(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2010 년 10 월 14 일 (14.10.2010)

PCT

(10) 국제공개번호
WO 2010/117155 A2

(51) 국제특허분류:
G06F 21/00 (2006.01) *H04B 1/40* (2006.01)

(21) 국제출원번호: PCT/KR2010/001853

(22) 국제출원일: 2010 년 3 월 26 일 (26.03.2010)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2009-0030671 2009 년 4 월 9 일 (09.04.2009) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **삼성에스디에스 주식회사 (SAMSUNG SDS CO., LTD.)** [KR/KR]; 서울시 강남구 역삼 2 동 707-19 이록빌딩, 135-918 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **유인선 (YOO, In Seon)** [KR/KR]; 서울특별시 노원구 하계 1 동 삼익아파트 2-103, 139-231 Seoul (KR).

(74) 대리인: **최태창 (CHOI, Tae Chang)**; 서울시 강남구 역삼동 642-6 성지하이츠 3 차 501 호, 135-717 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

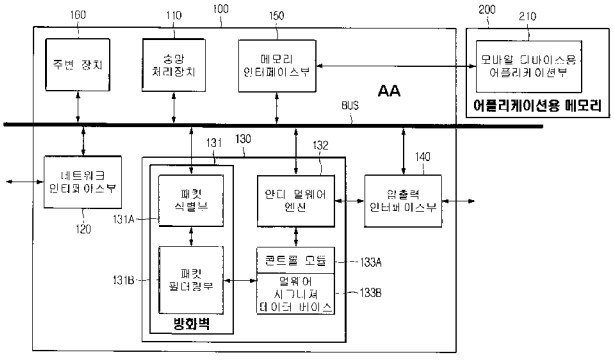
공개:
— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

WO 2010/117155 A2

(54) Title: SYSTEM-ON-CHIP MALICIOUS CODE DETECTION APPARATUS FOR A MOBILE DEVICE

(54) 발명의 명칭 : 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치

[Fig. 1]



AA ... BUS
110 ... Central processing unit
120 ... Network interface unit
131 ... Firewall
131A ... Packet identification unit
131B ... Packet-filtering unit
132 ... Antimalware engine
133A ... Control module
133B ... Malware signature database
140 ... Input/output interface unit
150 ... Memory interface unit
160 ... Peripheral device
200 ... Memory for application
210 ... Application unit for a mobile device

(57) **Abstract**: The present invention relates to a technique for constructing a firewall and an antimalware engine based on a memory for system-on-a-chip to detect malicious codes intruding on a mobile device. The object of the present invention is accomplished by a system-on-a-chip, comprising: a central processing unit which controls each unit of the system-on-a-chip to perform system-on-a-chip malicious code detection; said firewall which is based on the memory for system-on-a-chip and which classifies packets input by an external source via a network interface unit, performs a filtering process, including an allowing step and a dropping step, on the classified packets in accordance with settings, and outputs the result of the filtering process to a memory for application, or to the antimalware engine; said antimalware engine which is based on the memory for system-on-a-chip, and which performs a pattern-matching process between the code pattern in the file input from the firewall and the pattern of the malicious code registered in a malware signature database on the memory for system-on-a-chip, to detect malicious codes; and a control module which is based on the memory for system—on-a-chip, and which controls the operation of the firewall and of the antimalware engine in conjunction with the central processing unit.

(57) 요약서:

[다음 쪽 계속]

본 발명은 시스템온칩상에서 메모리 기반으로 방화벽과 안티멀웨어 엔진을 구축하여 휴대단말기로 유입되는 악성코드를 검출하는 기술에 관한 것이다. 이러한 본 발명은 시스템온칩 기반의 악성코드 검출을 위해 시스템온칩 내의 각부를 총괄제어하는 중앙처리장치와; 네트워크인터페이스부를 통해 외부로부터 입력되는 패킷들을 분류하고 기 설정된 내용에 따라 그 분류된 패킷에 대한 얼라우, 드롭 등의 필터링작업을 수행하여 그 결과를 어플리케이션용 메모리에 출력하거나, 안티 멀웨어 엔진에 출력하는 시스템온칩용 메모리 기반의 방화벽과; 상기 방화벽으로부터 입력되는 파일 내의 코드 패턴과 시스템온칩용 메모리상의 멀웨어 시그니쳐 데이터베이스에 등록된 악성코드의 패턴 간의 패턴 매칭 작업을 수행하여 악성코드를 검출하는 시스템온칩용 메모리 기반의 안티 멀웨어 엔진과; 상기 중앙처리장치와 연계하여, 상기 방화벽과 안티 멀웨어 엔진의 구동을 제어하는 시스템온칩용 메모리 기반의 콘트롤 모듈;로 구성된 시스템온칩에 의해 달성된다.

명세서

발명의 명칭: 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치

기술분야

[1] 본 발명은 휴대단말기에 적용되어 악성 코드를 검출하는 기술에 관한 것으로, 특히 휴대단말기의 자원 및 성능향상을 감안하여 시스템온칩상의 메모리 기반으로 방화벽과 안티멀웨어 엔진을 구축하여 휴대단말기로 유입되는 악성코드를 검출하도록 한 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치에 관한 것이다.

배경기술

[2] 근래 들어, 스마트폰, 개인휴대정보단말기(PDA: Personal Digital Assistant), 와이브로(WiBro) 단말기 등이 널리 보급되면서 이러한 휴대 단말기들은 현대인의 생활 필수품으로 자리매김하고 있다. 많은 사람들이 휴대단말기(mobile device)를 이용하여 서로 안부를 묻고 정보를 교환하며 음성 및 데이터 통신을 통하여 업무상 중요한 정보를 교환하기도 한다.

[3] 그런데, 휴대단말기의 하드웨어의 기능이 확대되고 고급화되면서 휴대단말기에서 수행되는 응용프로그램이 다양해지고 복잡해져 감에 따라 기존에 컴퓨터를 공격하던 악성코드가 휴대단말기에도 심각한 폐해를 일으킬 가능성이 높아지고 있다. 특히 WiBro 등 무선 휴대 인터넷 서비스가 확산되는 추세에 따라 기존 컴퓨터용 응용 프로그램의 취약성을 공격하는 악성코드에 더하여 블루투스(Bluetooth), MMS(MMS: Multimedia Messaging System) 등 휴대단말기용 응용 프로그램 및 서비스의 취약점을 공격하는 모바일 악성코드(mobile malware)가 등장하고 있다.

[4] 상기 모바일 악성코드의 예로써, 텔레포니카가 변경된 티모포니카 웜, 아이모드(I-Mode) 악성코드, SMS(SMS: Short Message Service), 팜 운영체제(Palm OS)에서 동작하는 바이러스(Phage, Vapor, Liberty) 등이 있다.

[5] 이러한 각종 악성코드들은 휴대단말기의 오동작을 유발시킬 뿐만 아니라 데이터를 삭제하거나 사용자의 개인정보를 유출하는 등의 심각한 피해를 입힐 수 있다. 따라서, 각종 악성코드로부터 휴대단말기를 효과적으로 보호할 수 있는 대책이 요구되고 있다.

[6] 종래의 휴대단말기에 적용되는 안티 멀웨어(바이러스 백신)(Anti-Malware) 솔루션들은 소프트웨어 기반으로 되어 있으며, 이의 기본적인 동작은 다음과 같다. 소프트웨어 기반의 백신 프로그램은 기본적으로 안티 멀웨어 엔진(Anti-malware engine)과 시그니쳐 매칭부를 구비하여, 바이러스 시그니쳐 데이터베이스(virus signature DB)가 주기적으로 업데이트되는 구조로 되어 있다.

[7] 이와 같은 구조에서 안티바이러스 소프트웨어(Anti-Virus Software)는 파일들을

스캐닝할 때 상기 데이터베이스에 존재하는 시그니쳐들과 매칭되는 것을 찾아 바이러스 감염 여부를 확인하거나 비정상적인 파일들을 검출한다. 또한, 종래의 휴대단말기에 적용되는 방화벽(firewall)은 정책 설정여부에 따라 외부로부터 입력되는 모든 네트워크 억세스를 차단하거나 외부의 특정 외부의 프로그램과의 네트워크 연결을 차단한다.

[8] 이와 같이 종래의 휴대단말기에 적용되는 안티 멀웨어(Anti-Malware) 솔루션들은 소프트웨어 기반으로 구축되어 그대로 모바일 디바이스로 사용되고 있다. 그런데, 모바일 디바이스는 중앙처리장치, 배터리와 같은 자원(recource)에 비교적 많은 제한을 받게 되므로 기존 모델을 그대로 사용할 경우 성능(performance) 저하로 인하여 사용자가 악성코드 검출 이외의 다른 작업을 수행하는데 불편함을 겪게 된다.

[9] 더욱이, 종래의 휴대단말기에 적용되는 소프트웨어 기반의 바이러스 백신 솔루션을 이용하는 경우, 네트워크를 통해 수신되는 패킷들을 감시할 때 성능 저하로 인하여 모든 패킷들을 모니터링하는데 어려움이 있었다.

발명의 상세한 설명

기술적 과제

[10] 따라서, 본 발명의 목적은 소프트웨어 기반의 바이러스 백신 솔루션의 성능저하를 근본적으로 해결하고, 소프트웨어 방식의 지협적인 멀웨어 시그니쳐(악성코드 서명) 데이터베이스의 한계를 벗어날 수 있도록 하기 위하여, 스템온칩상의 메모리 기반으로 방화벽과 안티멀웨어 엔진을 구축하고 바이러스 시그니쳐 데이터베이스를 지역적으로 반영되도록 변경하여 휴대단말기로 유입되는 악성코드를 검출하는 장치를 제공하는데 있다.

[11] 본 발명의 다른 목적은 시스템온칩상의 메모리 기반으로 방화벽과 안티멀웨어 엔진을 구축하여 악성코드를 검출함에 있어서, 시스템온칩용 메모리상의 멀웨어 시그니쳐 데이터베이스에 등록된 악성코드의 패턴을 참조하여 악성코드를 검출하는데 있다.

과제 해결 수단

[12] 상기와 같은 목적을 달성하기 위한 본 발명은,

[13] 시스템온칩 기반의 악성코드 검출을 위해 시스템온칩 내의 각부를 총괄제어하는 중앙처리장치와;

[14] 네트워크인터페이스부를 통해 외부로부터 입력되는 패킷들을 분류하고 기 설정된 내용에 따라 그 분류된 패킷에 대한 얼라우, 드롭 등의 필터링작업을 수행하여 그 결과를 어플리케이션용 메모리에 출력하거나, 안티 멀웨어 엔진에 출력하는 시스템온칩용 메모리 기반의 방화벽과;

[15] 상기 방화벽으로부터 입력되는 파일 내의 코드 패턴과 시스템온칩용 메모리상의 멀웨어 시그니쳐 데이터베이스에 등록된 악성코드의 패턴 간의 패턴 매칭 작업을 수행하여 악성코드를 검출하는 시스템온칩용 메모리 기반의

안티 멀웨어 엔진과;

[16] 상기 중앙처리장치와 연계하여, 상기 방화벽과 안티 멀웨어 엔진의 구동을 제어하는 시스템온칩용 메모리 기반의 콘트롤 모듈과;

[17] 상기 악성코드의 패턴이 저장되어 있는 멀웨어 시그니쳐 데이터베이스;로 구성한 시스템온칩을 포함하여 구성함을 특징으로 한다.

[18] 바람직하게, 상기 시스템온칩과 상호 작용하는 모바일 디바이스용 어플리케이션부는, 어플리케이션용 메모리에 구축되어 백신버전을 업데이트하고, 서버측에서 사용하는 네트워크에 따라 해당 접속방식을 채택하는 모바일디바이스용 어플리케이션부와 접속된다.

발명의 효과

[19] 본 발명은 시스템온칩상에서 시스템온칩 내의 메모리 기반으로 구성되어 휴대단말기로 유입되는 악성코드를 검출하도록 함으로써, 바이러스 스캐닝 및 매칭 성능이 향상된다. 이에 따라, 모바일 디바이스 상에서 다른 작업을 수행하면서 동시에 바이러스 백신 서비스를 수행할 수 있는 효과가 있다.

[20] 또한, 시스템온칩 내의 메모리 기반으로 구성된 방화벽을 통해 패킷들도 모두 모니터링할 수 있으므로 모바일 바이러스로부터 모바일 디바이스를 좀 더 안전한 상태로 유지할 수 있는 효과가 있다.

[21] 또한, 시스템온칩용 메모리상에 멀웨어 시그니쳐 데이터베이스를 구축하여 악성코드의 패턴을 등록해 둠으로써, 안티 멀웨어 엔진이 패턴 매칭작업을 빠르게 진행할 수 있으며, 멀웨어 시그니쳐 데이터베이스를 업데이트 할 때도 자동적으로 네트워크로부터 업데이트 할 수 있게 된다.

도면의 간단한 설명

[22] 도 1은 본 발명에 의한 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치의 블록도.

[23] 도 2는 도 1에서 모바일 디바이스용 어플리케이션부의 상세 블록도.

[24] ***도면의 주요 부분에 대한 부호의 설명***

[25] 100 : 시스템온칩 110 : 중앙처리장치

[26] 120 : 네트워크인터페이스부 130 : 시스템온칩용 메모리

[27] 131 : 방화벽 131A : 패킷식별부

[28] 131B : 패킷 필터링부 132 : 안티멀웨어 엔진

[29] 133A : 콘트롤모듈 133B : 멀웨어 시그니쳐 데이터베이스

[30] 140 : 입출력인터페이스부 150 : 메모리인터페이스부

[31] 160 : 주변장치 200 : 어플리케이션용 메모리

[32] 210 : 모바일디바이스용 어플리케이션부

[33] 211 : 어플리케이션 모듈 211A : 버전동기화 모듈

[34] 211B : 업데이트 모듈 211C : 센터컨넥션 모듈

[35] 212 : 데이터베이스 정보부 212A : 센터 URL 정보부

[36] 212B : 디바이스 정보부

발명의 실시를 위한 형태

[37] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하면 다음과 같다.

[38] 도 1은 본 발명에 의한 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치의 실시 구현예를 보인 블록도로서 이에 도시한 바와 같이,

[39] 시스템온칩(100)상에 구축된 중앙처리장치(110), 네트워크인터페이스부(120), 시스템온칩용 메모리(130), 입출력인터페이스부(140), 메모리인터페이스부(150), 주변장치(160)와;

[40] 상기 메모리인터페이스부(150)를 통해 시스템온칩(100)과 연결되어 연계동작하는 어플리케이션용 메모리(200)상의 모바일디바이스용 어플리케이션부(210);로 구성한다.

[41] 시스템온칩(100)은 휴대단말기의 메인피씨비(main PCB)상에 탑재되어 어플리케이션용 메모리(200) 상에 구축된 모바일 디바이스용 어플리케이션부(210)와 연계동작한다. 그리고, 상기 시스템온칩(100)은 입출력 데이터 흐름의 정상 작업 상태 규정으로 사전 프로그램되는 자율 감시 모드와, 현재의 상태가 정상 상태의 규정을 초과하는 경우 입력 및 출력 채널을 디스에이블하는 모드로 운용된다.

[42] 중앙처리장치(110)는 시스템온칩(100)상에 구축된 각 구성요소 즉, 네트워크인터페이스부(120), 시스템온칩용 메모리(130), 입출력인터페이스부(140), 메모리인터페이스부(150) 및 주변장치(160)의 구동을 총괄적으로 제어하는 역할을 수행한다. 또한, 상기 중앙처리장치(110)는 후술하는 바와 같이 시스템온칩용 메모리(130) 기반의 방화벽(131), 안티멀웨어 엔진(132), 콘트롤모듈(133A) 및 멀웨어 시그니쳐 데이터베이스(133B)를 구동시켜 악성코드를 검출함에 있어서, 배터리 전력소모를 감안하여 적절한 주기나 시점에서 수행되도록 제어하는 역할을 수행한다.
네트워크인터페이스부(120)는 외부로부터 새롭게 수신되어 어플리케이션용 메모리(200)에 저장될 패킷들을 상기 중앙처리장치(110)의 제어하에 시스템온칩용 메모리(130)에 전달하는 역할을 수행한다.

[43] 상기 시스템온칩용 메모리(130)는 추후 수정보완 작업이 가능한 악성 코드 검출을 위한 구성요소(코드)들이 구축되는 영역으로서, 패킷식별부(131A) 및 패킷 필터링부(131B)로 구성된 방화벽(firewall)(131), 안티멀웨어 엔진(Anti-malware engine)(132), 콘트롤모듈(133A) 및 멀웨어 시그니쳐 데이터베이스(Malware Signaature DB)(133B)로 구성된다.

[44] 상기 시스템온칩용메모리(130)의 방화벽(131)에서, 패킷 식별부(131A)는 입력 패킷들을 분류하여 패킷 필터링부(131B)에 출력한다. 이때, 상기 패킷 필터링부(131B)는 어플리케이션용 메모리(200)의 설정 내용에 따라 상기 입력

패킷에 대한 얼라우(allow), 드롭(drop) 등의 필터링작업을 수행한다.

[45] 상기 패킷 필터링부(131B)에서 필터링된 패킷들은 상기 중앙처리장치(110) 및 콘트롤모듈(133A)의 제어에 의해 내부버스(BUS) 및 메모리인터페이스부(150)를 통해 어플리케이션용 메모리(200)에 저장되거나, 그 내부버스(BUS)를 통해 안티 멀웨어 엔진(132)에 전달된다. 상기 어플리케이션용 메모리(200)에는 운영체제(OS: Operating System) 및 모바일 디바이스에서 사용되는 각종 프로그램이 탑재된다.

[46] 안티 멀웨어 엔진(132)은 상기 패킷 필터링부(131B)에서 출력되는 패킷 필터링된 파일 및 상기 입출력인터페이스부(20)로부터 새로 입력되는 파일을 대상으로 악성코드 검출(malware detection) 작업을 수행한다. 멀웨어 시그니쳐 데이터베이스(133B)는 시스템온칩용 메모리(130)상에 구축되는데, 상기 안티 멀웨어 엔진(132)은 악성코드 검출을 위해 그 멀웨어 시그니쳐 데이터베이스(133B)에 등록된 악성코드의 패턴과 상기 경로로 입력된 파일 내의 코드 패턴 간의 패턴 매칭 작업을 수행한다.

[47] 콘트롤모듈(133A)은 상기 중앙처리장치(110)와 연계하여 상기 방화벽(131) 및 안티 멀웨어 엔진(132)의 구동을 제어하여 이들이 상기와 같이 동작되도록 한다.

[48] 상기와 같이 동작하는 시스템온칩(100)은 네트워크를 통해 방화벽 코드(firewall code)나 안티 멀웨어 엔진의 코드 등이 변경되거나 수정될 때 업데이트 된다.

[49] 도 2는 어플리케이션용 메모리(200)상에 구축되어 상기 시스템온칩(100)과 연계 동작하는 상기 모바일 디바이스용 어플리케이션부(210)의 구조를 나타낸 것으로, 이에 도시한 바와 같이 크게 어플리케이션 모듈(211)과 데이터베이스 정보부(212)로 구성된다.

[50] 그리고, 상기 어플리케이션 모듈(211)은 버전동기화 모듈(Version sync module)(211A), 업데이트 모듈(Update module)(211B), 센터컨넥션 모듈(Center Connection module)(211C) 및 태그 발생 모듈(Tag generation module)(211D)로 구성되고, 데이터베이스 정보부(212)는 센터(center) URL 정보부(212A) 및 디바이스 정보부(212B)로 구성된다.

[51] 버전동기화 모듈(211A)은 서버의 백신 버전과 휴대단말기의 백신 버전을 소정 주기로 비교하여 그들이 상이할 경우, 업데이트 모듈(211B)을 동작시켜 휴대단말기의 백신 버전이 서버의 최신 버전으로 업데이트되도록 한다. 또한, 상기 버전동기화 모듈(211A)은 서버측의 멀웨어 시그니쳐 데이터베이스를 업데이트시켜야 하는 상황에서도 상기 업데이트 모듈(211B)을 동작시켜 휴대단말기의 백신 버전이 업데이트되도록 한다.

[52] 이와 같이 백신 버전을 끊임없이 발생하는 취약점을 기반으로 수시로 업데이트해야 보안 정책이 유효하다.

[53] 상기 버전동기화 모듈(211A)은 서버측의 시그니쳐 데이터베이스를 업데이트 해야 하는 상황에서도 상기 업데이트 모듈(211B)을 동작시켜 휴대단말기의 백신

버전이 최신 버전으로 업데이트되도록 한다.

[54] 센터컨넥션 모듈(211C)은 여러 방식의 접속 방법이 사용자에게 주어져있을 때, 그 접속 방식을 우선 순위화 하여 서버측에서 사용하는 네트워크에 따라 해당 접속방식을 채택한다. 예를 들어, WiFi를 사용할 수 있는 상태라면, 이동통신사를 선택하여 센터URL에 접속하는 대신에 WiFi를 통하여 접속하도록 한다. 이때, 센터 URL 정보부(212A)는 상기 채택된 접속방식(예: 무선랜(예: WiFi), 이동통신사)으로 상기 네트워크인터페이스부(120)를 통해 휴대단말기를 서버측의 네트워크와 연결하는데 사용된다.

[55] 태그발생 모듈(211D)은 상기 멀웨어 시그니쳐 데이터베이스(133B)상의 운영체제(OS)별로 태그(tag)를 발생하고, 이렇게 발생된 태그가 그 멀웨어 시그니쳐 데이터베이스(133B)에 저장된다.

[56] 또한, 상기 태그발생 모듈(211D)은 상기 멀웨어 시그니쳐 데이터베이스(133B)의 업데이트 시 해당 데이터베이스가 어느 지역정보인지, 어떤 버전정보인지 태깅하는 역할을 수행한다. 상기 버전정보 및 지역정보는 상기 태그발생 모듈(211D)에서 저장 관리된다.

[57] 디바이스 정보부(212B)는 해당 디바이스에서 필요로 하는 정보들을 유지시키는 역할을 수행한다.

[58] 이상에서 본 발명의 바람직한 실시예에 대하여 상세히 설명하였지만, 본 발명의 권리범위가 이에 한정되는 것이 아니라 다음의 청구범위에서 정의하는 본 발명의 기본 개념을 바탕으로 보다 다양한 실시예로 구현될 수 있으며, 이러한 실시예들 또한 본 발명의 권리범위에 속하는 것이다.

서열목록 Free Text

[59] 모바일 디바이스, 안티멀웨어, 시스템온칩, 방화벽, 안티멀웨어 엔진

청구범위

[청구항 1] 시스템온칩 기반의 악성코드 검출을 위해 시스템온칩 내의 각부를 총괄제어하는 중앙처리장치와;
네트워크인터페이스부를 통해 외부로부터 입력되는 패킷들을 분류하고 기 설정된 내용에 따라 그 분류된 패킷에 대한 얼라우, 드롭 등의 필터링작업을 수행하여 그 결과를 어플리케이션용 메모리에 출력하거나, 안티 멀웨어 엔진에 출력하는 시스템온칩용 메모리 기반의 방화벽과;
상기 방화벽으로부터 입력되는 파일 내의 코드 패턴 및 상기 입출력인터페이스부로부터 입력되는 파일 내의 코드 패턴과 시스템온칩용 메모리상의 멀웨어 시그니쳐 데이터베이스에 등록된 악성코드의 패턴 간의 패턴 매칭 작업을 수행하여 악성코드를 검출하는 시스템온칩용 메모리 기반의 안티 멀웨어 엔진과;
상기 중앙처리장치와 연계하여, 상기 방화벽과 안티 멀웨어 엔진의 구동을 제어하는 시스템온칩용 메모리 기반의 콘트롤 모듈과;
상기 악성코드의 패턴이 저장되어 있는 멀웨어 시그니쳐 데이터베이스;로 구성된 시스템온칩을 포함하여 구성한 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[청구항 2] 제1항에 있어서, 시스템온칩용 메모리는 네트워크인터페이스부를 통해 외부와 연결되고, 메모리 인터페이스부를 통해서는 상기 모바일 디바이스용 어프리케이션부와 연결되도록 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[청구항 3] 제1항에 있어서, 방화벽은
입력 패킷들을 분류하는 패킷 식별부와;
어플리케이션용 메모리의 설정 내용에 따라 상기 식별된 패킷에 대한 얼라우, 드롭 등의 필터링작업을 수행하는 패킷 필터링부;로 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[청구항 4] 제1항에 있어서, 시스템온칩은 네트워크를 통해 방화벽 코드나 안티 멀웨어 엔진의 코드 등이 변경되거나 수정될 때 업데이트되는 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[청구항 5] 제1항에 있어서, 시스템온칩 내의 멀웨어 시그니쳐

데이터베이스는 네트워크를 통해 업데이트되는 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[청구항 6] 제1항에 있어서, 모바일 디바이스용 어플리케이션부는 어플리케이션용 메모리에 구축된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

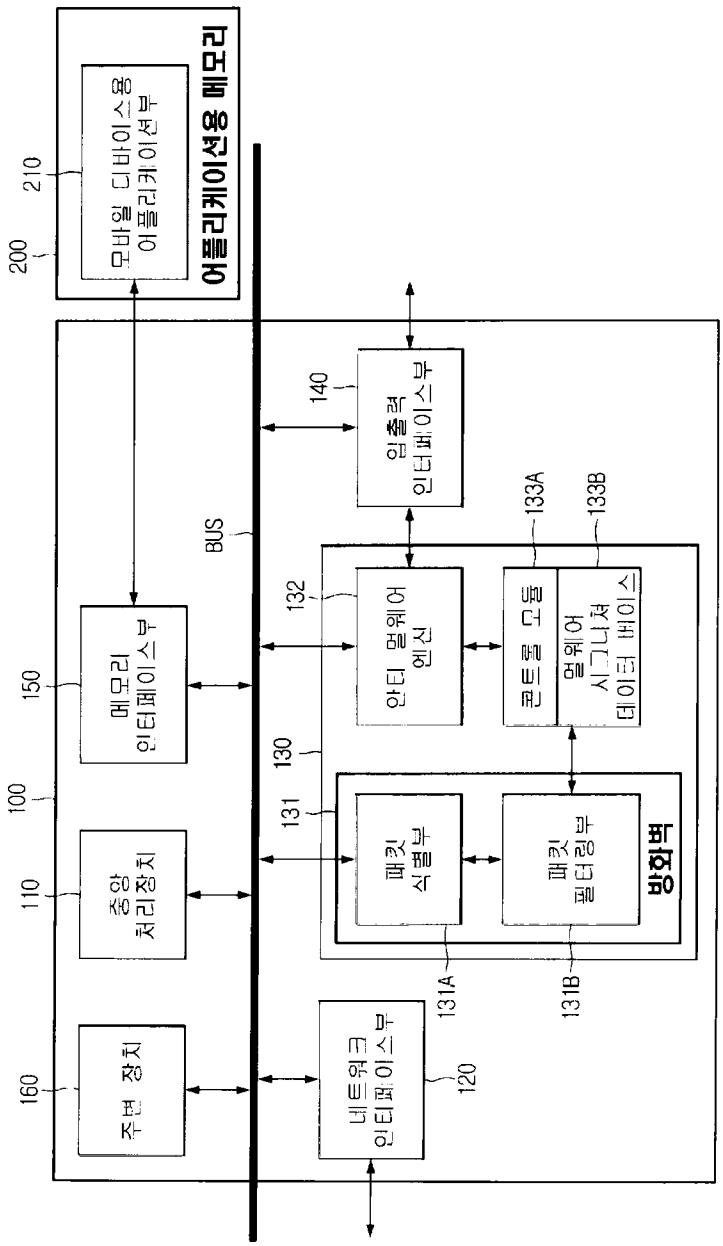
[청구항 7] 제1항에 있어서, 모바일 디바이스용 어플리케이션부는 서버의 백신 버전과 휴대단말기의 백신 버전을 소정 주기로 비교하여 그들이 상이할 경우, 업데이트 모듈을 동작시켜 휴대단말기의 백신 버전이 서버의 최신 버전으로 업데이트 되도록 하는 어플리케이션 모듈을 포함하여 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[청구항 8] 제7항에 있어서, 어플리케이션 모듈은 여러 방식의 접속 방법이 사용자에게 주어져있을 때, 그 접속 방식을 우선 순위화 하여 서버측에서 사용하는 네트워크에 따라 해당 접속방식을 채택하는 센터컨넥션 모듈을 포함하여 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

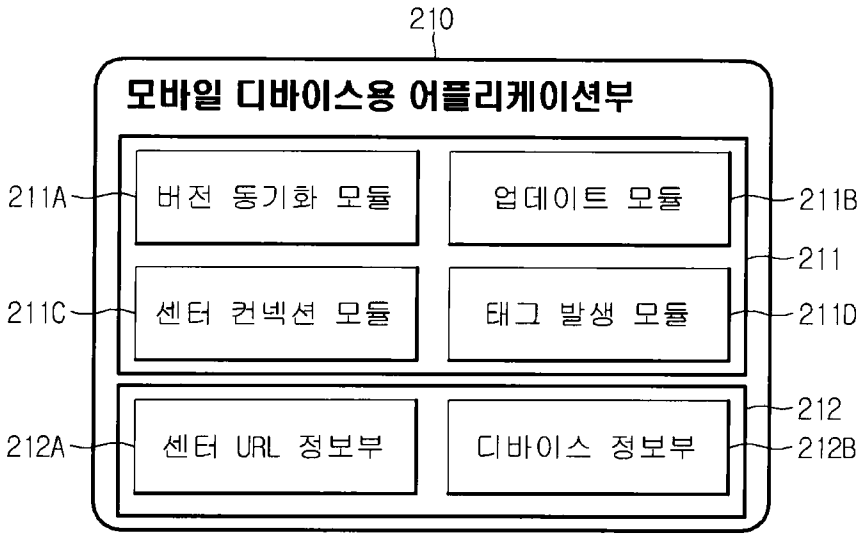
[청구항 9] 제7항에 있어서, 어플리케이션 모듈은 상기 멀웨어 시그니쳐 데이터베이스상의 운영체제별로 태그를 발생하여 그 멀웨어 시그니쳐 데이터베이스에 저장되도록 하는 태그발생 모듈을 포함하여 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[청구항 10] 제1항에 있어서, 모바일 디바이스용 어플리케이션부는 채택된 접속방식으로 상기 매체 접근 제어부를 통해 휴대단말기를 서버측의 네트워크와 연결하는 센터 URL 정보부와;
해당 디바이스에서 필요로 하는 정보들을 유지시키는 디바이스 정보부;로 구성된 데이터베이스 정보부를 포함하여 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[Fig. 1]


어플리케이션용 메모리
모바일 디바이스용 어플리케이션부
210
200
BUS
입출력 인터페이스부
140
133A
133B
안티 멀웨어 엔진
콘트롤 모듈
멀웨어 시그니쳐 데이터 베이스
132
130
131
패킷 식별부
패킷 필터링부
방화벽
131A
131B
메모리 인터페이스부
150
중앙 처리장치
110
100
주변 장치
160
네트워크 인터페이스부
120

[Fig. 2]


210
모바일 디바이스용 어플리케이션부
211A
버전 동기화 모듈
업데이트 모듈
211B
211
211C
센터 컨넥션 모듈
태그 발생 모듈
211D
212
212A
센터 URL 정보부
디바이스 정보부
212B