논문 16-41-09-15 The Journal of Korean Institute of Communications and Information Sciences '16-09 Vol.41 No.09
http://dx.doi.org/10.7840/kics.2016.41.9.1103

격리 네트워크를 활용한 네트워크 방어 기법

정 용 범◆, 박 민 호°

Network Defense Mechanism Based on Isolated Networks

Yongbum Jung◆, Minho Park°

요 약

현재까지 내부 네트워크에 접근하는 단말의 무결성을 검증하기 위한 방안으로 네트워크 접근제어 시스템 NAC (Network Access Control), 백신, 망분리, MDM(Mobile Device Management) 등 다양한 방법들을 이용하여 내부 네트워크의 자산을 보호하고자 하였다. 그러나 기존의 접근제어 시스템에서 사용하는 정책은 획일화 되어 사용자에게 적용되고 있고, 또한 APT(Advance Persistent Threat) 대응 솔루션, 방화벽, 백신 등의 보안 솔루션은 단말이 내부 네트워크에 접근한 이후에 이상 트래픽 등이 발생 시 이를 감지하고 처리하는 형태이므로 근본적으로 무결성 검사를 수행한 이후에 내부 네트워크에 접근하는 등의 방안이 필요하다. 따라서 본 논문에서는 악성코드에 감염된 단말이 내부 네트워크에 접속하기 이전에 이를 검증하고 조치하는 방안에 대한 보안네트워크 설계를 제시하고자 한다.

Key Words : Network separation, Integrity Check, Network Access Control

ABSTRACT

Network assets have been protected from malware infection by checking the integrity of mobile devices through network access control systems, vaccines, or mobile device management. However, most of existing systems apply a uniform security policy to all users, and allow even infected mobile devices to log into the network inside for completion of the integrity checking, which makes it possible that the infected devices behave maliciously inside the network. Therefore, this paper proposes a network defense mechanism based on isolated networks. In the proposed mechanism, every mobile device go through the integrity check system implemented in an isolated network, and can get the network access only if it has been validated successfully.

Ⅰ. 서 론

내부 네트워크에 접근하는 단말을 제어하기 위한 기술은 태블릿, 스마트폰과 같은 다양한 단말에 대한 이용증가와 더불어 다양한 방법으로 연구되어 왔고, 이러한 접근제어에 관한 연구는 PC와 같은 단말뿐만이 아니라 단말에 설치된 프로그램의 검증을 통한 접근제어 기법[1] 등 다양한 시각으로 연구가 진행되고 있다.

그러나 사용자 인증 및 에이전트 기반의 접근제어 기술만으로 내부 자산을 지키는 것은 쉬운일이 아니며,[2] 이와 더불어 보안 위협과 악의적인 공격에 대비할 수 있는 보안 플랫폼의 개발이 필요하다.[3]

내부 네트워크에 접속하는 단말의 무결성을 검증하

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2016-H8501-16-1008).
◆ First Author : Soongsil University Department of IT Convergence, ybjung@ssu.ac.kr, 학생회원
° Corresponding Author : Soongsil University Department of IT Convergence, mhpark@ssu.ac.kr, 종신회원
논문번호 : KICS2016-04-079, Received April 30, 2016; Revised July 7, 2016; Accepted August 16, 2016;

기 위한 기존의 방안으로는 백신 프로그램, NAC (Network Access Control), 망분리, MDM (Mobile Device Management) 등의 방안이 존재하지만 대부분의 통제 기법들은 모두 내부 네트워크에 접속한 이 후에 에이전트 등의 설치를 통한 검사 및 제어 또는 사용자 단말에서 발생되는 트래픽을 통한 제어 등에 대한 기술만 제공이 되므로 이미 악성코드나 웜에 감염된 단말이 내부 네트워크에 접속하여 해당 에이전트 프로그램을 설치하기 이전까지의 위험성은 보장이 되지 않는다.

현재 대부분의 기업환경에서 내부네트워크의 보호를 위해 백신과 같은 보안 프로그램의 설치를 의무화하고, 설치가 되지 않은 사용자를 네트워크 접근제어 등의 다양한 방법으로 통제하고 있다. 네트워크 접근제어 방식의 경우 기본 접근제어 절차는 그림 1.과 같다.

그림 1.과 같이 미설치 사용자를 구분하여 통제하기 위해서는 신규 단말이 내부 네트워크에 접속한 이후에 이를 검사할 수 있는 에이전트를 설치하여 검사를 진행하며, 검사가 종료된 후 미설치 사용자를 통제할 때에도 통제 방식에 따라 통제가 되지 않는 단말들로 인한 내부 네트워크의 위험성이 존재하게 된다.

실제로 위반 노드를 차단하는 대부분의 시스템은 맥 포이즈닝 또는 하이재킹 등의 기법을 통해 단말의 차단을 수행하지만, 맥 포이즈닝을 통해 통제를 할 경우 Static ARP 사용자의 탐지 및 차단 지연발생, 하이재킹을 통해 통제를 할 경우 대부분 미러로 구성이 되기 때문에 미러링을 설정하는 스위치까지 트래픽이 올라오지 않는 경우 (로컬 통신) 이에 대한 감지 및 차단이 지연되는 특징을 가지고 있다. 즉, 에이전트가 내부네트워크에 새로운 단말의 출현을 감지하고 이를 검사/통제 과정에서 지연이 발생할 경우 해당 단말은 지연시간 동안 특별한 제약 없이 네트워크 사용이 가능해진다. 이러한 문제를 해결하기 위해서 본 논문에서는 내부 네트워크에 접속하는 단말의 무결성 검증을 보다 내부 네트워크가 아닌 격리 구역에의 검사를 통해 보다 안정적으로 진행할 수 있는 방안을 제시하고자 한다.

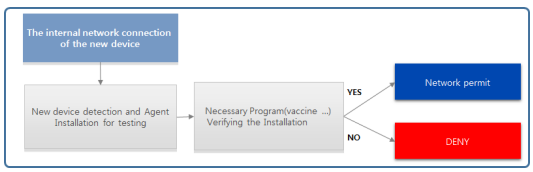

그림 1. 네트워크 접근제어 동작
Fig. 1. Network Access Control Mechanism

Ⅱ. 본 론

2.1 기존의 내부 네트워크 접근제어를 위한 방법

내부 네트워크를 보호하기 위한 기존의 방법으로는 NAC (Network Access Control), 백신, MDM (Mobile Device Management), 방화벽, IPS (Intrusion Prevention System) 등 다양한 방안들이 현재까지 사용되고 있다. 그러나 네트워크 기술과 단말의 다양화, 기업 비즈니스 환경의 확대 등으로 기존의 방식으로 네트워크의 보안을 유지하는 것에는 한계가 있다.[4] 내부 네트워크에 접근하는 단말의 검사와 네트워크 보호를 위해 표 1.과 같이 방화벽, NAC, MDM, 백신 등의 시스템이 현재 보편적으로 사용되

표 1. 기존 보안시스템의 역할 및 문제점
Table 1. The role and challenges of security systems

	Role	Issue
NAC	. verifying the installation of necessary security software . Pattern-based threats conduct inspections and perform policy-based inspection	. No control method until before the agent is installed . Policy control is possible, but is difficult to detect the malicious code
MDM	. authentication and control/management for mobile	. before to the app being installed no control method
Firewall	. internal ↔ external access control for traffic . Signature-based Detection and blocking	. Device does not perform for the Direct check, after over traffic information based generated by the device can be access control . Using Back-Connection, Many cases where malicious introduced In a form that is connected to a server outside in from the inside
vaccine	. Signature based Detection and Prevention	. Operation after the program is installed
Media Control	. control and block for the media	. Do not have a direct inspection of the device, perform autentication and media control

고 있으나 해당 시스템들은 표 1.에서 정의한 바와 같이 다양한 문제점들을 가지고 있다.

기존 보안 시스템의 접근제어 방식에 있어서, 공통적인 문제점으로는 무결성을 검증해야하는 단말이 내부 네트워크에 접속한 이 후에 모든 검사 및 제어 절차 이루어진다는 것이다. 내부 네트워크에 단말이 접근한 이후에 해당 단말을 검사하고 감시 및 제어를 하기 때문에 이미 악성코드에 감염된 단말이 내부 네트워크 접근했을 경우, 보안 시스템이 이를 감지하고 제어하기 이전까지 내부 네트워크는 위험에 노출된 상태라고 볼 수 있으며, 이를 근본적으로 막을 수 있는 접근제어 방안이 필요하다.

2.2 격리네트워크를 활용한 네트워크 설계

본 논문에서는 위에서 제시한 근본적인 문제들을 해결하기 위한 방법으로 격리네트워크를 활용한 네트워크 방어 기법을 제시하고자 한다. 단말에 대한 무결성을 검증하기 위해 내부네트워크 접속이 불가능한 격리된 네트워크에서 해당 단말의 무결성 검사를 통해 검증된 단말만이 내부 네트워크 접근을 하도록 함으로써, 내부 네트워크에 대한 안정성을 보장할 수 있다. 또한, DHCP와 연계하여 격리구역에서 신규 단말에 대한 검사가 완료되면 자동으로 DHCP Offer패킷을 전송하여 내부네트워크의 IP를 할당하게 되는 구조로 사용자의 개입 없이 자동으로 격리구역에서의 단말 검사와 내부 네트워크 IP 주소 할당까지 가능하게 되는 구조로 네트워크를 설계하였다. 격리 네트워크를 활용한 네트워크 방어 기법의 자세한 동작은 그림 2.와 같다

무결성이 검증된 단말만 내부 사용자 네트워크에 접근하도록 유도할 수 있는 방안으로 네트워크 접근 순서는 그림 2.와 같이 설계하였으며, 자세한 동작 순서는 아래와 같다.

1. DHCP 환경에서 사용자 단말은 네트워크에 접근하기 위한 IP를 할당받기 위해 DHCP서버로 DHCP request 패킷을 보낸다.
2. 사용자 단말이 보낸 DHCP request 패킷을 수신한 DHCP 서버는 이에 대한 응답으로, Offer 패킷에 격리구역(독립된 VLAN으로 내부 네트워크 및 인터넷 사용이 불가한 네트워크 영역, 단말의 무결성 검사를 수행하기 위한 네트워크)의 IP를 할당하고 게이트웨이 주소로 DHCP 서버의 주소를 기입하여 회신한다.
3. 격리 구역의 IP를 할당 받은 사용자 단말은 인터넷 접속을 시도하게 되면 단말의 무결성 검증을 위한 웹 서버로 리다이렉션 된다.
4. 해당 웹서버에서를 통해 신규 단말은 무결성 검사를 위한 클라이언트를 다운로드 받게 된다. 이 때 검사는 API를 지원하는 기존의 보안클라이언트를 활용하여 검사를 진행하며, 해당 기업의 내규에 적합한 보안검사를 여기에서 진행한다.
5. 무결성 검사가 정상적으로 완료되면 신규 단말은 검사완료 API를 웹서버로 전송한다.
6. API를 수신한 웹서버는 신규단말의 MAC 주소를 DHCP 서버로 전송하고, 이를 수신한 DHCP 서버는 신규 단말의 MAC 주소를 config에 등록하고 dhcpd reload를 실행한다.
7. 이 후 웹서버는 검사완료 API 의 응답을 신규 단말에 설치된 클라이언트로 전송한다.
8. API 응답을 전송받은 신규 단말은 인증 구역 IP를 재 할당 받기위해 DHCP request를 DHCP 서버로 재전송한다.
9. DHCP 서버는 인증구역(사용자 내부 네트워크)의 IP를 Offer 패킷에 기입하여 사용자 단말로 재전송

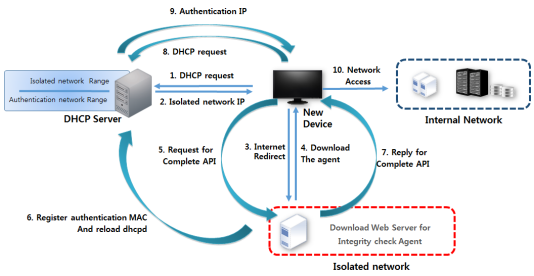

그림 2. 격리네트워크를 활용한 네트워크 방어기법
Fig. 2. A Network Defense Mechanism based on isolated Networks

표 2. 기존 무결성 검사 방안과의 차이점
Table 2. The difference from the conventional method

Conventional integrity checking method	The proposed method
. After the one allocated the IP access to the internal network proceeds integrity check. . In the event of a delay in the process to detect a new device block and the devicel is allowed to access the network.	. Progress integrity check of the new device in the isolated area that is not accessible to the internal network through an IP assignment of the isolated area to access to the internal network . Even if the delay occurs during the inspection so that the isolation area to protect the internal network.

한다.

10. 내부 네트워크에서 사용하는 IP주소를 재 할당 받은 단말은 내부 네트워크 접근권한을 가지고 네트워크 사용이 가능해 진다.

내부 네트워크에 신규로 접속하는 사용자는 위와 같은 여섯 단계의 접속과정을 거치게 되어, 사용자 단말에 대한 무결성 검증을 보다 안정적으로 진행할 수 있으며, 사용자 관점에서는 DHCP를 통해 자동으로 IP 가 할당되고 무결성 검증을 수행한 이후 자동으로 IP가 갱신되므로 IP할당 과정에서 사용자가 체감하는 번거러움은 없어진다.

본 논문을 통해 제시하는 단말의 무결성 검사방안과 기존의 무결성 검사방안과의 차이점은 아래의 표 2. 와 같이 설명될 수 있다.

2.3 격리네트워크 구현

본 논문에서 제시한 네트워크 설계방안을 검증하기 위해 격리 네트워크 환경에서 단말에 대한 무결성 검증 구현을 진행하였다.

구현 단계에서는 격리구역에서 무결성 검사와 API 호출을 위한 에이전트를 다운로드 하기 위한 웹서버를 설치하여 신규 단말에 대한 무결성 검사를 진행하고, 검사가 완료된 후 API 호출을 통해 DHCP 서버로부터 IP를 재할당 받을 수 있도록 구성하였다. API는 HTTP POST 방식으로 MAC Address 만 넘겨줬으며, 여러개의 MAC에 대한 식별 처리가 필요하므로 ipconfig /all 로 확인해서 격리구역 IP를 할당받은 NIC의 MAC을 식별해서 전송하도록 설정하였다. 한편 서버에서는 API 요청을 받으면 MAC을 config에 등록하고, dhcpd reload 명령으로 config reload로 처리하도록 설정했다. 정확한 동작에 대한 상세 흐름도는 그림 4.와 같다

최초 신규단말이 DHCP request를 보내게 되면 DHCP 서버는 허용 MAC 리스트에 존재하는지를 판단하여 격리구역 IP를 아래와 같이 부여하게 된다.

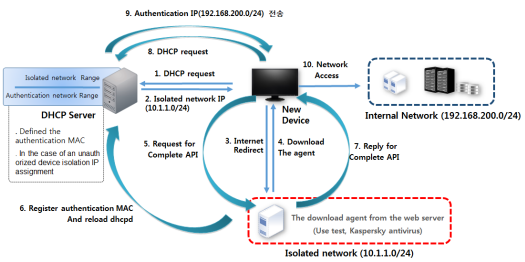

그림 3. 테스트 구성도
Fig. 3. Test Network

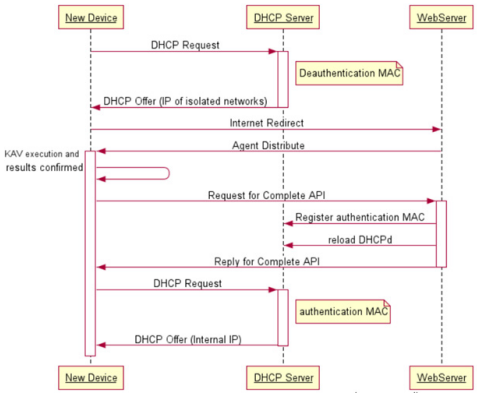

그림 4. 설계 흐름도
Fig. 4. sequence diagram

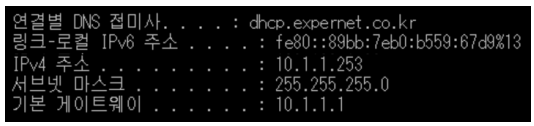

그림 5. 격리 구역 IP 할당
Fig. 5. IP of isolated networks

그림 4와 같이 격리 구역의 IP주소를 할당받은 단말이 격리네트워크 구역에서 네트워크에 접근을 시도하게 되면 그림 5와 같이 무결성 검사를 위한 웹페이지로 리다이렉션 된다. 해당 페이지 상에서 보안 검사를 위해 "보안검사 시작하기" 버튼을 클릭하게 되면 단말의 정보 수집 및 보안검사를 위한 에이전트 프로그램이 설치 및 실행된다.

여기서 설치되는 에이전트는 보안검사가 완료되면 검사 결과 값 전송 및 API를 호출하여 DHCP request를 재전송하는 역할을 수행한다. 구현 단계에서 해당 단말의 무결성 검사를 위해 백신 프로그램 (카스퍼스키)를 설치하여 신규 단말의 무결성 및 바이러스 감염 여부에 대한 검사를 진행 하였다.

다운로드 받은 에이전트 "avp scan /memory" 를 통해서 해당 단말의 무결성 검사를 실행하고 검사가 정상 종료되면 정상적으로 치료/확인된 단말이라 판단하고 DHCP request를 진행하게 된다. Offer 패킷을 받기 위해서 DHCP request OS 차원에서 필요한 것이기 때문에 ipconfig /renew로 IP를 다시 재 할당 받게 된다.

단말의 바이러스 검사 결과 검출된 바이러스가 없을 경우, 그림 6과 같이 인증구역 IP주소를 다시 할당받고, 내부 네트워크의 사용이 가능해진다.

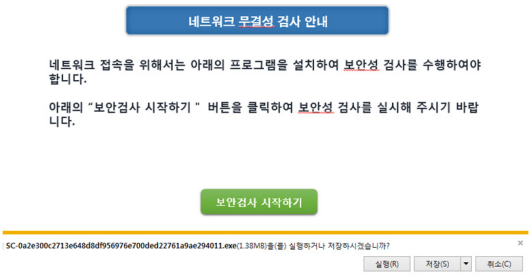

그림 6. 무결성 검증을 위한 웹페이지
Fig. 6. Web page for the integrity check

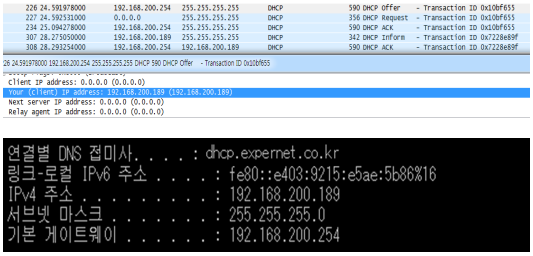

그림 7. 인증 구역 IP 할당
Fig. 7. IP of Authentication Network

Ⅲ. 결 론

본 논문에서는 비정상 단말의 내부네트워크 접근을 근본적으로 막을 수 있는 네트워크 접근 방안에 대해서 제안하였다. 그러나 DHCP 서버에서 격리 네트워크의 IP를 할당하여 무결성을 검증한 이후 내부 네트워크에 접근을 유도하는 방안은 이론적인 검증은 완료되었으나, 신규 단말을 어떤 검사를 어떻게 수행할지에 대해서는 환경에 따라 필요로 하는 검사 요소가 다를 수 있기 때문에 필요에 따라 무결성 검증 항목을 변경하여 적용할 수 있도록 하기 위한 지속적인 연구가 필요하다. 그리고 기존의 솔루션들을 이용하여 신규 단말의 무결성 검증에 대한 구체적인 방안과 이에 대한 테스트 및 API 연동 등을 시뮬레이션을 통해 지속적인 검증이 필요할 것이다.

References

[1] J.-D. Lim and J.-N. Kim, "A study on the trusted app.-based access control to the isolated trusted execution environment in mobile device," in *Proc. KICS Int. Conf. Commun.*, pp. 364-365, Jun. 2014.

[2] W.-J. Lee, K.-W. Kim, K.-D. Bu, and J. Woo, "A study on the adoption of NAC for guaranteeing reliability of u-Campus network," J. KIIT, vol. 7, no. 4, 2009.

[3] J. Bickford, R. O' Hare, A. Baliga, V. Ganapathy, and L. Iftode, " Rootkits on smart phones: Attacks, implications and opportunities," in *HotMobile'10*, ACM, Feb. 2010.

[4] S. H. Paik, S.-K. Kim, and H. B. Park, "Design and implementation of network access control for security of company network," *J. IEEK*, vol. 47, no. 12, Dec. 2010.

정 용 범 (Yongbum Jung)

2009년 2월 : 영산대학교 정보통신 공학과 졸업
2014년 9월~현재 : 숭실대학교 IT 융합학과 석사과정
<관심분야> 네크워크 보안, 네트워크 접근제어, 클라우드 보안

박 민 호 (Minho Park)

2000년 2월 : 고려대학교 공학사
2002년 2월 : 고려대학 공학석사
2010년 2월 : 서울대학교 공학박사
2002년 1월~2004년 7월 : 삼성전자 선임연구원
2010년 3월~2011년 4월 : 삼성전자 책임연구원
2011년 5월~2013년 2월 : 카네기멜론대학교 박사후과정
2013년 3월~현재 : 숭실대학교 전자정보공학부 조교수
<관심분야> SDN 및 SNS 보안, 클라우드 컴퓨팅, 무선네트워크