ROS2 및 SROS2 의 보안 취약점에 대한 조사

정성윤 [1], 서지원 [2]
[1] 단국대학교 산업보안학과 학부생
[2] 단국대학교 사이버보안학과 교수

jsy00317@dankook.ac.kr, jwseo@dankook.ac.kr

A Survey on Security Vulnerabilities in ROS2 & SROS2

Sung-Youn Jeong[1], Ji-Won Seo[1]
[1]Dept. of Cyber Security, Dankook University

요 약

ROS(Robot Operating System)은 복잡하고 분산된 로봇 애플리케이션 개발을 위해 유연한 프레임워크다. ROS 는 다양한 소프트웨어 컴포넌트 간의 통신을 가능하게 하는 미들웨어로, 로봇 제어 시스템 구축에 필요한 도구와 라이브러리를 제공한다. 본 논문에서는 ROS2 에 대한 소개 및 ROS2 대상 보안 기능을 제공하는 SROS2 에 대한 소개를 하고자 한다. 최근 SROS 를 대상으로 하는 취약점 연구들이 제안되고 있는데 이러한 취약점은 접근 정책을 우회하거나 시스템의 설정에 관한 정보를 탈취할 수 있는 위험이 있다. 본 논문은 이러한 취약점이 시스템의 보안성에 미치는 영향을 설명하고 최근 ROS 을 대상으로 하는 취약점들을 알아보고자 한다.

1. 서론

ROS(Robot Operating System)은 분산된 로봇 애플리케이션을 개발하기 위해 로봇 제어 시스템 구축에 필요한 도구와 라이브러리를 제공하는 프레임워크이다. 하지만, ROS 의 초기 설계 단계부터 보안에 대한 고려가 미흡하여 다양한 취약점이 존재한다는 문제가 지적되어 왔다. 특히, 네트워크 통신이 암호화되지 않은 상태로 수행되고, 접근 제어 및 인증 절차가 부족하여 ROS 시스템은 다양한 공격에 노출될 위험이 크다.

이러한 보안 위협에 대응하고자 ROS2 는 DDS(Data Distribution Service) 기반의 통신 방식을 채택하고, 보안 기능을 강화한 SROS2(Secure ROS2)를 도입하였다. DDS 는 분산형 통신을 가능하게 하고, 메시지 암호화, 인증, 접근 제어 기능을 제공한다. SROS2 는 ROS2 기반 시스템의 안전성을 향상 시키고, 분산 로봇 시스템에서 보다 안전한 보안 체계를 구축하기 위해 개발되었다.

그러나 SROS2 역시 완벽하지 않으며, 공격자가 이를 우회할 수 있는 다양한 보안 취약점이 보고되고 있다. 본 논문에서는 기존 연구를 바탕으로 ROS2 와 SROS2 의 보안 취약점을 조사하고, 특히 SROS2 의 설계상 문제로 발생하는 보안 취약점들의 원인과 그 영향을 이론적 분석을 통해 파악하는 데 중점을 두었다. 마지막으로, ROS2 및 SROS2 를 대상으로 하는 최근 취약점에 대한 조사를 하였다.

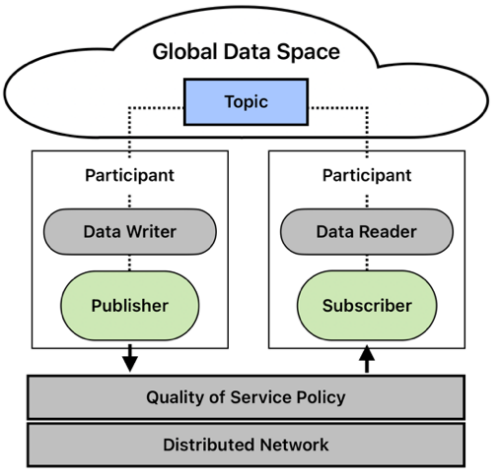
2. 배경지식

2.1 ROS2 (Robot Operating System2)

ROS2 는 기존 ROS 의 확장성, 실시간 처리 성능, 보안 측면에서의 한계를 개선하기 위해, DDS 기반의 분산 통신 방식을 도입하였다. DDS 는 실시간 시스템에서 데이터를 효율적으로 교환할 수 있는 Publish-Subscribe 방식을 사용하며, 노드 간의 통신이 분산된 방식으로 이루어진다. 이를 통해 로봇 시스템이 보다 유연하게 동작할 수 있으며, 특히 다중 로봇 시스템(Multi-Robot System, MRS)에서 다중 작업 수행이 가능하다

2.2 DDS (Data Distribution Service)

DDS 는 Global Data Space 를 중심으로 데이터를 효율적으로 관리하며, 분산 시스템에서 각 노드가 데이터를 주고받을 수 있는 기반을 제공한다. 그림 1 에서 볼 수 있듯이, Global Data Space 는 모든 데이터 객체, 즉 DDS Topic 이 존재하는 공간으로, 노드 간의 데이터 교환이 이루어지는 핵심 요소이다. Publisher 와 Subscriber 간의 데이터 교환은 이 공간을 통해 이루어진다. Participant 는 Publisher 또는 Subscriber 로 동작한다. Publisher 는 해당 토픽에서 데이터를 수신한다. 이 모든 과정은 분산통신의 형태로 진행된다.



(그림 1) DDS 통신 구조

DDS 는 이러한 통신을 제어하기 위해 QoS(Quality of Service)를 설정하여, Publisher 와 Subscriber 간의 통신에서 데이터를 전송하는 속성을 정의하며, 신뢰성, 전송 속도, 우선순위 등 다양한 속성을 설정할 수 있다. 또한, DDS 는 Real-Time Publisher/Subscribe Protocol 을 기반으로 데이터 전송이 이루어지며, 이를 통해 실시간으로 로봇 노드 간의 데이터 교환이 가능해진다.

2.3 SROS2 (Secure ROS2)

SROS 는 DDS 를 기반으로 통신을 보호하고, SROS2 에서는 DDS 의 보안 모듈을 사용하여 보다 안전한 보안 계층을 추가했다. SROS2 에서는 네트워크 트래픽 암호화, 인증, 접근제어와 같은 보안 기능을 제공한다.

기본적으로 ROS 및 ROS2 는 모든 네트워크 통신이 평문으로 처리되지만, SROS2 는 데이터를 암호화하여 기밀성을 보장한다. 또한 SROS2 는 각 노드 간의 신뢰성을 보장하기 위해 PKI(Public Key Infrastructure) 기반의 인증 시스템을 도입하였다.

SROS2 는 각 노드가 특정 데이터에 접근할 수 있는 권한을 정의하였다. 각 노드가 어떤 Topic 에 대해 Publish 하거나 Subscribe 할 수 있는지 권한 파일을 사용하여 제한한다. 이를 통해 허가되지 않은 접근을 차단하고 시스템의 보안성을 강화한다.

3. ROS2 의 보안 취약점

최근 ROS2 를 대상으로 하는 많은 취약점들이 보고되어 오고 있다[1,2]. 예를 들어, CVE-2024-30724 는 원격 공격자가 여러 ROS 노드에 대한 무단 접근, 권한 상승 및 임의 코드 실행이 가능하다. 이 취약점을 통해 로봇 동작을 제어하는 악성 행위에 악용될 수 있다. SROS 를 통해 공격자가 무단 접근하는 것을 어느 정도 차단 할 수 있으나, 이러한 취약점을 완전히 방어하려면 SROS 의 최신 보안 패치 적용이 필수적이다. 본 연구에서는 [1]을 바탕으로 보안 메커니즘을 무력화할 수 있는 심각한 결함을 정리하고자 한다. 특히 분산 로봇 시스템에서 발생할 수 있는 보안 위협을 조사하였다.

3.1 권한 파일 대상 취약점

ROS2 에서 권한 파일의 관리가 미흡하여 발생하는 취약점이 존재한다. 이전의 권한 파일의 폐기에 대한 미흡한 관리로 인해 공격자가 만료된 권한 파일을 사용하여 접근 제어 정책을 우회할 수 있다. 이를 통해 허가되지 않은 Topic 에 접근하고, 시스템의 보안 정책을 무력화할 수 있다. 또한, 권한 파일이 최소 권한의 원칙을 따르지 않고 과도하게 많은 정보를 포함하고 있어, 공격자가 다른 노드의 보안 설정이나 접근 권한을 추론할 수 있는 위험이 있다.

3.2 노드 서비스 갱신 거부 취약점

노드가 접근 제어 정책을 제때 업데이트하지 못하는 문제에서 발생한다. 노드는 새로운 정책을 적용하기 위해 노드 서비스의 재시작이 필요하지만, 공격자는 의도적으로 노드의 재시작을 거부할 수 있다. 이로써 이전에 부여된 권한을 유지하여 시스템의 접근 제어 정책을 우회할 수 있다.

3.3 기본 설정 오류 취약점

ROS2 의 Configuration 파일에는 암호화가 적용되지 않아 네트워크 상의 노드 간 통신을 도청할 수 있다. 공격자는 Publisher 나 Subscriber 의 participant 정보를 가로챌 수 있으며, 이를 악용하여 다른 노드에 다양한 공격을 수행하거나 시스템의 정상적인 동작을 방해할 수 있다. 더 나아가, 공격자는 노드 간의 통신을 감청하고 데이터 패킷을 조작할 수 있고, 이를 통해 민감한 정보를 탈취할 수 있다.

4. 결론

이번 조사를 통해 ROS2 와 SROS2 의 보안 메커니즘에 여러 취약점이 존재한다는 사실을 확인했다. 공격자가 이를 악용할 경우 심각한 보안 위협이 발생할 수 있다. 이러한 취약점들은 실시간 로봇 시스템에서 데이터 보호 및 접근 제어 정책이 얼마나 중요한지 보여준다. 향후 연구에서는 이러한 취약점을 해결하기 위한 보안 정책 개선과 자동화된 접근 제어 관리 방안이 필요하다.

사사문구

"본 연구는 2024 년 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학사업 지원을 받아 수행되었음"(2024-0-00035)

참고문헌

[1] Benhamouda, Fabrice, et al. “On the (in) security of ROS.” *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Cham: Springer International Publishing, 2021, pp. 33-53.

[2] Maruyama, Yuya, Shinpei Kato, and Takuya Azumi. “Exploring the performance of ROS2.” *Proceedings of the 13th International Conference on Embedded Software*, 2016, pp. 1-10.