(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년10월04일
(11) 등록번호 10-0985049
(24) 등록일자 2010년09월28일

(51) Int. Cl.
G06F 21/00 (2006.01) *G06F 21/20* (2006.01)
G06F 15/00 (2006.01)
(21) 출원번호 10-2008-0046325
(22) 출원일자 2008년05월19일
심사청구일자 2008년05월19일
(65) 공개번호 10-2009-0120343
(43) 공개일자 2009년11월24일
(56) 선행기술조사문헌
JP2007122692 A
JP2007020004 A
JP2007004415 A
KR1020080024804 A
전체 청구항 수 : 총 17 항

(73) 특허권자
주식회사 안철수연구소
서울 영등포구 여의도동 12 씨씨엠엠빌딩 6층
(72) 발명자
최동균
경기도 수원시 권선구 호매실동 453-16 풍림빌라 5동 101호
(74) 대리인
김문재

심사관 : 신상길

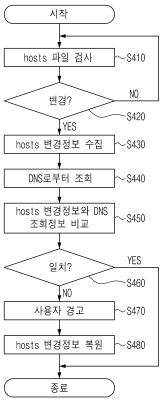
(54) 파밍감지 시스템 및 이를 제어하는 방법

(57) 요 약

본 발명은 파밍감지 시스템 및 이를 제어하는 방법에 관한 것으로, 더욱 상세하게는 단말기내에 있는 hosts 파일을 변경하여 예상치 못한 웹사이트로 이동하도록 하는 파밍(Pharming) 행위를 예방하는 시스템 및 제어방법에 관한 것이다.

본 발명에 따른 파밍감지 시스템은 hosts 파일의 변경을 감지하여, 변경된 경우에 올바른 변경인지를 판단하여 이에 따라 적절한 대응을 사용자에게 제공한다. 이에 따라, 올바르게 hosts 파일을 변경한 경우에는 변경된 내용을 복원시키지 않고 잘못된 변경인 경우에는 복원시킬 수 있게 된다

대 표 도 - 도4



특허청구의 범위

청구항 1

단말기 내부에 설치되어 파밍을 감지하는 파밍감지장치의 제어방법에 있어서,

상기 파밍감지장치가, IP주소와 도메인이름이 매핑된 정보를 가지고 상기 단말기에 저장된 텍스트파일의 변경 여부를 체크하는 단계;

상기 체크결과 변경이 발생하면, 상기 파밍감지장치가 상기 텍스트파일에서 변경된 정보를 추출하는 단계;

상기 파밍감지장치가 상기 추출된 정보와 대응되는 정보를 IP주소와 도메인이름을 저장하고 있는 외부 데이터베이스로부터 수신하는 단계; 및

상기 파밍감지장치가 상기 텍스트파일로부터 추출된 정보와 상기 데이터베이스로부터 수신된 정보를 비교하는 단계;를 포함하는 것을 특징으로 하는 파밍감지장치의 제어방법.

청구항 2

제 1항에 있어서,

상기 추출단계는

상기 텍스트파일에서 변경된 IP주소 및 이에 대응되는 도메인이름을 추출하는 것이고,

상기 수신단계는

상기 추출단계에서 추출된 정보의 도메인이름을 상기 데이터베이스로 전송한 후, 상기 전송한 도메인이름과 매핑되는 IP주소를 수신하는 것이고,

상기 비교단계는 상기 텍스트파일에서 추출된 IP주소와 상기 데이터베이스에서 수신된 IP주소가 일치하는지 여부를 비교하는 것을 특징으로 하는 파밍감지장치의 제어방법.

청구항 3

제 1항에 있어서,

상기 비교결과 불일치한 경우에는,

상기 파밍감지장치가 상기 단말기를 통해서 경고메세지를 출력하는 단계;를 더 포함하는 것을 특징으로 하는 파밍감지장치의 제어방법.

청구항 4

제 1항에 있어서,

상기 비교결과 불일치한 경우에는,

상기 파밍감지장치가 상기 텍스트파일의 변경된 IP주소를 상기 수신된 IP주소로 수정하는 단계;를 더 포함하는 것을 특징으로 하는 파밍감지장치의 제어방법.

청구항 5

제 1항에 있어서,

상기 데이터베이스는 2개 이상의 다수의 데이터베이스이며,

상기 비교단계는,

상기 다수의 데이터베이스에서 수신된 IP주소들이 모두 동일하면서, 그리고 상기 텍스트파일에서 추출된 IP주소와 상기 데이터베이스에서 수신된 IP주소들과 불일치한 경우에는 상기 파밍감지장치가 상기 텍스트파일의 IP주소를 상기 수신된 IP주소로 수정하고,

상기 다수의 데이터베이스에서 수신된 IP주소들이 모두 동일하지 않은 경우에는 상기 파밍감지장치가 상기 단말

기를 통해서 변조가능성이 있음을 나타내는 메세지를 출력하는 단계;를 더 포함하는 것을 특징으로 하는 파밍감지장치의 제어방법.

청구항 6

제 1항에 있어서,

상기 텍스트파일은 hosts 파일이고,

상기 데이터베이스는 DNS인 것을 특징으로 하는 파밍감지장치의 제어방법.

청구항 7

단말기 내부에 설치되어 파밍을 감지하는 파밍감지장치에 있어서,

IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경여부를 체크하는 무결성유지모듈;

IP주소와 도메인이름이 매핑된 정보를 저장하고 있는 외부 데이터베이스로부터 정보를 송수신하는 도메인조회모듈; 및

상기 무결성유지모듈을 통해서 상기 텍스트파일의 변경이 체크된 경우, 상기 텍스트파일에서 변경된 정보를 추출하고, 상기 변경된 정보와 대응되는 정보를 상기 데이터베이스로부터 수신한 후, 상기 변경된 정보 및 상기 수신된 정보를 서로 비교하는 제어모듈;을 포함하는 것을 특징으로 하는 파밍감지장치.

청구항 8

제 7항에 있어서,

상기 제어모듈은

상기 텍스트파일에서 변경된 IP주소 및 이에 대응되는 도메인이름을 추출하고, 상기 추출된 도메인이름을 상기 데이터베이스로 전송한 후, 상기 전송된 도메인이름과 매핑되는 IP주소를 수신한 후, 상기 추출된 정보의 IP주소와 상기 수신된 IP주소가 일치하는지 여부를 비교하는 것을 특징으로 하는 파밍감지장치.

청구항 9

제 7항에 있어서,

상기 제어모듈은

상기 비교결과 불일치한 경우 상기 텍스트파일의 IP주소를 상기 데이터베이스로부터 수신된 IP주소로 수정하는 것을 특징으로 하는 특징으로 하는 파밍감지장치.

청구항 10

제 7항에 있어서,

상기 텍스트파일은 hosts 파일이고,

상기 데이터베이스는 DNS인 것을 특징으로 하는 파밍감지장치.

청구항 11

네트워크를 통해서 서로 연결된 클라이언트모듈, 사업자서버 및 인증도메인DB를 포함하는 파밍감지시스템을 이용해서 파밍을 감지하는 방법에 있어서,

상기 클라이언트모듈이 IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경 여부

를 체크하는 단계;

상기 체크결과 변경이 발생하면, 상기 클라이언트모듈이 상기 텍스트파일에서 변경된 정보를 추출하는 단계;

상기 클라이언트모듈이 상기 추출된 정보를 사업자서버로 전송하는 단계;

상기 사업자서버가 상기 전송받은 추출정보와 대응되는 정보를 사업자에 의해서 관리되고 업데이트되며 IP주소와 도메인이름이 매핑된 정보를 저장하고 있는 인증도메인DB부터 수신하는 단계; 및

상기 사업자서버가 상기 추출된 정보와 상기 인증도메인DB부터 수신된 정보를 비교하는 단계;를 포함하는 것을 특징으로 하는 파밍감지방법.

청구항 12

제 11항에 있어서,

상기 텍스트파일은 hosts 파일이고,

상기 추출단계는

상기 hosts 파일에서 변경된 IP주소와 이에 대응되는 도메인이름을 추출하는 것이고,

상기 수신단계는

상기 추출단계에서 추출된 정보의 도메인이름을 상기 인증도메인DB로 전송한 후, 상기 전송한 도메인이름과 매핑되는 IP주소를 수신하는 것이고,

상기 비교단계는

추출된 정보의 IP주소와 상기 수신된 IP주소가 일치하는지 여부를 비교하는 것을 특징으로 하는 파밍감지방법.

청구항 13

제 12항에 있어서,

상기 사업자서버가 상기 비교결과 및 수신된 정보를 클라이언트모듈로 전송하는 단계; 및

상기 전송된 비교결과가 불일치한 경우, 상기 클라이언트모듈이 상기 hosts 파일의 변경된 IP주소를 상기 수신된 IP주소로 수정하는 것을 특징으로 하는 특징으로 하는 파밍감지방법.

청구항 14

제 11항에 있어서,

상기 사업자서버가

상기 추출된 정보,상기 수신된 정보 및 비교결과를 적재하는 단계를 더 포함하는 것을 특징으로 하는 특징으로 하는 파밍감지방법.

청구항 15

제 11항에 있어서,

상기 사업자서버가 상기 인증도메인DB의 정보를 외부의 한개 이상의 DNS의 정보와 비교하는 단계;를 더 포함하고,

상기 비교결과 인증도메인DB의 정보가 외부 DNS의 정보와 다른 경우에는 상기 사업자서버가 인증도메인DB의 정보가 변경되었음을 나타내는 메세지를 디스플레이 하는 단계를 더 포함하는 것을 특징으로 하는 특징으로 하는 파밍감지방법.

청구항 16

네트워크를 통해서 서로 연결된 클라이언트모듈, 사업자서버 및 인증도메인DB를 포함하는 파밍감지시스템에 있어서,

상기 클라이언트모듈은 사용자의 단말기에 설치되며,

IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경여부를 체크하는 무결성유지모듈; 및

상기 무결성유지모듈을 통해서 상기 텍스트파일의 변경이 체크된 경우, 상기 텍스트파일에서 변경된 정보를 추출하고, 이를 상기 사업자 서버로 전송하는 클라이언트제어모듈;을 포함하며,

상기 인증도메인DB는 사업자에 의해서 관리되고 업데이트되며 IP주소와 도메인이름이 매핑된 정보를 저장하고 있는 DB형태인것을 특징으로 하며,

상기 사업자의 서버는,

상기 클라이언트모듈로부터 변경정보를 수신하고, 상기 수신된 변경정보와 대응되는 정보를 상기 인증도메인DB에서 수신한 후, 상기 변경정보와 상기 수신정보를 비교한 후 비교결과를 클라이언트모듈로 전송하는 서버제어모듈;을 포함하는 것을 특징으로 하는 것을 특징으로 하는 파밍감지 시스템.

청구항 17

파밍감지장치가, IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경 여부를 체크하는 단계;

상기 체크결과 변경이 발생하면, 상기 파밍감지장치가 상기 텍스트파일에서 변경된 정보를 추출하는 단계;

상기 추출된 정보와 대응되는 정보를 IP주소와 도메인이름을 저장하고 있는 데이터베이스로부터 수신하는 단계; 및

상기 텍스트파일로부터 추출된 정보와 상기 데이터베이스로부터 수신된 정보를 비교하는 단계;를 수행할 수 있는 프로그램이 기록된 컴퓨터로 읽을 수 있는 기록매체.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 파밍감지 시스템 및 이를 제어하는 방법에 관한 것으로, 더욱 상세하게는 단말기내에 있는 hosts 파일을 변경하여 예상치 못한 웹사이트로 이동하도록 하는 파밍(Pharming) 행위를 예방하는 시스템 및 제어방법에 관한 것이다.

배 경 기 술

[0002] DNS(domain name server 또는 domain name system, 이하 DNS)란 특정 사이트에 접속하기 위해 일일이 숫자로 된 IP 주소를 기억하지 않고 도메인 네임만으로도 가능하게 하기 위해 도메인 네임을 IP 주소로 전환시켜 주는 시스템을 뜻한다. 예를 들어, IP 주소가 "111.112.113.114"와 같이 각 바이트마다 마침표로 구분된 4바이트 크기의 숫자 주소인 데 비해, 도메인 네임은 "www.abc.co.kr"과 같이 문자로 구성되어 있어서 숫자보다는 이름을 이해하거나 기억하기 쉽다.

[0003] 따라서 사용자들은 특정 웹사이트에 접속할 때, 해당 웹사이트의 IP주소를 기억할 필요가 없고, 도메인 네임을 기억해서 이를 익스플로러 등의 주소창에 입력하면 되는 것이다.

[0004] 그런데 컴퓨터는 도메인 이름을 IP주소로 변환할 때, 맨 처음부터 DNS를 검색하는 것은 아니고, 컴퓨터내부에 있는 hosts 파일을 먼저 참조한다. 사용자들이 사용하는 컴퓨터에는 Hosts라는 파일이 존재하는데, 이 파일은 IP주소와 도메인네임을 매핑 시켜주는 파일로서, 윈도우 운영체제뿐만 아니라 UNIX시스템에서도 같은 기능을 수

행한다. 따라서 hosts 파일에서 원하는 호스트명을 찾는다면 더이상 DNS에 IP주소를 요청하지 않는다.

[0005] 즉 사용자가 은행의 도메인을 입력하였는데, 만약 hosts 파일에 매칭되는 도메인 이름과 IP주소가 있다면, 컴퓨터는 더이상 dns 서버를 호출하지 않고 그냥 바로 hosts 파일에서 찾아낸 IP 주소로 접속하게 되는 것이다. 따라서 hosts 파일을 잘 활용하면 DNS로의 엑세스가 생략되어, 더 빠르게 자신의 원하는 웹사이트로의 이동이 가능해진다.

[0006] 그러나, 이러한 hosts 파일의 특성을 악용한 사례가 발생하고 있는 바 문제이며, 대표적인 사례가 "파밍(Pharming)"이다. 해킹 범죄자들이 한 웹 사이트의 인터넷 트래픽을 그 사이트와 똑같아 보이는 다른 사이트로 이동시켜 사용자가 아이디와 패스워드 등의 민감한 개인정보를 가짜 사이트의 데이터베이스에 입력하도록 속이는 행위를 "파밍(Pharming)"이라고 부른다. 해킹 범죄자들은 가짜 사이트로 부터 수집된 개인정보를 기반으로 사용자의 은행 계좌에 접근 하여 몰래 돈을 유출하거나, 개인 정보를 도용하여 또 다른 사기를 저지르는 등의 심각한 피해를 가져오고 있다. 실제 사이트와 유사하게 가짜 사이트를 만들고 사용자의 개인정보 입력을 유도하는 것은 "피싱(Phishing)" 사기와 비슷하지만, 사용자가 정확한 금융기관 도메인 주소를 입력하더라도 가짜 홈페이지로 이동하게 되는 점에 있어 기술적인 차이점을 가진다.

[0007] 이러한 "파밍"은 해킹 범죄자의 직접해킹 또는 악성코드 감염등으로 인해 사용자 컴퓨터의 hosts 파일을 변조시키는데, 이때 hosts 파일에는 잘못된 사이트 주소가 주입되어 진다. 사용자가 정확한 도메인 주소를 입력하여 인터넷 접속을 시도하면 컴퓨터는 hosts 파일을 참조하여 잘못된 사이트 주소로 인터넷 트래픽을 이동시켜 사용자에게 가짜 사이트를 보여주게 된다.

발명의 내용

해결 하고자하는 과제

[0008] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은, 사용자 컴퓨터의 hosts 파일이 변경된 경우 이러한 변경이 바른 변경인지 아니면 잘못된 변경인지를 검사하고, 잘못된 변경인 경우에는 hosts 파일을 복원하도록 하는 파밍감지 시스템 및 이의 제어방법을 제공함에 있다.

과제 해결수단

[0009] 상기 목적을 달성하기 위한 본 발명의 일면에 따라, 단말기 내부에 설치되어 파밍을 감지하는 파밍감지장치의 제어방법이 제공되며: 이 방법은, 상기 파밍감지장치가, IP주소와 도메인이름이 매핑된 정보를 가지고 상기 단말기에 저장된 텍스트파일의 변경 여부를 체크하는 단계; 상기 체크결과 변경이 발생하면, 상기 파밍감지장치가 상기 텍스트파일에서 변경된 정보를 추출하는 단계; 상기 파밍감지장치가 상기 추출된 정보와 대응되는 정보를 IP주소와 도메인이름을 저장하고 있는 외부 데이터베이스로부터 수신하는 단계; 및 상기 파밍감지장치가 상기 텍스트파일로부터 추출된 정보와 상기 데이터베이스로부터 수신된 정보를 비교하는 단계;를 포함하는 것을 특징으로 한다.

바람직하게는, 상기 추출단계는 상기 텍스트파일에서 변경된 IP주소 및 이에 대응되는 도메인이름을 추출하는 것이고, 상기 수신단계는 상기 추출단계에서 추출된 정보의 도메인이름을 상기 데이터베이스로 전송한 후, 상기 전송한 도메인이름과 매핑되는 IP주소를 수신하는 것이고, 상기 비교단계는 상기 텍스트파일에서 추출된 IP주소와 상기 데이터베이스에서 수신된 IP주소가 일치하는지 여부를 비교하는 것을 특징으로 한다.

바람직하게는, 상기 비교결과 불일치한 경우에는, 상기 파밍감지장치가 상기 단말기를 통해서 경고메세지를 출력하는 단계;를 더 포함하는 것을 특징으로 한다.

바람직하게는, 상기 비교결과 불일치한 경우에는, 상기 파밍감지장치가 상기 텍스트파일의 변경된 IP주소를 상기 수신된 IP주소로 수정하는 단계;를 더 포함하는 것을 특징으로 한다.

바람직하게는, 상기 데이터베이스는 2개 이상의 다수의 데이터베이스이며, 상기 비교단계는, 상기 다수의 데이터베이스에서 수신된 IP주소들이 모두 동일하면서, 그리고 상기 텍스트파일에서 추출된 IP주소와 상기 데이터베이스에서 수신된 IP주소들과 불일치한 경우에는 상기 파밍감지장치가 상기 텍스트파일의 IP주소를 상기 수신된 IP주소로 수정하고, 상기 다수의 데이터베이스에서 수신된 IP주소들이 모두 동일하지 않은 경우에는 상기 파밍감지장치가 상기 단말기를 통해서 변조가능성이 있음을 나타내는 메세지를 출력하는 단계;를 더 포함하는 것을 특징으로 한다.

바람직하게는, 상기 텍스트파일은 hosts 파일이고, 상기 데이터베이스는 DNS인 것을 특징으로 한다.

본 발명의 다른 일면에 따라 단말기 내부에 설치되어 파밍을 감지하는 파밍감지장치가 제공되며: 이 장치는, IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경여부를 체크하는 무결성유지모듈; IP주소와 도메인이름이 매핑된 정보를 저장하고 있는 외부 데이터베이스로부터 정보를 송수신하는 도메인조회모듈; 및 상기 무결성유지모듈을 통해서 상기 텍스트파일의 변경이 체크된 경우, 상기 텍스트파일에서 변경된 정보를 추출하고, 상기 변경된 정보와 대응되는 정보를 상기 데이터베이스로부터 수신한 후, 상기 변경된 정보 및 상기 수신된 정보를 서로 비교하는 제어모듈;을 포함하는 것을 특징으로 한다.

바람직하게는, 상기 제어모듈은 상기 텍스트파일에서 변경된 IP주소 및 이에 대응되는 도메인이름을 추출하고, 상기 추출된 도메인이름을 상기 데이터베이스로 전송한 후, 상기 전송된 도메인이름과 매핑되는 IP주소를 수신한 후, 상기 추출된 정보의 IP주소와 상기 수신된 IP주소가 일치하는지 여부를 비교하는 것을 특징으로 한다.

바람직하게는, 상기 제어모듈은 상기 비교결과 불일치한 경우 상기 텍스트파일의 IP주소를 상기 데이터베이스로부터 수신된 IP주소로 수정하는 것을 특징으로 하는 특징으로 한다.

바람직하게는, 상기 텍스트파일은 hosts 파일이고, 상기 데이터베이스는 DNS인 것을 특징으로 한다.

본 발명의 다른 일면에 따라 네트워크를 통해서 서로 연결된 클라이언트모듈, 사업자서버 및 인증도메인DB를 포함하는 파밍감지시스템을 이용해서 파밍을 감지하는 방법이 제공되며: 이 방법은, 상기 클라이언트모듈이 IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경 여부를 체크하는 단계; 상기 체크결과 변경이 발생하면, 상기 클라이언트모듈이 상기 텍스트파일에서 변경된 정보를 추출하는 단계; 상기 클라이언트모듈이 상기 추출된 정보를 사업자서버로 전송하는 단계; 상기 사업자서버가 상기 전송받은 추출정보와 대응되는 정보를 사업자에 의해서 관리되고 업데이트되며 IP주소와 도메인이름이 매핑된 정보를 저장하고 있는 인증도메인DB부터 수신하는 단계; 및 상기 사업자서버가 상기 추출된 정보와 상기 인증도메인DB부터 수신된 정보를 비교하는 단계;를 포함하는 것을 특징으로 한다.

바람직하게는, 상기 텍스트파일은 hosts 파일이고, 상기 추출단계는 상기 hosts 파일에서 변경된 IP주소와 이에 대응되는 도메인이름을 추출하는 것이고, 상기 수신단계는 상기 추출단계에서 추출된 정보의 도메인이름을 상기 인증도메인DB로 전송한 후, 상기 전송한 도메인이름과 매핑되는 IP주소를 수신하는 것이고, 상기 비교단계는 추출된 정보의 IP주소와 상기 수신된 IP주소가 일치하는지 여부를 비교하는 것을 특징으로 한다.

바람직하게는, 상기 사업자서버가 상기 비교결과 및 수신된 정보를 클라이언트모듈로 전송하는 단계; 및 상기 전송된 비교결과가 불일치한 경우, 상기 클라이언트모듈이 상기 hosts 파일의 변경된 IP주소를 상기 수신된 IP주소로 수정하는 것을 특징으로 하는 특징으로 한다.

바람직하게는, 상기 사업자서버가 상기 추출된 정보,상기 수신된 정보 및 비교결과를 적재하는 단계를 더 포함하는 것을 특징으로 하는 특징으로 한다.

바람직하게는, 상기 사업자서버가 상기 인증도메인DB의 정보를 외부의 한개 이상의 DNS의 정보와 비교하는 단계;를 더 포함하고, 상기 비교결과 인증도메인DB의 정보가 외부 DNS의 정보와 다른 경우에는 상기 사업자서버가 인증도메인DB의 정보가 변경되었음을 나타내는 메세지를 디스플레이 하는 단계를 더 포함하는 것을 특징으로 한다.

본 발명의 다른 일면에 따라 네트워크를 통해서 서로 연결된 클라이언트모듈, 사업자서버 및 인증도메인DB를 포함하는 파밍감지시스템이 제공되며: 이 시스템은, 상기 클라이언트모듈은 사용자의 단말기에 설치되며, IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경여부를 체크하는 무결성유지모듈; 및 상기 무결성유지모듈을 통해서 상기 텍스트파일의 변경이 체크된 경우, 상기 텍스트파일에서 변경된 정보를 추출하고, 이를 상기 사업자 서버로 전송하는 클라이언트제어모듈;을 포함하며, 상기 인증도메인DB는 사업자에 의해서 관리되고 업데이트되며 IP주소와 도메인이름이 매핑된 정보를 저장하고 있는 DB형태인것을 특징으로 하며, 상기 사업자의 서버는, 상기 클라이언트모듈로부터 변경정보를 수신하고, 상기 수신된 변경정보와 대응되는 정보를 상기 인증도메인DB에서 수신한 후, 상기 변경정보와 상기 수신정보를 비교한 후 비교결과를 클라이언트모듈로 전송하는 서버제어모듈;을 포함하는 것을 특징으로 한다.

본 발명의 또 다른 일면에 따라 컴퓨터로 읽을 수 있는 기록매체가 제공되며: 이 기록매체는, 파밍감지장치가, IP주소와 도메인이름이 매핑된 정보를 가지고 단말기에 저장된 텍스트파일의 변경 여부를 체크하는 단계; 상기 체크결과 변경이 발생하면, 상기 파밍감지장치가 상기 텍스트파일에서 변경된 정보를 추출하는

단계; 상기 추출된 정보와 대응되는 정보를 IP주소와 도메인이름을 저장하고 있는 데이터베이스로부터 수신하는 단계; 및 상기 텍스트파일로부터 추출된 정보와 상기 데이터베이스로부터 수신된 정보를 비교하는 단계;를 수행할 수 있는 프로그램이 기록된다.

[0010] 삭제

[0011] 삭제

[0012] 삭제

[0013] 삭제

[0014] 삭제

[0015] 삭제

[0016] 삭제

[0017] 삭제

[0018] 삭제

[0019] 삭제

[0020] 삭제

효 과

[0021] 이상 설명한 바와 같이, 본 발명에 따른 파밍감지 시스템은 hosts 파일의 변경을 감지하여, 변경된 경우에 올바른 변경인지를 판단하여 이에 따라 적절한 대응을 사용자에게 제공한다.

[0022] 이에 따라, 올바르게 hosts 파일을 변경한 경우에는 변경된 내용을 복원시키지 않고 잘못된 변경인 경우에는 복원시킬 수 있게 된다.

발명의 실시를 위한 구체적인 내용

[0023] 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

[0024] 도 1은 hosts 파일 및 DNS를 통해서 인터넷 접속이 이루어지는 과정의 일 예를 도시한 도면이다. 사용자의 컴퓨터(100)의 내부에는 hosts 파일(110)이 존재하고 있고(도 1에는 컴퓨터(100)의 외부에 Hosts파일(110)이 도시되어 있으나 이는 도시상의 편의를 위한 것이고, 실제로 Hosts 파일은 컴퓨터에 내장된 HDD디스크등의 저장장치에

파일형태로 기록됨), 컴퓨터(100)는 DNS(120)와 두개의 사이트(140,150)과 인터넷을 통해서 연결되어 있다.

[0025] 이 경우 우선 사용자가 www.def.com이라는 사이트로 접속을 하는 경우를 가정하자. 이때 사용자는 익스플로러의 주소창에 바로 111.112.123.124를 입력해도 되나 대부분의 경우에는 이렇게 IP 주소를 외우지 못하는바, www.def.com 이라고 입력할 것이다. 이러면 컴퓨터(100)는 맨 처음에 hosts파일(110)에서 www.def.com에 해당하는 IP주소가 입력되어 있는지를 검색한다. hosts파일(110)에는 www.def.com에 해당하는 IP주소가 없는 바, 다시 DNS(120)로 해당 IP주소에 대한 질의를 날린 후 111.112.123.124라는 주소를 응답받아서 www.def.com(150)에 접속하게 된다. 여기서 도1에서는 DNS(120)를 한개만 도시하였으나, 이는 설명의 편의를 위한 것이고 실제로는 여러개의 분산된 데이터베이스의 형태로 존재하게 된다. 즉 사용자가 입력한 도메인 네임은 사용자의 컴퓨터에 설정된 Local DNS에 질의 되어 IP주소 응답을 기다리게 된다. Local DNS는 질의된 도메인 네임에 대해 자신의 데이터베이스 테이블에서 조회를 하여 쌍을 이루는 IP주소가 있을경우 클라이언트에게 정보를 응답해 주며, 관련 정보를 찾을 수 없을 경우 Root Name Server 측으로 질의를 보내서 다시 조회를 하게 된다.

[0026] 한편 www.abc.com이라는 사이트로 접속을 하는 경우에는 hosts 파일에 이에 해당하는 IP주소로 111.112.113.114를 가지고 있는바 DNS(120)로 질의를 할 필요없이 바로 www.abc.com(140)에 접속할 수 있게 된다. 결과적으로 DNS로 유입되는 트래픽 부하를 감소 시키고, 사용자의 컴퓨터는 DNS 질의 절차를 생략할 수 있어 보다 빠른 인터넷 접속이 가능할 수 있게 된다.

[0027] 도 2는 변조된 Hosts 파일로 인해 피싱서버(160)(Phishing Server, 개인정보를 빼내는 등의 용도로 사용되는 가짜 웹 사이트, 이하 피싱서버라고 칭함)로 접속이 이루어지는 과정의 일 예를 도시한 도면이다.

[0028] Hosts 파일을 보면 www.abc.com에 대한 IP주소가 정상적인 주소가 아니라 피싱서버(160)의 주소로 변조되어 있다. 따라서 사용자가 주소창에 www.abc.com이라고 입력하면 hosts 파일에 주소가 있는바, DNS에 조회없이 바로 피싱서버(160)로 이동하게 된다.

[0029] 도 3은 본 발명의 일 실시예에 따른 파밍감지장치의 블럭도이다.

[0030] 도 3에 도시된 바와 같이 파밍감지장치(200)는 무결성유지모듈(210), 제어모듈(220) 및 도메인조회모듈(230)을 포함한다.

[0031] 파밍감지장치(200)는 사용자의 컴퓨터(100)에 설치된다. 이후 무결성유지모듈(210)은 실시간으로 컴퓨터(100)내에 있는 hosts 파일(110)의 변경여부를 체크한다.

[0032] 도메인조회모듈(230)은 제어모듈(220)의 제어에 따라서, 외부에 네트워크로 연결되어 있는 DNS(120)로부터 도메인과 IP로 이루어진 정보를 조회하고 수신하는 기능을 수행한다.

[0033] 제어모듈(220)은 파밍감지장치(200)의 전체적인 기능을 제어하며, 특히 상기 무결성유지모듈(210)을 통해서 hosts 파일이 변경이 체크된 경우, 도메인조회모듈(230)을 제어해서 DNS(120)로부터 정보를 조회한다. 그리고 hosts 파일의 변경된 정보와 DNS(120)로부터 조회된 정보를 비교해서 일치하지 않는 경우 hosts 파일을 복원하는 등의 기능을 수행한다.

[0034] 이러한 기능들에 대해서는 이하 도 4에서 보다 상세히 설명한다.

[0035] 도 4는 도 3에 도시된 파밍감지장치(200)의 제어방법의 설명에 제공되는 흐름도이다.

[0036] 우선 파밍감지장치(200)의 무결성유지모듈(210)은 hosts 파일이 변경되었는지를 검사한다(S410). 무결성유지모듈(210)의 감지 프로세스는 사용자의 컴퓨터(100)에 상주하고 있으며, 정해진 시간 간격을 기준으로 또는 주기적으로 hosts 파일의 변경 여부를 점검하거나, 사용자 직접 수정 또는 허가되지 않은 프로세스의 접근 등으로 hosts 파일이 변경이 일어나면 제어모듈(220)에게 바로 통지한다.

[0037] hosts 파일의 변경이 감지된 경우(S420-Y)에는, hosts 파일에서 변경된 부분에 해당하는 변경정보를 수집한다(S430).

[0038] 도 5는 hosts 파일과 DNS내의 데이터의 일 예를 도시한 도면이다. 도 5에서 www.abc.com의 IP주소가 111.112.113.115로 변경되었다고 가정하자. 이럴 경우에 hosts 파일의 변경정보는 "111.112.113.115, www.abc.com"이 될 것이다.

[0039] 이 후에 다시 파밍감지장치(200)는 상기 변경정보의 도메인네임과 대응되는 정보를 DNS(120)로부터 조회한다(S440). 도 5와 같은 경우라면 조회정보는 "111.112.113.114, www.abc.com"이 될 것이다.

[0040] 이렇게 변경정보와 조회정보를 추출한 후에, 양 정보를 비교한다(S450). 도 6은 hosts 파일의 변경정보와 DNS의 조회정보의 일 예를 도시한 도면이다. 도시된 바와 같이 변경정보와 조회정보의 IP주소가 일치하지 않는 경우에는(S460-N), 사용자에게 hosts 파일에 잘못된 변조가 있었음을 알려주는 경고를 수행한다(S470).

[0041] 그리고 hosts 파일의 변경정보를 조회정보에 맞춰서 복원하여 준다(S480).

[0042] 도 7은 변조된 hosts 파일(710)과 복원된 hosts 파일(720)의 일 예를 도시한 도면이다. 결국 변조된 hosts 파일(710)에서 www.abc.com에 해당하는 IP주소가 불일치하였고, 이를 DNS에서 조회된 데이터(620)에 맞춰서 복원한다.

[0043] 물론 설정에 따라서 사용자경고 단계(S470)를 생략하고 바로 복원하는 것도 가능하다. 또한 복원이 아니라 아예 hosts 파일에서 해당 정보를 삭제하는 것도 가능하고, 불일치가 발생할 때 사용자에게 선택창을 띄어주어서, 변경정보를 유지할지, 복원할지 아니면 아예 삭제할지를 선택하도록 하는 것 역시도 가능하다.

[0044] 한편 본 실시예에서 DNS(120)는 컴퓨터가 IP주소를 질의하는 DNS(120)인 경우가 일반적이나 이에 한정되지는 않는다. IP주소를 질의하는 DNS(120)는 상술한 바와 같이 도메인 이름과 이에 대응하는 IP 주소에 관한 데이터베이스를 유지하고 있다가 원하는 컴퓨터에게 제공하는데, 이러한 목록을 중앙에 1개 만을 유지하는 것은 비현실적이고 비효율적이기 때문에, 도메인 이름과 IP 주소 목록은 기관별 체계에 따라 인터넷 도처에 분산되어 있다.

[0045] 따라서 평소 사용하는 DNS는 사용자와 지리적으로 가까운 곳 어딘가에 있는 DNS이다. 이렇게 평소 컴퓨터가 인터넷 접속시에 주소로 변환하기 위해 사용되는 DNS를 이하에서는 로컬DNS로 호칭한다.

[0046] 반면에 이러한 로컬DNS 역시도 해커들의 공격으로 hosts 파일과 함께 변조될 가능성이 있다. hosts 파일과 함께 로컬DNS도 변조되었을 경우를 대비하여, 파밍감지 시스템을 위한 별도의 DNS서버를 구축하는 방법도 가능하다. 이러한 DNS는 이하 인증DNS라고 호칭한다. 즉 파밍감지 시스템에는 인증DNS의 주소가 내장되어 있어서, S440단계에서 조회시에 평소 사용하는 DNS(즉, 로컬DNS)로 접속하지 않고 인증DNS로 들어가서 정보를 조회하는 것이다. 인증DNS는 본 발명의 파밍감지 시스템을 공급하는 사업자가 수시로 관리하여 데이터의 안정성이 입증된 DNS인 바 보다 더 안전할 것이다.

[0047] 또는 S440단계에서 로컬DNS와 인증DNS 양측으로부터 정보를 조회해서, 변경정보와 로컬DNS조회정보 및 인증DNS 조회정보 세가지를 비교해서 셋다 일치여부를 검사하는 방법도 가능하다.

[0048] 한편 DNS를 로컬DNS 및 인증DNS 뿐만 아니라 아예 사용자의 컴퓨터에 내장하는 방법도 가능하다.

[0049] 또 다른 방법으로는 다수의 DNS와 비교하는 방법이다. 즉 상술한 바와 같이 로컬DNS 또는 사업자가 관리하는 인증DNS 각각 또는 상기 두개의 DNS와 호스트 화일을 비교하는 것에 한정하는 것이 아니고, 세개 이상의 다수의 DNS와 비교하는 것 역시도 가능하다. 즉 상술한 바와 같이 네트워크 상에는 다수의 DNS가 존재하는 바 여러개의 DNS의 주소를 가지고 있다가, S440단계에서 조회시에 여러개의 DNS들에 들어가서 전부의 일치여부를 판단하고 이러한 결과를 보여주는 방법도 가능하다.

[0050] 구체적인 방법으로는 우선 세개의 DNS를 이용해서 본 서비스를 한다고 가정할 때, 복수의 DNS간에 조회결과가 일치하면서, 호스트파일의 변경정보와도 일치한다면 정상적인 호스트파일 변경이라고 판단한다.

[0051] 만약에 복수의 DNS간에 조회결과가 일치하면서, 호스트파일의 변경정보와는 불일치한다면 호스트파일이 변조되었다고 판단한다.

[0052] 반대로 복수의 DNS간에 조회결과가 불일치하다면, 이 때에는 사용자에게 변조 가능성이 있다던가, 또는 현재 DNS가 문제가 있다는 정보등을 알려줄 수 있다.

[0053] 도 8은 본 발명의 다른 일 실시예에 따른 파밍감지 시스템의 블럭도이다. 도 8에 도시된 파밍감지 시스템은 크게 단말기(100)에 설치되는 클라이언트모듈(800), 사업자서버(830) 및 인증도메인DB를 포함한다.

[0054] 단말기(100)와 사업자서버(830) 및 인증도메인DB(840)는 서로 인터넷을 통해서 연결되어 있다. 사업자서버(830) 및 인증도메인DB(840)의 경우 도시된 바와 같이 별도로 구성되어 있는 경우가 많으나, 한개의 물리적인 서버시스템에 같이 구현해도 무방하다.

[0055] 우선 클라이언트모듈(800)이 사용자의 단말기(100)에 설치된다. 이렇게 설치된 클라이언트모듈(800)는 무결성유지모듈(810) 및 클라이언트제어모듈(820)을 포함한다.

[0056] 무결성유지모듈은 hosts파일(110)이 변경되었는지 여부를 체크하는 기능을 수행하며, 클라이언트제어모듈(820)은 hosts파일(110)에서 변경된 정보를 추출하여, 사업자서버(830)로 전송하거나 hosts파일(110)을 수정 및 삭제하는 기능을 수행한다.

[0057] 사업자서버(830)는 사업자가 본 서비스를 수행하기 위해서 구비한 서버로서 여러명의 클라이언트제어모듈(820)과 네트워크로 연결된다. 이 경우 각각의 사용자들이에 IP 및 Password 를 할당해서 로그인을 하여 접속하게도 가능하다.

[0058] 사업자서버(830)는 상기 클리이언트모듈로부터 변경정보를 수신하고, 상기 수신된 변경정보와 대응되는 정보를 상기 인증도메인DB(840)에서 조회한 후, 상기 변경정보와 상기 조회정보를 비교한 후 비교결과를 클라이언트모듈로 전송하는 서버제어모듈(832)와 상기 추출된 정보,상기 조회된 정보 및 비교결과를 적재하고 통계내는 기능을 수행하는 통계모듈(834)을 포함한다.

[0059] 그 외에도 서버로서 구동하기 위한 여러모듈들 예를 들어 웹서비스모듈등이 필요하나 이는 당업자라면 당연한 내용인바 생략한다.

[0060] 그리고 인증도메인DB(840)는 사용자의 컴퓨터가 인터넷에 접속시에 사용하는 일반적인 LOCAL DNS와는 별도로 사업자가 본 파밍감지 시스템을 구현하기 위해서 별도로 운영하는 DNS의 일종이다. 이렇게 별도로 DNS를 운영함으로서 만에 하나 해커가 사용자들의 컴퓨터내에 있는 hosts 파일뿐만 아니라 LOCAL DNS까지 해킹된 경우까지도 대비할 수 있게된다.

[0061] 한편 이러한 인증도메인DB(840)를 유지하는 방법 중 하나로서, 임의 시간마다 복수의 DNS와 비교하는 프로세스를 수행한다. 즉 인증도메인DB(840)에서 특정 도메인 정보와 상기 복수의 DNS의 정보가 모두 일치하면 유지하고, 만약에 인증도메인DB(840)에서 특정 도메인 정보와 상기 복수의 DNS의 정보가 일치하지 않다면, 사업자에게 경고등의 메세지를 띄어서 현재 인증도메인DB(840)가 신뢰할 수 없다는 것을 알리고, 이에 따라 사업자가 확인작업을 거칠 수 있게 된다.

[0062] 도 9는 도 8에 도시한 파밍감지 시스템(800)의 제어방법의 설명에 제공되는 흐름도이다.

[0063] 여기서 S910단계 내지 S930단계는 도 4의 S410단계 내지 S430단계와 유사한바 자세한 설명은 생략한다.

[0064] S930단계에서 변경정보 수집 후, 변경정보 즉 변경된 IP주소와 이에 매핑되는 도메인이름을 사업자서버(830)로 전송한다(S935).

[0065] 이후에 사업자서버(830)내에 있는 서버제어모듈(832)은 상기 변경된 정보에 해당하는 도메인이름에 대응되는 IP주소를 인증도메인DB(840)에서 조회한다(S940).

[0066] 그후 사업자서버(830)는 상기 변경정보의 IP주소와 상기 조회된 IP주소를 비교한다(S950). 만약 일치하지 않은 경우(S960-N), 통계모듈(834)은 해당 도메인이름, 변경정보의 IP주소 및 조회된 IP주소를 적재하고 통계데이타를 작성한다(S965). 이렇게 작성된 통계데이타는 현재 기승을 부리는 파밍형태를 감지하고, 사용자들에게 미리 경고 메세지를 보내는등 여러가지 부가서비스에 이용될 수 있다.

[0067] 그리고 나서 서버제어모듈(832)은 상기 비교결과 및 조회된 정보를 클라이언트모듈(800)의 클라이언트모듈로 전송한다(S970).

[0068] 이 후에 상기 클라이언트제어모듈(820)은 상기 hosts 파일의 변경된 IP주소를 상기 서버제어모듈(832)로부터 수신한 조회된 IP주소로 수정한다(S980).

[0069] 여기서 수정전에 사용자에게 hosts 파일이 변조되었음을 알리는 경고를 표시하고, 또한 수정할지 여부를 문의한 후에 수정하는 것이 바람직할 것이다. 또한 수정할지 아예 삭제할지를 물어보는 질의창을 띄운후 수정대신 hosts 파일의 변경된 부분을 통째로 삭제하는 것도 가능하다.

[0070] 지금까지, 파밍감지 시스템을 사용해서 변조된 hosts 파일을 검색하고 복원하는 과정에 대해, 바람직한 실시예를 들어 상세히 설명하였다.

[0071] 본 실시예에서는 단말기의 일 예로서 컴퓨터를 들어 설명하였으나, 컴퓨터는 설명의 편의를 위한 일 실시예에 불과하다. 따라서 DNS 및 hosts 파일을 이용하여 네트워크로 접속하는 장치라면 그 어느 것이라도 본 발명이 적용될 수 있음은 물론이다.

[0072] 또한 본 실시예에서는 hosts 파일이라고 호칭하였으나, 이것이 hosts 라는 이름을 가진 파일에 한정되는 것은

아니다. 본 발명에서 hosts 파일이란 DNS에 접속하는 과정을 생략하기 위해서 도메인이름과 IP주소로 이루어진 데이타파일을 의미하며, 따라서 차후 운영체제에서 상기 기능을 하는 파일의 명칭이 hosts에서 다른 이름으로 변경되더라도 본 발명의 적용될 수 있음은 물론이다.

[0073] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

도면의 간단한 설명

[0074] 도 1은 hosts 파일 및 DNS를 통해서 인터넷 접속이 이루어지는 과정의 일 예를 도시한 도면,

[0075] 도 2는 변조된 Hosts 파일로 인해 phishing 서버로 접속이 이루어지는 과정의 일 예를 도시한 도면,

[0076] 도 3은 본 발명의 일 실시예에 따른 파밍감지 시스템의 블럭도,

[0077] 도 4는 본 발명의 일 실시예에 따른 파밍감지 시스템의 제어방법의 설명에 제공되는 흐름도,

[0078] 도 5는 hosts 파일과 DNS내의 데이터의 일 예를 도시한 도면,

[0079] 도 6은 hosts 파일의 변경정보와 DNS의 조회정보의 일 예를 도시한 도면,

[0080] 도 7은 변조된 hosts 파일과 복원된 hosts 파일의 일 예를 도시한 도면,

[0081] 도 8은 본 발명의 다른 일 실시예에 따른 파밍감지 시스템의 블럭도, 및

[0082] 도 9는 본 발명의 다른 일 실시예에 따른 파밍감지 시스템의 제어방법의 설명에 제공되는 흐름도이다.

[0083] * 도면의 주요 부분에 대한 부호의 설명 *

[0084] 100 : 컴퓨터 110 : hosts 파일

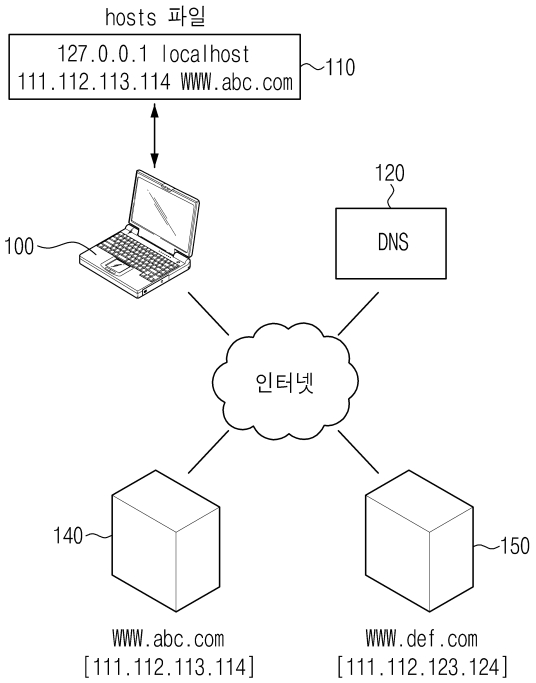
[0085] 120 : DNS 200 : 파밍 감지 장치

[0086] 210 : 무결성 유지모듈 220 : 제어모듈

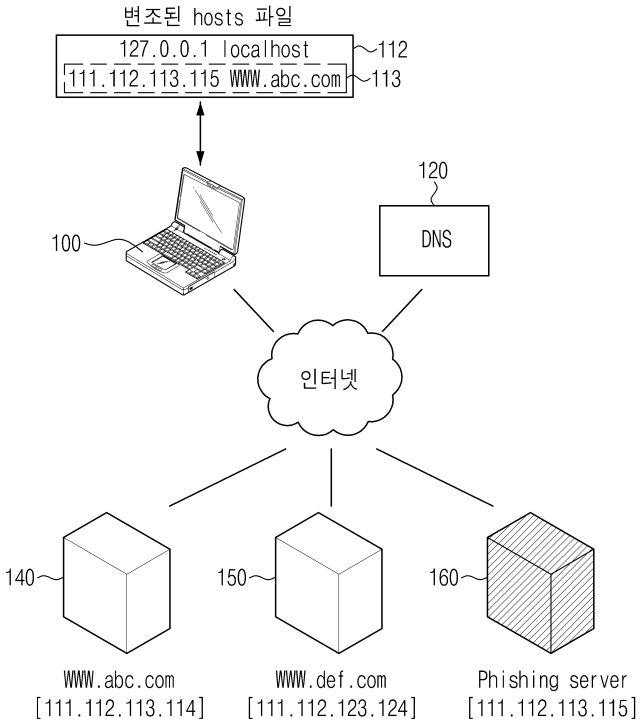
[0087] 230 : 도메인 조회 모듈

도면

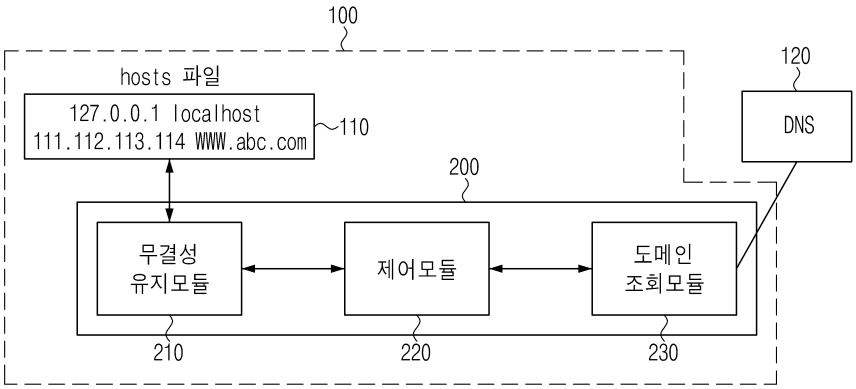
도면1


hosts 파일
127.0.0.1 localhost
111.112.113.114 WWW.abc.com
110
120
DNS
100
인터넷
140
150
WWW.abc.com
[111.112.113.114]
WWW.def.com
[111.112.123.124]

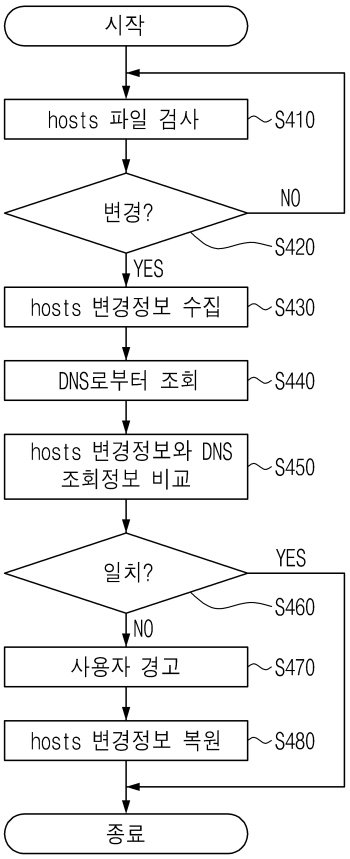
도면2


변조된 hosts 파일
127.0.0.1 localhost
111.112.113.115 WWW.abc.com
112
113
120
DNS
100
인터넷
140
150
160
WWW.abc.com
[111.112.113.114]
WWW.def.com
[111.112.123.124]
Phishing server
[111.112.113.115]

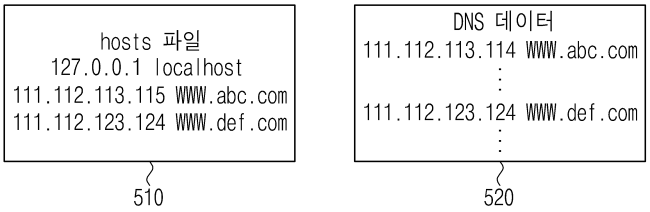
도면3


100
120
hosts 파일
127.0.0.1 localhost
111.112.113.114 WWW.abc.com
110
DNS
200
무결성
유지모듈
제어모듈
도메인
조회모듈
210
220
230

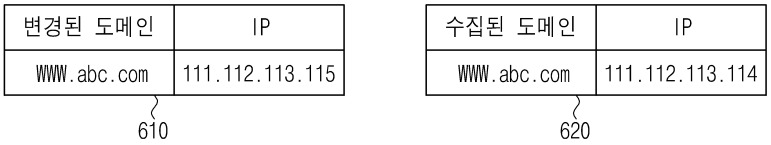
도면4


시작
hosts 파일 검사
S410
변경?
NO
S420
YES
hosts 변경정보 수집
S430
DNS로부터 조회
S440
hosts 변경정보와 DNS
조회정보 비교
S450
일치?
YES
S460
NO
사용자 경고
S470
hosts 변경정보 복원
S480
종료

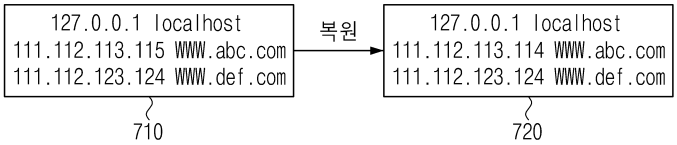
도면5


hosts 파일
127.0.0.1 localhost
111.112.113.115 WWW.abc.com
111.112.123.124 WWW.def.com
510
DNS 데이터
111.112.113.114 WWW.abc.com
111.112.123.124 WWW.def.com
520

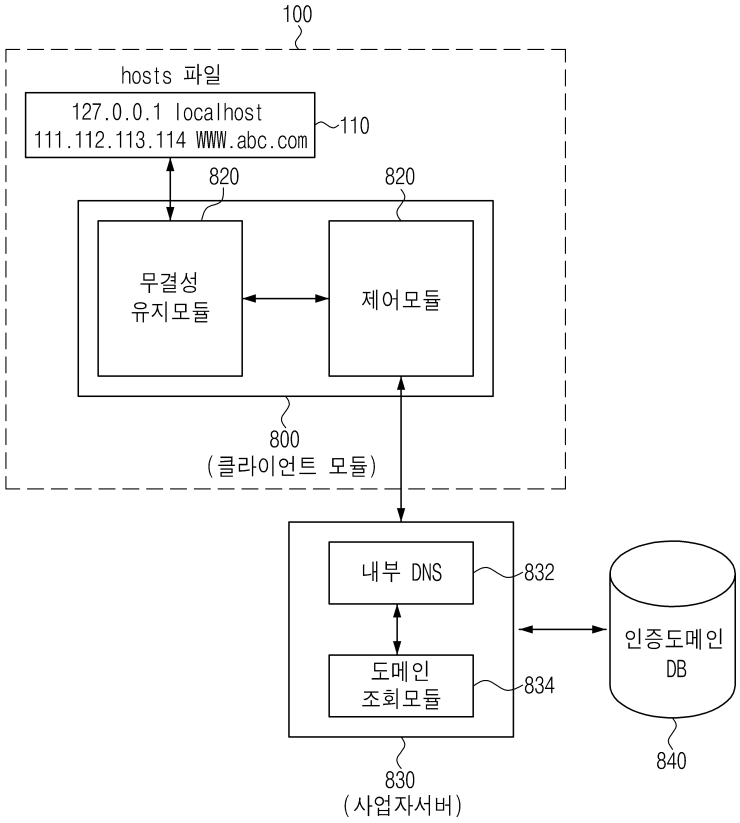
도면6


변경된 도메인
IP
WWW.abc.com
111.112.113.115
610
수집된 도메인
IP
WWW.abc.com
111.112.113.114
620

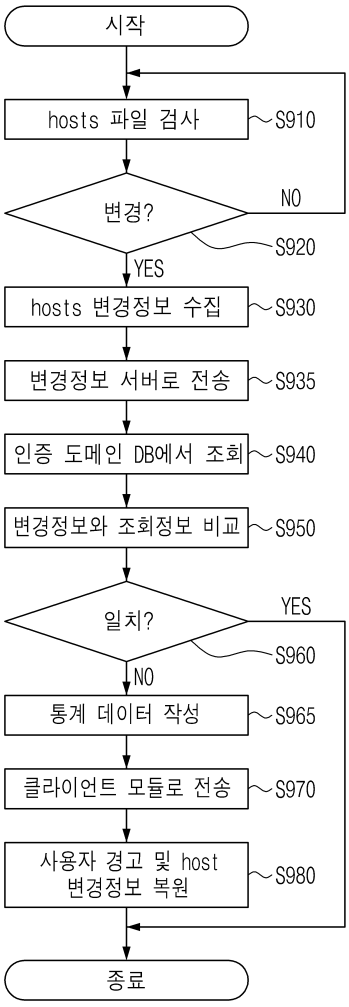
도면7


127.0.0.1 localhost
111.112.113.115 WWW.abc.com
111.112.123.124 WWW.def.com
710
복원
127.0.0.1 localhost
111.112.113.114 WWW.abc.com
111.112.123.124 WWW.def.com
720

도면8


100
hosts 파일
127.0.0.1 localhost
111.112.113.114 WWW.abc.com
110
820
820
무결성
유지모듈
제어모듈
800
(클라이언트 모듈)
내부 DNS
832
도메인
조회모듈
834
830
(사업자서버)
인증도메인
DB
840

도면9


시작
hosts 파일 검사
S910
변경?
NO
S920
YES
hosts 변경정보 수집
S930
변경정보 서버로 전송
S935
인증 도메인 DB에서 조회
S940
변경정보와 조회정보 비교
S950
일치?
YES
S960
NO
통계 데이터 작성
S965
클라이언트 모듈로 전송
S970
사용자 경고 및 host
변경정보 복원
S980
종료