(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0106893
(43) 공개일자 2007년11월06일

(51) Int. Cl.
H04L 12/22(2006.01) *H04L 9/32*(2006.01)
H04L 29/06(2006.01)
(21) 출원번호 10-2006-0039324
(22) 출원일자 2006년05월01일
심사청구일자 없음

(71) 출원인
이형우
경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호
충남대학교산학협력단
대전광역시 유성구 궁동 220번지 충남대학교
(뒷면에 계속)
(72) 발명자
이형우
경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호
양성욱
서울 광진구 구의동 235-38 102호
(74) 대리인
이선우

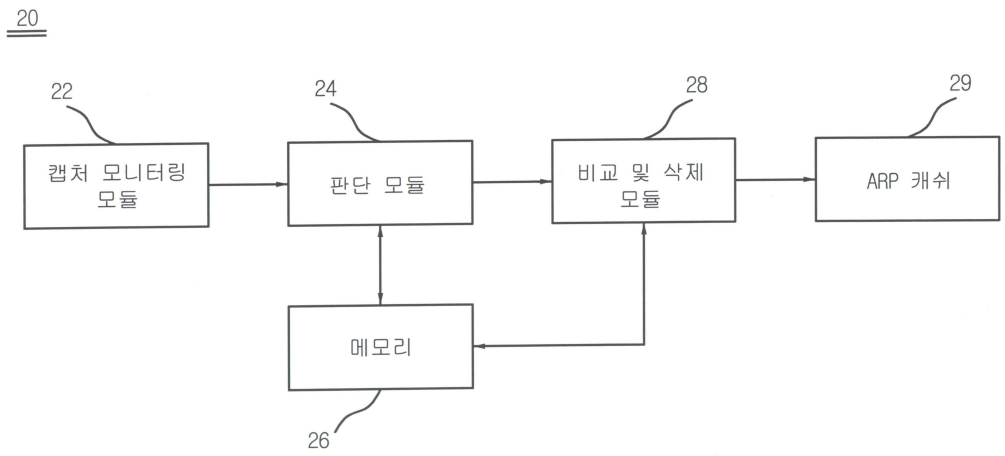
전체 청구항 수 : 총 1 항

(54) 에이알피 포이즌 공격차단방법

(57) 요 약

본 발명은 에이알피(ARP : Address Resolution Protocol) 포이즌(Poison) 공격차단방법에 관한 것으로, 모든 에이알피 리퀘스트 패킷(ARP request packet)을 캡처하여 모니터링하는 단계와; 캡처된 브로드캐스트 에이알피 리퀘스트 패킷(broadcast ARP request packet)의 소스 아이피(Source IP)와 소스 맥(source MAC(Media Access Control))을 해쉬테이블에 등록하는 단계와; 유니캐스트 에이알피 리퀘스트 패킷(unicast ARP request packet)과 에이알피 리플라이 패킷(ARP reply packet)의 소스 아이피와 소스 맥을 해쉬테이블에 등록된 정보와 비교하는 단계; 및 비교결과 저장된 정보와 일치하지 않을 경우 에이알피 캐쉬값을 삭제하는 단계;를 포함하여 이루어진 것을 특징으로 한다.

대표도 - 도3



(71) 출원인
양성욕
서울 광진구 구의동 235-38 102호

한신대학교 산학협력단
경기 오산시 양산동 한신대학교내

특허청구의 범위

청구항 1

모든 에이알피(ARP:Address Request Protocol) 패킷을 캡처하여 모니터링하는 단계와;

캡처된 브로드캐스트(broadcast) ARP 리퀘스트 패킷(request packet)의 소스 아이피(Source IP)와 소스 맥(source MAC(Media Access Control)을 메모리의 해쉬테이블에 등록하는 단계와;

유니캐스트(unicast) ARP 리퀘스트 패킷(request packet)과 ARP 리플라이 패킷(reply packet)의 소스 아이피와 소스 MAC을 메모리의 해쉬테이블에 등록된 정보와 비교하는 단계; 및

비교결과 저장된 정보와 일치하지 않을 경우 ARP 캐쉬(Cache) 값을 삭제하는 단계;를 포함하여 이루어진 것을 특징으로 하는 에이알피 포이즌 공격차단방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<12> 본 발명은 에이알피 포이즌 공격차단방법에 관한 것으로, 특히 에이알피 포이즌 공격을 차단하기 위해서 브로드캐스트 에이알피 리퀘스트 패킷의 소스 아이피와 소스 맥(MAC : Media Access Control: 이하 'MAC'이라 함)을 저장해 두고, 유니캐스트 에이알피 리퀘스트 패킷과 에이알피 리플라이 패킷의 소스 아이피와 소스 맥을 비교해서 저장된 정보와 같지 않으면 에이알피 캐쉬(ARP cache) 테이블에서 삭제하는 에이알피 포이즌 공격차단방법에 관한 것이다.

<13> 유선랜 스위치 환경에서 상대방의 패킷을 훔쳐보는 방법으로 에이알피(ARP : Address Resolution Protocol:이하 'ARP'라 함) 포이즌(Poison) 공격을 시도한 뒤 패킷을 캡처한다. ARP 포이즌(Poison) 공격 방법은 공격자가 패킷을 훔쳐보기 위해서 피해자 컴퓨터의 ARP 캐쉬(cache) 테이블의 내용을 바꾸는 것을 말한다.

<14> 내부 유선망 스위치 환경에서 가장 빈번하게 일어나고 있는 공격이 상대방의 정보를 훔쳐보는 스니핑(sniffing) 공격이다. 스니핑(sniffing)을 이용하면 상대방의 개인 정보를 훔쳐보는 것이 가능하며 현재 다수의 스니핑 전용 해킹 소프트웨어들이 존재한다.

<15> 스위치 장비로 구성된 랜 환경에서는 ARP 포이즌(Poison) 공격을 먼저 수행해야 스니핑(sniffing) 공격을 수행할 수 있다. 그러므로 ARP 포이즌(poison) 공격만 차단할 수 있다면 유선랜 환경에서는 스니핑(sniffing) 공격을 차단할 수 있게 된다.

<16> 도 1은 종래기술에 따른 에이알피 포이즌 공격의 개념을 나타낸 개념도이다.

<17> 도 1을 참조하면, 아이피어드레스(IP)가 192.168.1.33인 공격자 컴퓨터(11)로부터 아이피어드레스(IP)가 192.168.1.88 및 192.168.1.1인 상대방 컴퓨터들(12,13)을 에이알피 포이즌 공격하는 과정을 살펴본다. 먼저, 아이피어드레스(IP)가 192.168.1.33인 공격자 컴퓨터(11)는 아이피어드레스(IP)가 192.168.1.88 및 192.168.1.1인 상대방 컴퓨터들(12,13)에 대한 맥 포이즌 공격을 시작한다. 이후 각각의 상대방 컴퓨터들(12,13)은 에이알피 테이블에서 각각 아이피어드레스(IP)가 192.168.1.1 및 192.168.1.88인 상대방 컴퓨터들(12,13)을 MAC이 192.168.1.33의 맥으로 변경된다. 이후 공격자 컴퓨터(11)는 아이피어드레스(IP)가 192.168.1.88 및 192.168.1.1로 부터 오는 트래픽을 포워딩(forwarding)하여 스니핑 공격이 가능하게 된다.

<18> 현재 ARP 포이즌(poison)을 차단하기 위해서 스위치 장비에서 게이트웨이의 MAC이 포이즌(poison)되지 않도록 하기 위해서 매초 전체 네트워크를 대상으로 정상적인 게이트웨이의 MAC을 뿌리는 방법을 택하고 있다. 이 방법은 이와 같은 기능을 가진 장비가 별도로 필요하며 네트워크의 많은 트래픽 과부하를 초래하고, 내부 랜 상에서 서로 통신할 경우의 스니핑(sniffing) 공격은 막지 못하는 문제점이 있다.

<19>

발명이 이루고자 하는 기술적 과제

<20> 본 발명의 목적은 상기한 바와 같은 종래 기술에서의 문제점을 해결하기 위하여 제안된 것으로서, ARP 포이즌(Poison) 공격을 차단하기 위해서 브로드캐스트(Broadcast) ARP 리퀘스트(Request) 패킷의 소스 아이피(Source IP)와 소스(Source) MAC을 저장해 두고, 유니캐스트(Unicast) ARP 리퀘스트(Reqeust) 패킷과 ARP 리플라이(Reply) 패킷의 소스 아이피(Source IP)와 소스(Source) MAC을 비교해서 저장된 정보와 같지 않으면 ARP 캐쉬(cache) 테이블에서 삭제하는 에이알피 포이즌 공격차단방법을 제공하는 데 있다.

<21>

발명의 구성 및 작용

<22> 상기한 바와 같은 목적을 달성하기 위한 본 발명의 바람직한 실시예에 의하면, 모든 에이알피(Address Request Protocol) 패킷을 캡처하여 모니터링하는 단계와; 캡처된 브로드캐스트 에이알피 리퀘스트 패킷(broadcast ARP request packet)의 소스 아이피(Source IP)와 소스 맥(source MAC)을 해쉬테이블에 등록하는 단계와; 유니캐스트 에이알피 리퀘스트 패킷(unicast ARP request packet)과 에이알피 리플라이 패킷(ARP reply packet)의 소스 아이피와 소스 맥을 해쉬테이블에 등록된 정보와 비교하는 단계; 및 비교결과 저장된 정보와 일치하지 않을 경우 에이알피 캐쉬값을 삭제하는 단계;를 포함하여 이루어진 것을 특징으로 하는 에이알피 포이즌 공격차단방법이 제공된다.

<23> 본 발명은 사용자 컴퓨터에서 실행되는 사용자 영역 프로그램으로서 ARP 패킷들을 모니터링하여 ARP 포이즌(poison) 공격이 발생할 경우 ARP 캐쉬(cache) 테이블에서 제거하는 기법에 대한 내용이다.

<24> 본 발명은 커널 영역 프로그램이 아닌 사용자 영역 프로그램으로도 구현되었다.

<25> 도 2는 본 발명에 따른 에이알피 포이즌 공격차단방법의 개념을 나타낸 개념도이다.

<26> 도 2를 참조하면, 아이피어드레스(IP)가 192.168.1.1인 송신자 컴퓨터(112)로부터 아이피어드레스(IP)가 192.168.1.12, 192.168.1.14, 192.168.1.23, 192.168.1.65 및 192.168.1.97인 상대방 컴퓨터들(12,13)을 향해 브로드캐스트 에이알피 리퀘스트 패킷이 전송된다(특정한 상대방 컴퓨터 예를 들면 아이피어드레스가 192.168.1.65인 상대방 컴퓨터에 대한 MAC를 포함할 수 있다). 상기 브로드캐스트 에이알피 리퀘스트 패킷을 수신한 다수의 상대방 컴퓨터들(113 내지 117)은 송신자 컴퓨터(112)의 아이피와 MAC 정보를 저장한다.

<27> 이후 아이피어드레스(IP)가 192.168.1.3인 공격자 컴퓨터(111)가 아이피어드레스(IP)가 192.168.1.14인 상대방 컴퓨터(114)에 대한 에이알피 포이즌 공격을 시작한다. 즉, 유니캐스트(unicast) 에이알피 리퀘스트와 에이알피 리플라이를 이용하여 에이알피 포이즌 공격을 시작한다. 상기 상대방 컴퓨터(114)는 접수된 유니캐스트 에이알피 리퀘스트/에이알피 리플라이 패킷을 저장된 정보와 비교후에 상이한 경우에는 에이알피 테이블에서 삭제함으로써 에이알피 포이즌 공격을 차단하게 된다.

<28> 도 3은 본 발명에 따른 에이알피 포이즌 공격차단장치의 개략적인 블록구성도이고, 도 4는 도 3에 따른 동작을 나타내는 흐름도이다.

<29> 도 3 및 도 4를 참조하면, 본 발명에 따른 에이알피 포이즌 공격차단장치(20)는 모든 APR 패킷을 캡처하여 모니터링하는 캡처모니터링 모듈(22)과; 캡처된 브로드캐스트(broadcast) ARP 리퀘스트 패킷(request packet)의 소스 아이피(Source IP)와 소스 맥(source MAC)을 메모리(26)의 해쉬테이블에 등록하는 판단모듈(24)과; 캡처된 에이알피 패킷 중 유니캐스트 에이알피 리퀘스트 패킷(unicast ARP request packet)과 에이알피 리플라이 패킷(ARP reply packet)의 소스 아이피와 소스 MAC을 해쉬테이블에 등록된 정보, 즉 브로드캐스트 에이알피 리퀘스트 패킷(broadcast ARP request packet)의 소스 아이피(Source IP)와 소스 MAC과 비교하고, 비교결과 저장된 정보와 일치하지 않을 경우 에이알피 캐쉬(ARP cache)(29)에 저장된 에이알피 캐쉬값을 삭제하는 비교 및 삭제 모듈(28);을 포함하여 이루어진다.

<30> 이하 본 발명에 따른 에이알피 포이즌 공격차단방법에 대하여 첨부도면을 참조로 상세히 설명한다.

<31> 먼저, 캡처모니터링 모듈(22)을 통해 모든 ARP 패킷들을 캡처하여 모니터링한다(ST-2). 이후, 판단모듈(24)을 통해 상기 캡처된 ARP 패킷이 브로드캐스트(Broadcast) ARP 리퀘스트(Request) 패킷인지를 판단한다(S-4). 상기 판단결과 캡처된 ARP 패킷이 브로드캐스트 에이알피 패킷인 경우에는, 해당 브로드캐스트 에이알피 리퀘스트 패킷의 소스 아이피(Source IP) 와 소스(Source) MAC을 메모리(26)의 해쉬테이블에 저장한다(소스 아이피 및 맥

등록과정)(ST-6). 캡쳐된 브로드캐스트(Broadcast) ARP 리퀘스트(Request) 패킷의 소스 아이피(Source IP) 와 소스(Source) MAC을 해시테이블에 등록하는 이유는 브로드캐스트(Broadcast) ARP 리퀘스트(Request) 패킷의 소스 아이피(Source IP)와 소스(Source) MAC은 변조되지 않기 때문이다. 그러므로 정상적인 아이피(IP)와 MAC 정보를 등록하기 위해서 위의 동작을 한다.

<32> 이후, 상기 판단모듈(24)은 상기 캡쳐된 ARP 패킷이 브르도캐스트(Broadcast) ARP 리퀘스트(Request) 패킷이 아닌 경우에는 유니캐스트 에이알피 리퀘스트 패킷과 에이알피 패킷으로 판단하고, 이후 비교 및 삭제모듈(28)에서 유니캐스트 에이알피 리퀘스트 패킷과 에이알피 패킷의 소스 아이피와 소스 맥 정보를 등록된 정보와 비교한다(ST-8).

<33> 상기 유니캐스트(Unicast) ARP 리퀘스트(Reqeust) 패킷과 ARP 리플라이(Reply) 패킷의 소스 아이피(Source IP)와 소스(Source) MAC을 해시테이블에 등록된 정보와 비교하는 이유는 ARP 포이즌(Poison) 공격이 유니캐스트(Unicast) ARP 리퀘스트(Request) 패킷과 ARP 리플라이(Reply) 패킷을 이용하기 때문이다.

<34> 상기 단계 ST-8의 비교결과, 유니캐스트 ARP 리퀘스트 패킷과 ARP 패킷의 소스 아이피와 소스 MAC 정보가 등록된 정보와 동일한 경우에는 접수된 정보에 따른 기능을 수행하게 되고, 유니캐스트 ARP 리퀘스트 패킷과 ARP 패킷의 소스 아이피와 소스 MAC 정보가 등록된 정보와 상이한 경우에는 ARP 캐쉬(Cache)를 삭제하게 된다(ST-10). 즉, 상기 저장된 정보와 일치하지 않을 경우 이미 ARP 캐쉬(Cache) 테이블이 변조된 값으로 포이즌(poison) 되었기 때문에 ARP 캐쉬(cache) 테이블에서 이 변조된 값을 삭제한다.

발명의 효과

<35> 상기 설명된 바와 같이, 본 발명에 따른 에이알피 포이즌 공격차단방법에 의하면, 에이알피 포이즌 공격을 차단하기 위해서 브로드캐스트(Broadcast) ARP 리퀘스트(Reqeust) 패킷의 소스 아이피(Source IP)와 소스(Source) MAC을 저장해 두고, 유니캐스트(Unicast) ARP 리퀘스트(Reqeust) 패킷과 ARP 리플라이(Reply) 패킷의 소스 아이피(Source IP)와 소스(Source) MAC을 비교해서 저장된 정보와 같지 않으면 ARP 캐쉬(cache) 테이블에서 삭제함으로써 ARP 포이즌 공격차단을 별도의 장치없이 구현할 수 있으므로 ARP 포이즌 공격차단을 쉽게 수행할 수 있는 효과가 있다.

<36> 또한 별도의 기능을 가진 장비없이, 트래픽의 과부하를 초래하지 않으면서 동시에 내부 랜 상에서 서로 통신할 경우 즉, 내부 유선랜 환경에서 스니핑 공격을 차단할 수 있는 효과가 있다.

<37> 본 발명은 상기한 바람직한 실시예를 중심으로 기술하였지만, 본 발명은 이에 한정되는 것은 아니며, 본 발명의 기술분야에 익숙한 기술자라면 첨부되는 특허청구범위를 토대로 하여 다양하게 변형실시가 가능할 것이다.

도면의 간단한 설명

<1> 도 1은 종래기술에 따른 에이알피 포이즌 공격의 개념을 나타낸 개념도이다.

<2> 도 2는 본 발명에 따른 에이알피 포이즌 공격차단방법의 개념을 나타낸 개념도이다.

<3> 도 3은 본 발명에 따른 에이알피 포이즌 공격차단장치의 개략적인 블록구성도이다.

<4> 도 4는 도 3에 따른 동작을 나타내는 흐름도이다.

<5> * 도면의 주요부분에 대한 부호의 설명 *

<6> 20 :에이알피 포이즌 공격차단장치

<7> 22: 캡처모니터링 모듈

<8> 24: 판단모듈

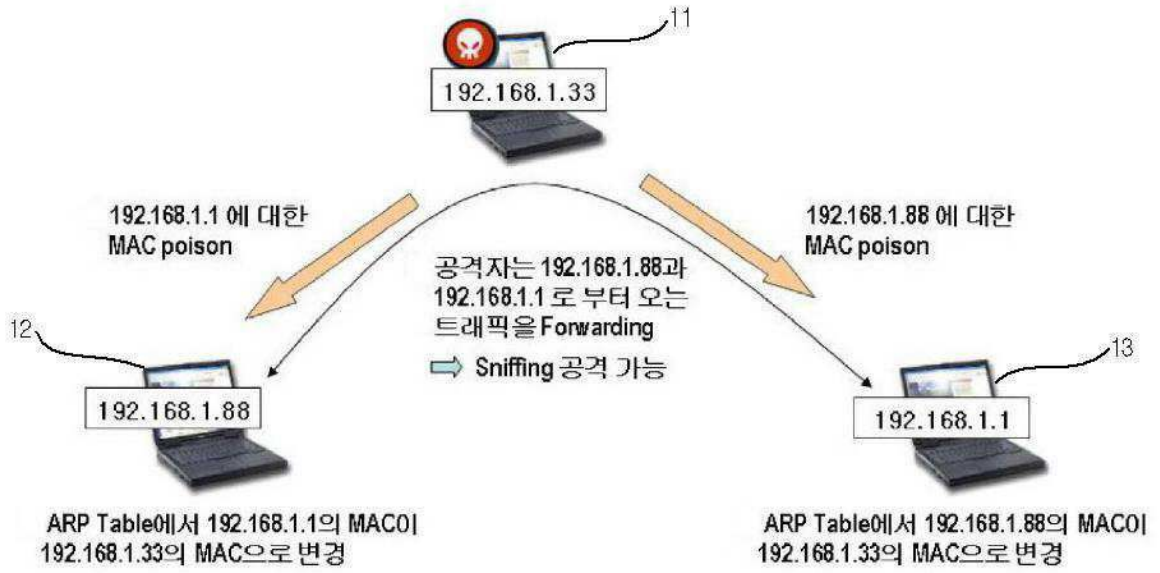
<9> 26: 메모리

<10> 28: 비교 및 삭제모듈

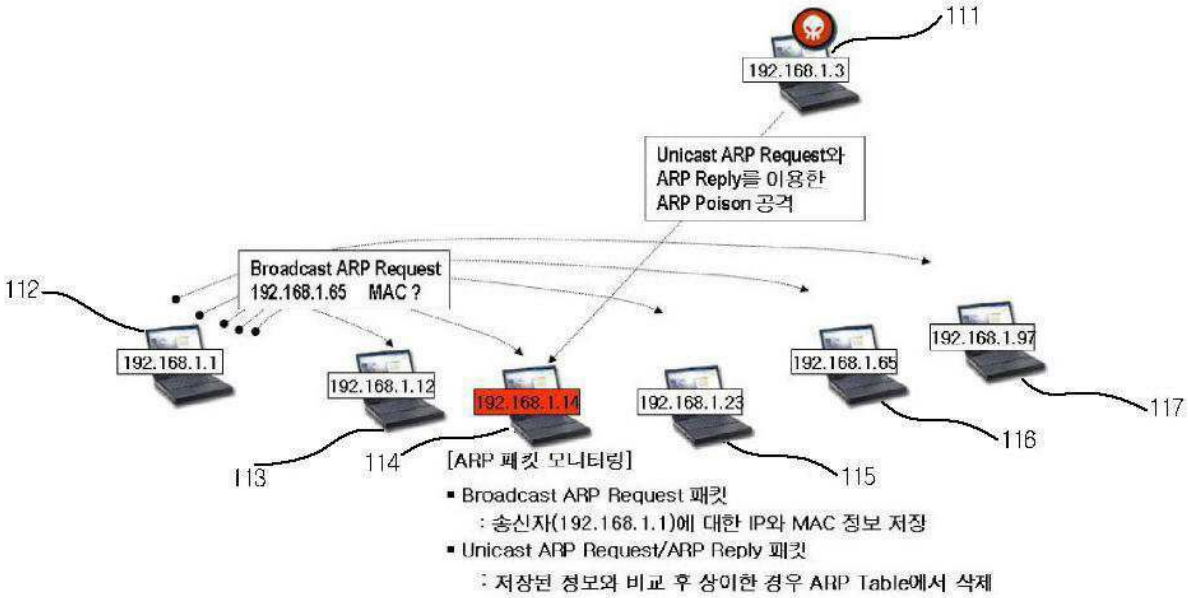
<11> 29: 에이알피 캐쉬(ARP cache)

도면

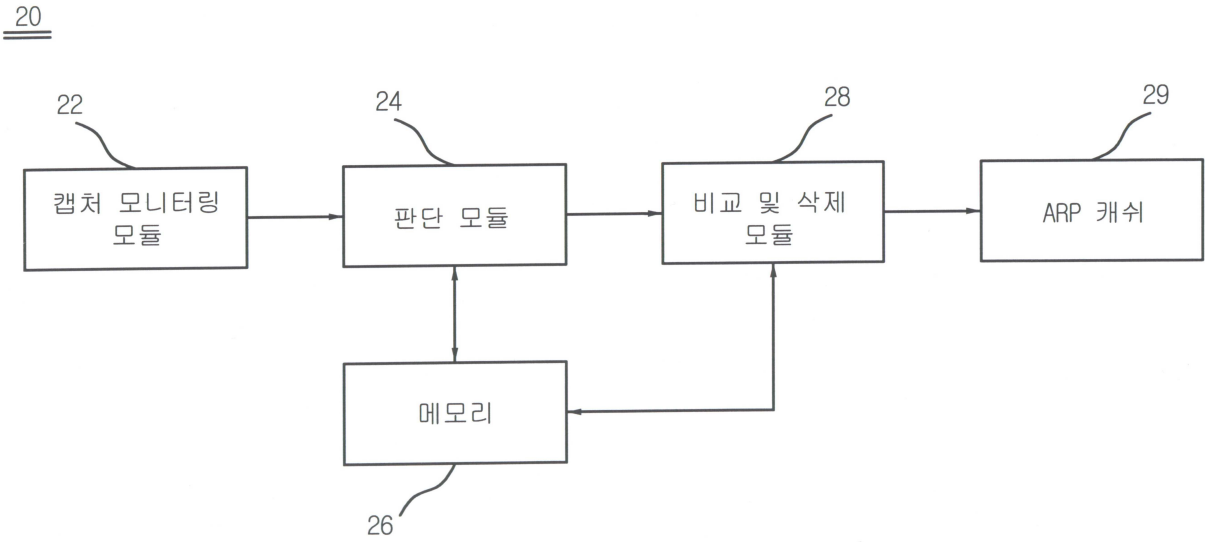
도면1


11
192.168.1.33
192.168.1.1 에 대한
MAC poison
192.168.1.88 에 대한
MAC poison
공격자는 192.168.1.88과
192.168.1.1 로 부터 오는
트래픽을 Forwarding
⇨ Sniffing 공격 가능
12
192.168.1.88
13
192.168.1.1
ARP Table에서 192.168.1.1의 MAC이
192.168.1.33의 MAC으로 변경
ARP Table에서 192.168.1.88의 MAC이
192.168.1.33의 MAC으로 변경

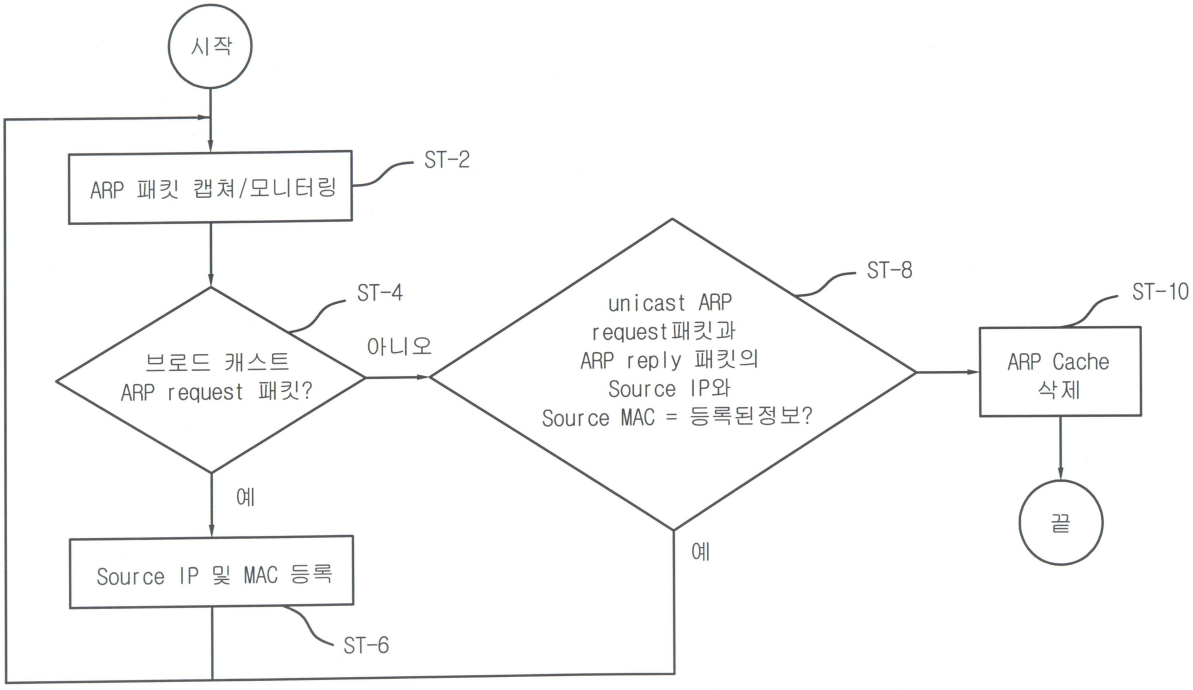
도면2


111
192.168.1.3
Unicast ARP Request와
ARP Reply를 이용한
ARP Poison 공격
Broadcast ARP Request
192.168.1.65 MAC ?
112
192.168.1.1
192.168.1.12
192.168.1.14
192.168.1.23
192.168.1.65
192.168.1.97
113
114
[ARP 패킷 모니터링]
115
116
117
▪ Broadcast ARP Request 패킷
: 송신자(192.168.1.1)에 대한 IP와 MAC 정보 저장
▪ Unicast ARP Request/ARP Reply 패킷
: 저장된 정보와 비교 후 상이한 경우 ARP Table에서 삭제

도면3


20
22
캡처 모니터링 모듈
24
판단 모듈
28
비교 및 삭제 모듈
29
ARP 캐쉬
메모리
26

도면4


시작
ARP 패킷 캡쳐/모니터링
ST-2
ST-4
브로드 캐스트 ARP request 패킷?
아니오
예
ST-8
unicast ARP request패킷과 ARP reply 패킷의 Source IP와 Source MAC = 등록된정보?
예
ST-10
ARP Cache 삭제
끝
Source IP 및 MAC 등록
ST-6