Journal of the Korea Convergence Society
Vol. 7. No. 4, pp. 39-44, 2016
http://dx.doi.org/10.15207/JKCS.2016.7.4.039

IoT 환경에서의 CoAP을 이용한 ARP Spoofing 공격 시나리오 및 대응방안

서초롱, 이근호*
백석대학교 정보통신학부

ARP Spoofing attack scenarios and countermeasures using CoAP in IoT environment

Cho-Rong Seo, Keun-Ho Lee*
Division of Information Communication, BaekSeok University

요 약 최근 IT시대인 만큼 IT기술의 눈부신 발전으로 인해 사물 대 사물, 사물 대 사람, 사람 대 사람 간의 정보 전달 기술이 활발해지고 있다. 정보 전달 기술이 활발해 지고 있는 만큼 IoT는 우리 일상생활에 밀접하게 다가와 언제 어디에서나 흔하게 볼 수 있을 만큼 우리 일상생활의 한 부분을 차지하고 있다. IoT 환경에서는 주로 웹 기반 프로토콜인 CoAP 프로토콜을 사용한다. CoAP 프로토콜은 전송 속도가 낮고 손실이 큰 네트워크에서 주로 사용되기 때문에 IoT 환경에서 주로 사용된다. 그러나 IoT는 보안적으로 취약하다는 단점이 있다. 만약, IoT 환경에서 보안에 노출 될 경우 개인정보 또는 기업의 기밀 정보 등이 유출 될 가능성이 있다. 공격자가 IoT 환경에서 대상 디바이스를 감염 시킨 후 감염된 디바이스가 공공장소에서 흔히 사용되는 무선인터넷에 접속 했을 시 장악된 디바이스는 내부망에 있는 디바이스들에게 arp spoofing을 보낸다. 그 후 내부망 패킷의 흐름을 장악한 후에 내부망에 있는 디바이스들이 보내는 패킷을 감염된 디바이스가 받아 지정된 해커의 서버에 보낸다. 본 논문에서는 이에 관한 공격 방법과 대응방안을 제안한다.

• 주제어 : 융합, 사물인터넷, 무선인터넷, CoAP, 딥러닝

Abstract Due to the dazzling development of IT in this IT-oriented era, information delivering technology among objects, between objects and humans, and among humans has been actively performed. As information delivery technology has been actively performed, IoT became closely related to our daily lives and ubiquitous at any time and place. Therefore, IoT has become a part of our daily lives. CoAp, a web-based protocol, is mostly used in IoT environment. CoAp protocol is mostly used in the network where transmission speed is low along with the huge loss. Therefore, it is mostly used in IoT environment. However, there is a weakness on IoT that it is weak in security. If security issue occurs in IoT environment, there is a possibility for secret information of individuals or companies to be disclosed. If attackers infect the targeted device, and infected device accesses to the wireless frequently used in public areas, the relevant device sends arp spoofing to other devices in the network. Afterward, infected devices receive the packet sent by other devices in the network after occupying the packet flow in the internal network and send them to the designated hacker's server. This study suggests counter-attacks on this issues and a method of coping with them.

• Key Words : Convergence, IoT, Wifi, CoAP, Deep learning

*Corresponding Author : 이근호 (leekeunho1004@gmail.com)
Received June 21, 2016 Revised June 22, 2016
Accepted August 12, 2016 Published August 31, 2016

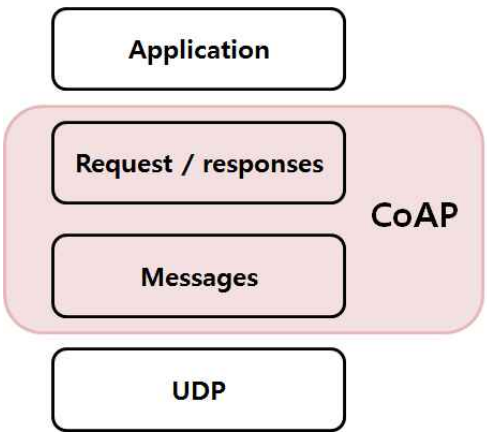
1. 서론

사물인터넷(Internet of Things) 일명 IoT란, 사물-사물, 사물-사람, 사람-사람 사이를 인터넷으로 연결하여 서로 통신하는 것이다. 최근 각종 디바이스들에서 산출되는 데이터들을 인터넷을 통해 서로 통신하여 최대한의 시너지를 발휘하려는 움직임이 다양한 분야에서 적용중이다. 또한 IT분야의 리서치 기업인 가트너에 따르면, 2015년에는 IoT 환경으로 연결된 사물이 49억대로 사용될 전망이며, 향후 2020년에는 250억대로 증가할 것으로 예측 했다[1]. 외부 나라에서 대한민국은 IT강국이라 불리지만 화려한 정보통신 기술에 비해 보안적인 문제로는 항상 주요 이슈이다[2]. IoT의 목적은 심장박동기, 가스 배관, 무인 자동차 등 일상생활 속에서 흔히 접할 수 있는 제품들을 인터넷으로 연결하여 인간들에게 더욱 더 편리하게 이용할 수 있도록 하는 것이 목적이다. 하지만 보안적인 기술의 부재로 인하여 해킹 당했을 시 개인정보유출 뿐만 아니라 기업정보유출 또는 국가적 테러와 사람의 목숨을 위협하는 무기가 될 수 있다[3]. IoT 디바이스들은 주로 CoAP 프로토콜을 사용한다. 이 CoAP 프로토콜은 웹 기반 응용 프로토콜이며, 한정된 자원의 기기에서 사용하기 위해 연결 지향형 TCP가 아닌 UDP를 사용하도록 설계되었다. 따라서 비교적 메모리 크기가 적고 컴퓨팅 파워가 부족한 IoT 환경의 디바이스에서 사용하기에 유리하다[4,5]. 웹은 정보를 전달하는 능력이 뛰어나 기업, 조직 내에 긍정적 영향을 미치고 있어 주로 사용된다[6]. 따라서 본 논문에서 제안하는 보안위협으로는 IoT 환경에서 웹 기반 응용 프로토콜인 CoAP을 이용한다. 사전에 공격자는 직접 제작한 웹 또는 다른 웹을 장악한 후 디바이스가 해당 웹에 접속 시 악성 스크립트를 실행 시켜 디바이스를 악성코드에 감염시킨다. 그러면 공격자는 악성코드로 인해 감염된 디바이스의 권한을 획득하게 된다. 그런 후 감염된 디바이스를 통해 공공장소에 흔히 사용되고 있는 무선 인터넷에 접속을 한다. 감염된 디바이스로 무선인터넷에 접속 할 경우, 무선 인터넷 내부망에 있는 다른 디바이스들에게 ARP Spoofing을 시도할 수 있는 기회가 생긴다. ARP Spoofing을 시도할 경우 ARP Spoofing 공격을 당한 디바이스들의 패킷 정보들을 1차로 감염된 디바이가 획득하게 된다. 획득한 패킷 정보들은 공격자에게 전송되는 가정을 제시한다.

2. 관련연구

2.1 CoAP Protocol

CoAP(Constrained Application Protocol)은 IETF core WG에서 개발한 웹 기반 프로토콜이며 에너지, 성능, 메모리 md에서 제약을 가진 CN으로 구성되어 전송속도가 낮고 손실이 큰 네트워크에서 사용되며 REST (Representational Status Transfer) 구조를 가진 응용 프로토콜이다[3]. CoAP은 기본적으로 트랜스포트 계층 위에서 UDP와 같은 데이터 그램 방식의 비동기적으로 전송되는 것을 다룬다. 또한 보안적인 부분을 위해서 CoAP 계층과 UDP 계층 사이에 DTLS(Datagram Transport Layer Security) 계층이 사용 될 수 있다. 그리고 CoAP은 리셋(reset), 승인(acknowledgement), 확인형(confirmable), 비확인형(non-confirmable)의 4가지 메시지 타입을 정의한다[7,8,9,10].



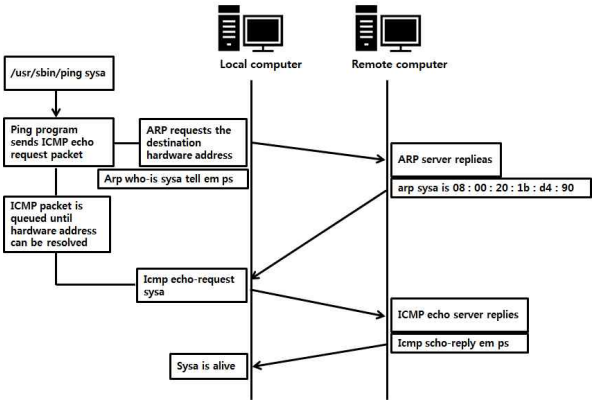
[Fig. 1] CoAP Protocol Stack

본 논문에서 CoAP 프로토콜을 사용한 이유는 CoAP 프로토콜은 손실이 크고 전송 속도가 낮은 네트워크에서 사용되는 웹 기반 프로토콜이므로 IoT 환경에서 주로 사용되기 때문이다. 또한 IoT 환경에서 주로 사용 되는 웹 기반 프로토콜이므로 CoAP 프로토콜을 공격할 경우 많은 피해가 발생 될 것이라 예상되기 때문이다. 그리고 기존에 존재하는 웹 기반 프로토콜에 대한 공격에 공격당할 우려가 있다. 또한 그로인해 IoT 환경을 갖춘 디바이스의 권한이 장악당할 수도 있는 가능성을 제시한다.

2.2 ARP(Address Resolution Protocol)

ARP(Address Resolution Protocol)은 DNS가 도메인

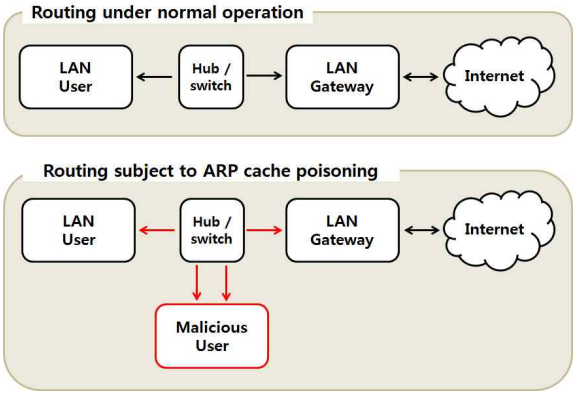
주소를 IP 주소로 바꾸어 주는 것과 같이 IP 주소를 MAC(Media Access Control) 주소로 변환해 주는 프로토콜이다. 일반적인 ARP Protocol의 경우, 이더넷의 주소는 48bit의 크기를 가지고 있고 IP 데이터 그램에서 IP 주소는 32bit 구조로 되어 있다. 상대방 호스트의 이더넷 주소를 알게 되면 또 다른 호스트로 네트워크에 연결 할 수 있게 된다. 즉, 사용자는 IP 주소를 이용하여 네트워크에 연결을 하지만 이더넷 상에서는 이더넷 주소를 이용하게 된다[11,12].



[Fig. 2] ARP Protocol

2.3 ARP Spoofing

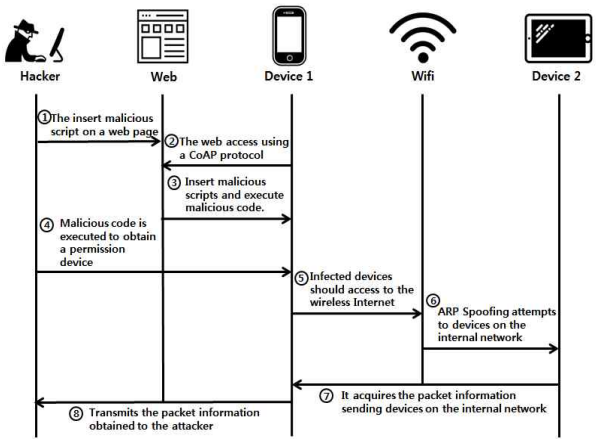
ARP Spoofing 공격은 공격자가 공격하고자 하는 호스트들의 ARP 캐시 테이블 정보를 변경하여 공격자의 컴퓨터로 트래픽 방향을 우회시키는 공격이다. 더 쉽게 말을 하자면, 동일한 네트워크에 존재하는 공격 대상 디바이스의 IP 주소를 공격자 자신의 랜카드 주소와 연결하여 다른 디바이스에 전달되어야 하는 정보를 가로채는 공격이라고도 말할 수 있다. 공격 대상에는 스위치 또는 기타 네트워크 장비뿐만 아니라 네트워크망에 접속하는 또 다른 컴퓨터들이 해당될 수 있다. 그렇기 때문에 공격자는 우회된 트래픽을 이용하여 개인정보 또는 기업정보뿐만 아니라 각종 보안 문서 및 패스워드 등 중요한 정보들을 마음껏 획득할 수 있다[13,14,15]. 또한 동일한 내부망의 모든 디바이스들이 감염된 디바이스를 게이트웨이로 인식하여 외부 네트워크와 통신하기 위해 발생하는 모든 패킷을 감염된 디바이스로 전송하므로 네트워크 속도가 크게 느려진다.



[Fig. 3] ARP Spoofing

3. 보안 위협

본 그림은 IoT 환경에서 CoAP 프로토콜을 이용하여 공격하는 방법이다. 먼저, 공격자는 이용자가 많은 홈페이지를 해킹하거나 해당 홈페이지에 악성 스크립트를 삽입한다. 그런 후 IoT 환경에서 IoT 디바이스로 CoAP 프로토콜을 이용하여 공격자가 악성스크립트를 삽입한 웹페이지에 접속한다. 이럴 경우 접속한 디바이스에 악성스크립트가 실행되어 공격자가 해당 디바이스의 권한을 얻게 된다. 감염된 디바이스로 공공장소에서 흔히 사용되고 있는 무선 인터넷에 접속할 경우 내부망에 있는 또 다른 디바이스들에게 ARP Spoofing 공격을 시도할 수 있게 된다. ARP Spoofing 공격을 시도했을 시 내부망에서 감염된 디바이스들의 패킷 정보들이 처음 감염된 디바이스에게 전송된다. 마지막으로 공격자에 의해 해킹당한 디바이스로부터 공격자는 내부망에서 감염된 디바이스들의 패킷 정보들을 획득할 수 있다.

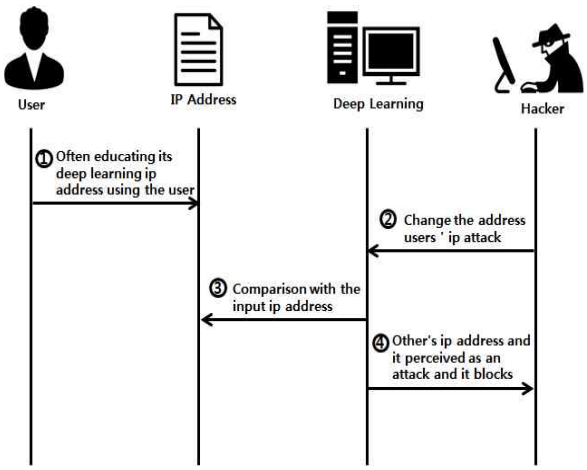


[Fig. 4] Attack scenarios

① 공격자는 이용자가 많은 웹 페이지를 해킹한 후, 악성코드가 실행 될 수 있도록 악성 스크립트를 삽입한다.
② 디바이스 1은 IoT 환경에서 사용되는 CoAP Protocol을 이용하여 웹 페이지에 접속한다.
③ 디바이스 1이 웹 페이지에 접속하는 순간 공격자가 웹 페이지에 미리 삽입해 두었던 악성 스크립트가 실행되며 디바이스 1이 악성코드에 감염된다.
④ 공격자가 삽입한 악성코드에 의해 공격자는 디바이스 1의 권한을 획득한다.
⑤ 감염된 디바이스 1으로 공공장소에서 흔히 사용되고 있는 무선 인터넷에 접속한다.
⑥ 해당 무선 인터넷 내부망에 있는 또 다른 디바이스들에게 ARP Spoofing을 시도한다.
⑦ 내부망에 있던 또 다른 디바이스들이 2차로 감염되어 감염된 디바이스 2들이 보내는 패킷 정보들은 디바이스 1이 획득하게 된다.
⑧ 디바이스 1은 디바이스 2에게 받은 패킷 정보들을 공격자에게 전송한다.

4. 대응방안

IoT 환경에서 주로 사용되는 웹 기반 응용 프로토콜인 CoAP 프로토콜은 기존에 존재하는 웹 해킹에 의해 영향을 받기 쉽다. 따라서 웹 운영자는 기본적으로 보안 패치, 백신 프로그램 업데이트 등의 조치를 사전에 수행해야 된다. 또한 위에서 언급했듯이 ARP Spoofing에 감염되었을 시 MAC 주소를 모니터링 하여 감염원을 파악하거나 백신을 이용하여 치료를 하거나 자동 혹은 수동으로 장비들을 리셋 하여 장비를 재정비 해주어야 한다. 본 논문에서 제시한 IoT 환경에서의 CoAP을 이용한 ARP Spoofing 공격기법의 대응방안으로는 딥러닝 기술을 이용하는 것이다. ARP Spoofing 공격이 공격 대상의 디바이스의 IP 주소를 공격자가 변형하여 감염된 디바이스의 패킷 정보를 가로채는 공격이므로 반복학습 기술인 딥러닝 기술로 사용자의 IP 주소를 주기적으로 체크하는 학습을 시킨다. 이때, 대상 디바이스들은 주로 핸드폰, 노트북, 아이패드 같은 휴대용 디바이스들이기 때문에 IP 주소들이 자주 바뀔 것이다. 이럴 경우 사용자가 자주 사용하는 네트워크의 IP 주소들을 저장 한다. 딥러닝 기술은 새로운 IP 주소가 인식 될 때마다 사용자가 저장 해둔 IP 주소와 비교한다. 만약 사용자가 저장해 둔 IP 주소 이외의 주소가 인식 될 경우에 공격자의 IP로 인지하여 IP를 차단시키는 대응방안을 제시한다.



[Fig. 5] Countermeasures

① 사용자는 자신이 자주 이용하는 네트워크의 IP 주소를 딥러닝 반복 학습 기술에 입력시킨다.
② 공격자가 ARP Spoofing 공격으로 사용자의 IP 주소를 변경한다.
③ 딥러닝 반복 학습 기술은 새로운 IP 주소가 인식 될 때마다 사용자가 입력시킨 IP 주소와 비교한다.
④ 사용자가 입력한 IP 주소 외일 경우 공격자의 IP로 인지하여 IP를 차단시킨다.

5. 결론

최근 IT기술의 눈부신 발달로 인해 사물인터넷이 급격히 발전해 가고 있다. 사물인터넷은 가스 밸브, 실내조명, 심장박동기기, 스마트 밴드, 무인자동차 등 우리의 일상생활에서 흔히 접할 수 있는 디바이스들 또는 자신의 건강을 위하여 건강 체크를 실시하는 디바이스 등을 인터넷과 연결하여 정보 공유를 보다 더 쉽게 할 수 있도록 도와주고 사용자들이 더욱 더 편하게 생활 할 수 있도록 해준다. 하지만 IoT가 일상생활에 밀접하게 관계되어 있는 만큼 보안적인 문제에서는 매우 취약하다. 만약 사물인터넷이 해킹 될 경우엔 개인정보 뿐만 아니라 기업정보, 각종 보안 문서, 기술 문서 등 중요한 문서들이 유출될 가능성이 높으므로 위험에 대해 보안을 강화할 뿐만

아니라 만일의 상황에 대비하여 대응방안 또한 준비를 하고 있어야 한다. 본 논문에서는 이럴 경우를 대비하고자 하여 사물인터넷 환경에서 주로 사용되고 있는 웹 기반 응용 프로토콜인 CoAP 프로토콜을 대상으로 한 공격 기법에 대한 시나리오와 그에 대응하는 대응방안을 제시하였다. 위에서 보았듯이 CoAP 프로토콜은 웹 기반 응용 프로토콜이므로 기존에 존재하던 웹 해킹 방법으로 쉽게 정보가 탈취 될 수 있다. 그러므로 향후 다가오는 IoT 시대에 걸맞도록 그에 대한 보안적인 문제를 강화시켜야 하고 인터넷이 세계를 지배할 만큼 우리의 일상생활 속에서 밀접하게 접해 있으므로 웹 보안 또한 지속적으로 발전시켜야 한다.

ACKNOWLEDGMENTS

이 논문은 2013년도 정부 (미래창조과학부)의 재원으로 한국 연구재단의 기초연구사업 지원을 받아 수행된 것입니다.(2013 RIAIAIA05012348)

REFERENCES

[1] Wanjin Chang, Yongtae Shin, “A Study on the Network and Security for the Internet of Things”, Korean Institute Of Information Technology, pp. 19-21, 2015.

[2] Jun-Young Go, Keun-Ho Lee, “SNS di s closure of pe rsonal information in M2M envi ronment threats and counte rmeasures”, Korea Convergence Society, Vol. 5, No.1, pp. 29-34, 2014.

[3] Seung-Hyeon Choi, Cho-Rong Seo, Keun-Ho Lee, “Device Hacking Scenario and Countermeasures with CoAP in the Internet of Things Environment”, Journal of the Korea Convergence Society

[4] Joosang Youn, Hun Choi, "CoAP-based Reliable Message Transmission Scheme in IoT Environments", The Korean Society Of Computer And Information, pp. 79-84, 2016.

[5] Kyong-Ho Han, Seong-Ho Lee, "A Study on the Security Threats of IoT Devices Exposed in Search Engine", The Korean Institute of Electrical Engineers, pp. 128-134, 2016.

[6] Hyeon-Su Byeon , Mi-Ra Kang, “The Study of Factors on Information System Success through Web Assimilation”, The Korea Society of Digital Policy, Vol. 13, No.11, pp. 85-97, 2015.

[7] Cheol-Min Kim, Hyung-Woo Kang, Ji-In Kim, Seok-Joo Koh, “An Implementation of the Low Power Device Communication using CoAP Protocol in Internet of Things Environment”, Korea Institute of Communication Sciences, pp. 102-103, 2015.

[8] Seok-Kap Go, Il-Gyun Park, Seung-Cheol Son, Byeong-Tak Lee, “Trends of IETF CoAP Based Sensor Connection Protocol Technology”, ETRI, Vol. 28, No. 6, pp. 133-139, 2013.

[9] Nam-Hui Gang, “Standard technology trends for the security of the internet objects”, Korea Institute of Communication Sciences, Vol. 31, No. 9, pp. 40-45, 2014.

[10] Woo-Il Seo, Hyun-Min Park, Byeong-Seong Choe, Jae-Hyun Park, “A Study on Detection and trace for TCP Connection ARP Spoofing/Hijacking”, Korea Institute of Communication Sciences, pp. 1115-1118, 2000.

[11] Woo-Il Seo, Hyun-Min Park, Byeong-Seong Choe, Jae-Hyun Park, “A Study on Detection and trace for TCP Connection ARP Spoofing/Hijacking”, Korea Institute of Communication Sciences, pp. 1115-1118, 2000.

[12] Bong-Koo Ko, Seung-Jong Chung, Gi-hwan Cho, “A Design of Network Management System for Efficiently Isolating Devices Infected with ARP Spoofing Virus”, Korea Institute of Communication Sciences, Vol. 17, No. 3, pp. 641-648, 2013.

[13] Seung-Pyo Hong, “An efficient prevention technique using the relible ARP table for ARP spoofing attacks”, Soongsil University, pp. 1-25, 2011.

[14] Hyun-Uk Hwang, Eun-Shin Park, Jong-Baek Park, “A Study on ARP Spoofing ingAttack and Prevention Method”, Korea Institute of Communication Sciences, pp. 1821-1824, 2001.

[15] Ji-Woo Kang, Jea-Gi Son, Jea-Hoon An, “ARP Spoofing Detection and Prevention Method using Spark Streaming”, The Institute of Electronics Engineers of Korea, pp. 194-195, 2016.

저자소개

서 초 롱(Cho-Rong Seo) [학생회원]

· 2015년 3월 ~ 현재 : 백석대학교 정보통신학부 학생

<관심분야> : 융합보안, 개인정보보호, IoT보안

이 근 호(Keun-Ho Lee) [정회원]

· 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)

· 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : 이동통신 보안, 융합 보안, 개인정보보호