Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.449

VLAN을 이용한 네트워크 분할 환경에서의 네트워크 접근 제어 우회 공격 탐지 및 방어 기법

김 광 준,[1†] 황 규 호,[2] 김 인 경,[2] 오 형 근,[2] 이 만 희[1‡]
[1]한남대학교, [2]국가보안기술연구소

Detection and Prevention of Bypassing Attack on VLAN-Based Network Segmentation Environment

Kwang-jun Kim,[1†] Kyu-ho Hwang,[2] In-kyoung Kim,[2]
Hyung-geun Oh,[2] Man-hee Lee[1‡]
[1]Hannam University, [2]National Security Research Institute

요 약

불필요한 트래픽의 송수신을 통한 분리된 조직/부서 간의 내부 자료 유출을 방지하기 위해 많은 조직에서 네트워크를 분할하여 망을 관리한다. 물리적으로 별도의 장비를 기반으로 하는 것이 가장 근본적인 네트워크 분할 방식이나 이보다 적은 비용으로 구축이 가능한 가상랜(Virtual LAN, VLAN) 네트워크 접근 제어 기능을 활용하여 논리적으로 네트워크를 분할·운영하는 사례가 존재한다. 본 연구에서는 VLAN ID값을 검색하는 스캐닝 기법과 Double Encapsulation VLAN Hopping 공격기법을 활용해 VLAN을 이용하여 분할된 네트워크 간 통신 우회 가능성을 제시한 후, 스캐닝을 통해 획득한 VLAN ID 정보를 이용한 자료 유출 시나리오를 제시한다. 또한 이 공격을 탐지 및 차단하기 위한 기법을 제안하고 구현을 통해 제시된 기법의 효과에 대해 검증한다. 본 연구는 궁극적으로 VLAN으로 분리된 네트워크 취약점을 활용한 자료 유출 또는 외부 사이버 공격을 차단함으로써 VLAN 이용 환경의 보안성 향상에 기여할 것으로 기대한다.

ABSTRACT

Many organizations divide the network to manage the network in order to prevent the leakage of internal data between separate organizations / departments by sending and receiving unnecessary traffic. The most fundamental network separation method is based on physically separate equipment. However, there is a case where a network is divided and operated logically by utilizing a virtual LAN (VLAN) network access control function that can be constructed at a lower cost. In this study, we first examined the possibility of bypassing the logical network separation through VLAN ID scanning and double encapsulation VLAN hopping attack. Then, we showed and implemented a data leak scenario by utilizing the acquired VLAN ID. Furthermore, we proposed a simple and effective technique to detect and prevent the double encapsulation VLAN hopping attack, which is also implemented for validation. We hope that this study improves security of organizations that use the VLAN-based logical network separation by preventing internal data leakage or external cyber attack exploiting double encapsulation VLAN vulnerability.

Keywords: Virtual LAN, double encapsulation VLAN attack, Virtual Network, Network separation, Data leakage

Received(11. 15. 2017), Modified(03. 12. 2018), Accepted(03. 15. 2018)

† 주저자, kimkwangjun.kr@gmail.com
‡ 교신저자, manheelee@hnu.kr(Corresponding author)

I. 서 론

2016년 5월 발생한 인터파크 개인정보 유출 사고로 인하여 네트워크 분할의 중요성이 다시 한 번 수면위로 부각되었다. 인터파크 침해사고 관련 조사 결과에 따르면 외부망이 연결된 직원 PC에 악성코드를 최초 감염 시킨 후, 파일공유서버를 통해 내부망의 다른 PC들로 감염을 확산하였다[1]. 언론사에 따르면 인터파크는 내·외부 네트워크를 분할하였으나 데이터베이스 관리자 등 일부 직원을 제외한 대다수의 직원들은 PC 1대로 내·외부망을 자유롭게 사용 가능한 것으로 확인되었다[2].

인터파크의 침해사고 사례처럼 분할되어야 할 네트워크 사이에 부주의 또는 취약점에 의해 접점이 존재하는 경우 내부 정보의 유출, 취약한 네트워크를 통한 공격 등의 보안사고가 일어날 수 있다. 이를 예방하기 위해서는 물리적으로 별도의 네트워크 장비를 통해 분리된 망을 구축하는 것이 가장 근본적인 대처 방안이라 할 수 있다.

하지만, 조직 내 소규모의 내부 조직/부서 또는 데이터 유형 별 상호 격리를 목적으로 별도의 장비를 구비하여 별도의 망을 구축하는 것은 매우 비효율적인 방식이다. 이와 같은 경우에 가상랜(Virtual Local Area Network, VLAN) 기술을 이용하여 망을 분할 구축하는 경우가 존재한다. VLAN은 단일 2계층 네트워크를 분할하여 여러 개의 브로드캐스트 도메인을 생성하는 기술로써, 이 기술을 사용하면 추가 장비 구입 없이 기존 스위치의 환경 설정 변경만으로도 기대하는 효과를 얻을 수 있으므로 네트워크 장비 분리의 비용을 줄일 수 있어 경제적인 네트워크 분할 기법으로 활용되고 있다.

하지만 다수의 스위치 장비에서 사용 중인 국제표준 IEEE 802.1Q VLAN은 기능상 취약점으로 인해 스위치의 특정 환경에서 네트워크 패킷이 도달해서는 안 되는 서로 다른 VLAN 영역 간에 네트워크 패킷 도달 공격이 가능하다[3][4]. 이 공격은 보안상 매우 중요한 의미를 가진다. VLAN을 통해 논리적으로 분할된 네트워크에서 서로 다른 VLAN 영역 간에 패킷이 도달할 수 있다는 것은 해당 조건을 만족하는 경우 자료 유출 또는 외부로부터의 공격도 가능하다는 것을 의미하기 때문이다. 현재까지 각 스위치 제조사들은 이 취약점이 VLAN ID 번호의 초기 값과 관련된 내용이므로 이 초기 값을 임의의 값으로 설정하는 것을 권고하는 것으로 임시 해결책을 제시하고 있다[5][6].

본 연구에서는 스위치에 설정되어 있는 VLAN ID값을 검색하는 VLAN ID Scanning 기법을 통해 스위치 제조사들이 제시하고 있는 임시 해결책이 짧은 시간 내에 우회가 가능함을 보인다. 이와 더불어, 해당 공격기법의 파급효과를 보이기 위해 VLAN 기반의 논리적 네트워크 분할을 우회하여 내부 자료의 외부 유출 가능성 시나리오를 제시하고 구현하였다. 마지막으로 이러한 VLAN기반 네트워크 접근 제어 우회 공격의 탐지 및 차단 기법을 제안한다.

본 논문은 다음과 같이 구성된다. 먼저 2장에서는 VLAN에 대한 관련 연구를 기술하고, 3장에서는 VLAN ID값을 검색하는 VLAN Scanning 기법을 통한 네트워크 접근 제어 우회 가능성을 제시한다. 그 후 획득한 ID값을 Double Encapsulation에 이용하여 자료 유출 가능성 시나리오를 제시한다. 4장에서는 실시간 패킷 모니터링을 통해 우회 기법을 탐지 및 방어하는 기법에 대하여 제시 및 검증한다. 그리고 5장에서는 결론에 대해 기술한다.

II. 관련 연구

2.1 VLAN

VLAN은 스위치의 물리적인 네트워크를 논리적으로 분할하여 복수개의 브로드캐스트 도메인으로 운영하는 기술이다. 스위치는 논리적으로 나눈 동일한 그룹 내에 있는 단말기에 패킷을 전달하기 위하여 Fig.1과 같이 기존 의 프레임 구조에 802.1Q Tag를 부착한다. 이 중 스위치는 12bit에 해당되는 VID 필드에서 예비 값으로 사용되는 0과, 4095번의 ID를 제외한 4094개의 VLAN ID값을 할당하여 사용하게 된다[7][8].

VLAN 태그는 스위치에 저장되는 정보이므로 PC는 자신이 속한 VLAN 정보를 알지 못한다. 따라서 PC는 일반적인 이더넷 프레임을 전송하게 되고, 이때 스위치는 프레임이 유입된 포트에 설정되어

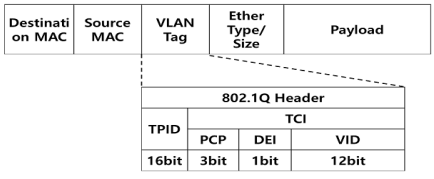


Fig. 1. VLAN frame structure

있는 VLAN 태그 정보를 프레임에 삽입한 후 목적지로 스위칭 한다. 전송된 프레임이 목적지 PC가 연결된 스위치에 도착하면 해당 스위치는 프레임에 삽입되어 있는 VLAN 태그 정보와 목적지 PC가 연결되어 있는 포트의 VLAN 정보를 비교한다. 두 VLAN ID가 일치하면 스위치는 프레임에 부착되어 있는 VLAN 정보를 제거하고 일반 프레임을 PC에 전달한다. 왜냐하면, PC는 VLAN 정보를 이해할 수 없기 때문이다. VLAN 정보가 일치하지 않는다면 해당 포트로 프레임을 전달하지 않고 프레임을 폐기한다.

이 기본 기능을 이용해서 네트워크 접근 제어를 구현하는 방법은 다음과 같다. 제어하고자 하는 PC들을 두 개의 그룹으로 나눈 후 각 그룹에 서로 다른 VLAN ID를 할당한다. 각 PC가 연결된 스위치에 VLAN 기능을 활성화한 후 해당 PC가 연결된 포트의 VLAN ID를 해당 그룹의 VLAN ID로 설정한다. ARP 브로드캐스팅은 하나의 VLAN 내에서 동작하므로 다른 VLAN에 속한 시스템과의 통신은 라우터 또는 L3 스위치를 통해서만 가능하다. 라우터와 L3 스위치에 라우팅이 되지 않도록 라우팅 테이블 또는 IP 스위칭 기능을 설정하면 두 VLAN 간은 서로 통신이 되지 않는다. 설사 분리된 VLAN에 속한 PC의 MAC 주소를 알아 목적지 MAC 주소로 설정한 프레임을 생성하여 네트워크로 주입하더라도 최종적으로 VLAN 번호가 다르므로 목적지 스위치에서 해당 프레임은 폐기된다. 또한 목적지 PC의 VLAN ID를 예측하여 임의의 VLAN 추가한 프레임을 생성하여 네트워크로 주입하면 송신 PC에 연결된 스위치가 프레임의 형식 오류로 판단하여 프레임을 폐기한다. 이로써 일반적인 상황에서 VLAN을 이용한 네트워크 접근 제어 서비스가 제공된다.

2.2 Native VLAN

VLAN기반 네트워크 접근 제어를 우회할 수 있는 환경은 Native VLAN(또는 untagged VLAN)을 활용하는 경우이다. Native VLAN은 VLAN 태그를 붙이는 않는 통신으로써 허브로 구성된 레거시 네트워크와 VLAN을 사용하는 네트워크와의 원활한 통신 및 물리적으로 네트워크를 구분하는 라우터와 통신을 해야 하는 WAN 구간 통신, 낮은 딜레이가 매우 중요한 실시간 통화를 위한 IP폰 통신 등에 사용된다[9].

허브는 VLAN을 구분할 수 있는 기능이 없다. 만약 VLAN 태그가 붙은 프레임을 수신한 허브는 해당 프레임을 모든 포트에 그대로 브로드캐스트로 전달하게 되고 해당 프레임을 수신한 PC는 VLAN 태그가 붙은 프레임을 형식 오류로 인해 정상적으로 인식하지 못한다. 반대로 허브에 연결된 PC에서 송신한 프레임은 VLAN 태깅이 되어 있지 않고, 허브 또한 VLAN 태깅 기능을 제공하지 않기 때문에 non-Natvie VLAN(또는 tagged VLAN) 내에서 적절한 프레임 처리가 불가능하다.

Native VLAN이 이를 해결하는 방법은 VLAN 태그가 부착되지 않은 프레임을 수신한 스위치는 해당 프레임을 Native VLAN에 속한 VLAN 그룹으로 인정하고 스위칭을 진행한다. Fig.2의 PC C에서 PC A로 전송하는 프레임의 경우, 허브는 VLAN 태그를 붙이지 않고 스위치 A로 전송하고 스위치 A는 PC A가 Native VLAN에 속해져 있으므로 정상적으로 프레임을 전송한다. PC D에서 PC A로의 전송도 같은 방법으로 진행된다. PC B와 PC E 사이의 통신은 일반 VLAN 이므로 이 프레임을 받은 스위치는 해당 VLAN 태그인 V2를 붙여서 전송한다. 이때 Native VLAN에 속한 포트를 나타내기 위해 Native VLAN도 ID가 할당되며, 일반적으로 1번을 사용한다. 따라서 스위치 A의 포트 1번, 스위치 B의 포트 1번은 VLAN ID 1번이 할당된다[10].

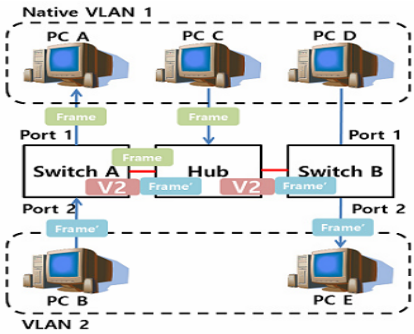


Fig. 2. Native VLAN configuration diagram

2.3 Double Encapsulation VLAN Hopping Attack

일반적인 경우, 라우터나 L3스위치와 같은 네트워크 3계층 장비를 통하지 않으면 논리적으로 분할된 서로 다른 VLAN간의 통신은 불가능하다. 하지

만 Native VLAN에 연결된 시스템(예, Fig.2의 PC A)은 다른 VLAN에 연결된 시스템(예, Fig.2의 PC E)으로 프레임 전송이 가능하며 이를 Double Encapsulation VLAN Hopping 공격이라고 한다[3][4].

공격 원리는 다음과 같다. Native VLAN에 연결된 시스템(Fig.2의 PC A)에 침입한 공격자는 일반 프레임(Fig.3.a)에 VLAN 태그 2개를 삽입하여(Fig.3.b) 스위치로 전송한다. 이때 첫 번째 태그는 자신의 속한 Native VLAN ID 정보를, 두 번째 태그는 목적지 PC가 속한 다른 VLAN ID 정보를 사용한다. 이 프레임을 받은 스위치 A는 VLAN 태그가 붙어 있는 것을 발견한다. 일반 PC에서 태그가 붙어오는 것은 일반적이지 않지만 해당 VLAN ID와 동일하면 정상 프레임으로 인정하고 스위칭을 해준다. 일반 VLAN의 경우는 해당 VLAN 태그를 그대로 붙여서 스위칭을 해주지만, Native VLAN인 경우 태그가 없이 스위칭이 되어야하므로 Native VLAN ID 정보를 가진 태그를 제거한 후 프레임을 계속 스위칭하게 된다. 결국 남은 프레임은 목적지 VLAN 태그를 가진 프레임이 된다. 이를 수신한 스위치 B는 정상 VLAN ID = 2를 가진 같은 VLAN 내 통신으로 판단하고 PC E로 프레임을 전송한다.

결국, 패킷이 변조되어 프레임이 2중으로 태깅됨에도 불구하고, 스위치에서는 해당 프레임에 대한 검증절차 없이 첫 번째 프레임을 한 번만 해석한다는 기능적인 취약점을 이용하여 다른 VLAN으로의 통신을 가능케 하였다.

본 공격에 대한 프로토콜상의 완전한 방지법은 없으나 본 공격이 실제적이지 않도록 하기 위해 스위치 제조사들은 Native VLAN의 ID를 기본 값인 1번을 사용하지 않고 임의의 값을 사용하도록 권고하고 있다[5][6]. Native VLAN에 속한 PC 한 대만 점유한 공격자의 경우, 임의의 값으로 바뀐 Native VLAN ID도 예측하기 어렵고, 다른 VLAN에 속한

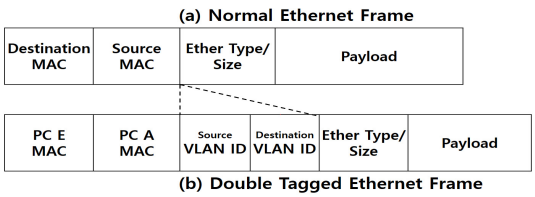


Fig. 3. 802.1Q Tag Double Insertion

시스템의 MAC 주소와 VLAN ID 또한 알 수 없기 때문에 이중 태그를 만드는 것은 거의 불가능함으로 실질적인 공격이 어렵다. 따라서 일반적인 경우 Native VLAN ID를 임의의 값으로 변경하는 것만으로도 효과적인 공격 방지가 된다고 할 수 있다.

III. VLAN Scanning 공격 기법

3.1 위협 모델

VLAN을 이용한 네트워크 분할 환경의 경우, 일반적으로 서로 다른 업무를 진행하는 부서를 분리하거나 서로 다른 목적으로 사용되는 네트워크 사이의 데이터를 분리하는 용도로 쓰인다. 그렇기 때문에 대부분의 일반 사용자는 분할된 네트워크의 한쪽에 접속되어있다. 그러나 여러 부서를 관리하는 상위 관리자 혹은 부서 내부에서 특수한 목적으로 네트워크를 분할하여 사용하는 경우 각각의 분할된 네트워크에 접속된 PC를 가진 사용자는 충분히 존재할 수 있다.

본 연구가 고려한 위협 모델은 이와 같이 분할된 네트워크 환경에서 각각 네트워크에 접속할 수 있는 PC를 소유한 사용자가 악의적인 의도를 가지고 타 부서에서 접근할 수 없는 내부 자료를 타 부서로 유출하고자 하는 상황을 고려한다. 사용자는 두 PC에 대해 프로그램 설치가 가능하고 MAC 주소 확인 등의 작업을 수행할 수 있어야 한다. 설명을 위해 유출하고자 하는 자료가 있는 네트워크를 Native VLAN으로 구성하고 내부 자료에 원칙적으로 접근이 불가능한 타 부서의 네트워크는 일반 VLAN으로 구성하여 내부 자료 유출을 목표로 한다. 이와 반대로 일반 VLAN으로 구성된 네트워크의 자료를 Native VLAN으로 구성된 네트워크로 유출하는 것은 제안된 공격 기법의 특성상 불가능 하지만 추후 다른 취약성 분석 연구 등을 통해 지속적으로 연구해 보고자 한다.

또한, 네트워크 관리자는 네트워크 보안 권고에 따라 Native VLAN ID를 임의의 값으로 바꾸었다고 가정한다. 모든 VLAN ID는 네트워크 관리자만 알고 있고 사용자는 VLAN ID에 대한 아무런 사전 지식이 없다. 결국 본 연구는 유출하고자 있는 자료가 있는 부서망(이하, 유출소스망) PC와 자료 유출의 대상이 되는 타 부서망(이하, 유출대상망)에 연결된 PC가 Native VLAN 또는 일반 VLAN에 속해 있는지 전혀 모르는 사용자가 Native VLAN에

PC로부터 일반 VLAN에 속해 n있는 PC로 자료 유출이 효과적인 시간 내에 가능하다는 것을 보인다.

Fig.4는 본 실험을 위한 네트워크 환경을 설명한다. 유출소스망의 VLAN은 Native VLAN으로 구성하고 임의의 값인 ID=10을 설정하였고, 유출대상망의 VLAN은 ID=20으로 설정하였다. Native VLAN에 속한 내부 PC 또는 서버팜과의 통신은 VLAN 태그가 없는 프레임이 사용되고, 유출대상망에 접속된 시스템들 간의 통신은 VLAN ID=20 태그를 사용한다.

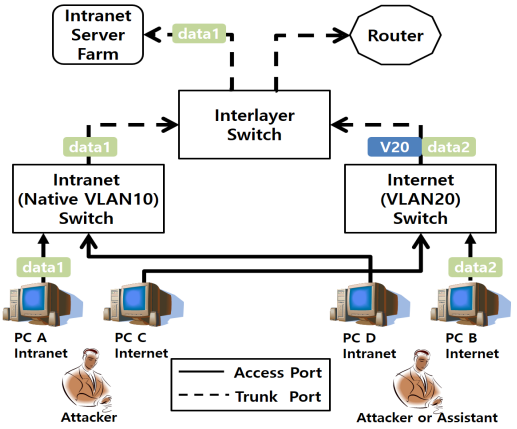


Fig. 4. Network diagram for attack scenarios

3.2 VLAN Scanning 기법

Double Encapsulation VLAN Hopping 공격을 위해 유출소스망 PC가 속한 Native VLAN ID와 유출대상망 PC가 속한 VLAN ID 정보가 필요하다. 이를 위해 본 절에서는 UDP 프로토콜을 이용한 Brute Force 방법을 사용하여 두 ID를 찾는 방법을 제안한다.

스캐닝 환경 구성은 다음과 같다. 유출대상망 PC에 특정 UDP 포트를 열고 패킷을 기다리는 서버 프로그램을 설치하고 실행한다. 이 프로그램은 수신한 UDP 패킷에 저장된 텍스트 자료를 화면에 띄우는 기능을 수행한다. 유출소스망 PC에는 UDP 패킷을 이용해 VLAN ID를 스캐닝하는 클라이언트를 설치하고, 그 동작 알고리즘은 Fig.5와 같다.

Block_Scanning함수는 유출대상망 PC에 Brute Force식 스캐닝을 실행한다. 이때, VLAN ID 길이는 12bit로써 예비값인 0과 4095를 제외한 1~4094까지의 ID를 이용해 스캐닝한다.

UDP 패킷에 탑재하는 데이터 필드에는 삽입된 VLAN ID 값을 추가적으로 저장한다. 그 이유는 스캐닝 패킷이 유출대상망 PC에 전송되기 직전에 스위치에 의해 802.1Q 태그가 제거되기 때문이다. 따라서 유출대상망 PC와 유출소스망 PC의 VLAN ID를 전달하기 위해 두 VLAN ID를 데이터 필드에 저장하는 것이다(Fig.6의 유출대상망 PC 결과).

한편, 본 기법에서 UDP 패킷을 사용하는 이유는 TCP 패킷을 사용할 수 없기 때문이다. 3-way handshake를 이용하여 유출소스망 PC에서 유출대상망 PC로 TCP 세션을 맺기 위한 SYN 패킷을 보내었을 때, 그 응답 값으로 ACK 패킷이 도착하면 그때 사용된 VLAN ID를 찾을 수 있다고 생각할 수 있다. 하지만 이 시나리오는 작동될 수 없다. 왜냐하면 유출소스망 PC에서 보낸 SYN 패킷은 double encapsulation을 통해 Native VLAN 스위치와 목적지 VLAN 스위치를 통과해서 도착할 수는 있으나, 이 패킷을 받은 유출대상망 PC가 일반 ACK 패킷을 응답하더라도 이를 받은 유출대상망 스위치는 ACK 패킷에 유출대상망 VLAN ID를 삽입하므로 Native VLAN 에 속한 유출소스망 PC로 패킷이 도착하지 않는다. 이로 인해 유출대상망 PC에 도착하는 패킷을 수신하고 출력하는 서버를 구동하였고, 세션 성립과정 없이 패킷 하나에 필요한 정보를 빠르게 보낼 수 있는 UDP를 사용하였다.

또한 Block_Scanning함수에 사용하는 start,

```
Block_Scanning(start, end, MAC)
  For i := start to i := end do
    For j := 1 to j := 4094 do
      PacketSending(Native VLAN i,
                    Destination VLAN j, MAC)
```

Fig. 5. VLAN Scanning Results

```
Intranet PC, VLAN10_PC
C:₩VLAN10_PC>python VLAN_Scanning.py
dst_mac : 00:E0:4C:37:91:A4
Scanning Start : 1 1025
Scanning Start : 1025 2049
Scanning Start : 2049 3073
Scanning Start : 3073 4097
Scanning Complete : 3073 4097
Scanning Complete : 1025 2049
Scanning Complete : 2049 3073
Scanning Complete : 1 1025
Running Time : 13466.14

Internet PC, VLAN20_PC
C:₩VLAN20_PC>python VLAN_Scanning_Receiver.py
NativeVLAN:10 yourVLAN:20
```

Fig. 6. VLAN Scanning Results

end 값을 적절히 나누어 실행하면 성능 향상을 기대할 수 있다. 본 실험에 사용한 프로그램은 4개의 프로세스에 나누어 실행시켰고 그 결과는 Fig.6과 같다. 싱글 프로세서에서 수행시 약 10시간 정도 수행되므로 프로세서 개수만큼의 성능향상을 얻을 수 있었다. 본 실험이 사용한 시스템은 i5-3470 CPU, 메모리 4GByte, 네트워크 카드 Intel 82579LM 이었으며 일반적인 개인용 PC 사양이라고 할 수 있다. 즉, 일반 PC로 평균 두 시간 만에 double encapsulation 공격에 필수 정보인 두 VLAN ID를 추출할 수 있으므로, 발생 가능한 위협에 비해 비교적 쉽게 공격을 수행할 수 있다고 볼 수 있다.

3.3 자료유출 기법

스캐닝 작업을 통해 알아낸 VLAN ID 정보를 바탕으로 2차 추가적인 공격을 진행한다면 내부 자료 유출 및 외부 침해 사고 등의 원인이 될 수 있다. 두 VLAN ID를 알아낸 공격자는 유출소스망 PC에는 자료유출 클라이언트를 구동하고, 유출대상망의 PC에는 자료수신 서버를 구동한다. 앞서 설명한 대로 서버에서 클라이언트로의 통신은 불가하므로 전송한 파일의 무결성 검증과 안정적인 송·수신을 위해 서버·클라이언트는 Fig.7과 같은 흐름으로 수행한다.

서버는 자료 수신 모듈을 구동하여 지정한 포트를 개방하고 데이터 수신을 기다린다. 클라이언트 모듈로부터 파일명과 파일 사이즈, 그 파일의 해시 값을 전송받게 되면 서버는 전송 받은 파일명으로 파일을 생성하고 파일을 수신한다. 끝으로 데이터 송신의 끝을 의미하는 Flag를 받게 되면 초기에 전송받은 해시 값과 수신한 파일의 해시 값을 비교함으로써 파일의

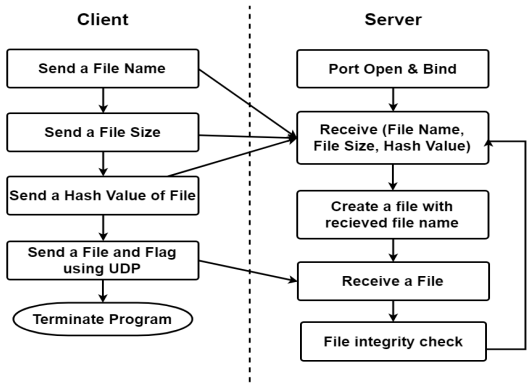


Fig. 7. Server · Client operation flow chart

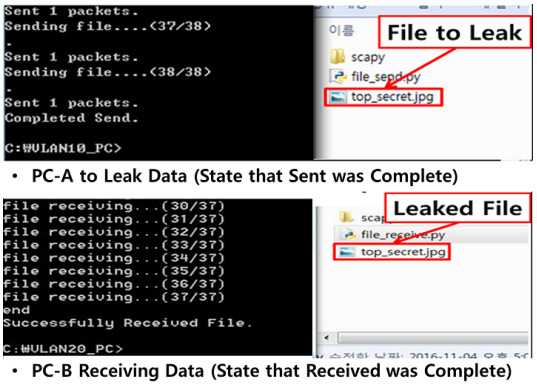


Fig. 8. Successful reception of leaked data

무결성 검사를 진행한다. 무결성 검사 실패시 생성한 파일을 삭제하고 성공시 파일을 유지한다(Fig.8).

IV. Double Encapsulation VLAN Hopping 공격 탐지 기법

본 절에서는 VLAN ID 스캐닝 및 Double Encapsulation VLAN Hopping 공격을 탐지하는 방법을 제시한다. 공격 패킷의 핵심적 특징은 이더넷 프레임에 VLAN 태그가 두 개 삽입된 것이다. 공격 탐지는 포트 미러링을 사용한 실시간 Traffic Monitoring 방법과 pcap 파일에 저장된 패킷을 사용하는 오프라인 Analysis 방법이 있다. Fig.9는 오프라인 Analysis의 흐름도이다. pcap 파일에서 패킷을 하나씩 읽은 뒤 VLAN ID 두개가 삽입된 프레임을 검출하는 알고리즘을 수행하고, 이중 태깅이 검출되면 프레임을 전송한 인터페이스를 차단하도록 스위치에 명령을 내린다.

Fig.10은 자료유출 공격 시도를 탐지한 결과이다. 이중 태깅된 프레임을 탐지하면 해당 패킷의 출발지 IP, 목적지 IP, VLAN 태그 및 MAC을 출력함으로써 공격자 PC를 쉽게 찾을 수 있다. 이중 태깅된 프레임의 탐지는 자료 유출 혹은 악성코드 유입 공격이 진행되고 있음을 의미하므로 이중 태깅 프레임을 생성하는 포트를 즉시 차단하는 것이 바람직하다.

Fig.11은 본 연구에서 개발한 시스코 스위치 대상 Switch Management Control 모듈의 소스코드 일부이다. 시리얼 통신을 통해 스위치의 콘솔모드로 접속한 후 공격이 탐지된 인터페이스를 shutdown 함으로써 이더넷 포트 차단 기능을 수행한다. 실제 스위치 명령모드에서 특정 인터페이스에

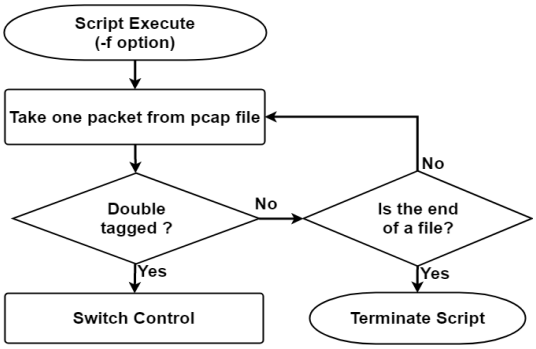


Fig. 9. Detection and Defense Module Flowchart

```
root@kali:/VLAN_module# python VLANtagMonitoring.py -m
OutPutFileName is [ 2016-12-12.txt ]
[Start] Monitoring Mode
Run to VLAN Double Encapsulation Attack Check Module.
VLAN Double Encapsulation Attack Non-detection !
VLAN Double Encapsulation Attack Detection !
 Source IP      Destination IP      Packet Frame Structure          Source MAC
10.10.10.10 -> 255.255.255.255  ethernet frame, V10, V20, payload  24:f5:aa:dd:ba:64
10.10.10.10 -> 255.255.255.255  ethernet frame, V10, V20, payload  24:f5:aa:dd:ba:64
10.10.10.10 -> 255.255.255.255  ethernet frame, V10, V20, payload  24:f5:aa:dd:ba:64
                    [24F5.AADD.BA64] interface disable Success.
```

Fig. 10. Double Encapsulation detection results

접근한 후 shutdown 명령어를 수행하는 것과 동일한 기능을 하며, 수행 결과 인터페이스의 Status가 connected에서 disabled로 변경된다. 본 탐지기법을 위해서 각 스위치는 포트미러링 기능을 활성화해야 하고 이 트래픽을 수신하여 분석하는 시스템을 도입해야 한다. 포트미러링 자체는 스위치의 사용에 크게 영향을 미치지 않는 것으로 알려져 있고, 분석시스템은 모든 트래픽을 저장하지 않고 더블 태그가 발견된 패킷 일부만 저장하므로 시스템의 리소스 부담을 줄일 수 있다.

V. 결 론

본 논문은 VLAN을 이용한 논리적 네트워크 분할 환경에서 Double Encapsulation VLAN Hopping 기법으로 네트워크 접근 제어를 우회하여 자료 유출 또는 악성코드 유입 공격 위험성을 증명하였다. 또한 해당 취약점을 이용한 공격의 탐지 및 방어 기법을 제안하였다. 본 연구 결과는 VLAN을 이용하여 논리적 네트워크 분할을 구축했거나 추진 중인 조직에서 반드시 확인해야 할 사안으로써 그 중요성이 있다고 할 수 있다.

```
# state : interface settins, execute "no shutdown"
if 'console(config-if-Gi1/0/' in input_data:
    console.write("shutdown \r\n")
    time.sleep(1)
    input_data = console.read(console.inWaiting())
    console.write("end\r\nend\r\n")
```

Fig. 11. Source code fragment of Switch Management Control

향후 연구방향으로는 본 연구의 VLAN 스캐닝 공격의 제한점인 서로 다른 VLAN에 위치한 두 PC에 모두 접근 가능해야 한다는 조건 없이 하나의 PC를 이용한 스캐닝 공격의 가능성을 검토할 예정이다.

References

[1] Hong-soon Shin and Sun-cheol Hwang, "Result of the survey about an intrusion on personal information in Interpark," Ministry of Science, ICT, Future Planning and Korea Communications Commission, pp. 1-3, Aug. 2016.

[2] Dong-cheol Kang, "Interpark leaked customer information… 'Internet network separation' was insufficient," Chosunbiz, pp. 1, July. 2016.

[3] Steve A. Rouiller, "Virtual LAN Security weaknesses and countermeasures,", SANS Institute, pp. 8-9, Dec. 2006.

[4] Yusuf Bhaiji, "Layer 2 Attacks & Mitigation Techniques," Cisco Systems, pp. 21-26, Aug. 2006.

[5] Hyun-Jin Oh and Jae-Oh Moon, "Analysis and Prevention of network attacks that target weakness in Data link layer," University of Dongseo, pp. 12, Dec. 2011.

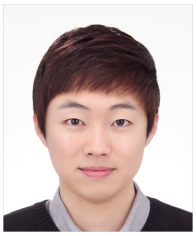
[6] Yusuf Bhaiji, "Understanding, Preventing, and Defending Against Layer 2 Attacks," Cisco Systems, pp. 15, 2009.

[7] CISCO, "Inter-Switch Link and IEEE 802.1Q Frame Format," Document ID 17056, pp. 5-6, Aug. 2006.

[8] IEEE Computer Society, "IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks," ISBN 978-0-7381-4877-9, pp. 74-78, May. 2006.

[9] Google, "VLAN's," https://sites.google.com/site/nikiccnawiki/swithes/vlans
[10] Isiaka A. Alimi and Akeem O. Mufutau, "Enhancement of Network Performance of an Enterprises Network with VLAN," American Journal of Mobile Systems, Applications and Services, vol. 1, no. 2, pp. 82-93, July. 2015.

〈저자소개〉



김 광 준 (Kwang-Jun Kim) 학생회원
2017년 2월: 한남대학교 컴퓨터공학과 학사
2017년 3월~현재: 한남대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 침입 탐지, 네트워크/시스템 보안

황 규 호 (Kyu-ho Hwang) 정회원
2006년 8월: 연세대학교 전기전자공학과 학사
2008년 8월: 연세대학교 전기전자공학과 석사
2013년 8월: 연세대학교 전기전자공학과 박사
2013년 12월~현재: 국가보안기술연구소 재직
〈관심분야〉 네트워크장비 보안, 소프트웨어 정의 네트워크(SDN), 네트워크 기능 가상화(NFV)

김 인 경 (In-kyoung Kim) 정회원
2010년 2월: 한양대학교 컴퓨터공학과 학사
2012년 2월: 한양대학교 전자통신컴퓨터공학과 석사
2011년 12월~현재: 국가보안기술연구소 재직
〈관심분야〉 소프트웨어 역공학, 네트워크/시스템 보안, 소프트웨어 평가 및 검증

오 형 근 (Hyung-geun Oh) 종신회원
2000년 2월: 한국사이버페이먼트(KCP) 선임연구원
2006년 12월: 미국 퍼듀대학교 방문연구원
2013년 2월: 고려대학교 정보보호학과 박사
2000년 8월~현재: 국가보안기술연구소 재직
〈관심분야〉 악성코드 및 취약점 분석, IoT 보안, 보안적합성 검증

이 만 희 (Man-hee Lee) 종신회원
1995년 2월: 경북대학교 컴퓨터공학과 공학사
1997년 2월: 경북대학교 공학석사
2008년 8월: Texas A&M 대학교 컴퓨터공학과 공학박사
1997년~2003년: 한국과학기술정보연구원 연구원
2008년~2009년: Cisco Systems, San Jose
2010년~2012년: 국가보안기술연구소 선임연구원
2012년~현재: 한남대학교 부교수
〈관심분야〉 네트워크/시스템/스마트폰 보안, 고성능 시스템, 컴퓨터교육