중소기업융합학회 논문지 제4권 제1호 pp. 47-53, 2014

도메인 네임 스푸핑 공격과 그 대응책

홍성혁
백석대학교, 정보통신학부

ARP spoofing attack and its countermeasures

Sunghyuck Hong
Baekseok University, Division of Information and Communication

요 약 DNS스푸핑은 DNS서버를 통해 특정 웹서버의 주소로 번역하는 과정에서 이를 가로채서 공격자가 원하는 위조된 웹서버로 접근하게 하는 방법이다. ARP 스푸핑은 ARP 프로토콜의 요청과 응답메시지에 대한 인증을 하지않고 잘못된 정보가 와도 ARP Cache Table에 그대로 저장하는 취약점을 이용해 자신의 MAC주소를 다른 컴퓨터의 MAC주소인 것처럼 속이는 기법이다. 이러한 DNS/ARP 스푸핑 공격 방법에 대해서 상세히 알아보고 이를 예방하는 방안을 제안하였다.

주제어 : DNS/ARP 스푸핑 공격, DNS/ARP 스푸핑 공격 분석, Countermeasure ARP spoofing

Abstract DNS spoofing, the DNS server with the address of a specific web server intercepts them in the process of translating the attacker wants to forge a Web server that is a way to access. ARP spoofing ARP request and response messages for the protocol without authentication vorticity incorrect information as to the ARP Cache Table to store the MAC addresses of their vulnerability using the MAC address of the other computer as if it were a lie technique. These DNS / ARP spoofing attacks in detail to find out about how it looks at ways to prevent. Think about the future research directions.

Key Words : Spoofing, DNS Attack, ARP Attack, ARP Spoofing Prevent

1. 서론

DNS(Domain Name System)스푸핑은 DNS서버를 통해 특정 웹 서버의 URL(Uniform Resource Locator)을 IP(Internet Protocol)주소로 번역하는 과 정에서 이를 가로채서 공격자가 원하는 위조된 웹 서버로 접근하게 하는 방법을 말한다. 그리고 이 위조된 웹 서버는 Malware 같은 악성 코드를 삽입하여 서버 접근자의 시스템을 파괴 할 수 도 있고, 간단한 스크립트 프로그램을 활용하여 사용자의 ID나 password같은 개인 정보를 취할 수도 있다. 또한 이 공격은 DNS서버를 공격하여 DoS(Denial of Service)공격을 유발하게 할 수 있다.

ARP 스푸핑은 ARP 프로토콜의 요청과 응답메시지에 대한 인증을 하지 않고 잘못된 정보가 와도 ARP Cache Table에 그대로 저장하는 취약점을 이용해 자신의 MAC 주소를 다른 컴퓨터의 MAC주소인것처럼 속이는 기법이다. 본 논문에서는 이러한 DNS/ARP 스푸핑 공격 방법에 대해서 상세히 알아보고, 이를 예방하는 방안에 대해

이 논문은 2014년도 백석대학교 대학연구비에 의하여 수행된 것임.
논문접수일 : 2014년 2월 11일 심사완료일 : 2014년 2월 15일 논문게재일: 2014년 3월 31일
*제1저자 : 홍성혁(shong@bu.ac.kr)

살펴본다.[3]

2. 관련 연구

2.1 인터넷 보안 위협 현황

최근 악의적인 공격자들의 공격 기법이 종래 운영체제 취약점을 이용하는데서 벗어나 애플리케이션 레벨로 공격의 초점이 옮겨지고 있다. 여전히 운영체제를 대상으로 하는 공격도 계속 되고 있지만, DNS 서버나 웹 애플리케이션, P2P파일 공유 애플리케이션, 네트워크와 다른 기기간의 설정 상에 나타난 약점, 보안 담당자의 권한 설정, 사용자의 환경의 문제 등을 공격하고 있다[1].

최초의 웜(Worm)으로 알려진 모리스(Morris, 1988) 이후, 신종 악성 코드 위협이 급격하게 증가했다. 이런 증가의 원인으로는 온라인 사기를 조장하기 위한 상품 및 서비스 요구를 지원하는 전문적인 악성코드 개발을 들 수 있다.

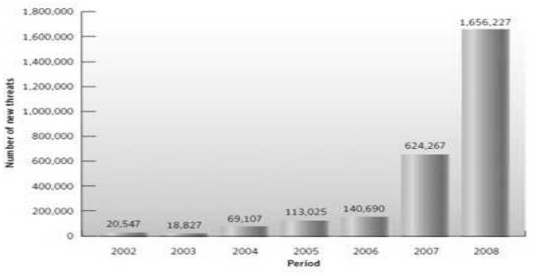

Figure 1. 인터넷 악성코드의 증가

공격방법의 변화는 공격자들이 방화벽, 라우터 등의 전통적인 경계 보안 장비를 타깃으로 한 다양한 목적을 가진 대량 공격 유형에서 벗어나 국지적 타깃, 웹 애플리케이션, 데스크탑 등을 공격해 개인, 금융 및 중요 정보를 얻어내, 이를 통해 금전적인 이득을 노린 사이버 범죄 행위를 노리고 있다는 것을 알 수 있다.[3]

3. ARP Spoofing

ARP(Address Resolution Protocol)은 네트워크상에서 IP주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜로 상대방의 IP주소만 알고 MAC(Media Access Control)주소는 알지 못할 때 사용한다 ARP스푸핑은 ARP프로토콜의 요청과 응답메시지에 대한 인증을 하지않고 잘못된 정보가 와도 ARP Cache Table에 그대로 저장하는 취약점을 이용해 자신의 MAC주소를 다른 컴퓨터의 MAC주소인 것처럼 속이는 기법이다.[5]

3.1 ARP Spoofing 공격 기법

스위치는 모든 트래픽을 MAC 주소를 기반으로 해서 전송하게 된다. 공격자는 LAN상의 모든 호스트 IP-MAC 주소 매핑을 ARP Request 브로드캐스팅을 통해 정확하게 알아 낼 수 있어 공격자에게 악용될 수 있다. 아래 (그림2)은 호스트-A와 호스트-B의 정상적인 스위치 상에서의 트래픽이 전송되는 모습이다.

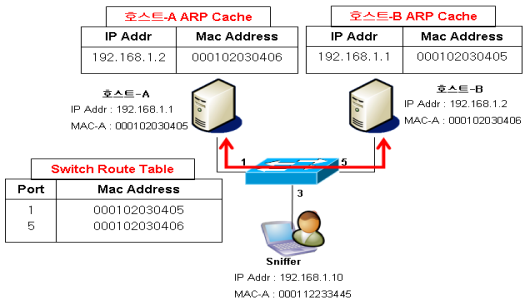

Figure 2. 정상적인 통신

ARP 프로토콜은 인증을 요구하는 프로토콜이 아니기 때문에 간단한 ARP Reply 패킷을 각 호스트에 보내서 쉽게 ARP Cache를 업데이트시킬 수 있다. 그림2-1처럼 스니퍼는 각 호스트들에게 위조한 MAC 주소(상대방의 MAC 주소 = 스니퍼 MAC 주소)를 보내 각 호스트의 ARP Cache를 업데이트 시키게 되고 스위치에서는 스니퍼의 MAC 주소와 포트 매핑 정보가 테이블에 등록된다.

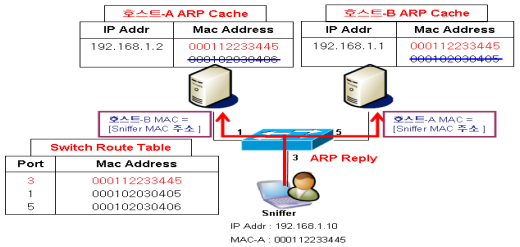

Figure 2-1. ARP Spoofing 공격

계속해서 스니퍼는 Cache가 사라지기 전에 변조된 ARP Reply를 지속적으로 보내므로 각 호스트들의 ARP Cached의 변조된 MAC 주소의 정보는 계속해서 유지된다. 이때 스니퍼는 두 방향으로 정확히 재전송해 줄 수 있는 기능이 있어야만 호스트 A와 B는 통신을 할 수 있다. 공격에 성공하면 두 호스트는 서로의 MAC 주소를 스니퍼의 MAC 주소로 인식하고 있기 때문에 모든 트래픽을 스니퍼에게 전달하게 된다. 스니퍼는 이 두 호스트에게 재전송할 수 있는 기능이 있으며 또한 모든 패킷들을 캡쳐 할 수 있게 된다.[4]

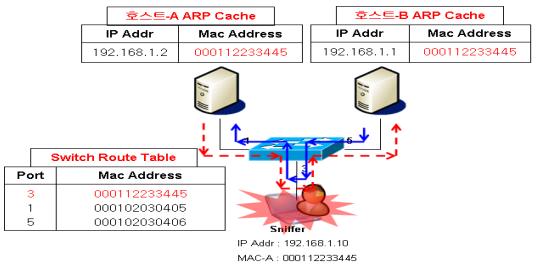

Figure 2-2. ARP Spoofing후 스니핑

3.2 공격 분석

3.2.1 피해 시스템에서의 증상

ARP Spoofing을 위해 서버와 클라이언트 같은 종단간의 통신을 가로채어 재전송 하는 시스템이 있기 때문에 네트워크 속도의 저하가 발생한다. 패킷을 가로챈 후 변조하는 경우에는 대부분의 웹 페이지가 공통적으로 사용하는 태그를 인식하여 악성코드를 삽입하기 때문에 웹 페이지가 시작되는 head, title 등의 태그 주변에 삽입한다.

그 이유는 패킷의 중간이나 끝부분에 삽입하고자 하면 TCP 패킷의 전송 특성상 대체하고자 하는 문자열이 분리(fragmentation)와 재조합 과정에서 나누어져서 문자열을 인식할 수 없는 가능성있기 때문이다. 피해 시스템에서 관리하는 ARP table을 계속해서 변조한 상태로 유지하기 위해 공격자는 조작한 ARP 패킷을 지속적으로 발송하므로, ARP패킷의 수신량이 증가된다.[4]

3.2.2 피해 시스템에서의 탐지방법

윈도우즈나 유닉스/리눅스 계열 모두 arp -a 명령과 같이 ARP table을 조회하는 명령으로 주변 시스템의 IP와 MAC주소를 확인한다. 단, 평소에 통신을 하지 않던 시스템의 MAC주소도 확인해야 하므로, 동일 서브네트워크의 모든 host에 ping 명령이나 nmap등의 도구를 사용하여 IP와 MAC주소로 위장하기 때문에 이 부분을 유심히 살펴본다. 만약 게이트웨이의 MAC주소가 실제 게이트웨이의 MAC주소와 다르다면 ARP Spoofing으로 인한 결과일 확률이 대단히 높다.

또한, ARP table에 동일한 MAC주소가 서로 다른 IP에서 사용되고 있는지 확인한다. 즉, 아래 그림의 경우처럼 게이트웨이 IP(172.16.4.1)에서 사용하는 MAC을 다른 IP(172. 1 6.4.163)도 사용하고 있다면, ARP Spoofing을 의심해 볼 수 있다. 다만, 시스템 설정에 따라 하나의 NIC에 여러 IP를 사용 할 수도 있고, ARP Spoofing을 수행하는 시스템에 IP를 넣지 않는 경우 등은 예외이다.[4]

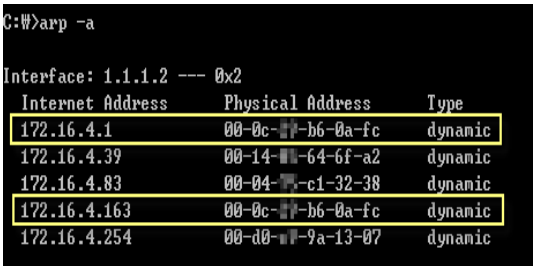

Figure 2-3. ARP table

4. ARP Spoofing 공격 방지

4.2 시스템에서의 방지 대책

4.2.1 정적인 ARP table 관리

윈도우즈계열에서 사용하는 시작/종료 스크립트에 정적으로 관리하고자 하는 시스템의 IP와 MAC주소를 입력하는 스크립트를 지정하거나, 리눅스계열에서의 rc3.d와 같이 시작 스크립트를 기동하는 곳에서 스크립트를 실행하도록 하여 재부팅 시에도 항상 정적인 ARP table이 관리될 수 있도록 한다. 아래는 윈도우즈 계열의 경우에 ARP table을 정적으로 관리하는 명령이다. 특히, Gateway의 IP와 MAC 주소를 정적으로 고정시킴으로써 잘못된 ARP Reply 정보가 오더라도 이를 ARP Table에 반영하지 못하도록 한다.[4]

Figure 3. ARP table

4.2.2 ARP Spoofing

지금까지 신고/접수되어 분석한 대부분의 ARP Spoofing 서버들은 본래의 용도 외에 침입자가 설치한 프로그램으로 인해 네트워크 트래픽 변조 서버로 악용된 것이었다. 그러므로 전체적인 보안수준을 강화하여, 공격자에게 악용되지 않도록 관리하여야 한다.[4]

4.2.3 중요 패킷의 암호화

자신의 서버를 안전하게 구축하였다고 하더라도 공격자는 동일 서브네트워크내의 취약한 서버를 해킹하여 트래픽의 도청 및 변조가 가능하다. 따라서 네트워크를 통해 아이디, 패스워드, 주민번호, 금융정보 등 중요 데이터가 송수신될 경우 이 정보 또한 공격자에 의해 유출되거나 변조될 수 있으므로 이러한 데이터에 대한 암호화가 바람직하다. 국내에서는 정보통신망 이용촉진및정보보호에관한법률에 의해 인터넷상에서 개인정보가 송수신되는 웹서버의 경우 보안서버를 구축 하도록 규정하고 있으므로, 개인정보나 금융정보가 네트워크를 통해 송수신되는 서버의 경우 SSL(secure Socket Layer) 방식 등을 이용하여 웹 트래픽을 암호화할 필요가 있다.[4]

4.3 네트워크장비에서의 방지 대책

4.3.1 MAC Flooding

이더넷 스위치 환경의 경우, 허브 환경과는 다르게 단순히 자신의 시스템만 promiscuous mode로 동작시킨다고 해서 Sniffing 할 수 없기 때문에 다양한 방법 들을 동원하여 Sniffing하게 된다. 그 중에서 MAC Flooding방법은 수 많은 위장 MAC주소를 생성하여 스위칭에 필요한 CAM(Content Addressable Memory)을 관리하는 자원을 고갈시킴으로써 이더넷 프레임들을 모든 포트에 전송토록 하는 공격을 일컫는데, 시스코 장비의 예를 들면, 이 공격을 차단하기 위해서 아래의 그림과 같이 Port security라는 기능을 사용하는 것이 효과적이다.

Figure 3-1. Port Security 기능 설정 예

이 기능에는 물리적인 포트가 수용할 수 있는 MAC주소의 개수를 지정하거나 사용 가능한 MAC주소를 지정할 수 있으므로, 수많은 MAC주소가 발생해도 CAM의 관리에 어려움이 없게 된다. IDC와 같이 시스템의 변경이 빈번하지 않은 환경이라면 충분히 효과적으로 활용할 수 있다. 참고로, MAC주소의 정적인 관리는 양쪽의 시스템 모두에서 이루어 져야 한다. 만약 서버 측에서만 정적인 ARP table을 관리한다면 ARP Spoofing 발생 시 네트워크 트래픽 흐름이 Client → G/W → S/W → ARP Spoofing Server → 피해서버 → S/W → G/W → Client 순서로 이동하기 때문에, Sniffing에 의한 정보유출이나 조작된 정보입력 등의 피해가 발생할 수 있으므로, 반드시 네트워크 장비와 Host시스템 양측 모두 정적인 ARP 관리가 되어야 효과적인 차단이 가능하다.[4]

4.3.2 ARP 패킷 검사

앞서 살펴본 Port Security기능과 유사한 기능으로써 스위치에 수신되는 ARP 패킷들을 검사하여 마치 IP 필터링을 하는 방화벽의 동작과 유사하게 지정된 경로로만 ARP 패킷이 전송되도록 하는 기능을 사용하는 것도 효과적이다. 시스코 장비의 경우 ARP Inspection이라고 한다.[4]

4.3.3 사설 VLAN 기능 활용

동일 서브네트워크이지만, 지정한 호스트만 통신을 가능하도록 하는 사설 VLAN 기능을 활용하여 서로 통신할 필요가 없는 서버들을 격리시켜 운용한다. 아래의 그림은 사설 VLAN 개념도이다.

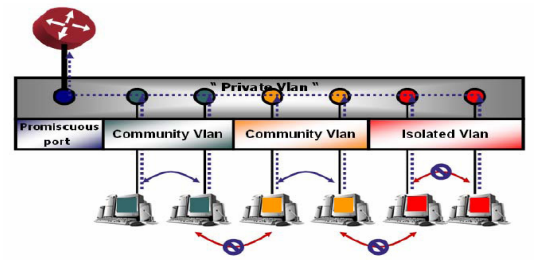

Figure 3-3. 사설 VLAN 개념도

예를 들어 서버호스팅의 경우 서로 다른 고객이 사용하는 서버가 같은 서브네트워크에 있다고 하더라도 서로 통신할 필요가 전혀 없기 때문에, 이러한 경우에는 고객별 사설 VLAN으로 격리한다면 더욱 더 안전한 시스템 운용을 할 수 있다.[4]

5. DNS 스푸핑을 이용한 공격 분석

5.1 DNS 스푸핑을 이용한 공격 방법

<Figure4>은 일반적 경우의 DNS 질의를 통한 웹 서버 접속 과정이다.

(1) 사용자 : Web서버로 접근하기 위해 DNS서버에 질의
(2) DNS서버 : DNS서버가 IP주소를 알려준다.
(3) 사용자 : Web에 접속

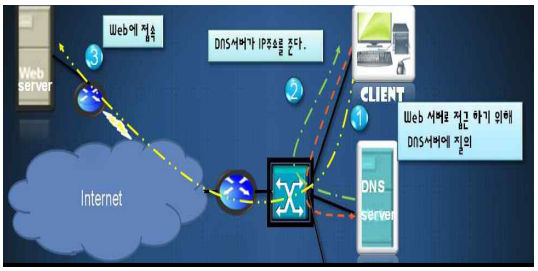

Figure 4. 일반적 DNS 질의를 통한 Web 서버 접속

<Figure4-1>는 DNS 스푸핑 과정이다.

(1) 공격자 : 유사 사이트 제작
(2) 공격자 -> 위조된 서버 : 유사 사이트 설치
(3) 공격자 -> 사용자 : ARP 스푸핑으로 DNS 질의 가로채기
(4) 사용자 : 위조된 사이트로 접속

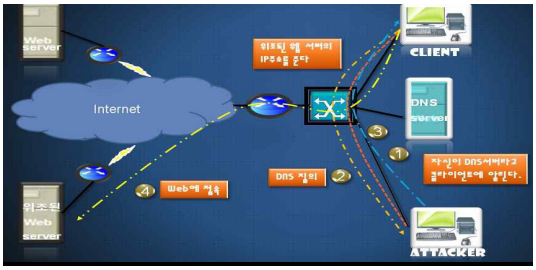

Figure 4-1. DNS스푸핑

[Figure 4-1] DNS스푸핑으로 위조된 웹 서버로 접속 스니핑을 이용한 DNS 스푸핑은 네트워크에서 스푸핑 툴 등을 이용하여 사용자의 DNS 질의를 가로채어 사용자에게 다른 IP를 반환하는 방법이다.

공격자는 사용자의 시스템에 ARP 스푸핑하여 DNS 질의를 관찰하다가 사용자가 특정 웹 서버에 대한 DNS 질의를 요청하였을 때, 사용자에게 공격자가 변조한 사이트의 IP를 반환한다. 사용자의 PC에는 정상적인 사이트로 표시되지만, 공격자가 변조한 사이트에 접속하게 된다.[1]

5.2 공격 구현

공격을 위해 공격자의 시스템에 Wincap(Window Packet Capture)를 설치하고, Winarp, Win_dnsspoof 프로그램을 이용 공격을 구현하였다[2].

5.2.1 DNS 스푸핑

<Figure 4-2>는 Win_dnsspoof 툴로 ′www.daum.net ‘’을 요청하는 DNS 질의에 대해 위조된 웹 서버의 IP 주소(220.149.189.227)로 전달한다.

Figure 4-2. 일반적 DNS 질의를 통한 Web 서버 접속

DNS 질의는 데이터 링크 계층의 프로토콜로 MAC 주소를 이용해 통신하기 때문에 사용자는 ARP 스푸핑 때

문에 잘못된 MAC 주소를 알고 있고, ARP와 DNS프로토콜은 인증 절차를 거치지 않기 때문에 공격자는 손쉽게 DNS 질의를 가로채서 위조 서버의 IP주소를 광고 할 수 있다[2].

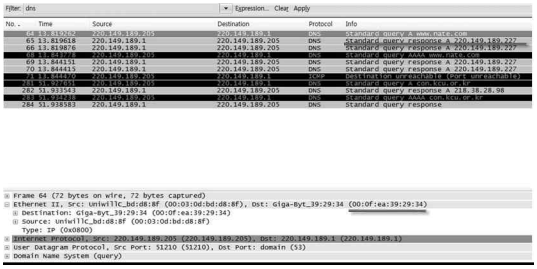

Figure 4-3. DNS 질의 과정의 DNS 패킷

5.2.2 DNS 스푸핑 결과

공격당한 사용자는 'www.daum.net'라는 웹 사이트를 요청하지만 공격자에 의해 위조된 웹 서버로 접속하게 된다.<Figure 4-4> 사용자의 시스템은 돌려받은 질의에 대한 결과를 DNS 테이블에 저장하기 때문에 테이블 삭제 전까지 해당 웹 서버에 대해서는 질의를 보내지 않는다.[2]

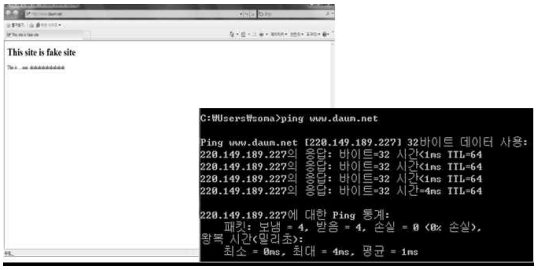

Figure 4-4. 위조된 웹 접속과 ping을 통한 확인

5.3 방지대책

5.3.1 정적 ARP table 운용

DNS 스푸핑을 방지하는 방법으로 가장 쉬운 방법은 ARP Table을 정적으로 관리하는 방법이다.

개인 시스템의 각 사용자가 arp -s 명령을 통해 정적으로 관리한다.

```
C:₩>arp -s 192.168.0.10  00-00-00-00-00-01
```

또한 네트워크 관리자가 게이트웨이에서, 스위칭 장비에서 각 포트별로 정적으로 table을 관리하고, 서버에서도 정적 ARP cache 운용으로 방지 할 수 있다.[1]

5.3.2 S-ARP(Secure ARP) 운용

DNS 스푸핑의 기본 단계인 ARP 스푸핑은 ARP가 인증을 통한 사용자 확인 없이 패킷을 주고받는 것을 이용한 공격 이다. S-ARP는 인증된 한 쌍의 키를 사용한다. 각 Host들은 LAN상에서 지정된 CA(Ceeitifcation Authoriry)와 같이 동작하는 local trusted party에 의해 증명된 공개키/비밀 키 쌍을 가지고 있으며 이를 통해 전달 되어온 ARP 패킷이 정당한 권리자의 것인지를 확인한다.

이를 위해서 추가적인 Header가 필요로 하고, 별도의 키 관리 DataBase를 필요로 한다. 또한 S-ARP를 채택한 Host는 기존 ARP를 처리할 수 없다는 한계가 있다.[1]

5.3.3 Shared Vlan 사용

동일 broadcast domain network에서는 broadcast-traffic이 동일 subnet에 속한 모든 사용자에게 전달된다.

따라서 공격자는 하나의 시스템만 공격하면 동일 subnet의 다른 시스템을 공격하기는 쉽다. 따라서 broadcast domain을 나눠서 관리하면 공격에 의한 피해 시스템을 줄일 수 있는데 물리적으로 domain을 나누기 위해서는 더 많은 I2 switch가 필요로 하게 된다.

하지만 switch의 소프트웨어는 논리적으로 domain을 나눌 수 있는 Shared Vlan 기능이 있다. 이 기능은 물리적으로는 같은 broadcast domain을 논리적으로 분할하여 broadcast traffic에 의한 해킹을 방지할 수 있다.[1]

6. 결론 및 향후 연구방향

사용자 입장에서 공격에 대한 탐지는 사실상 어렵고, 현재 웹에서는 ARP/DNS 두 프로토콜을 표준으로 사용하기 때문에 근본적 해결을 하는 방법은 쉽지 않다. 향후, Secure-ARP의 인증 시 별도의 Database가 필요한 문제와 기존 ARP와 호환문제를 해결하는 새로운 프로토콜을 디자인이 필요할 것으로 생각된다.

참 고 문 헌

[1] Other ryuseungwoo, hacker4u hacking security notes, cyber Publishers, 2003
[2] Chris Sanders, one practical packet analysis using Wireshark
[3] Other two major one, and practice Introduction to Information Security, O'Reilly Media, 2003
[4] Korea Internet & Security Agency (KISA)
[5] http://blog.naver.com/sunksw?RedIrect=Log&logNo=144042283597

홍 성 혁 (Sunghyuck Hong)

▪ 1995년 2월 : 명지대학교 컴퓨터 공학과 (공학사)
▪ 2007년 8월 : Texas Tech University, Computer Science (공학박사)
▪ 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
▪ E-Mail : shong@bu.ac.kr
<관심분야> : 네트워크 보안, 해킹, 센서네트워크 보안