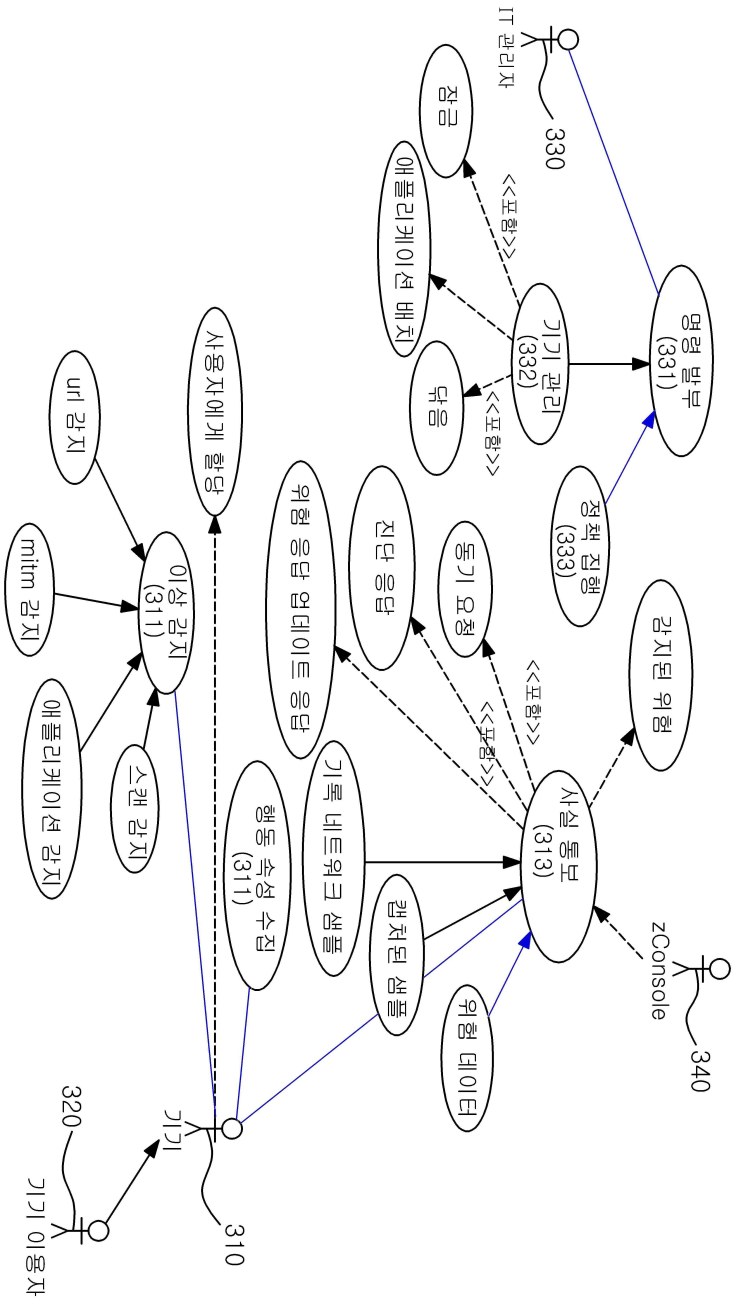
도면2


(200)
펌웨어 (100)
WIFI 기기 구동기 (201)
zCore kernel 확장자 (202)
zCore API (203)
zDefender (204)
서드 파티 (205)

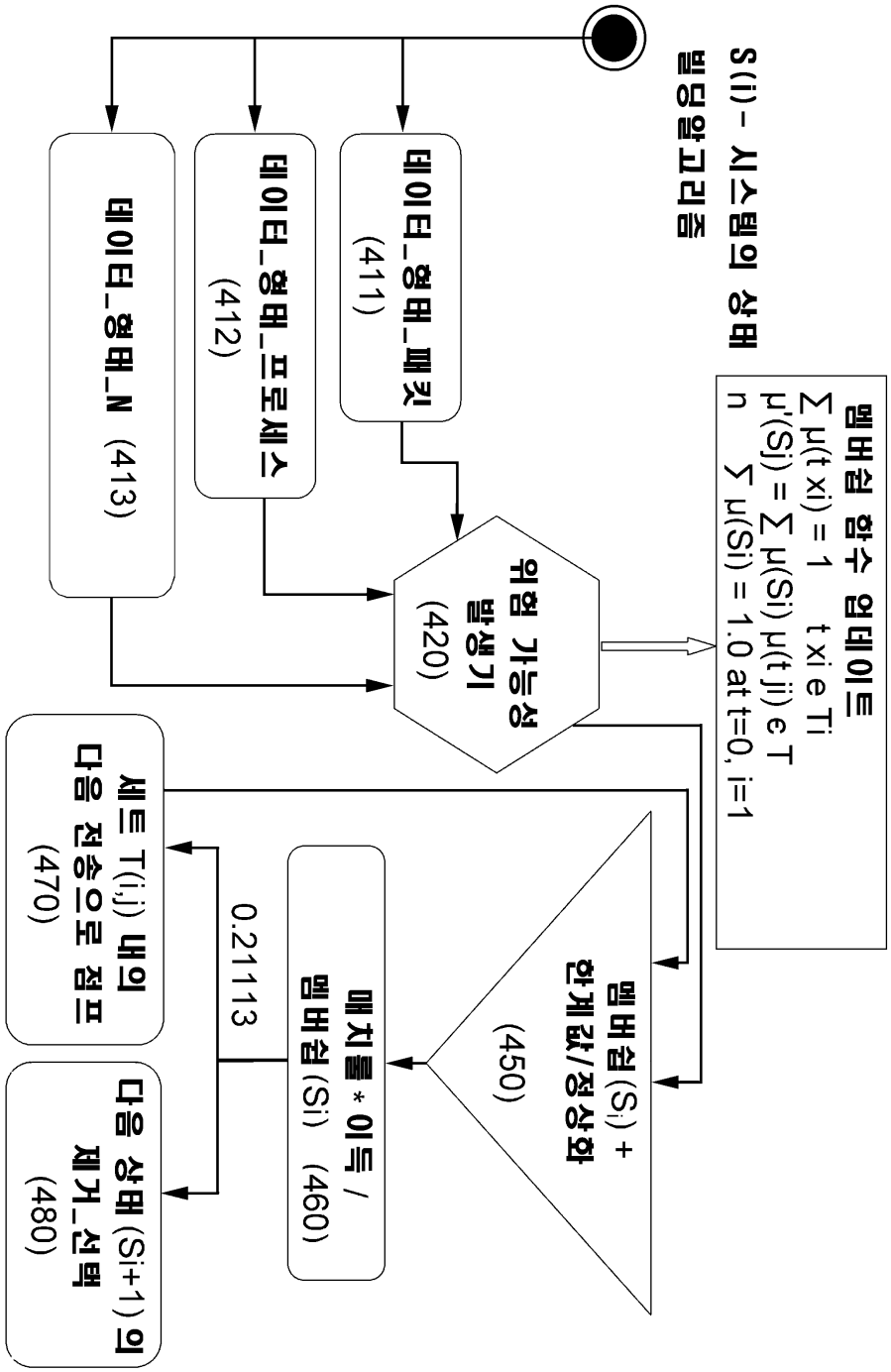
도면3a



도면3b


IT 관리자
330
잠금
애플리케이션 배치
닦음
<<포함>>
<<포함>>
기기 관리
(332)
명령 발부
(331)
정책 집행
(333)
사용자에게 할당
url 감지
mitm 감지
애플리케이션 감지
스캔 감지
이상 감지
(311)
위험 응답 업데이트 응답
진단 응답
동기 요청
<<포함>>
<<포함>>
감지된 위험
사실 통보
(313)
기록 네트워크 샘플
캡처된 샘플
행동 속성 수집
(311)
위험 데이터
zConsole
340
320
기기 이용자
기기
310

도면4


S(i) - 시스템의 상태
빌딩알고리즘
데이터_형태_패킷 (411)
데이터_형태_프로세스 (412)
데이터_형태_N (413)
위험 가능성 발생기 (420)
멤버쉽 함수 업데이트
∑ μ(t xi) = 1 t xi e Ti
μ'(Si) = ∑ μ(Si) μ(t ji) ϵ T
n ∑ μ(Si) = 1.0 at t=0, i=1
멤버쉽 (Si) + 한계값/정상화 (450)
매치률 * 이득 / 멤버쉽 (Si) (460)
0.21113
세트 T(i,j) 내의 다음 전송으로 점프 (470)
다음 상태 (Si+1) 의 제거_선택 (480)

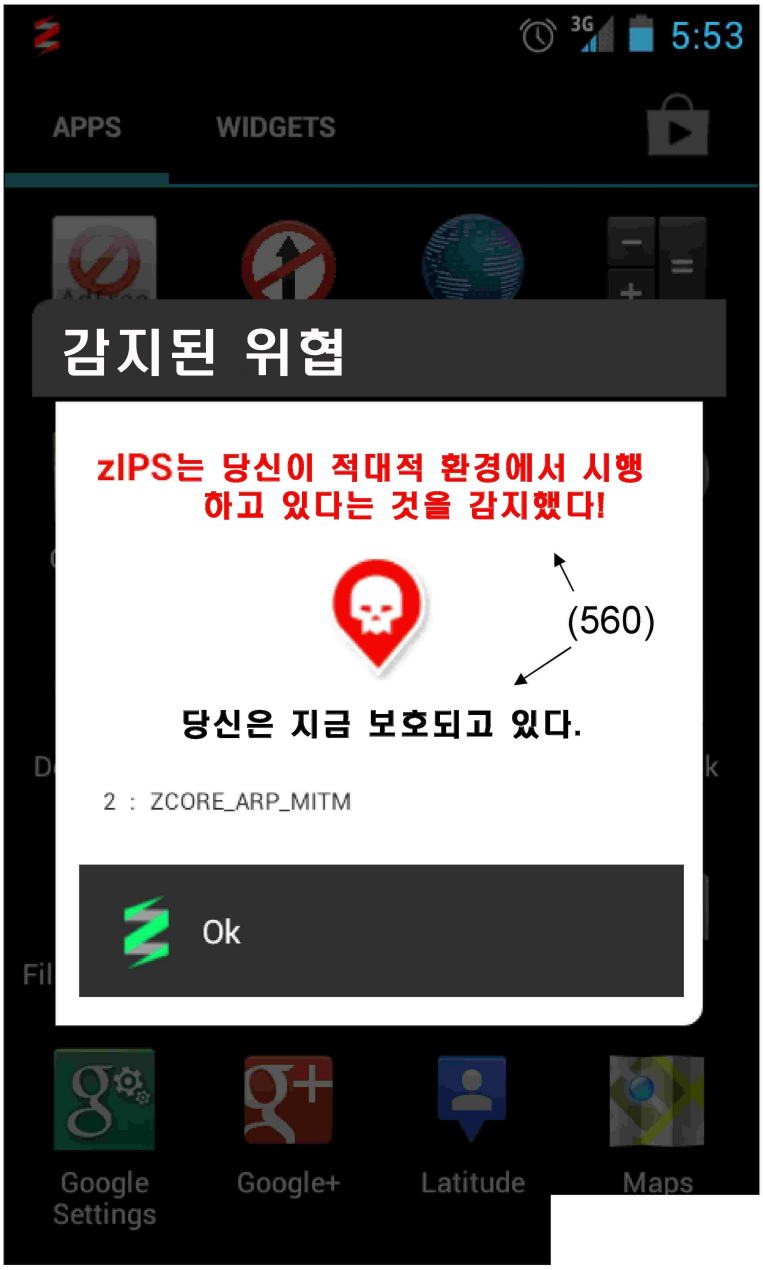
도면5a


관찰 1D 1w 3w 1m 1y (510)
대시보드 (501)
기기
사용자
그룹
정책
설정
보고서
10
Threat Prevented
고위험
중간위험
저위험
보안 상태 (542)
공격하의 4 장지
신용 레벨
— 39.9%
로드 상태
— 13.7%
이벤트 로그(541)
TCP scan
Detected TCP scan from 192...
TRM
Finished threat response acti...
Detected TCP scan from 10.0...
공격 지리위치 (520)
감지된 93공격들 (530)
Google
Netanya
Kfar Yona
Tul Karm
Petah Tikva
Rishon LeTsiyon
Lod
Modi'in Maccabim Re'ut
Yavne
Rehovot
Kiryat Ekron
Yahud Monosson
Shoham
Elad
10 km
쓸모없는 기기들 (543)
Others (5)
Android 4.0.4 (3)
Android 4.1.1 (1)
Android 4.0.3 (1)

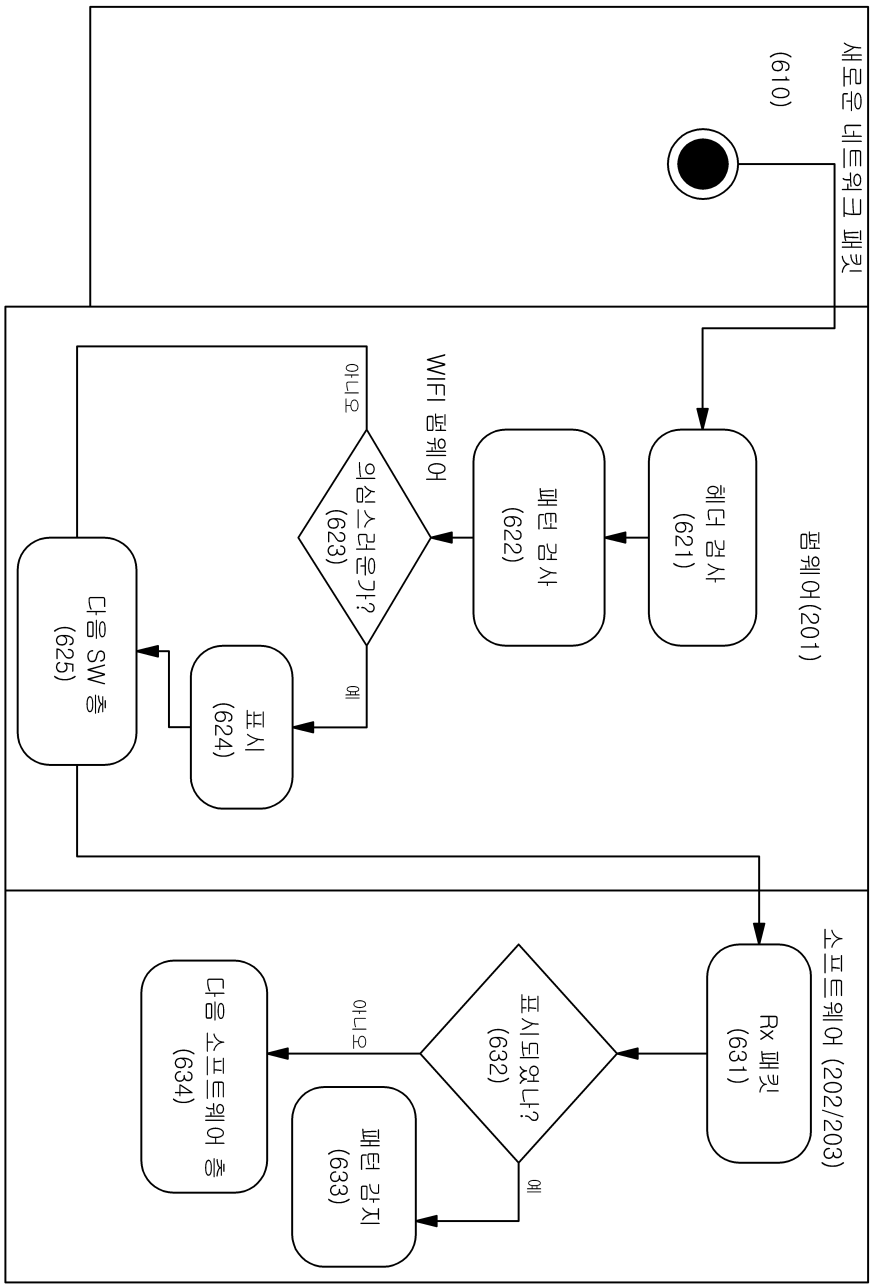
도면5b


CONSOLE
BY ZIMPERIUM
대시보드
기기 (502)
사용자
Z 그룹
Z정책
설정
Z보고서
위험 응답 매트릭스 (550)
Reset
Services
MitM (551)
▶ 차단 WiFi
TCP scan
▶ alert only (552)
user defined
enforce wlan
filter src
disconnect wifi
tunnel traffic
Last Seen
Print Layout View
100%

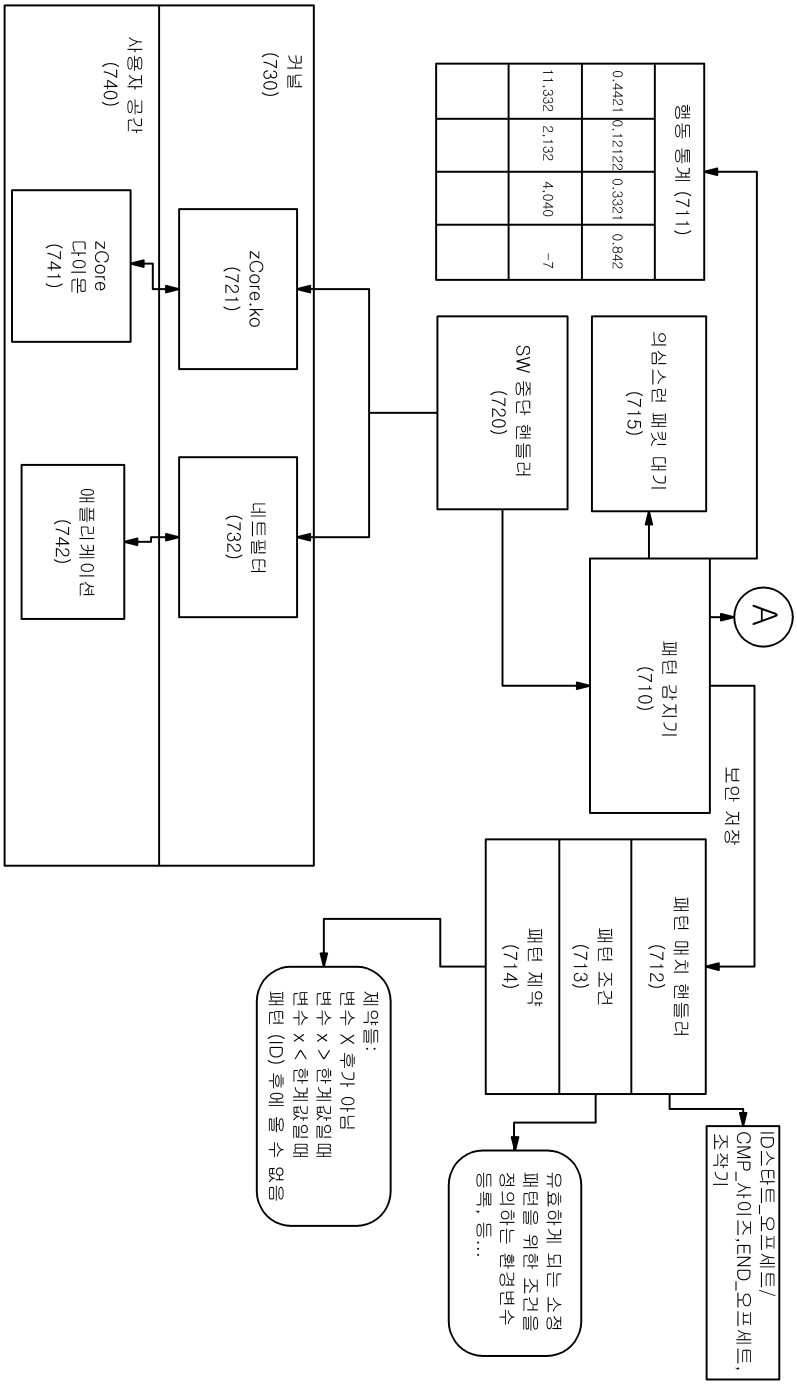
도면5c


5:53
APPS
WIDGETS
감지된 위협
zIPS는 당신이 적대적 환경에서 시행 하고 있다는 것을 감지했다!
(560)
당신은 지금 보호되고 있다.
2 : ZCORE_ARP_MITM
Ok
Google Settings
Google+
Latitude
Maps

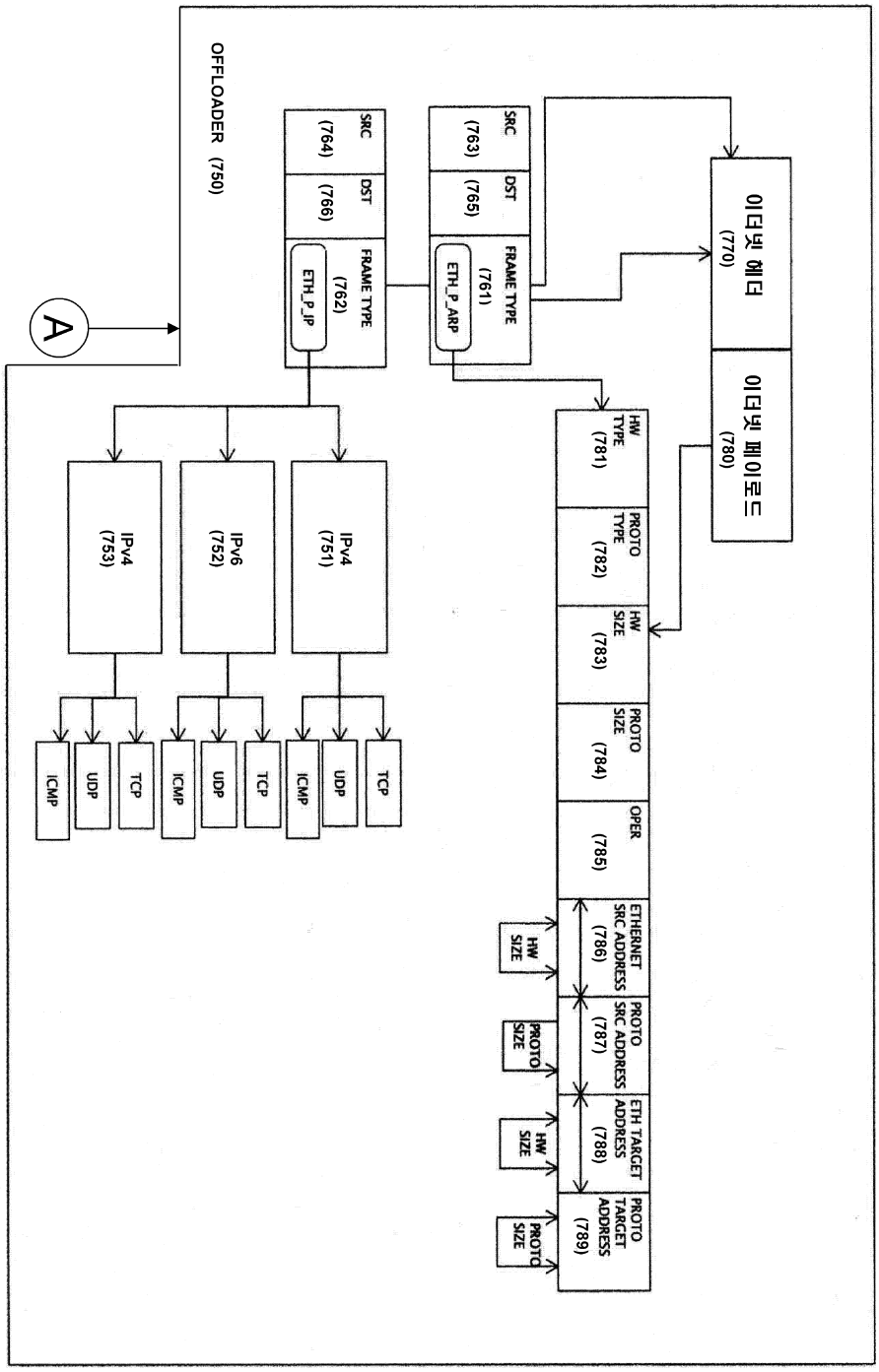
도면6


새로운 네트워크 패킷
(610)
펌웨어(201)
헤더 검사
(621)
패턴 검사
(622)
WIFI 펌웨어
의심스러운가?
(623)
아니오
예
표시
(624)
다음 SW 층
(625)
소프트웨어 (202/203)
Rx 패킷
(631)
표시되었나?
(632)
아니오
예
패턴 감지
(633)
다음 소프트웨어 층
(634)

도면7a


커널
(730)
사용자 공간
(740)
zCore.ko
(721)
zCore
다이몬
(741)
네트필터
(732)
애플리케이션
(742)
SW 중단 핸들러
(720)
행동 통계 (711)
0.4421 0.12122 0.3321 0.842
11.332 2.132 4.040 -7
의심스런 패킷 대기
(715)
A
패턴 감지기
(710)
보안 저장
패턴 매치 핸들러
(712)
패턴 조건
(713)
패턴 제약
(714)
ID스타트_오프셋트/
CMP_사이즈,END_오프셋트,
조작기
유효하게 되는 소정
패턴을 위한 조건을
정의하는 환경변수
등록, 등...
제약들:
변수 X 후가 아님
변수 x > 한계값일때
변수 x < 한계값일때
패턴 (ID) 후에 올 수 없음

도면7b



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 17

【변경전】

상기 결정론적 패턴 및

【변경후】

결정론적 패턴 및

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 19

【변경전】

특징으로 통신기기

【변경후】

특징으로 하는 통신기기