

(43) 국제공개일
2010년 10월 14일 (14.10.2010)

- (51) 국제특허분류:
G06F 21/00 (2006.01) H04B 1/40 (2006.01)
- (21) 국제출원번호: PCT/KR2010/001850
- (22) 국제출원일: 2010년 3월 26일 (26.03.2010)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2009-0030668 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: 겸
- (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

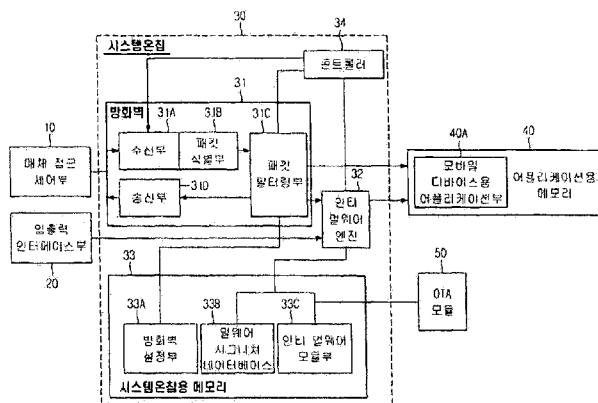
- 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

[다음 쪽 계속]

(54) Title: SYSTEM-ON-CHIP MALICIOUS CODE DETECTION APPARATUS AND APPLICATION-SPECIFIC INTEGRATED CIRCUIT FOR A MOBILE DEVICE

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

[Fig. 1]



- 10 ... Media access control unit
20 ... Input/output interface unit
30 ... System-on-a-chip
31 ... Firewall
31A ... Receiving unit
31B ... Packet identification unit
31C ... Packet-filtering unit
31D ... Transmitting unit
32 ... Antimalware engine
33 ... Memory for system-on-a-chip
33A ... Firewall set unit
33B ... Malware signature database
33C ... Antimalware module unit
34 ... Controller
40 ... Memory for application
40A ... Application unit for a mobile device
50 ... OTA module

(57) Abstract: The present invention relates to a technique for configuring a system-on-a-chip and application-specific integrated circuit (ASIC)-based hardware for detecting malicious code intruding on a mobile device. The present invention is accomplished by a system-on-a-chip comprising: a hardware-based firewall which performs a packet-filtering process on the packet received from an external source via a media access control unit in accordance with the firewall settings established by a firewall set unit on a memory for a system-on-a-chip, and stores the result of the packet-filtering process in a memory for an application, or transmits the result of the packet-filtering process to an antimalware engine; a hardware-based antimalware engine which performs a pattern-matching process among the code patterns in the file transmitted by the firewall or the file received via an input/output interface unit with the pattern of the malicious code registered in a malware signature database of an application unit for a mobile device, to detect malicious code; said memory for a system-on-a-chip, which provides the firewall settings, and supports a file-decoding function for file format recognition in the antimalware engine; and a hardware-based controller which controls switching operations to transmit the file filtered by the firewall directly to the memory for application, or to the antimalware engine, and controls the malicious code detection cycle of the antimalware engine.

(57) 요약서:

[다음 쪽 계속]



본 발명은 시스템온칩상에서 주문형반도체(ASIC) 기반의 하드웨어로 구성되어 휴대단말기로 유입되는 악성코드를 검출하는 기술에 관한 것이다. 이러한 본 발명은 매체 접근 제어부를 통해 외부로부터 수신되는 패킷에 대해 시스템온칩용 메모리상의 방화벽 설정부의 설정 내용에 따라 패킷 필터링작업을 수행한 후 어플리케이션용 메모리에 저장하거나, 안티 멀웨어 엔진에 전달하는 하드웨어 기반의 방화벽과; 상기 방화벽으로부터 전달받은 파일이나 임출력인터페이스부를 통해 수신받은 파일 내의 코드 패턴과 모바일 디바이스용 어플리케이션부의 멀웨어 시그니처 데이터베이스에 등록된 악성코드의 패턴 간의 패턴 매칭 작업을 수행하여 악성코드를 검출하는 하드웨어 기반의 안티 멀웨어 엔진과; 상기 방화벽의 설정내용을 제공함과 아울러, 상기 안티 멀웨어 엔진에서의 파일 포맷 인식을 위한 파일 디코딩 기능을 지원하는 시스템온칩용 메모리와; 상기 방화벽에서 필터링된 파일이 직접 어플리케이션용 메모리에 전달되도록 하거나 안티 멀웨어 엔진에 전달되도록 스위칭 동작을 제어하고, 그 안티 멀웨어 엔진의 악성코드 검출 주기를 제어하는 하드웨어 기반의 컨트롤러;로 구성된 시스템온칩에 의해 달성된다.

명세서

발명의 명칭: 휴대단말기에서의 시스템온칩 및 주문형반도체 기반의 악성코드 검출 장치

기술분야

- [1] 본 발명은 휴대단말기에 적용되어 악성 코드를 검출하는 기술에 관한 것으로, 특히 휴대단말기의 자원 및 성능 향상을 고려하여 시스템온칩상에서 주문형반도체(ASIC) 기반의 하드웨어로 방화벽과 안티멀웨어 엔진을 구축하여, 휴대단말기로 유입되는 악성코드를 검출하도록 한 휴대단말기에서의 시스템온칩 및 주문형반도체 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, 시스템온칩상에서 주문형반도체(ASIC) 기반의 하드웨어로 방화벽과 안티 멀웨어를 구성하고, 바이러스 시그니처 데이터베이스를 지역적으로 반영되도록 변경시킴으로써, 휴대단말기로 유입되는 악성코드를 검출하는 장치를 제공하는데 있다.

과제 해결 수단

- [11] 상기와 같은 목적을 달성하기 위한 본 발명은,
- [12] 메체 접근 제어부를 통해 외부로부터 수신되는 패킷에 대해 시스템온칩용 메모리상의 방화벽 설정부의 설정 내용에 따라 패킷 필터링작업을 수행한 후 어플리케이션용 메모리에 저장하거나, 안티 멀웨어 엔진에 전달하는 하드웨어 기반의 방화벽과;
- [13] 상기 방화벽으로부터 전달받은 파일이나 입출력인터페이스부를 통해 수신받은 파일 내의 코드 패턴과 모바일 디바이스용 어플리케이션부의 멀웨어 시그니처 데이터베이스에 등록된 악성코드의 패턴 간의 패턴 매칭 작업을 수행하여 악성코드를 검출하는 하드웨어 기반의 안티 멀웨어 엔진과;
- [14] 상기 방화벽의 설정내용을 제공함과 아울러, 상기 안티 멀웨어 엔진에서의 파일 포맷 인식을 위한 파일 디코딩 기능을 지원하는 시스템온칩용 메모리와;
- [15] 상기 방화벽에서 필터링된 파일이 직접 어플리케이션용 메모리에 전달되도록 하거나 안티 멀웨어 엔진에 전달되도록 스위칭 동작을 제어하고, 그 안티 멀웨어

엔진의 악성코드 검출 주기를 제어하는 하드웨어 기반의 컨트롤러;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 주문형반도체(ASIC) 기반의 하드웨어로 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, 하드웨어로 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 및 주문형반도체 기반의 악성코드 검출 장치의 블록도.
- [20] 도 2는 도 1에서 모바일 디바이스용 어플리케이션부의 상세 블록도.
- [21] ***도면의 주요 부분에 대한 부호의 설명***
- [22] 10 : 매체 접근 제어부 20 : 입출력인터페이스부
- [23] 30 : 시스템온칩 31 : 방화벽
- [24] 31A : 수신부 31B : 패킷 식별부
- [25] 31C : 패킷 필터링부 31D : 송신부
- [26] 32 안티 멀웨어 엔진 33 : 시스템온칩용 메모리
- [27] 33A : 방화벽 설정부 33B : 디코딩모듈
- [28] 33C : 안티멀웨어 모듈부 34 : 컨트롤러
- [29] 40 : 어플리케이션용 메모리 40A : 모바일 디바이스용 어플리케이션부
- [30] 41 : 어플리케이션 모듈 41A : 버전동기화 모듈
- [31] 41B : 업데이트 모듈 41C : 센터컨넥션 모듈
- [32] 42 : 데이터베이스 정보부 42A : 센터 URL 정보부
- [33] 42B : 디바이스 정보부 42C : 멀웨어 시그니처 데이터베이스
- [34] 50 : OTA 모듈

발명의 실시를 위한 형태

- [35] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하면 다음과 같다.
- [36] 도 1은 본 발명에 의한 휴대단말기에서의 시스템온칩 및 주문형반도체 기반의 악성코드 검출 장치의 실시 구현예를 보인 블록도로서 이에 도시한 바와 같이,

- 매체 접근 제어부(MAC: media access control)(10), 입출력인터페이스부(20), 시스템온칩(30), 어플리케이션용 메모리(40) 및 OTA 모듈(50)로 구성한다.
- [37] 상기 시스템온칩(30)은 방화벽(31), 안티 멀웨어 엔진(Anti-malware engine)(32), 시스템온칩용 메모리(33) 및 컨트롤러(34)로 구성되는데, 이들은 ASIC 기반의 하드웨어로 구현된다.
- [38] 상기 방화벽(31)은 수신부(31A), 패킷 식별부(31B), 패킷 필터링부(31C) 및 송신부(31D)로 구성한다.
- [39] 상기 시스템온칩용 메모리(33)는 방화벽 설정부(33A), 디코딩모듈(33B) 및 안티멀웨어 모듈부(33C)로 구성한다.
- [40] 시스템온칩(30)은 휴대단말기의 메인피씨비(main PCB)상에 탑재되어 주변의 매체 접근 제어부(10), 입출력인터페이스부(20), 어플리케이션용 메모리(40) 상에 구축된 모바일 디바이스용 어플리케이션부(40A) 및 OTA 모듈(50)과 연계동작한다. 그리고, 상기 시스템온칩(30)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.
- [41] 매체 접근 제어부(10)는 OSI 기본 참조 모델의 데이터 연결 계층의 일부로서, 동일한 매체를 여러 노드가 공유하는 특성상에 존재하는 구내 정보 통신망(LAN) 고유의 계층이다. 통신(무선통신)을 통해 외부로부터 수신되는 패킷들이 상기 매체 접근 제어부(10)를 통해 시스템온칩(30)에 전달된다.
- [42] 상기 매체 접근 제어부(10)를 통해 시스템온칩(30)에 전달된 패킷들은 방화벽(31)을 통해 그대로 어플리케이션용 메모리(40)에 저장되거나, 안티 멀웨어 엔진(32)에 전달된다. 상기 어플리케이션용 메모리(40)에는 운영체제(OS: Operating System) 및 모바일 디바이스에서 사용되는 각종 프로그램이 탑재된다.
- [43] 상기 방화벽(31)에서, 수신부(31A)는 상기 매체 접근 제어부(10)를 통해 수신되는 패킷들을 수신처리하여 패킷 식별부(31B)에 전달한다. 이때, 상기 패킷 식별부(31B)는 입력 패킷들을 분류하여 패킷 필터링부(31C)에 출력한다. 상기 패킷 필터링부(31C)는 시스템온칩용 메모리(33)의 방화벽 설정부(33A)의 설정 내용에 따라 상기 입력 패킷에 대한 얼라우(allow), 드롭(drop) 등의 필터링작업을 수행한 후 그 필터링된 패킷들을 그대로 어플리케이션용 메모리(40)에 저장하거나, 안티 멀웨어 엔진(32)에 전달한다.
- [44] 입출력인터페이스부(20)는 입출력형 칩이나 카드, 블루투스 모듈 등을 포함하는 것으로, 모바일 디바이스용 어플리케이션부(40A)에 사용될 파일들을 상기 안티 멀웨어 엔진(32)에 전달한다.
- [45] 안티 멀웨어 엔진(32)은 상기 패킷 필터링부(31C)에서 출력되는 패킷 필터링된 파일 및 상기 입출력인터페이스부(20)로부터 새로 입력되는 파일을 대상으로 악성코드 검출(malware detection) 작업을 수행한다. 멀웨어 시그니처 데이터베이스(42C)는 모바일 디바이스용 어플리케이션부(40A)의 데이터베이스

- 정보부(42)상에 구축되는데, 상기 안티 멀웨어 엔진(32)은 악성코드 검출을 위해 그 멀웨어 시그니처 데이터베이스(42C)에 등록된 악성코드의 패턴과 상기 경로로 입력된 파일 내의 코드 패턴 간의 패턴 매칭 작업을 수행한다.
- [46] 상기 안티 멀웨어 엔진(32)이 상기와 같이 패턴 매칭작업을 수행하기 위해서는 상기 패킷 필터링부(31C)로부터 입력되는 파일의 포맷(File format, Archive format)을 인식한 후 디코딩 작업을 수행해야 하는데, 이 기능을 지원하는 것이 디코딩모듈(33B)이다.
- [47] 안티멀웨어 모듈부(33C)는 시스템온칩(30)에서의 악성코드 검출을 위한 부가적인 기능을 지원한다. 예를 들어, 멀웨어 시그니처 데이터베이스의 일정기간이 지났을 때 데이터베이스를 정리하는 기능, 악성코드 검출의 병렬처리나 주기적인 셋팅 기능, 등을 들 수 있다.
- [48] 상기 디코딩모듈(33B) 및 안티멀웨어 모듈부(33C)는 OTA 모듈(50)을 통해 수동으로 또는 기 설정된 주기로 자동 업데이트된다.
- [49] 콘트롤러(34)는 상기 패킷 필터링부(31C)로부터 출력되는 파일이 상기 안티 멀웨어 엔진(32)에 전달되어 악성코드 검출작업이 수행되도록 하거나, 그대로 어플리케이션용 메모리(40)에 출력되어 저장되도록 하는 스위칭 동작을 제어하고, 악성코드 검출을 수행함에 있어서 배터리 전력소모를 감안하여 적절한 주거나 시점에서 수행되도록 제어하는 역할을 수행한다.
- [50] 도 2는 상기 시스템온칩(30)과 연계하여 동작하는 상기 모바일 디바이스용 어플리케이션부(40A)의 구조를 나타낸 것으로 이에 도시한 바와 같이 크게 어플리케이션 모듈(41)과 데이터베이스 정보부(42)로 구성된다.
- [51] 그리고, 상기 어플리케이션 모듈(41)은 버전동기화 모듈(Version sync module)(41A), 업데이트 모듈(Update module)(41B) 및 센터컨넥션 모듈(Center Connection module)(41C)로 구성되고, 데이터베이스 정보부(42)는 센터(center) URL 정보부(42A), 디바이스 정보부(42B) 및 멀웨어 시그니처 데이터베이스(Malware Signaature DB)(42C)로 구성된다.
- [52] 버전동기화 모듈(41A)은 서버의 백신 버전과 휴대단말기의 백신 버전을 소정 주기로 비교하여 그들이 상이할 경우, 업데이트 모듈(41B)을 동작시켜 휴대단말기의 백신 버전이 서버의 최신 버전으로 업데이트되도록 한다. 또한, 상기 버전동기화 모듈(41A)은 서버측의 멀웨어 시그니처 데이터베이스를 업데이트시켜야 하는 상황에서도 업데이트 모듈(41B)을 동작시켜 휴대단말기의 백신 버전이 업데이트되도록 한다.
- [53] 이와 같이 백신 버전을 끊임없이 발생하는 취약점을 기반으로 수시로 업데이트해야 보안 정책이 유효하다.
- [54] 상기 버전동기화 모듈(41A)은 서버측의 시그니처 데이터베이스를 업데이트 해야 하는 상황에서도 상기 업데이트 모듈(41B)을 동작시켜 휴대단말기의 백신 버전이 최신 버전으로 업데이트되도록 한다.
- [55] 센터컨넥션 모듈(41C)은 여러 방식의 접속 방법이 사용자에게 주어졌을 때,

그 접속 방식을 우선 순위화 하여 서버측에서 사용하는 네트워크에 따라 해당 접속방식을 채택한다. 예를 들어, WiFi를 사용할 수 있는 상태라면, 이동통신사를 선택하여 센터URL에 접속하는대신에 WiFi를 통하여 접속하도록 한다. 이때, 센터 URL 정보부(42A)는 상기 채택된 접속방식(예: 무선랜(예: WiFi), 이동통신사)으로 상기 매체 접근 제어부(10)를 통해 휴대단말기를 서버측의 네트워크와 연결하는데 사용된다.

[56] 디바이스 정보부(42B)는 해당 디바이스에서 필요로 하는 정보들을 유지시키는 역할을 수행한다.

[57] 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

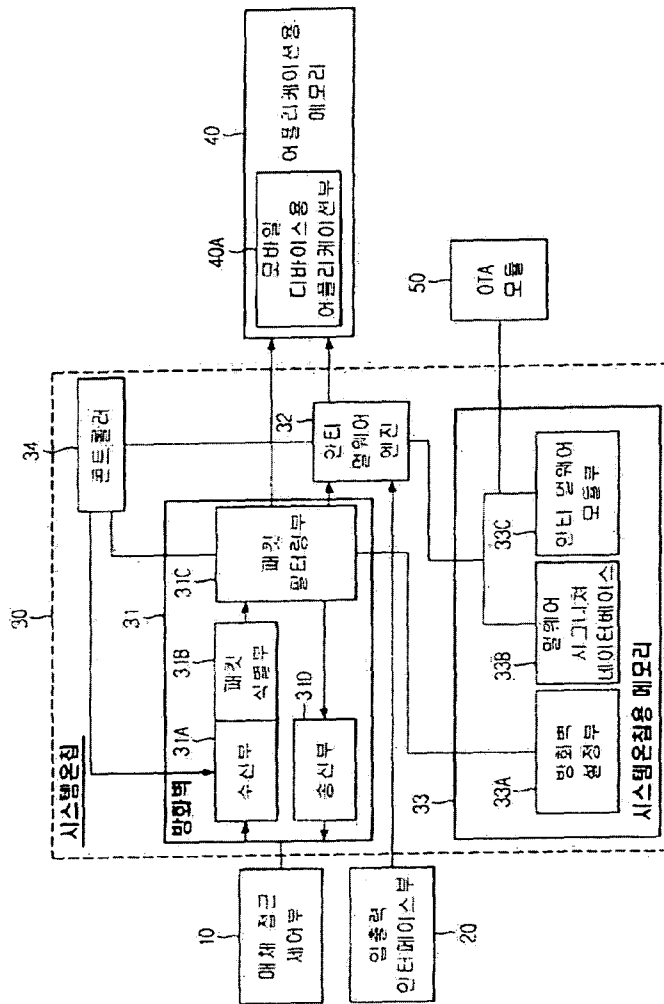
[58] 모바일 디바이스, 안티멀웨어, 시스템온칩, 망화벽, 안티멀웨어 엔진

청구범위

- [청구항 1] 매체 접근 제어부를 통해 외부로부터 수신되는 패킷에 대해 시스템온칩용 메모리상의 방화벽 설정부의 설정 내용에 따라 패킷 필터링작업을 수행한 후 어플리케이션용 메모리에 저장하거나, 안티 멀웨어 엔진에 전달하는 하드웨어 기반의 방화벽과; 상기 방화벽으로부터 전달받은 파일이나 입출력인터페이스부를 통해 수신받은 파일 내의 코드 패턴과 모바일 디바이스용 어플리케이션부의 멀웨어 시그니처 데이터베이스에 등록된 악성코드의 패턴 간의 패턴 매칭 작업을 수행하여 악성코드를 검출하는 하드웨어 기반의 안티 멀웨어 엔진과; 상기 방화벽의 설정내용을 제공함과 아울러, 상기 안티 멀웨어 엔진에서의 파일 포맷 인식을 위한 파일 디코딩 기능을 지원하는 시스템온칩용 메모리와; 상기 방화벽에서 필터링된 파일이 직접 어플리케이션용 메모리에 전달되도록 하거나 안티 멀웨어 엔진에 전달되도록 스위칭 동작을 제어하고, 그 안티 멀웨어 엔진의 악성코드 검출 주기를 제어하는 하드웨어 기반의 컨트롤러;로 구성된 시스템온칩을 포함하여 구성한 것을 특징으로 하는 휴대단말기에서의 시스템온칩 및 주문형반도체 기반의 악성코드 검출 장치.
- [청구항 2] 제1항에 있어서, 시스템온칩은 주문형반도체인 것을 특징으로 하는 휴대단말기에서의 시스템온칩 및 주문형반도체 기반의 악성코드 검출 장치.
- [청구항 3] 제1항에 있어서, 방화벽은 상기 매체 접근 제어부를 통해 수신되는 패킷들을 수신처리하여 패킷 식별부에 전달하는 수신부와; 입력된 패킷들을 분류하여 패킷 필터링부에 출력하는 패킷 식별부와; 시스템온칩용 메모리의 방화벽 설정부의 설정 내용에 따라 입력 패킷에 대한 얼라우, 드롭 등의 필터링작업을 수행하는 패킷 필터링부;로 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 및 주문형반도체 기반의 악성코드 검출 장치.
- [청구항 4] 제1항에 있어서, 시스템온칩용 메모리는 상기 방화벽 내의 패킷 필터링부의 패킷 필터링을 위한 설정값이 저장된 방화벽 설정부와; 상기 안티 멀웨어 엔진의 파일 포맷 인식을 위해 디코딩 작업을 수행하는 디코딩 모듈과; 시스템온칩에서의 멀웨어 시그니처 데이터베이스의 일정기간이

- 지났을 때 데이터베이스를 정리하는 기능, 악성코드 검출의 병렬처리나 주기적인 셋팅 기능 등을 수행하는 안티멀웨어 모듈부;로 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 및 주문형반도체 기반의 악성코드 검출 장치.
- [청구항 5] 제4항에 있어서, 방화벽 설정부와 디코딩 모듈 및 안티멀웨어 모듈부는 네트워크를 통해 방화벽 코드나 상기 안티멀웨어 엔진의 코드 등이 변경 또는 수정될 때 OTA 모듈을 통해 업데이트되는 것을 특징으로 하는 휴대단말기에서의 시스템온칩 및 주문형반도체 기반의 악성코드 검출 장치.
- [청구항 6] 제1항에 있어서, 모바일 디바이스용 어플리케이션부는 어플리케이션용 메모리에 구축된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 및 주문형반도체 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 업데이트되도록하는 어플리케이션 모듈을 포함하여 구성된 것을 특징으로 하는 휴대단말기에서의 시스템온칩 및 주문형반도체 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 및 주문형반도체 기반의 악성코드 검출 장치.
- [청구항 9] 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 및 주문형반도체 기반의 악성코드 검출 장치.

[Fig. 1]



[Fig. 2]

