

(12) 특허협력조약에 의하여 공개된 국제출원

정정판

(19) 세계지식재산권기구
국제사무국



(43) 국제공개일
2010년 10월 14일 (14.10.2010)

PCT

(10) 국제공개번호
WO 2010/117153 A9

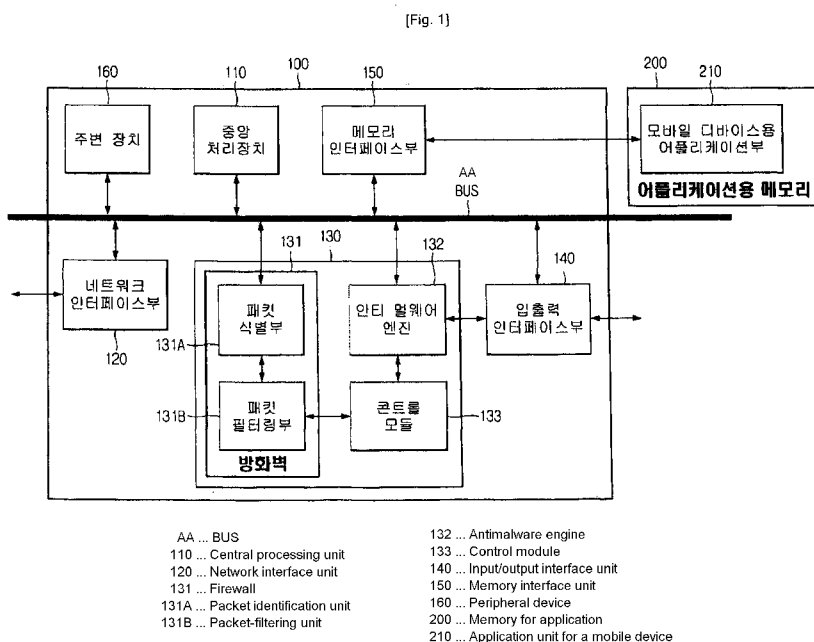
- (51) 국제특허분류:
G06F 21/00 (2006.01) H04B 1/40 (2006.01)
- (21) 국제출원번호: PCT/KR2010/001851
- (22) 국제출원일: 2010년 3월 26일 (26.03.2010)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2009-0030669 2009년 4월 9일 (09.04.2009) KR
- (71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): 삼성에스디에스 주식회사 (SAMSUNG SDS CO., LTD.) [KR/KR]; 서울시 강남구 역삼 2동 707-19 이록빌딩, 135-918 Seoul (KR).
- (72) 발명자: 김
- (75) 발명자/출원인 (US 에 한하여): 유인선 (YOO, In Seon) [KR/KR]; 서울특별시 노원구 하계 1동 삼익아파트 2-103, 139-231 Seoul (KR).

- (74) 대리인: 최태창 (CHOI, Tae Chang); 서울시 강남구 역삼동 642-6 성지하이츠 3차 501호, 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),

[다음 쪽 계속]

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

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



(57) Abstract: The present invention relates to a technique for constructing a firewall and an antimalware engine on the basis of a memory for a system-on-a-chip to detect malicious code intruding on a mobile device. The aim 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 from 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 among the code patterns in the file input from the firewall and the patterns of the malicious code registered in a malware signature database of

an application unit for a mobile device, to detect malicious code; 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]



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(88) 국제조사보고서 공개일:

2011 년 1 월 20 일

(48) 본 정정판 공개일:

2011 년 3 월 10 일

(15) 정정사항에 관한 정보:

2011 년 3 월 10 일 자 공지 참조

공개:

- 국제조사보고서와 함께 (조약 제 21 조(3))
- 규칙 91.3(b) 규정에 의한 명백한 잘못의 정정 허가에 관한 정보와 함께 (규칙 48.2(i))

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 모바일 디바이스용 어플리케이션부의 멀웨어 시그니처 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 피해를 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 시그니처 매칭부를 구비하여, 바이러스 시그니처 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 시그니처들과 매칭되는 것을 찾아 바이러스 감염 여부를 확인하거나 비정상적인 파일들을 검출한다. 또한, 종래의 휴대단말기에 적용되는 방화벽(firewall)은 정책 설정여부에 따라 외부로부터 입력되는 모든 네트워크 액세스를 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(resource)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 시그니처(악성코드 서명) 데이터베이스의 한계를 벗어날 수 있도록 하기 위하여, 시스템온칩상의 메모리 기반으로 방화벽과 안티멀웨어 엔진을 구축하고 바이러스 시그니처 데이터베이스를 지역적으로 반영되도록 변경하여 휴대단말기로 유입되는 악성코드를 검출하는 장치를 제공하는데 있다.

과제 해결 수단

- [11] 상기와 같은 목적을 달성하기 위한 본 발명은,
 [12] 시스템온칩 기반의 악성코드 검출을 위해 시스템온칩 내의 각부를 총괄제어하는 중앙처리장치와;
 [13] 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;
 [14] 상기 방화벽으로부터 입력되는 파일 내의 코드 패턴과 모바일 디바이스용 어플리케이션부의 멀웨어 시그니처 데이터베이스에 등록된 악성코드의 패턴 간의 패턴 매칭 작업을 수행하여 악성코드를 검출하는 시스템온칩용 메모리 기반의 안티 멀웨어 엔진과;
 [15] 상기 중앙처리장치와 연계하여, 상기 방화벽과 안티 멀웨어 엔진의 구동을 제어하는 시스템온칩용 메모리 기반의 컨트롤 모듈;로 구성된 시스템온칩을 포함하여 구성함을 특징으로 한다.

- [16] 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

- [17] 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.
- [18] 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.

도면의 간단한 설명

- [19] 도 1은 본 발명에 의한 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치의 블록도.
- [20] 도 2는 도 1에서 모바일 디바이스용 어플리케이션부의 상세 블록도.
- [21] ***도면의 주요 부분에 대한 부호의 설명***
- [22] 100 : 시스템온칩 110 : 중앙처리장치
- [23] 120 : 네트워크인터페이스부 130 : 시스템온칩용 메모리
- [24] 131 : 방화벽 131A : 패킷식별부
- [25] 131B : 패킷 필터링부 132 : 안티멀웨어 엔진
- [26] 133 : 콘트롤모듈 140 : 입출력인터페이스부
- [27] 150 : 메모리인터페이스부 160 : 주변장치
- [28] 200 : 어플리케이션용 메모리 210 : 모바일디바이스용 어플리케이션부
- [29] 211 : 어플리케이션 모듈 211A : 버전동기화 모듈
- [30] 211B : 업데이트 모듈 211C : 센터컨넥션 모듈
- [31] 212 : 데이터베이스 정보부 212A : 센터 URL 정보부
- [32] 212B : 디바이스 정보부 212C : 멀웨어 시그니처 데이터베이스

발명의 실시를 위한 형태

- [33] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하면 다음과 같다.
- [34] 도 1은 본 발명에 의한 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치의 실시 구현예를 보인 블록도로서 이에 도시한 바와 같이,
- [35] 시스템온칩(100)상에 구축된 중앙처리장치(110), 네트워크인터페이스부(120), 시스템온칩용 메모리(130), 입출력인터페이스부(140), 메모리인터페이스부(150), 주변장치(160)와;
- [36] 상기 메모리인터페이스부(150)를 통해 시스템온칩(100)과 연결되어

연계동작하는 어플리케이션용 메모리(200)상의 모바일디바이스용 어플리케이션부(210);로 구성한다.

- [37] 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.
- [38] 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) 및 콘트롤모듈(133)을 구동시켜 악성코드를 검출함에 있어서, 배터리 전력소모를 감안하여 적절한 주기나 시점에서 수행되도록 제어하는 역할을 수행한다.
- [39] 네트워크인터페이스부(120)는 외부로부터 새롭게 수신되어 어플리케이션용 메모리(200)에 저장될 패킷들을 상기 중앙처리장치(110)의 제어하에 시스템온칩용 메모리(130)에 전달하는 역할을 수행한다.
- [40] 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(133)로 구성된다.
- [41] 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.
- [42] 상기 패킷 필터링부(131B)에서 필터링된 패킷들은 상기 중앙처리장치(110) 및 콘트롤모듈(133)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.
- [43] 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 시그니처 데이터베이스(212C)는 모바일 디바이스용 어플리케이션부(210)의 데이터베이스 정보부(212)상에 구축되는데, 상기 안티 멀웨어 엔진(132)은

악성코드 검출을 위해 그 멀웨어 시그니처 데이터베이스(212C)에 등록된 악성코드의 패턴과 상기 경로로 입력된 파일 내의 코드 패턴 간의 패턴 매칭 작업을 수행한다.

- [44] 컨트롤모듈(133)은 상기 중앙처리장치(110)와 연계하여 상기 방화벽(131) 및 안티 멀웨어 엔진(132)의 구동을 제어하여 이들이 상기와 같이 동작되도록 한다.
- [45] 상기와 같이 동작하는 시스템온칩(100)은 네트워크를 통해 방화벽 코드(firewall code)나 안티 멀웨어 엔진의 코드 등이 변경되거나 수정될 때 업데이트 된다.
- [46] 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.
- [47] 상기 어플리케이션 모듈(211)은 버전동기화 모듈(Version sync module)(211A), 업데이트 모듈(Update module)(211B) 및 센터컨넥션 모듈(Center Connection module)(211C)로 구성되고, 데이터베이스 정보부(212)는 센터(center) URL 정보부(212A), 디바이스 정보부(212B) 및 멀웨어 시그니처 데이터베이스(Malware Signaature DB)(212C)로 구성된다.
- [48] 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 시그니처 데이터베이스를 업데이트시켜야 하는 상황에서도 업데이트 모듈(211B)을 동작시켜 휴대단말기의 백신 버전이 업데이트되도록 한다.
- [49]
- [50] *이와 같이 백신 버전을 끊임없이 발생하는 취약점을 기반으로 수시로 업데이트해야 보안 정책이 유효하다.
- [51] 상기 버전동기화 모듈(211A)은 서버측의 시그니처 데이터베이스를 업데이트 해야 하는 상황에서도 상기 업데이트 모듈(211B)을 동작시켜 휴대단말기의 백신 버전이 최신 버전으로 업데이트되도록 한다.
- [52] 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.
- [53] 디바이스 정보부(212B)는 해당 디바이스에서 필요로 하는 정보들을 유지시키는 역할을 수행한다.

- [54] 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

- [55] 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 모바일 디바이스용 어플리케이션부의 멀웨어 시그니처 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 컨트롤 모듈;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 통해서 상기 모바일 디바이스용 어플리케이션부와 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, 모바일 디바이스용 어플리케이션부는 어플리케이션용 메모리에 구축된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.
- [청구항 6] 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 업데이트되도록 하는 어플리케이션 모듈을 포함하여 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

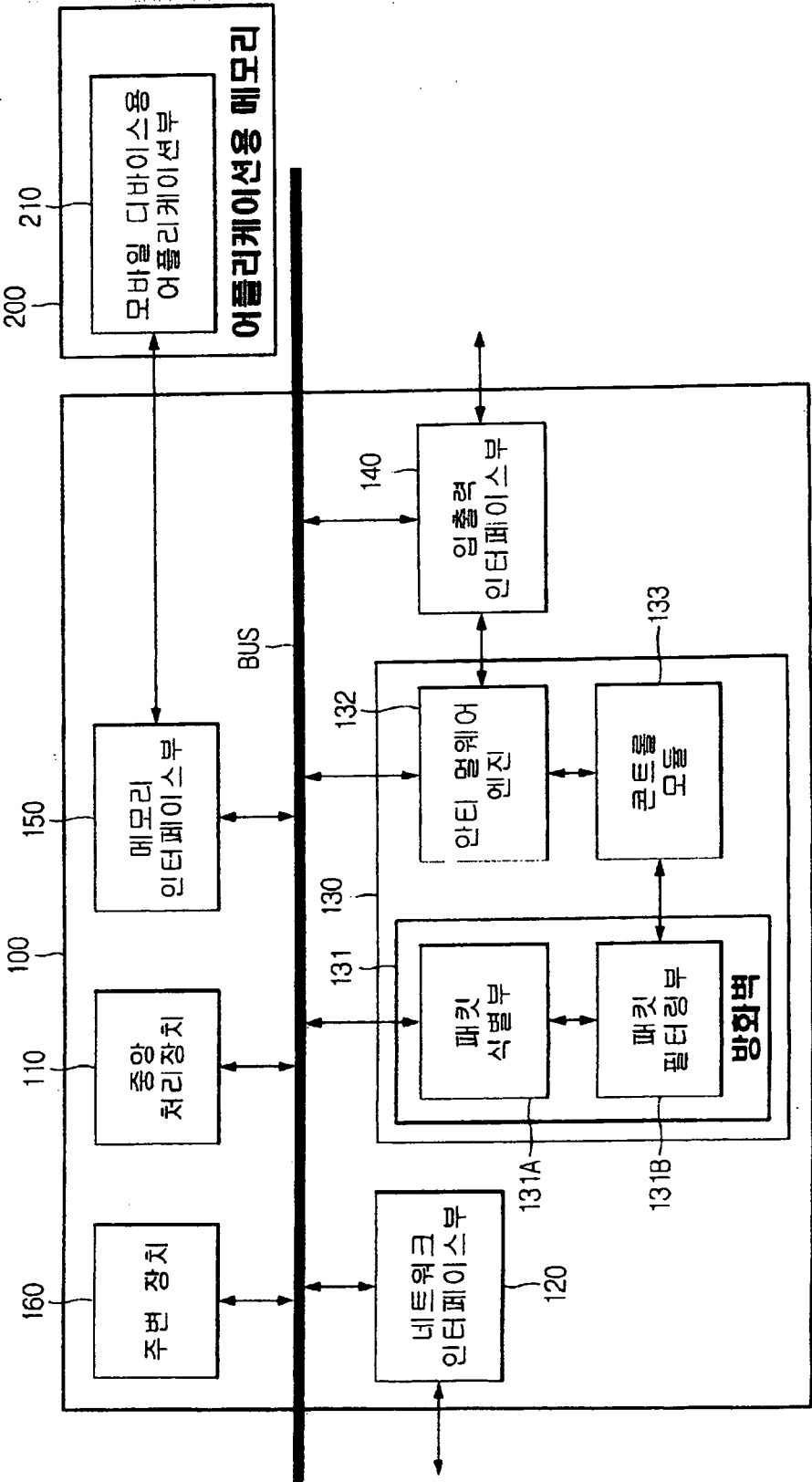
[청구항 7]

제6항에 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.

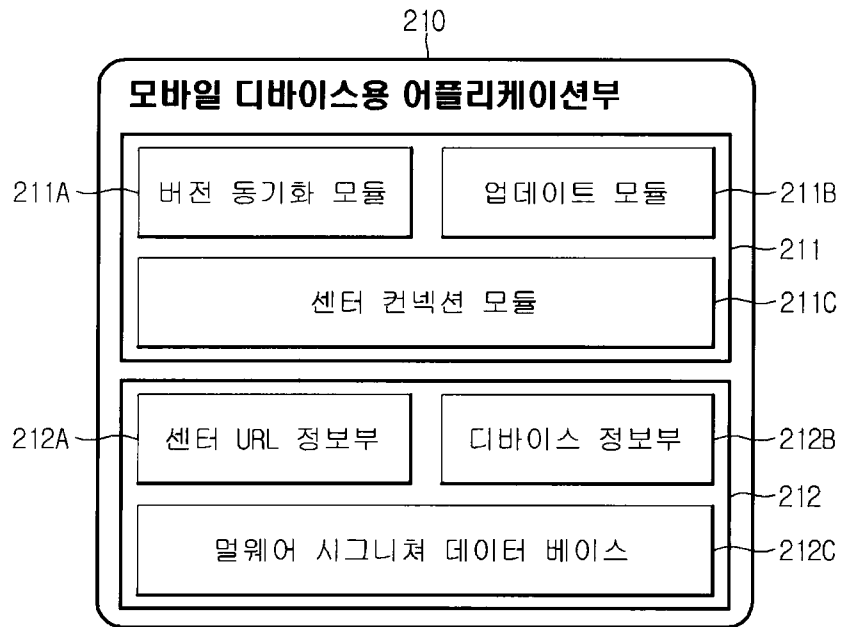
[청구항 8]

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 정보부와; 악성코드 검출을 위한 악성코드의 패턴을 저장관리하는 멀웨어 시그니처 데이터베이스;로 구성된 데이터베이스 정보부를 포함하여 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 기반의 악성코드 검출 장치.

[Fig. 1]



[Fig. 2]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2010/001851**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/00(2006.01)i, H04B 1/40(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/00; H04W 88/02; G06F 9/445; H04W 12/06; H04B 1/40; H04L 12/22; G06F 11/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: firewall, pattern matching, filtering, signature, wireless, mobile, chip, system on chip, malignant code, virus, vaccine

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2008-0113087 A (TELECOM ITALIA S.P.A.) 26 December 2008 Abstract, paragraphs [0060]-[0187], figures 2, 4, 5.	1-9
Y	J.W.LOCKWOOD et al., 'An Extensible, System-On-Programmable-Chip, Content-Aware Internet Firewall', In: FIELD-PROGRAMMABLE LOGIC AND APPLICATIONS Proceedings, LNCS, Vol.2778/2003, pp.859-868 30 September 2003 Abstract, Chapter 2.	1-9
Y	KR 10-2003-0030044 A (BIZMODELINE CO., LTD.) 18 April 2003 Abstract, pages 7-8, figures 4, 5.	6
Y	KR 10-2008-0056548 A (LG CNS CO., LTD.) 23 June 2008 Abstract, paragraphs [0028]-[0046], figures 2, 5.	1-9
Y	JP 2009-037598 A (4THPASS INC) 19 February 2009 Abstract, paragraphs [0050]-[0066], [0071]-[0074], [0094]-[0095], figure 16.	6
A	KR 10-2008-0074271 A (SAMSUNG ELECTRONICS CO., LTD.) 13 August 2008 Abstract, paragraphs [0049]-[0067], [0091]-[0120], figures 2, 3, 7, 8, 11.	1-9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

16 NOVEMBER 2010 (16.11.2010)

Date of mailing of the international search report

17 NOVEMBER 2010 (17.11.2010)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2010/001851

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2004-0090373 A (AHNLAB, INC. et al.) 22 October 2004 Abstract, pages 3-4, figures 1a-1c.	1-9
A	KR 10-2001-0105116 A (CYZENTECH CO., LTD.) 28 November 2001 Abstract, pages 6-7, figures 3, 5, 8a.	1-9

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2010/001851

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2008-0113087 A	26.12.2008	EP 2002634 A1 WO 2007-110094 A1	17.12.2008 04.10.2007
KR 10-2003-0030044 A	18.04.2003	NONE	
KR 10-2008-0056548 A	23.06.2008	CN 101252467 A US 2008-0163356 A1	27.08.2008 03.07.2008
JP 2009-037598 A	19.02.2009	AU 2002-226995 A8 AU 2002-26995 A1 AU 2002-306608 B2 CN 1489736 A EP 1340167 A2 EP 1397769 A2 JP 04-139228 B2 JP 2004-530958 A JP 2005-509322 A JP 2007-179557 A JP 2007-329937 A WO 02-084947 A2 WO 02-084947 A3 WO 02-44892 A2 WO 02-44892 A3	11.06.2002 11.06.2002 23.08.2007 14.04.2004 03.09.2003 17.03.2004 27.08.2008 07.10.2004 07.04.2005 12.07.2007 20.12.2007 24.10.2002 24.10.2002 06.06.2002 06.06.2002
KR 10-2008-0074271 A	13.08.2008	NONE	
KR 10-2004-0090373 A	22.10.2004	NONE	
KR 10-2001-0105116 A	28.11.2001	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/00(2006.01)i, H04B 1/40(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/00; H04W 88/02; G06F 9/445; H04W 12/06; H04B 1/40; H04L 12/22; G06F 11/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 방화벽, 패턴매칭, 필터링, 시그니처, 무선, 모바일, chip, 시스템온칩, 악성코드, 바이러스, 백신

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2008-0113087 A (텔레콤 이탈리아 소시에떼 퍼 아찌오니) 2008.12.26 요약문, 단락 [0060]-[0187], 도면 2,4,5.	1-9
Y	J.W.LOCKWOOD et al., 'An Extensible, System-On-Programmable-Chip, Content-Aware Internet Firewall', In: FIELD-PROGRAMMABLE LOGIC AND APPLICATIONS Proceedings, LNCS, Vol.2778/2003, pp.859-868 2003.09.30 요약문, Chapter 2.	1-9
Y	KR 10-2003-0030044 A (주식회사 비즈모델라인) 2003.04.18 요약문, 페이지 7-8, 도면 4, 5.	6
Y	KR 10-2008-0056548 A (주식회사 엘지씨엔에스) 2008.06.23 요약문, 단락 [0028]-[0046], 도면 2, 5.	1-9
Y	JP 2009-037598 A (4THPASS INC) 2009.02.19 요약문, 단락 [0050]-[0066], [0071]-[0074], [0094]-[0095], 도면 16.	6
A	KR 10-2008-0074271 A (삼성전자주식회사) 2008.08.13 요약문, 단락 [0049]-[0067], [0091]-[0120], 도면 2,3,7,8,11.	1-9

☒ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2010년 11월 16일 (16.11.2010)

국제조사보고서 발송일

2010년 11월 17일 (17.11.2010)

ISA/KR의 명칭 및 우편주소

 대한민국 특허청
(302-701) 대전광역시 서구 선사로 139,
정부대전청사
팩스 번호 82-42-472-7140

심사관

정연정

전화번호 82-42-481-8536



C (계속). 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2004-0090373 A (주식회사 안철수연구소 외 2명) 2004.10.22 요약문, 페이지 3-4, 도면 1a-1c.	1-9
A	KR 10-2001-0105116 A (주식회사 사이젠텍) 2001.11.28 요약문, 페이지 6-7, 도면 3,5,8a.	1-9

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2008-0113087 A	2008.12.26	EP 2002634 A1 WO 2007-110094 A1	2008.12.17 2007.10.04
KR 10-2003-0030044 A	2003.04.18	없음	
KR 10-2008-0056548 A	2008.06.23	CN 101252467 A US 2008-0163356 A1	2008.08.27 2008.07.03
JP 2009-037598 A	2009.02.19	AU 2002-226995 A8 AU 2002-26995 A1 AU 2002-306608 B2 CN 1489736 A EP 1340167 A2 EP 1397769 A2 JP 04-139228 B2 JP 2004-530958 A JP 2005-509322 A JP 2007-179557 A JP 2007-329937 A WO 02-084947 A2 WO 02-084947 A3 WO 02-44892 A2 WO 02-44892 A3	2002.06.11 2002.06.11 2007.08.23 2004.04.14 2003.09.03 2004.03.17 2008.08.27 2004.10.07 2005.04.07 2007.07.12 2007.12.20 2002.10.24 2002.10.24 2002.06.06 2002.06.06
KR 10-2008-0074271 A	2008.08.13	없음	
KR 10-2004-0090373 A	2004.10.22	없음	
KR 10-2001-0105116 A	2001.11.28	없음	