(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0037547
(43) 공개일자 2012년04월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/20 (2006.01) *G06F 21/06* (2006.01)
(21) 출원번호 10-2010-0099064
(22) 출원일자 2010년10월12일
심사청구일자 2010년10월12일

(71) 출원인
단국대학교 산학협력단
경기도 용인시 수지구 죽전동 126 단국대학교 내
(72) 발명자
김준모
경기도 용인시 기흥구 구성로39번길 13, 우림아파트 102동 908호 (마북동)
나연묵
서울특별시 강남구 압구정로29길 57, 510호 (압구정동, 현대아파트206동)
방성일
경기도 성남시 분당구 양현로 272, 경남아파트 706동 404호 (야탑동, 탑마을)
(74) 대리인
남정길

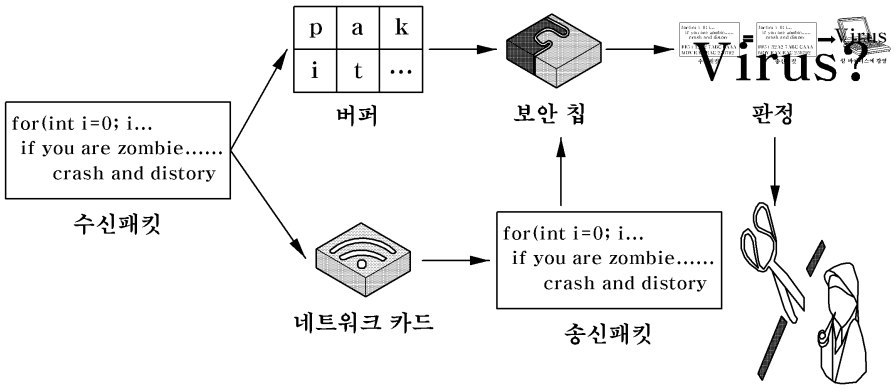
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **악성 패킷 차단 방법 및 시스템**

(57) 요 약

악성 패킷 차단 방법에 있어서, 컴퓨터가 네트워크로부터 수신 패킷을 수신하는 단계; 보안 칩이 상기 수신 패킷을 모니터링하여 동일한 내용이 반복되면 해당 수신 패킷을 상기 보안 칩의 버퍼에 저장하는 단계; 상기 컴퓨터가 상기 네트워크로 송신 패킷을 송신하는 단계; 및 상기 보안 칩이 상기 버퍼에 저장된 상기 수신 패킷과 상기 송신 패킷의 내용의 동일성을 비교하는 단계를 포함한다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	91064
부처명	지식경제부
연구사업명	산업원천기술개발SW기반구축사업
연구과제명	소프트웨어 공학 방법론과 금융공학 지식 기반 차세대 금융 SW 프레임워크
주관기관	단국대학교
연구기간	2010.04.01 ~ 2010.12.31

특허청구의 범위

청구항 1

컴퓨터가 네트워크로부터 수신 패킷을 수신하는 단계;

보안 칩이 상기 수신 패킷을 모니터링하여 동일한 내용이 반복되면 해당 수신 패킷을 상기 보안 칩의 버퍼에 저장하는 단계;

상기 컴퓨터가 상기 네트워크로 송신 패킷을 송신하는 단계; 및

상기 보안 칩이 상기 버퍼에 저장된 상기 수신 패킷과 상기 송신 패킷의 내용의 동일성을 비교하는 단계를 포함하는 악성 패킷 차단 방법.

청구항 2

제 1 항에 있어서,

상기 패킷을 저장하는 단계는

상기 반복하여 수신되는 수신 패킷의 내용 일부가 동일한 경우에 상기 보안 칩의 상기 버퍼에 저장하는 악성 패킷 차단 방법.

청구항 3

제 2 항에 있어서,

상기 패킷의 동일성을 비교하는 단계는

상기 송신 패킷과 상기 버퍼에 저장된 수신 패킷의 내용 일부가 동일한 경우에 악성 패킷으로 판단하는 악성 패킷 차단 방법.

청구항 4

제 1 항에 있어서,

상기 패킷의 동일성을 비교하는 단계는

상기 송신 패킷과 상기 버퍼에 저장된 수신 패킷의 내용 일부가 동일한 경우에 사용자에게 알리는 악성 패킷 차단 방법.

청구항 5

제 1 항에 있어서,

상기 패킷을 비교하는 단계는

상기 송신 패킷 전체와 상기 버퍼에 저장된 수신 패킷 전체의 동일성을 비교하는 악성 패킷 차단 방법.

청구항 6

제 1 항에 있어서,

상기 보안 칩은 주기적으로 초기화되는 악성 패킷 차단 방법.

청구항 7

네트워크로부터 수신 패킷을 수신하고 송신 패킷을 송신하는 컴퓨터; 및

상기 수신 패킷을 모니터링하여 동일한 내용이 반복되면 해당 수신 패킷을 버퍼에 저장하고, 상기 송신 패킷과 상기 버퍼에 저장된 상기 수신 패킷의 내용의 동일성을 비교하는 보안 칩을 포함하는 악성 패킷 차단 시스템.

청구항 8

제 7 항에 있어서,

상기 보안 칩은 상기 반복하여 수신되는 수신 패킷의 내용 일부가 동일한 경우에 상기 버퍼에 저장하는 악성 패킷 차단 시스템.

청구항 9

제 8 항에 있어서,

상기 보안 칩은 상기 송신 패킷과 상기 버퍼에 저장된 수신 패킷의 내용 일부가 동일한 경우에 악성 패킷으로 판단하는 악성 패킷 차단 시스템.

청구항 10

제 7 항에 있어서,

상기 보안 칩은 상기 송신 패킷과 상기 버퍼에 저장된 수신 패킷의 내용 일부가 동일한 경우에 사용자에게 알리는 악성 패킷 차단 시스템.

청구항 11

제 7 항에 있어서,

상기 보안 칩은 상기 송신 패킷 전체와 상기 버퍼에 저장된 수신 패킷 전체의 동일성을 비교하는 악성 패킷 차단 시스템.

청구항 12

제 7 항에 있어서,

상기 보안 칩은 주기적으로 초기화되는 악성 패킷 차단 시스템.

명 세 서

기 술 분 야

[0001] 개시된 기술은 악성 패킷 차단 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] DDOS(Distribute Denial of Service) 해킹으로 인한 피해액이 2009년에 최소 360억 이상이라는 보고서가 현대경제 연구소에서 발표되었다. DDOS 공격의 대부분은 웜(Worm) 바이러스를 통한 좀비 컴퓨터를 확보하여 목표 서버에 일시적으로 패킷을 무제한 발생하게 한다.

[0003] 웜 전파에 대응하기 위한 다양한 방법이 존재하는데, 대부분의 방법들은 네트워크상에서 웜을 전파하는 패킷들이 전송되는 과정 및 경로를 차단하는 것이다. 웜 전파에 대해 개개의 컴퓨터 및 서버가 직접적으로 대응할 수 있는 방법은 없기 때문이다. 개개의 컴퓨터 및 서버에 웜 전파 패킷들이 유입되면 그들은 좀비 컴퓨터(Zombie Computer)가 되고, 좀비 컴퓨터로부터 네트워크로 웜 전파 패킷들이 다량 방출된다. 좀비 컴퓨터에 의한 피라미드식 전파가 웜 전파의 기본방식이다.

[0004] 종래에는 네트워크에서 웜 바이러스를 전파하는 패킷들이 전송되는 과정 및 경로를 차단하기 위하여 주로 사람이 감시하며, 일단 감염된 PC등에 대한 조처는 고려하지 않았다. 네트워크에서 패킷을 전송되는 과정을 차단해도, 좀비 컴퓨터는 남아 있으며, 컴퓨터 사용자는 좀비 컴퓨터라는 사실을 모르는 경우가 많다. 따라서 근본적으로 패킷을 발송하는 좀비 컴퓨터의 확산을 막아야 제2차, 제3차 공격을 막을 수 있다. 좀비 컴퓨터가 자가 진단으로 적절한 보안 조치를 취하면 웜 바이러스의 감염을 줄일 수 있다.

발명의 내용

해결하려는 과제

[0005] 개시된 기술이 이루고자 하는 기술적 과제는, 사용자의 컴퓨터가 웜에 감염되더라도 좀비 컴퓨터가 되지 않도록 하는 데 있다.

[0006] 또한, 개시된 기술이 이루고자 하는 기술적 과제는, 유입되는 패킷과 전송하는 패킷을 비교하는 독립적인 하드웨어 구조를 만들어, 컴퓨터가 감염되더라도 보안을 위한 최소한의 기능은 유지할 수 있게 하는 데 있다.

과제의 해결 수단

[0007] 상기의 기술적 과제를 이루기 위해 개시된 기술의 제 1 측면은, 악성 패킷 차단 방법에 있어서, 컴퓨터가 네트워크로부터 수신 패킷을 수신하는 단계; 보안 칩이 상기 수신 패킷을 모니터링하여 동일한 내용이 반복되면 해당 수신 패킷을 상기 보안 칩의 버퍼에 저장하는 단계; 상기 컴퓨터가 상기 네트워크로 송신 패킷을 송신하는 단계; 및 상기 보안 칩이 상기 버퍼에 저장된 상기 수신 패킷과 상기 송신 패킷의 내용의 동일성을 비교하는 단계를 포함한다.

[0008] 상기의 기술적 과제를 이루기 위해 개시된 기술의 제 2 측면은, 악성 패킷 차단 시스템에 있어서, 네트워크로부터 수신 패킷을 수신하고 송신 패킷을 송신하는 컴퓨터; 및 상기 수신 패킷을 모니터링하여 동일한 내용이 반복되면 해당 수신 패킷을 버퍼에 저장하고, 상기 송신 패킷과 상기 버퍼에 저장된 상기 수신 패킷의 내용의 동일성을 비교하는 보안 칩을 포함한다.

발명의 효과

[0009] 개시된 기술은 다음의 효과를 가질 수 있다. 다만, 특정 실시예가 다음의 효과를 전부 포함하여야 한다거나 다음의 효과만을 포함하여야 한다는 의미는 아니므로, 개시된 기술의 권리범위는 이에 의하여 제한되는 것으로 이해되어서는 아니 될 것이다.

[0010] 개시된 기술에 따르면, 컴퓨터에 입력된 패킷과 출력된 패킷을 비교하고, 일정한 시간범위 내에서 두 패킷이 동일하면 웜 바이러스 감염을 의심하고, 규정된 보안 절차를 진행할 수 있다.

[0011] 또한, 개시된 기술에 따르면, 개개의 컴퓨터 및 서버에 웜 전파 패킷들이 유입될 때, 해당 컴퓨터가 직접적으로 대응을 하지 못하거나 웜 바이러스에 감염이 되었더라도, 자기 자신이 좀비 컴퓨터가 되지 않도록 할 수 있다.

[0012] 또한, 개시된 기술에 따르면, DDOS 해킹 피해액을 줄일 수 있고, 사용자가 자신의 컴퓨터의 웜 바이러스를 알아낼 수 있다.

도면의 간단한 설명

[0013] 도 1은 종래의 컴퓨터와 네트워크의 통신을 나타내는 도면이다.

도 2는 종래의 웜 바이러스 감염 형태를 나타내는 도면이다.

도 3은 개시된 기술의 일 실시예에 따른 악성 패킷 차단 방법을 나타내는 도면이다.

도 4는 개시된 기술의 일 실시예에 따른 악성 패킷 차단 시스템을 나타내는 블록도이다.

도 5는 개시된 기술의 일 실시예에 따른 악성 패킷 차단 방법을 나타내는 순서도이다.

도 6은 개시된 기술의 일 실시예에 따른 악성 패킷 차단 방법을 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 개시된 기술에 관한 설명은 구조적 내지 기능적 설명을 위한 실시예에 불과하므로, 개시된 기술의 권리범위는 본문에 설명된 실시예에 의하여 제한되는 것으로 해석되어서는 아니 된다. 즉, 실시예는 다양한 변경이 가능하고 여러 가지 형태를 가질 수 있으므로 개시된 기술의 권리범위는 기술적 사상을 실현할 수 있는 균등물들을 포함하는 것으로 이해되어야 한다.

[0015] 한편, 본 출원에서 서술되는 용어의 의미는 다음과 같이 이해되어야 할 것이다.

[0016] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함하다" 또는 "가지다" 등의 용어는 설시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는

이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0017] 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 단계들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0018] 여기서 사용되는 모든 용어들은 다르게 정의되지 않는 한, 개시된 기술이 속하는 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한 이상적이거나 과도하게 형식적인 의미를 지니는 것으로 해석될 수 없다.

[0019] 도 1은 종래의 컴퓨터와 네트워크의 통신을 나타내는 도면이다. 도 1을 참조하면, 컴퓨터는 네트워크에 접속하여 서버와 통신을 하게 된다. 하나의 컴퓨터에 웜 전파 패킷이 유입되면, 잠시 후 좀비 컴퓨터(Zombie Computer)가 된 컴퓨터는 유입된 패킷과 같은 웜 전파 패킷을 방출하게 된다. 좀비 컴퓨터는 악성 코드에 감염된 컴퓨터를 의미한다.

[0020] 도 2는 종래의 웜 바이러스 감염 형태를 나타내는 도면이다. 도 2를 참조하면, 컴퓨터가 네트워크로부터 수신한 수신 패킷과 컴퓨터가 네트워크로 송신한 송신 패킷이 동일하면 웜 바이러스 감염을 의심할 수 있다. 일 예로서, 수신 패킷과 송신 패킷의 일부인 'for(int i=0,1... if you are zombie...crash and distory'가 동일하게 존재하는 경우에 웜 바이러스 감염을 의심할 수 있다. 다른 일 예로서, 수신 패킷 전체와 송신 패킷 전체가 'for(int i=0,1... if you are zombie...crash and distory FF54 32A2 7ABC CAAA MOV EAX EAC 256792'로 동일한 경우에도 웜 바이러스 감염을 의심할 수 있다.

[0021] 도 3은 개시된 기술의 일 실시예에 따른 악성 패킷 차단 방법을 나타내는 도면이다. 도 3을 참조하면, 보안 칩은 컴퓨터가 네트워크로부터 수신된 수신 패킷을 모니터링하여, 동일한 패킷들이 반복적으로 유입되면 웜 전파를 위한 패킷으로 의심하고, 의심된 패킷이 포함되는 코드를 보안 칩의 버퍼에 저장한다. 일 예로서, 도 3에 나타난 'for(int i=0,1... if you are zombie...crash and distory'는 패킷이 포함하는 코드 중 일부를 나타내는 것이다. 동일한 패킷들이 반복적으로 유입되는 것을 모니터링하는 데 있어, 패킷의 모든 내용을 비교할 필요 없이, 일부 내용만 비교함으로써 실행 시간 소모를 줄일 수 있다. 또한, 컴퓨터가 수신하는 패킷이 동일한 패킷인지 비교하는 동작은 보안 칩이 수행한다. 여기에서, 보안 칩은 별도의 장치로서 컴퓨터의 메인 프로세서와 메인 메모리 등이 감염되어도 영향받지 않고 악성 패킷의 방출을 중단시킬 수 있게 한다.

[0022] 보안 칩은 컴퓨터에서 네트워크로 송신되는 송신 패킷과 버퍼에 저장된 패킷을 비교하여 동일한지 판단한다. 보안 칩은 동일성을 판단하여, 동일성이 있는 경우에 웜 바이러스 감염을 의심할 수 있다. 또한, 보안 칩은 웜 바이러스 감염이 의심되는 패킷을 사용자에게 알려 보안 절차를 진행하게 할 수 있다. 일 예로서, 도 3에 나타난 패킷이 포함하는 코드 중 일부인 'for(int i=0,1... if you are zombie...crash and distory'가 동일하여도 웜 바이러스 감염을 의심할 수 있다. 보안 칩은 웜 전파 패킷인 것으로 판단한 경우에 사용자에게 팝업(pop-up) 알람을 띄울 수 있고, 팝업 알람 이후의 사용자의 처리과정은 일반적인 보안 절차에 따른다. 또한, 웜 전파 패킷은 하나의 패킷에 악성 행위를 하는 짧은 실행코드를 포함하는 형태로서, 팝업 알람 발생 시에 해당 패킷의 형태를 파악하여, 악성 패킷으로 파악되면 보안전문가에 신고하도록 한다. 보안 칩은 컴퓨터의 메인 프로세서와 메인 메모리가 감염되어도 별도로 동작하므로 악성 패킷의 방출을 중단시킬 수 있어 좀비 컴퓨터가 되지 않도록 할 수 있다.

[0023] 도 4는 개시된 기술의 일 실시예에 따른 악성 패킷 차단 시스템을 나타내는 블록도이다. 도 4를 참조하면, 악성 패킷 차단 시스템은 컴퓨터(100), 보안 칩(200) 및 네트워크(300)를 포함한다.

[0024] 컴퓨터(100)는 네트워크(300)에 접속하여 네트워크(300)로부터 수신 패킷을 수신하고 네트워크(300)로 송신 패킷을 송신한다. 컴퓨터는 일반적으로 사용되는 PC(Personal Computer), PDA(Personal Digital Assistants), 태블릿(Tablet) PC 또는 스마트 폰(Smart Phone)을 포함할 수 있다. 하나의 컴퓨터에 웜 전파 패킷이 유입되면, 잠시 후 좀비가 된 컴퓨터는 유입된 패킷과 같은 웜 전파 패킷을 방출하게 되면서 좀비 컴퓨터가 된다.

[0025] 보안 칩(200)은 컴퓨터(100)가 네트워크(300)로부터 수신 패킷을 수신할 때에 동일한 패킷들이 반복적으로 유입되면 보안 칩(200) 내부의 버퍼에 수신 패킷을 저장한다. 또한, 보안 칩(200)은 컴퓨터(100)가 네트워크(300)로 송신 패킷을 송신할 때에 버퍼에 저장된 수신 패킷과 송신 패킷의 동일성을 비교하여 웜 전파 패킷을 판단하고, 웜 전파 패킷으로 의심된 경우에는 사용자에게 알린다. 보안 칩(200)은 컴퓨터(100)에 대하여 별도의 장치로서,

컴퓨터(100)의 메인 프로세서와 메인 메모리 등이 감염되어도 영향받지 않고, 컴퓨터(100)가 네트워크(300)로 악성 패킷을 방출하는 것을 중단시킬 수 있다. 보안 칩(200)의 버퍼는 악성 패킷의 정보를 지속적으로 저장하고 변경 불가능하게 하기 위하여 ROM(Read Only Memory)을 포함할 수 있다.

[0026] 네트워크(300)는 컴퓨터(100)에 패킷을 송신하고 컴퓨터(100)로부터 패킷을 수신하는 일을 반복적으로 수행한다. 패킷을 송?수신하는 행위를 통하여 웜 바이러스가 전파될 수 있다.

[0027] 도 5는 개시된 기술의 일 실시예에 따른 악성 패킷 차단 방법을 나타내는 순서도이다. 도 5를 참조하면, 컴퓨터(100)가 네트워크(300)로부터 수신 패킷을 수신한다(S410). 컴퓨터(100)가 네트워크(300)로부터 웜 전파 패킷이 유입되면, 잠시 후 좀비가 된 컴퓨터는 유입된 패킷과 같은 웜 전파 패킷을 방출하게 되면서 좀비 컴퓨터가 될 수 있다. 컴퓨터는 일반적으로 사용되는 PC(Personal Computer), PDA(Personal Digital Assistants), 태블릿(Tablet) PC 또는 스마트폰(Smart Phone)을 포함할 수 있다.

[0028] 보안 칩(200)이 수신 패킷을 모니터링하여 동일한 내용의 패킷이 반복되면 해당 수신 패킷을 보안 칩(200)의 버퍼에 저장한다(S420). 여기에서 동일한 내용이란 전체 패킷의 동일뿐만 아니라 패킷의 일부 내용이 동일한 경우도 포함된다. 다시 말해서, 도 1에서 반복된 수신 패킷에 나타난 내용 전체가 'for(int i=0,1... if you are zombie...crash and distory FF54 32A2 7ABC CAAA MOV EAX EAC 256792'로 동일한 경우에 버퍼에 저장할 수 있고, 수신 패킷의 내용의 일부인 'for(int i=0,1... if you are zombie...crash and distory'가 동일하게 포함된 패킷이 반복되어 수신되어도 버퍼에 저장할 수 있다. 보안 칩(200)은 컴퓨터(100)에 대하여 별도의 장치로서, 컴퓨터(100)의 메인 프로세서와 메인 메모리 등이 감염되어도 영향받지 않는다. 보안 칩(200)의 버퍼는 악성 패킷의 정보를 지속적으로 저장하고 변경 불가능하게 하기 위하여 ROM(Read Only Memory)을 포함할 수 있다.

[0029] 컴퓨터(100)는 네트워크(300)로 송신 패킷을 송신한다(S430). 컴퓨터(100)가 네트워크(300)로부터 웜 전파 패킷을 수신하면, 잠시 후 좀비 컴퓨터가 된 컴퓨터는 수신 패킷과 동일한 웜 전파 패킷을 송신할 것이다.

[0030] 보안 칩(200)이 버퍼에 저장된 수신 패킷과 송신 패킷의 내용의 동일성을 비교한다(S440). 보안 칩(200)은 버퍼에 저장된 수신 패킷과 송신 패킷의 내용 전체가 동일한 경우뿐만 아니라 버퍼에 저장된 수신 패킷의 내용 일부와 송신 패킷의 내용 일부가 동일한 경우에도 송신 패킷을 악성 패킷으로 판단할 수 있다. 일 예로서, 도 1에서 송신 패킷과 버퍼에 저장된 수신 패킷의 내용 중 'for(int i=0,1... if you are zombie...crash and distory'가 동일하게 존재할 경우에는 나머지가 상이하더라도 송신 패킷을 웜 전파 패킷으로 의심할 수 있다. 다른 일 예로서, 도 1에서 송신 패킷과 버퍼에 저장된 수신 패킷의 내용이 'for(int i=0,1... if you are zombie...crash and distory FF54 32A2 7ABC CAAA MOV EAX EAC 256792'로 동일한 경우에는 송신 패킷을 웜 전파 패킷으로 의심할 수 있다. 보안 칩(200)은 버퍼에 저장된 수신 패킷과 송신 패킷의 내용의 동일성이 인정되지 않는 경우에는 사용자에게 알리지 않는다.

[0031] 보안 칩(200)이 송신 패킷과 버퍼에 저장된 수신 패킷의 내용의 동일성이 인정되는 경우에는 사용자에게 알릴 수 있다(S450). 송신 패킷과 버퍼에 저장된 수신 패킷의 동일성이 인정되면 송신 패킷은 웜 전파 패킷에 해당할 가능성이 높으므로 사용자에게 팝업(pop-up) 알람을 띄울 수 있다. 팝업 알람 이후의 사용자의 처리 과정은 일반적인 보안 절차에 따른다. 웜 전파 패킷은 하나의 패킷에 악성 행위를 하는 짧은 실행코드를 포함하는 형태로서, 팝업 알람 발생 시 해당 패킷의 형태를 파악하여, 웜 전파 패킷으로 파악되면 보안전문가에 신고할 수 있다. 보안 칩(200)은 컴퓨터(100)의 메인 프로세서와 메인 메모리가 웜 바이러스에 감염되어도 별도로 동작하므로 악성 패킷의 방출을 중단시킬 수 있다.

[0032] 도 6은 개시된 기술의 일 실시예에 따른 악성 패킷 차단 방법을 나타내는 순서도이다. 도 6을 참조하면, 컴퓨터(100)가 네트워크(300)로부터 수신 패킷을 수신한다(S510). 컴퓨터(100)가 네트워크(300)로부터 웜 전파 패킷이 유입되면, 잠시 후 좀비가 된 컴퓨터는 유입된 패킷과 같은 웜 전파 패킷을 방출하게 되면서 좀비 컴퓨터가 될 수 있다. 컴퓨터는 일반적으로 사용되는 PC(Personal Computer), PDA(Personal Digital Assistants), 태블릿(Tablet) PC 또는 스마트폰(Smart Phone)을 포함할 수 있다.

[0033] 보안 칩(200)은 수신 패킷을 모니터링한다(S520). 보안 칩(200)은 컴퓨터(100)에 대하여 별도의 장치로서, 수신 패킷을 모니터링하여 웜 전파 패킷인지 여부를 판단한다.

[0034] 보안 칩(200)은 모니터링을 통하여, 내용 일부가 동일한 패킷이 반복적으로 유입되는지 판단한다(S530). 도 1에서는 반복적으로 수신되는 수신 패킷에 나타난 내용의 일부가 'for(int i=0,1... if you are zombie...crash and distory'를 포함하고 있는 경우를 의미한다. 동일한 패킷들이 반복적으로 유입되는 것을 모니터링하는데 있

어, 패킷의 모든 내용을 비교할 필요없이 일부 내용만 비교함으로써 실행 시간 소모를 줄일 수 있다.

[0035] 보안 칩(200)이 내용 일부가 동일한 패킷이 반복적으로 유입되는 것이 아닌 것으로 판단한 경우에는, 보안 칩(200)은 내용 전체가 동일한 패킷이 반복적으로 유입되는지 판단한다(S531). 도 1에서는 반복적으로 수신되는 수신 패킷에 나타난 내용 전체가 'for(int i=0,1... if you are zombie...crash and distory FF54 32A2 7ABC CAAA MOV EAX EAC 256792'로서 동일한 경우를 의미한다.

[0036] 보안 칩(200)이 내용 전체가 동일한 패킷이 반복적으로 유입되지 않는 것으로 판단한 경우에는, 웜 전파 패킷이 아닌 것으로 판단하고, 컴퓨터(100)는 네트워크(300)로 송신 패킷을 송신한다(S532).

[0037] 보안 칩(200)이 내용 일부가 동일한 패킷이 반복적으로 유입되는 것으로 판단한 경우에는 보안 칩(200) 내부의 버퍼에 수신 패킷을 저장한다(S540). 보안 칩(200)은 컴퓨터(100)에 대하여 별도의 장치로서, 컴퓨터(100)의 메인 프로세서와 메인 메모리 등이 감염되어도 영향받지 않는다. 보안 칩(200)의 버퍼는 악성 패킷의 정보를 지속적으로 저장하고 변경 불가능하게 하기 위하여 ROM(Read Only Memory)을 포함할 수 있다.

[0038] 컴퓨터(100)는 네트워크(300)로 송신 패킷을 송신한다(S550). 컴퓨터(100)가 네트워크(300)로부터 웜 전파 패킷을 수신하면, 잠시 후 좀비 컴퓨터가 된 컴퓨터는 수신 패킷과 동일한 웜 전파 패킷을 송신할 것이다.

[0039] 보안 칩(200)은 송신 패킷과 버퍼에 저장된 수신 패킷의 내용 일부의 동일성을 비교한다(S560). 도 1에서 버퍼에 저장된 수신 패킷과 송신 패킷이 'for(int i=0,1... if you are zombie...crash and distory'를 공통적으로 포함하고 있는 지 여부를 판단할 수 있다.

[0040] 보안 칩(200)이 송신 패킷과 버퍼에 저장된 수신 패킷의 내용 일부가 동일하지 않은 것으로 판단한 경우에는, 송신 패킷과 버퍼에 저장된 수신 패킷의 내용 전체의 동일성을 비교한다(S561). 도 1에서 버퍼에 저장된 수신 패킷과 송신 패킷이 'for(int i=0,1... if you are zombie...crash and distory FF54 32A2 7ABC CAAA MOV EAX EAC 256792'를 공통적으로 포함하는 경우를 의미한다. 보안 칩(200)이 송신 패킷과 버퍼에 저장된 수신 패킷의 내용 전체가 동일하지 않은 것으로 판단한 경우에는 웜 전파 패킷이 아닌 것으로 판단하여 사용자에게 알리지 않는다.

[0041] 보안 칩(200)이 송신 패킷과 버퍼에 저장된 수신 패킷의 일부 내용이 동일하거나, 송신 패킷과 버퍼에 저장된 수신 패킷의 전체 내용이 동일한 경우에는 사용자에게 알릴 수 있다(S570). 송신 패킷과 버퍼에 저장된 수신 패킷의 동일성이 인정되면 송신 패킷은 웜 전파 패킷에 해당할 가능성이 높으므로 사용자에게 팝업(pop-up) 알람을 띄울 수 있다. 팝업 알람 이후의 사용자의 처리 과정은 일반적인 보안 절차에 따른다. 웜 전파 패킷은 하나의 패킷에 악성 행위를 하는 짧은 실행코드를 포함하는 형태로서, 팝업 알람 발생 시 해당 패킷의 형태를 파악하여, 웜 전파 패킷으로 파악되면 보안전문가에 신고할 수 있다. 보안 칩(200)은 컴퓨터(100)의 메인 프로세서와 메인 메모리가 웜 바이러스에 감염되어도 별도로 동작하므로 악성 패킷의 방출을 중단시킬 수 있다.

[0042] 상기에서는 본 발명의 바람직한 실시예를 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.

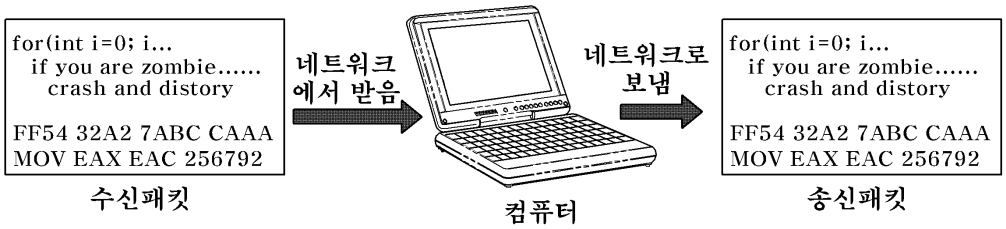
부호의 설명

[0043] 100 : 컴퓨터 200 : 보안 칩

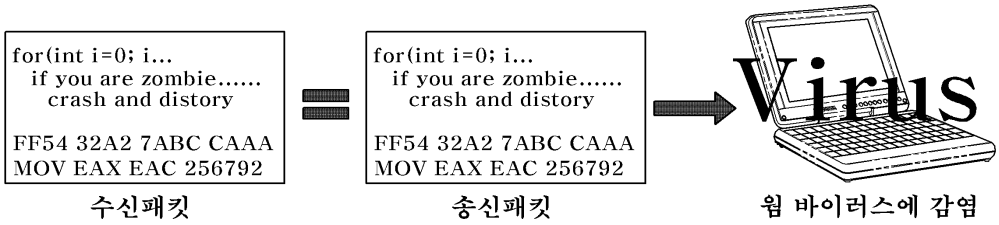
300 : 네트워크

도면

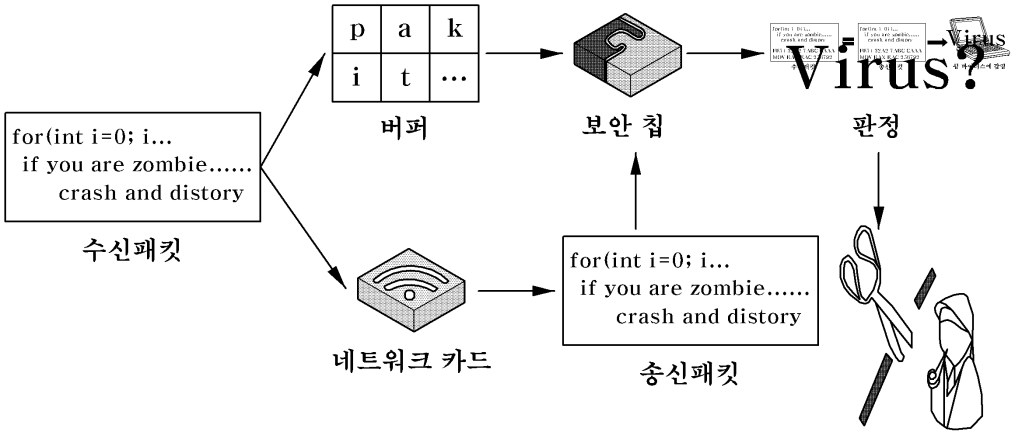
도면1



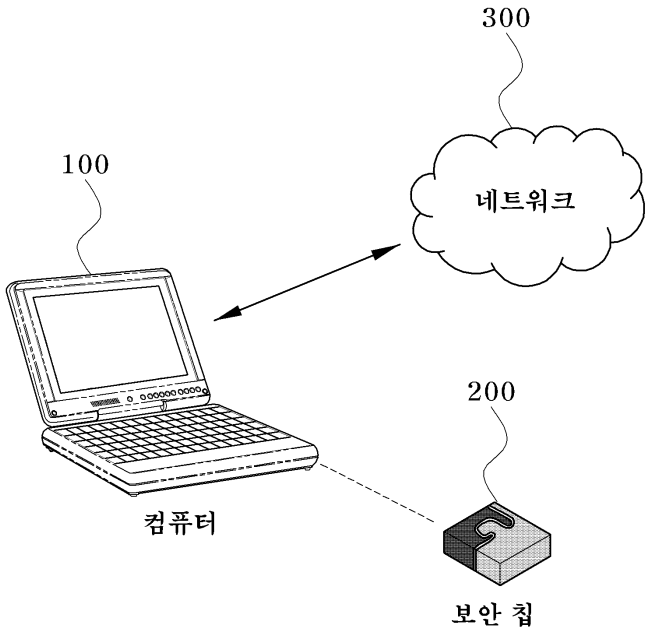
도면2



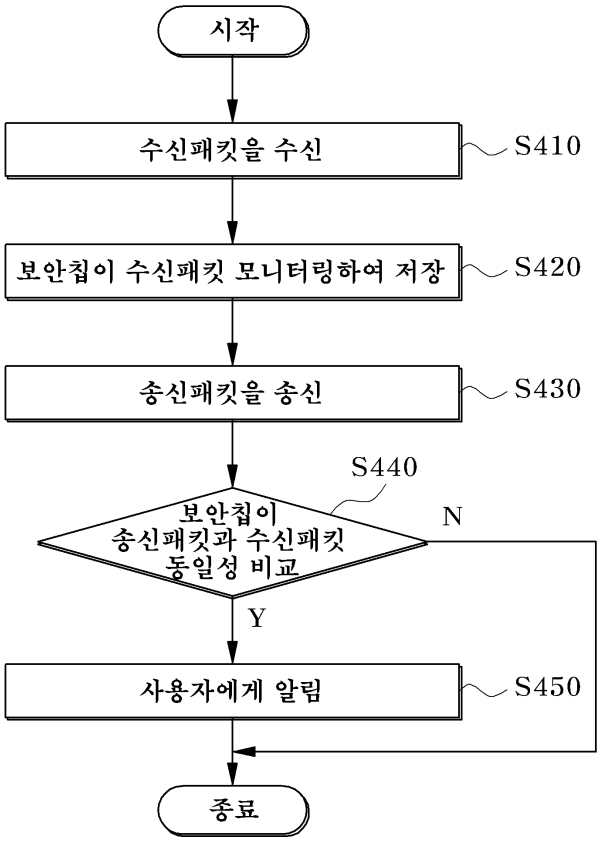
도면3



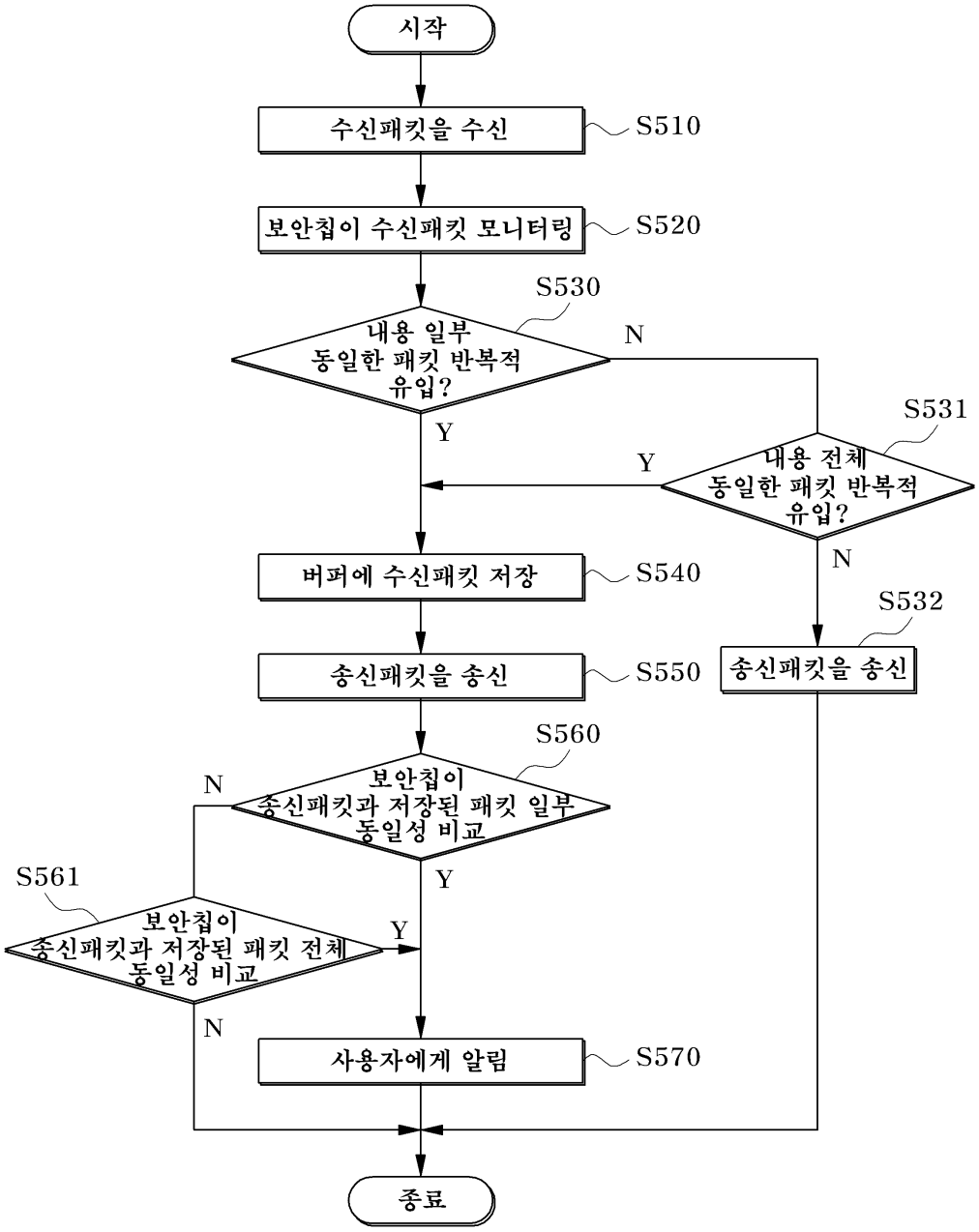
도면4


300
100
네트워크
200
컴퓨터
보안 칩

도면5


시작
수신패킷을 수신
S410
보안칩이 수신패킷 모니터링하여 저장
S420
송신패킷을 송신
S430
S440
보안칩이
송신패킷과 수신패킷
동일성 비교
N
Y
사용자에게 알림
S450
종료

도면6


시작
수신패킷을 수신
S510
보안칩이 수신패킷 모니터링
S520
S530
내용 일부 동일한 패킷 반복적 유입?
N
Y
S531
내용 전체 동일한 패킷 반복적 유입?
Y
N
버퍼에 수신패킷 저장
S540
S532
송신패킷을 송신
송신패킷을 송신
S550
S560
보안칩이 송신패킷과 저장된 패킷 일부 동일성 비교
N
Y
S561
보안칩이 송신패킷과 저장된 패킷 전체 동일성 비교
Y
N
사용자에게 알림
S570
종료