보안 Data Distribution Service (DDS)의 Discovery 취약점 연구

이경연, 최원석*, 이동훈*

고려대학교 대학원생, *고려대학교 교수

gyeongyeon@korea.ac.kr, beb0396@korea.ac.kr, donghlee@korea.ac.kr

A Study on Vulnerability in the Discovery Process of Secure Data Distribution Service (DDS)

Gyeongyeon Lee, Wonsuk Choi and Dong Hoon Lee

School of Cybersecurity, Korea University

요 약

Data Distribution Service (DDS)는 통신 미들웨어로, 실시간 처리가 요구되는 군사, 의료, 로봇, 산업용 IoT 등의 분산 시스템 환경에서 널리 사용되고 있다. DDS는 다른 미들웨어와는 달리 다양한 QoS(Quality of Service) 설정과 보안 기능이 내재되어 있다는 특징이 있다. 그러나 보안이 적용된 DDS에도 취약점이 존재하는 것으로 알려져 있다. 개체 간 통신을 하기 전에 상호 간 탐색과 인증, 정보 교환을 수행하는 Discovery 단계에서 각 개체의 권한 파일이 평문으로 노출되는 것이 기존 연구에서 발표되었다. 권한 파일을 이용해 공격자는 시스템의 구조를 파악하고, 공격 계획을 수립할 수 있다. 본 논문에서는 DDS의 개념과 DDS의 보안 기능인 DDS Security, 그리고 Discovery 과정에 대해 살펴본다. 또한 기존 연구에서 발표된 Discovery 단계에서의 취약점에 대해 알아보고 가상환경에서 직접 실험을 진행해 위험성을 파악한다. 더불어 해당 취약점에 대한 대응 방법을 제시한다.

Ⅰ. 서 론

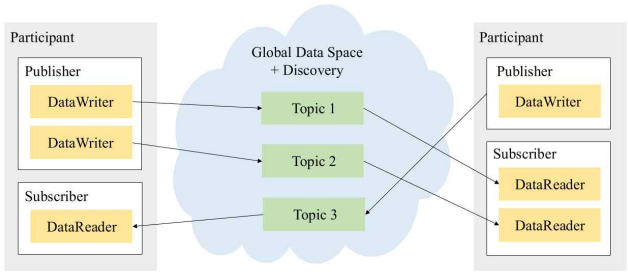
Data Distribution Service (DDS)는 분산 시스템 환경에서 개체 간 통신을 도와주는 산업 표준 통신 미들웨어이다 [1]. 메시지를 통해 데이터를 교환할 수 있게 하여 메시징 프로토콜이라고도 한다. 기존 Client-Server 방식과는 다르게 Publish-Subscribe 구조로 구성되어 개체 간 의존성을 낮춰준다. DDS에는 개체 인증과 암호화, 권한 부여 등의 기능을 제공해주는 DDS Security가 존재한다. DDS를 미들웨어로 사용하는 애플리케이션은 DDS Security 기능을 이용해 안전한 통신을 할 수 있다. 그러나 DDS Security 기능을 적용해도 여전히 보안 취약점이 존재한다는 것이 발견되었다 [2]. 개체 간 데이터 통신을 수행하기 전에 서로를 인지하고 정보를 교환하는 Discovery 과정에서, 각 개체의 접근 권한 파일이 데이터 패킷에 평문으로 노출된다. 해당 파일은 시스템 구조에 대해 알지 못하는 공격자로 하여금 그 구조를 파악할 수 있게 하고, 취약한 부분을 인지할 수 있게 해 공격자는 구체적인 공격 계획을 수립할 수 있다.

본 논문에서는 DDS의 개념과 구조를 살펴보고, DDS Security에 대해서 알아본다. 또한 취약점이 존재하는 Discovery 과정에 대해 직접 실험을 진행해 살펴보고 대응 방법을 제시한다.

Ⅱ. 본론

2.1 Data Distribution Service (DDS)

Data Distribution Service (DDS)는 국제 표준화 기구인 Object Management Group (OMG)에서 표준화한 산업 표준 통신 미들웨어로, 군사, 의료, 로봇 등의 분산 시스템 환경에서 사용되고 있다. DDS는 메시지를 발행(Publish) 혹은 구독(Subscribe)하는 Publish-Subscribe 구조로 구성되어 있다. 전통적인 Client-Server 방식은 Client가 Server에게 요청하고 응답이 올 때까지 기다려야 되지만, Publish-Subscribe 구조는 서로 간의 직접적인 연결 없이 메시지를 발행 및 구독하여 여러 개체가 한 번에



〔그림 1〕 DDS 구조

통신을 수행할 수 있다. 이는 시스템의 효율을 향상시켜 실시간 처리와 대용량 데이터 트래픽이 오가는 분산 시스템 환경에 매우 적합하다.

DDS는 [그림 1]과 같이 구성되어 있다. Participant는 통신에 참여하는 개체로 특정 Topic에 대해 발행 및 구독을 수행하며 통신한다. Participant는 여러 개의 Publisher와 Subscriber를 가질 수 있고, 그 안에는 DataWriter와 DataReader로 세분화되어 있다. 실질적으로 통신을 수행하는 개체는 DataWriter와 DataReader로 볼 수 있다. 각 Participant는 Global Data Space라는 전역 공간에 Topic을 올려 통신한다. Global Data Space는 Domain이라고도 하며, 데이터를 주고받기 위한 논리적인 공간이다. 같은 Domain 영역에 있는 Participant들끼리만 통신할 수 있다.

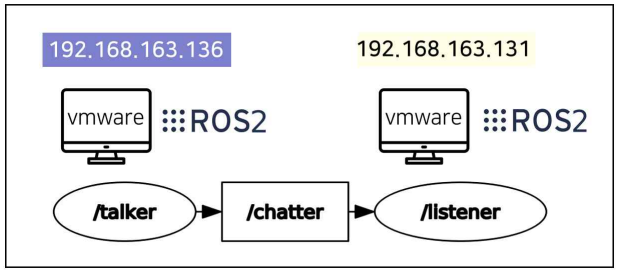
2.2 DDS Security

DDS Security는 DDS에 내재되어 있는 보안 기능이다. DDS Security는 Authentication, Access Control, Cryptography, Logging, Data tagging의 5가지 기능을 제공해 안전한 통신을 가능하게 한다. 그러나 DDS의 Default 상태는 Security 기능이 비활성화되어 있다. 보안 기능을 적용하기 위해서는 DDS Security를 활성화해 줘야 한다.

DDS Security는 두 개의 인증기관 (Certificate Authority, CA)과 두 개의 정책 파일로 구성되어 개체 인증과 접근 제어를 시행한다. CA는

구분	종류
Host OS	Windows 11
Virtual Machine	Linux Mint 20.1
Middleware	Robot Operating System2 (ROS2) Foxy
Traffic Capture	Wireshark

〔표 1〕 실험 환경 구성



〔그림 2〕 ROS2 시스템 구조

Identity CA와 Permissions CA가 존재한다. Identity CA는 각 Participant에게 X.509 인증서를 발급해주고, Permissions CA는 정책 파일에 디지털 서명을 생성한다. 정책 파일은 Governance Policy 파일과 Permissions Policy 파일이 존재한다. Governance Policy 파일은 Domain과 Topic에 대한 접근 제어 파일이고, Permissions Policy 파일은 Participant에 대한 접근 제어 파일이다. Permissions Policy 파일을 통해 각 Participant가 어떤 Topic을 구독하고 발행하는지 알 수 있다.

2.3 DDS Discovery

DDS Discovery는 각 Participant가 서로를 탐색할 수 있게 해주는 기능이다. 메시지 통신을 하기 전에 서로의 존재를 인식하고 자신의 정보를 교환하는 단계라고 볼 수 있다. DDS Discovery는 다음과 같이 세 단계로 이루어진다.

① Simple Participant Discovery Protocol (SPDP)

Participant 간에 서로를 인지하는 단계이다. 멀티캐스트로 자신의 IP 주소와 포트 번호 등을 보내 자신의 존재를 네트워크에 주기적으로 알린다.

② 3-way Handshake

질의-응답 (Challenge-Response) 방식으로 개체 인증을 수행한다. 이 과정은 DDS Security가 활성화되지 않았다면 이루어지지 않는다.

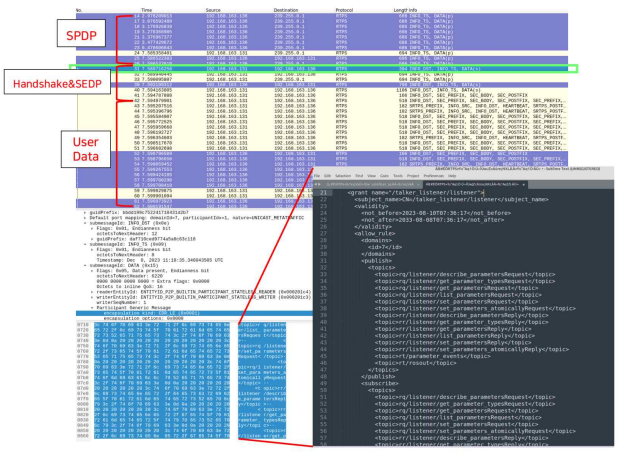
③ Simple Endpoint Discovery Protocol (SEDP)

SPDP에서 얻은 주소 정보를 이용하여 실질적으로 통신을 수행하는 개체인 Endpoint의 정보를 주고받고, 매칭되는 Endpoint를 찾아 서로의 Topic, Data type, QoS 등의 정보를 주고받는 단계이다.

두 번째 단계인 3-way Handshake에서 개체 인증 시 인증서 등과 함께 Permissions Policy 파일이 전송되는데, 이때 Permissions Policy 파일이 데이터 트래픽에 평문으로 노출되는 현상이 발생한다. 공격자가 네트워크를 스니핑하고 있는 상태에서 해당 데이터 패킷을 발견하게 된다면, 노출된 파일을 이용해 타겟 시스템의 구조를 파악할 수 있다.

2.4 평가

해당 취약점을 확인하기 위해 가상환경 위에서 실험을 진행하였다. 실험 환경 구성은 [표 1]과 같다. 두 개의 가상환경에 Linux를 설치하고, DDS를 미들웨어로 사용하고 있는 Robot Operating System2 (ROS2)를 설치하여 Wireshark로 패킷을 캡쳐하였다. 두 가상환경은 같은 네트워크 대역에 존재한다. ROS2 시스템 구조는 [그림 2]와 같다. talker는 Publisher이



〔그림 3〕 DDS Discovery 단계 Wireshark 캡쳐

고, listener는 Subscriber이며 “/chatter”라는 Topic에 대해 통신한다. [그림 3]은 DDS Security를 활성화한 상태에서 두 개체 간의 통신 트래픽을 Wiershark로 확인한 모습이다. Discovery 과정인 SPDP, 3-way Handshake, SEDP의 패킷들이 캡쳐된 모습을 볼 수 있고, 이 중 3-way Handshake 패킷에서 Permissions Policy 파일이 평문 상태로 전송되는 것을 확인할 수 있다. 공격자는 해당 파일을 이용해 네트워크 토폴로지를 형성하여 시스템 구조를 파악할 수 있고, 타겟을 정해 DoS Attack 등의 공격 계획을 세울 수 있다.

2.5 대응 방법

Permissions Policy 파일은 한 개체가 발행 및 구독하는 모든 Topic의 정보가 기술되어 있기 때문에, 최소 권한의 원칙을 위반한다는 특징이 있다. 즉 통신에 참여하는 상대방의 모든 발행 및 구독 정보를 알 수 있다는 것이다. 필요한 것 이상의 정보를 노출하지 않으면서 접근 제어를 수행한다면 Permissions Policy 파일이 평문으로 전송되어도 시스템 구조에 대해 쉽게 파악할 수 없을 것이다.

Ⅲ. 결론

DDS의 내재된 보안 기능은 다른 미들웨어 프로토콜과 비교되는 강력한 장점으로 꼽힌다. 그러나 보안을 적용한 DDS에도 지속적으로 새로운 취약점이 발견되고 있다. 분산 시스템 환경은 앞으로도 더욱 늘어날 것이며 DDS를 도입하는 애플리케이션도 다양해질 것이다. 증가하는 수요와 점점 중요해지는 역할에 대응하여 취약점을 해결할 수 있는 방법을 찾아야 할 것이다.

ACKNOWLEDGMENT

이 논문은 2023년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0023522, 2023년 산업혁신인재성장 지원사업)

참 고 문 헌

[1] “OMG Data Distribution Service (DDS)”, Object Management Group, 2015.

[2] White, Ruffin, et al. "Network reconnaissance and vulnerability excavation of secure DDS systems." 2019 IEEE European symposium on security and privacy workshops (EUROS&PW). IEEE, 2019.