CoAP 멀티캐스트 보안취약점 분석

허신욱*, 김호원*
*부산대학교 전기컴퓨터공학부
e-mail : shinwookheo@gmail.com

Analysis on Vulnerability of CoAP Multicast

Shin-Wook Heo*, Ho-Won Kim*
*Dept. of Electric Computer Science, Pusan National University

요 약

CoAP 은 제한된 성능을 가진 디바이스들이 사용할 수 있도록 설계된 경량 프로토콜이다. 이는 최근 많은 관심을 받고 있는 사물인터넷에 사용되는 경량 디바이스들에 적용될 수 있다. 또한 CoAP 은 멀티캐스트를 지원하기 때문에 많은 디바이스가 사용되는 사물인터넷 환경에서 효율적인 트래픽 관리가 가능하다. 하지만 CoAP 멀티캐스트의 경우에는 COAP 유니캐스트에 비해 상대적으로 보안에 취약하다. 따라서 본 논문에서는 CoAP 멀티캐스트 보안 취약점에 대해 조사하고 분석한다.

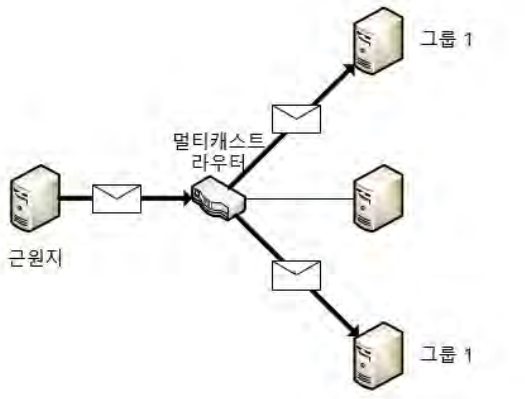
1. 서론

사물인터넷에 대해 관심이 높아짐에 따라 사물인터넷에 사용되는 다양한 프로토콜들과 보안문제에 대해서 많은 연구가 이루어지고 있다. 특히 사물인터넷은 제한된 자원(CPU, 메모리, 저장공간, 배터리) 을 가진 장치들이 많이 사용되기 때문에 CoAP, MQTT 와 같은 경량 프로토콜에 대한 관심이 증가하고 있다. 이러한 경량 프로토콜들은 유니캐스트은 물론이고 멀티캐스트까지 지원한다. 하지만 CoAP 의 경우 멀티캐스트에 대한 보안 취약점이 존재한다.

사물인터넷의 경우 가상공간 뿐만 아니라 현실세계에 직접적인 영향을 줄 수 있는 센서와 작동장치들이 많기 때문에 CoAP 멀티캐스트의 보안 취약점은 심각한 악영향을 미칠 수 있다. 따라서 본 논문에서는 CoAP 멀티캐스트에 대한 보안 취약점을 조사하고 분석한다.

2. 배경지식

CoAP 은 4 바이트의 고정된 헤더를 가지는 경량 프로토콜로써 유니캐스트와 멀티캐스트를 지원한다. 유니캐스트란 데이터그램이 하나의 목적지를 가지고 전송되는 것을 의미하고 멀티캐스트는 [그림 1]과 같이 하나의 목적지를 가지는 데이터그램이 아닌 하나 이상의 목적지 주소로 이루어진 목적지 그룹으로 데이터가 전송되는 방식이다. 유니캐스트는 멀티캐스트의 한 유형이라고 생각할 수 있다. 일반적으로 멀티캐스트 방식은 멀티캐스트가 가능한 라우터가 필요하다. 멀티캐스트 라우터는 멀티캐스트 데이터그램을 여러 목적지에 전송하기 위해서 인터페이스를 통한 멀티캐스트 데이터그램 복사기능을 제공해야 한다. [1]



(그림 1) 멀티캐스트

3. 본론

CoAP 표준문서인 RFC7252 에 따르면 현재 멀티캐스트에 대한 보안은 CoAP 에서 지원하지 않는 상태이다. CoAP 보안의 상당 부분을 차지하는 Datagram Transport Layer Security(DTLS)의 경우 유니캐스트만을 지원하는 상황이다. 따라서 CoAP 멀티캐스트를 사용할 경우 많은 보안 취약점이 발생하게 된다.[2]

먼저 사물인터넷의 특징에 의해 발생하는 보안 취약점이 있다. 사물인터넷의 경우 다양하고 많은 장치가 같은 네트워크에 존재하게 된다. 이것은 공격자가 CoAP 멀티캐스트 메시지에 대해서 많은 장치들을 관

찰할 수 있다는 것을 뜻한다. 이 경우에는 CoAP 멀티캐스트 메시지가 암호화되어 있더라도 공격자에게 side-channel 정보를 줄 수 있게 되고 보안 취약점이 발생하게 된다.

CoAP 의 경우 사물인터넷에 주로 사용되기 때문에 CoAP 트래픽은 인간과 밀접한 관련을 가진 장치를 제어하거나 중요한 시설물들을 모니터링할 가능성이 높다. 이것은 CoAP 트래픽이 공격자의 목표가 되기 쉽다는 것과 공격자에게 공격당했을 경우에 치명적인 결과를 초래할 수 있다는 것을 뜻한다. 특히 CoAP 멀티캐스트 트래픽의 경우, 유니캐스트 트래픽에 비해 공격자가 가로채기 쉽기 때문에 더욱 더 보안에 신경을 써야 한다.

위와 같은 보안 문제점 외에도 그룹 키 교환과 그룹 인증등과 같은 기존의 멀티캐스트 보안기법들을 CoAP 멀티캐스트는 제공하지 않기 때문에 이를 해결하기 위해서는 다음과 같은 애플리케이션 레벨의 보안 기법, 링크계층의 보안 기법들을 응용하여 CoAP 멀티캐스트의 보안 취약점을 완화시켜야 한다.

먼저 외부 네트워크와 연결된 내부 네트워크환경에서 CoAP 멀티캐스트를 사용할 경우, 침입자의 멀티캐스트 그룹 참여를 막기 위한 방법으로 내부 네트워크에서 제공하는 암호화를 사용하는 방법이 있다. 이때 사용하는 주거용 게이트웨이, 홈 네트워킹 어탭터, 인터넷 접근 게이트웨이와 같은 외부 네트워크와 연결된 Customer Premises Equipment(CPE) 에서 자체적으로 외부의 멀티캐스트 그룹과 내부 멀티 캐스트 그룹을 분리시킬 수 있는 필터를 제공할 경우에도 보안 취약점을 완화시킬 수 있다.

또한 저전력 무선 사설 네트워크인 6LoWPAN 네트워크환경에서 CoAP 멀티캐스트를 사용할 경우 링크계층의 암호화로 멀티캐스트 그룹에 참여하려는 침입자를 막을 수 있다. Multi-Subset 6LoWPAN 의 경우, 백본망에 Port Authentication 을 구현하여 인증된 장치만이 이더넷 백본에 참여할 수 있도록 하여 악의적인 의도를 가진 침입자의 멀티캐스트 그룹 참여를 방지할 수 있다.[3]

현재 위와 같은 문제점들을 해결하기 위해 IETF 에서는 유니캐스트에서 보안을 위해 사용되는 DTLS 를 멀티캐스트의 그룹통신에서도 사용할 수 있도록 개발하고자 한다.[4]

4. 결론

사물인터넷의 경우 가상공간뿐만 아니라 실생활에 직접적인 영향을 미치기 때문에 보안 취약점이 있을 경우 심각한 악영향을 미칠 수 있다. 또한 사물인터넷의 특성상 많은 디바이스들이 상호작용하기 때문에 많은 네트워크 트래픽이 발생할 수 있다. 이를 해결하기 위한 한가지 방법으로 멀티캐스트를 사용하는 방법이 있다. 멀티캐스트의 경우 유니캐스트와는 달리 하나의 데이터그램으로 여러 목적지에 데이터를 전송할 수 있기 때문에 네트워크 트래픽을 효율적으로 관리할 수 있다. 하지만 멀티캐스트를 사용하기 위해서는 라우터에서 멀티캐스팅을 지원해야 하고 추가적으로 발생할 수 있는 보안 문제에 대해서 고려해야 한다. 따라서 본 논문에서는 사물인터넷에 많이 사용되고 있는 경량 프로토콜인 CoAP 의 멀티캐스트의 보안 취약점과 멀티캐스트와 사물인터넷의 결합으로 인해 발생할 수 있는 보안 취약점을 조사하고 이를 해결하기 위한 방법들을 찾아봄으로써 추후에 발생할 수 있는 보안 문제들의 해결방향을 제시한다.

참고문헌

[1] Forouzan, “Data Communications and Networking” 5th Ed, McGraw Hill

[2] Shelby, Zach, Klaus Hartke, and Carsten Bormann. "The Constrained Application Protocol (CoAP)." (2014).

[3] Rahman, Akbar, and Esko Dijk. "Group Communication for the Constrained Application Protocol (CoAP)." Group (2014).

[4] Keoh, S., Kumar, S., Garcia-Morchon, O., Dijk, E., and A.Rahman, “DTLS-based Multicast Security in Constrained Environment”, Work in Progress, draft-keoh-dice-multicast-security-08, July 2014.