정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

ROS2 공격 기술 동향 분석

허 재 웅*, 이 예 지**, 조 효 진*

요 약

Industry 4.0의 진행으로 이기종의 IoT 장비들 간의 통신을 위해 다양한 산업용 통신 미들웨어들이 등장했다. 그 중 Robotics 분야에서 활발히 사용되는 Robot Operating System (ROS)는 개발자 커뮤니티와 로봇 개발 도구들을 기반으로 지속적인 시장 점유율 증가세를 보이고 있다. 초기 발표된 ROS1의 경우 보안이 전혀 고려되지 않은 설계로 Packet Injection 공격등의 사이버 보안 위협에 취약했지만, ROS2의 경우 통신 미들웨어인 Data Distribution Service (DDS) 통신 규격을 전송 계층에 적용하여 메시지 전송에 대한 보안 기능을 제공하고 있다. 그러나 최근 연구에서는 DDS와 관련된 ROS2 취약점이 발표되고 있다. 따라서 본 논문에서는 DDS와 관련된 ROS2의 공격 기술 동향을 소개한다.

Ⅰ. 서 론

Industry 4.0 환경에서는 스마트 팩토리를 필두로 다양한 산업분야에서 최신 IT 기술이 적용된 자동화가 이루어지고 있다. 이 과정에서 다양한 IoT 장비 제조사에 의해 만들어진 IoT 장비들 간의 원활한 통신을 위해 표준화된 통신 미들웨어 기술들이 표준화 되고 있다. 특히, 산업용 통신 미들웨어 기술은 대부분 이더넷 기반 프로토콜이며 데이터 통신 과정에서 실시간성, 확장성, 상호 운용성 등의 특징을 갖는 것을 주요 목적으로 한다[1]. 산업용 통신 미들웨어 프로토콜은 목적에 따라 여러 표준 및 오픈소스의 형태로 발표되었으며 종류로는 Open Platform Communications Unified Architecture (OPC UA), Message Queueing Telemetry Transport (MQTT), Robot Operating System (ROS), Data Distribution Service (DDS) 등이 있다[2][3].

특히, ROS는 로봇 개발을 위한 도구로서 개발자 커뮤니티를 기반으로 시장 점유율 증가를 보이고 있다[4]. ROS는 각종 이기종 기기들의 통신을 위해 호스트 운영체제 위에 구조화된 통신 계층을 기반으로하며, package, build, launch 등 로봇 프로그래밍을 위한 각종 기능을 제공한다[5]. 하지만 초기 ROS 버전에 해당하는 ROS1의 경우 보안을 고려하지 않은 설계로 인해 ROS1에 대한 각종 해킹 연구들이 발표되었다[6].

ROS2에서는 산업현장에서 많이 사용되는 통신 미들웨어 기술인 DDS 프로토콜을 기존 ROS1 내 전송 계층에 적용하여 ROS1의 보안 모듈 부재 문제는 해결하였다. 하지만, 최근 연구에서는 ROS2 내 DDS 통신 관련 취약점이 발표되고 있다. 따라서 본 논문에서는 ROS2에 적용된 DDS 통신 대상 공격 기술 동향에 대해 소개한다.

본 논문의 구성은 다음과 같다. 2장에서는 ROS2 공격 이해를 위한 배경지식을 다루고, 3장에서는 ROS2 공격 기술 동향에 대해 소개한다. 마지막으로 4장에서는 결론을 맺는다.

Ⅱ. 배경지식

2.1. ROS 메시지

ROS는 사용자들의 재사용성을 극대화하기 위해 그 목적에 따라 세분화된 최소 실행 프로그램인 노드의 형태로 개발되며, 각각의 노드와 노드는 메시지를 통해 데이터를 주고받으며 하나의 커다란 프로그램이 된다. 이러한 메시지 통신에는 Topic, Service, Action의 세 가지 방식이 있다.

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.00218853, 안전한 스마트홈 IoT 서비스를 위한 취약점 모니터링 연구)
* 숭실대학교 소프트웨어학과 (대학원생, wkdgjwodnd26@gmail.com; 조교수, hyojin.jo@ssu.ac.kr))
** 서울여자대학교 정보보호학과 (학부생, rubyzxc@naver.com)

(1) Topic

Topic 메시지 통신은 정보를 송신하는 Publisher와 정보를 수신하는 Subscriber가 Topic 메시지 형태로 정보를 송수신하는 것이다. 토픽을 수신받기 원하는 Subscriber가 노드는 ROS master에 등록된 Topic 이름에 해당하는 Publisher 정보를 받고, Subscriber가 노드는 Publisher 노드와 직접 연결하여 메시지를 송수신한다.

(2) Service

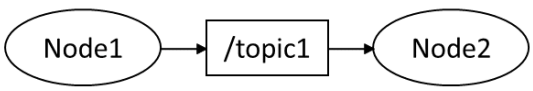
Service 메시지 통신은 서비스를 요청하는 서비스 클라이언트와 서비스 응답을 담당하는 서비스 서버간의 동기적 양방향 서비스 통신이다. 요청이 있을 때만 응답하는 서비스 서버와 요청하고 응답받는 서비스 클라이언트로 나뉘며, Topic과는 달리 일회성 메시지 통신이다. 따라서 Service의 요청과 응답이 완료되면 연결된 두 노드의 접속이 끊기게 된다.

(3) Action

Action 메시지 통신은 요청 처리 후 응답까지 오랜 시간이 걸리고 중간 결과값이 필요한 경우 사용되는 메시지 통신 방식이다. 서비스와 차이점인 피드백은 액션 클라이언트와 액션 서버간의 비동기식 양방향 메시지 통신을 수행한다. 피드백을 통해 목표값 전달 후에도 임의의 시점에서 목표를 취소하는 명령어를 전달 가능하다.

2.2. ROS 통신 구조

ROS는 특정 기능을 수행하는 독립된 프로세스인 노드를 기반으로 하는 통신구조를 갖고 있으며, 노드 간 통신 시 publish-subscribe 모드로 데이터를 송/수신한다. 그림 1과 같이 각 프로세스에 해당하는 노드들 간에 토픽, 서비스, 액션 형태의 메세지가 교환되는 형식으로 동작한다. ROS는 버전에 각각의 고유한 데이터 처리 방식을 갖는데, ROS1에서는 XMLRPC/TCPROS 통신을, ROS2에서는 DDS 통신을 사용한다.

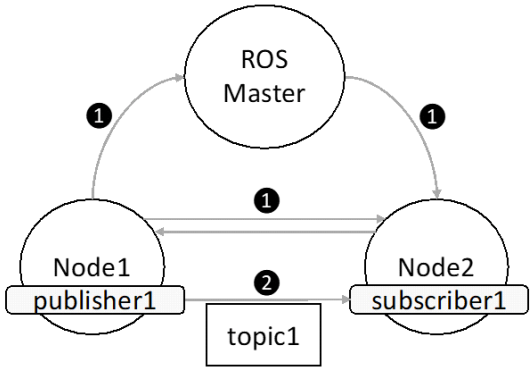


〔그림 1〕 노드 2개의 토픽 통신 rqt_graph

(1) ROS1 - XMLRPC/TCPROS 통신

ROS1의 경우 ROS Master가 ROS 노드들 간의 모든 통신을 중앙에서 제어하게 됨으로 그림 2와 같은 통신 구조를 갖는다. 그림 2의 ❶ 과정에서 ROS Master는 XMLRPC API를 통해 노드들 간의 publish/subscribe 관계를 파악하고, 각 노드들에게 대응되는 노드의 정보를 알린다. 이를 기반으로 ❷과정에서 노드들 간의 연결이 수립되어 TCPROS로 통신을 수행하며 이는 서버-클라이언트 구조와 유사하다.

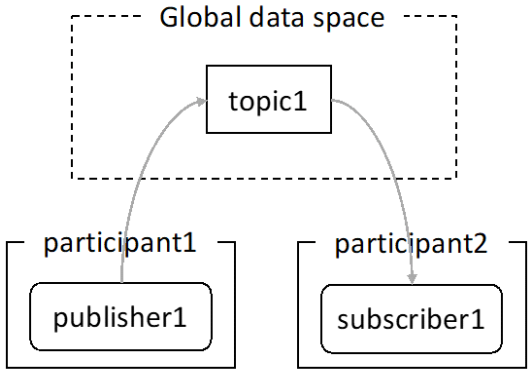
이와 같이 ROS1은 모든 노드들이 마스터 노드를 통해서 통신을 하기 때문에 분산 로봇 환경인 Multi-Robot System (MRS) 시스템에 부적합 하다. 특히, ROS Master에 문제가 생길 경우 모든 ROS 노드들 간의 통신이 불가능한 Single Point of Failure 문제가 존재하고, ROS1의 보안 기술 부재로 인한 메시지 인증, 암호화, 접근 제어 등의 보안을 제공하지 못한다는 특징을 갖는다.



〔그림 2〕 ROSXMLRPC/TCPROS통신

(2) ROS2 - DDS(RTPS) 통신

ROS2에서는 산업용 통신 프로토콜로서 확장성과 보안성을 강화하기 위해 DDS를 전송 계층에 포함하였다. DDS는 OMG(Object Management Group)에서 발표한 표준이며, 전송 계층에 RTPS(Real Time Publish Subscribe)가 적용되어 있다[7],[8]. 또한, DDS 기술을 구현하고 서비스하는 복수의 서비스 업



〔그림 3〕 ROS2DDS/RTPS 통신

체들이 다양한 개발 언어로 구현된 DDS 서비스를 API 형태로 제공하기 때문에, ROS2의 DDS 기술을 구현할 때 다양한 API 중에서 선택하는 것이 가능하다[9].

ROS2의 노드 간 통신 구조가 DDS 통신으로 전화하기 위해서는, 첫째 ROS Client Library (RCL)에 의해 노드 기반 통신 구조가 생성되어야 하고, 둘째 ROS Middleware(RMW)는 ROS 통신 구조에 따른 DDS 구조 및 파라미터를 설정하여 DDS API를 호출한 후, DDS API가 DDS System 구조를 구성하는 단계로 이뤄진다. 그림 3과 같이 ROS2의 통신에서는 DDS System 구조에서 노드 내에 실제 통신을 수행하는 publisher 및 subscriber가 participant들로 구성되어 Global data space 내의 데이터를 주고 받는다.

2.3. SROS2

Secure ROS2 (SROS2)는 ROS2 내에 수행되는 DDS 관련 보안 기능을 아우르고 있으며, RCL코드 혹은 SROS2 cli를 통해 SROS2를 설정 가능하다. 일반적으로 DDS는 아래와 같이 다섯 가지 보안 기능을 제공한다 [10].

- Authentication
- Access control
- Cryptography
- Logging
- Data tagging

이 중 ROS2에서 SROS2 형태로 제공되는 기능은 총 3가지인 Authentication, Access control, 그리고 Cryptography이다[11].

Ⅲ. ROS2 공격 동향

3.1. DDS 구현 소프트웨어 공격

Blackhat Europe 2021에서 발표된 T.Yen 등의 연구 및 Trend Micro report에서는 DDS 구현 소프트웨어에 존재하는 13개의 취약점들이 발표되었다[12,13]. ROS2 내에 DDS가 통신 미들웨어로 내장되어 있으므로, 본 연구에서 발견된 모든 취약점들은 ROS2와 연관성이 있다.

(1) Fuzzing 기반 취약점 분석

해당 연구의 취약점 분석 대상은 각종 DDS 서비스 업체들이 제작한 API로 OpenDDS, RTI ConnextDDS 등의 소스코드였다. 표 1은 분석대상에 대한 정보를 보여주고 있다.

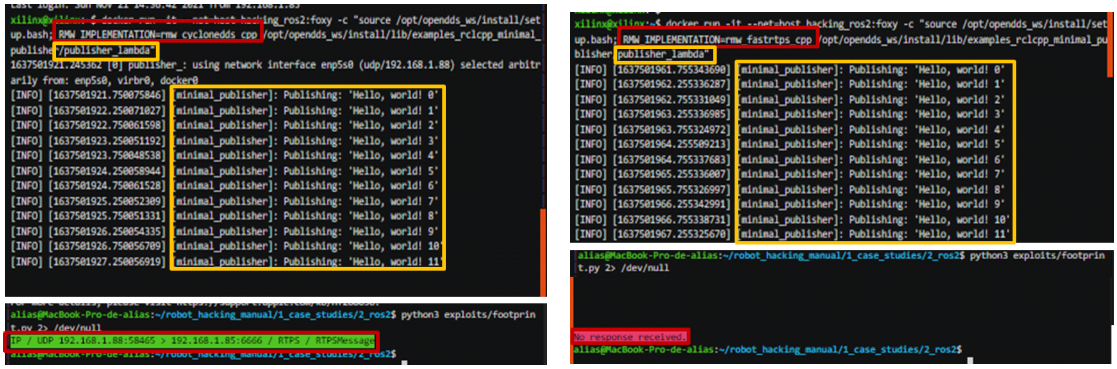
분석자들은 RTPS 패킷, XML 파일 기반 환경설정 등의 DDS 동작 원리에 대한 이해를 기반으로 Fuzzing 기법을 이용한 취약점 분석을 진행했다. 특히 본 연구에서 RTPS 네트워크 패킷을 분해 및 제작하는 기능을 오픈소스인 scapy 내에 구현하여 취약점 분석 및 공격을 진행하였다.

〔표 1〕 ROS2 대상 공격 기법 분석

Targets	Developer	Open Source
Fast-DDS	eProsima	Apache License 2.0
Cyclone DDS	Eclipse Foundation	Eclipse Public License
OpenDDS	OCI	Custom
Context DDS	RTI	Extensions are open soucre
CoreDX DDS	TwinOaks	Not open source
Gurum DDS	Gurum Networks	Not open source

(2) 취약점

본 연구에서 발표된 취약점은 DDS 표준을 구현한 여러 DDS 서비스 업체의 소프트웨어 취약점에 해당한다. 취약점은 RTPS 패킷 관련 오동작 및 정보유출로 이어질 수 있는 취약점과 XML 파일 관련 취약점에 해당하며, Reflection 공격, Buffer Overflow 공격



〔그림 4〕 DDS 서비스에 대한 Reconnaissance 공격 예시〔12〕(좌: Cyclone DDS, 우: FastRTPS)

등으로 이어질 수 있다.

(3) ROS2 대상 공격

본 연구팀이 발견한 DDS 취약점은 ROS2 시스템 내 특정 노드를 대상으로 reconnaissance, reflection attack, node crashing 공격을 수행할 수 있음을 확인되었다.

Reconnaissance 공격의 경우, 공격 목표와 표적을 조사하고 식별하기 위한 과정으로 정의되며 사이버 킬 체인 단계중 하나이다. ROS2를 사용하는 서비스에 대한 Reconnaissance 공격을 수행하기 위해서는, DDS에서 제공되는 discovery 메시지를 이용할 수 있다. 예를 들어 각 DDS 서비스 제공 업체들이 제공하는 API에서 사용되는 discovery 요청 메시지를 ROS2 노드에 보내고, 이에 대한 응답이 있다면 해당 DDS 서비스 API를 사용하는 노드임을 식별할 수 있다. 그림 4는 Cyclone DDS 서비스에 대한 Reconnaissance 공격 성공과 FastRTPS 서비스에 대한 Reconnaissance 공격 실패 사례를 보여준다.

Reflection attack의 경우 OMG의 RTPS 스펙에 정의된 multicast interaction 관련 파라미터 내에 IP 주소 관련 화이트리스트가 없는 것을 이용한 공격이다. 공격자가 RTPS 내 IP 파라미터에 대량의 악성 트래픽을 전송할 수 있는 서버 주소를 설정하면 reflection 공격으로 이어질 수 있다.

Node crashing의 경우 OpenDDS 구현에서 RTPS 패킷 내 QoS 관련 파라미터 길이를 제대로 체크하지 않는 것을 이용한 공격이다. 따라서 해당 공격이 발생될 경우 ROS2 노드는 memory corruption이 발생하게 되어 강제 종료된다.

3.2. ROS2 DDS 통신 프로토콜 공격

ACM CCS 2022에 발표된 G.Deng 등의 연구에서는 Model Checking을 이용한 ROS2 취약점 분석 방법론이 제시되었고, 이를 통해 4개의 취약점을 발견하였다[14]. 해당 연구에서 발견된 취약점은 ROS2의 노드 간 통신을 수행하는 DDS 관련 코드 상에 존재하며, SROS2가 적용된 ROS2 시스템에도 해당 취약점을 이용한 공격이 가능하다.

(1) Model Checking 기반 취약점 분석

해당 연구에서 취약점 분석 대상은 ROS2 내 DDS 통신 관련 코드에 해당하는 RCL, RMW 소스코드였다. G.Deng 등은 Model Checking 기법을 ROS2 통신 코드에 적용하여 취약점 분석을 진행했고, ROS2 내 통신 관련 주체인 ROS2 Node, Participant, system owner 사이의 상호작용을 구체화하여 함수 호출 그래프에 대한 Model을 만들었다. 또한, ROS2 공식 문서를 기반으로 표 2와 같은 6개의 보안 요구사항을 제안하였다. 해당 연구에서는 ROS2 Node, Participant, system owner 사이의 상호작용에 대한 Model과 표 2에 명시된 6개의 보안 요구사항을 기준으로 Model Checking을 수행 하였고, 4가지의 취약점을 발견했다.

〔표 2〕 ROS2 보안요구사항〔14〕

Security Requirements	Description
R1	시스템 내 각 노드는 최소 하나의 토픽에 대해 publish 혹은 subscribe하기 위한 access control rules을 가져야 한다

Security Requirements	Description
R2	각 토픽은 최소 한 개 이상의 노드에 의해 publish되거나, subscribe되어야 한다
R3	참여자에 의해 publish된 메시지에 대한 access control rules는 시스템 소유자에 의해 선언된 것과 같아야 한다.
R4	참여자의 메시지 subscription에 대한 access control rules는 시스템 소유자에 의해 선언된 것과 같아야 한다.
R5	참여자 i는 j토픽 채널의 버퍼가 채워지지 않고, j 토픽 발행하는 publisher i가 1개일 때만 토픽 j를 publish하는 것이 가능하다.
R6	노드 i가 토픽 j를 합법적으로 subscribe할 때, 해당 노드는 합법적인 노드로부터 발행된 해당 j 토픽만 전송 받을 수 있다.

(2) 취약점

해당 연구에서 발견된 취약점은 V1:Permission File Replacement, V2: Outdated Node Service, V3:Default Mis-configuration, V4:Permission File Inference이고, 자세한 내용은 표 3과 같다.

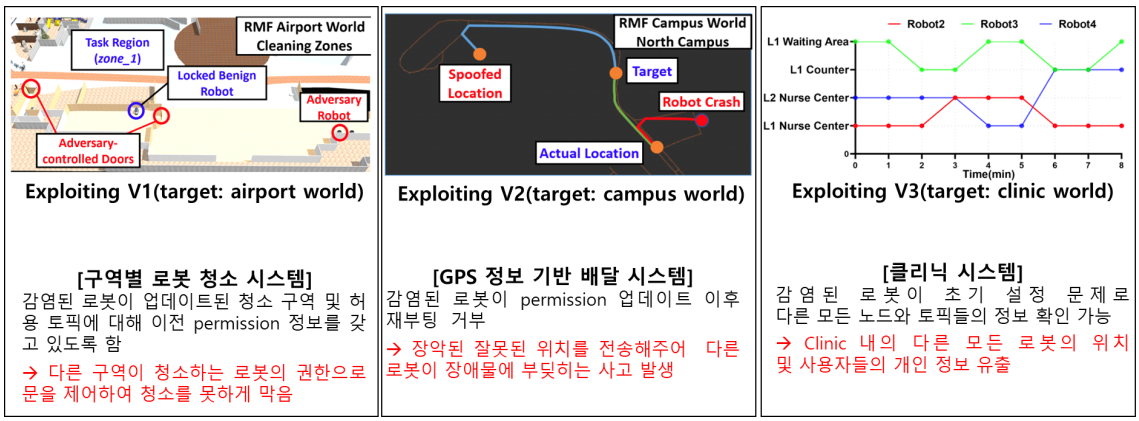
V1과 V2의 경우 ROS2의 설계 상 결함으로 SROS2 내부 레이어들 간의 access control 정책 동기화 실패를 야기하는 취약점이며, V3과 V4의 경우 기본 환경설정 파일 셋팅 및 사용자의 파일 권한 설정 문제를 이유로 발생하는 취약점이다.

〔표 3〕 Model Checking〔14〕을 통해 발견된 취약점 4개

Vulnerabilities	Violation of Security Requirements	Root Causes
V1 (Permission File Replacement)	R3, R4	ROS2 design flow (SROS2 내부레이어들 간의 accesscontrol 정책 동기화 실패)
V2 (Outdated Node Service)	R3, R4	
V3 (Default Mis-configuration)	R6	Default Mis-configuration
V4 (Permission File Inference)	-	Permission 파일에 least privilege 원칙 미적용

(3) ROS2 공격 시나리오

취약점은 SROS2로 보안조치된 오픈소스 MRS 대상 공격으로 이어질 수 있음이 확인되었다. MRS 내 하나의 로봇에 대한 full control 권한을 획득한 공격자는 Airport, Campus, Clinic Center 내에서 access 권한 정보 업데이트를 거부하여 시스템에서 부여한 권한 외의 동작을 하거나, 다른 로봇에게만 권한이 부여된 토픽 및 노드들의 정보를 얻을 수 있다. 자세한 공격 사례에 대한 설명은 그림 5와 같다.



〔그림 5〕 ROS2 공격 시나리오〔14〕

3.3. ROS2 취약점 정리

본 논문에서 다룬 ROS2의 취약점은 ROS2에서 사용하고 있는 통신 모듈인 DDS와 관련된 취약점으로 ROS2뿐만 아니라 DDS를 사용하고 있는 산업환경에도 적용가능한 취약점이다. 본 논문에서 소개한 취약점에 대한 요약은 표 4와 같다.

〔표 4〕 ROS2 취약점 정리

	T.Yen 등의 연구 〔12〕	G.Deng등의 연구 〔14〕
분석 대상 SW	OpenDDS, RTI ConnextDDS, Gurum DDS, CycloneDDS, eProsima FastDDS, …	RMW, RCL of ROS2
취약점 분석 기법	Fuzzing	Model Checking
취약점 종류	소프트웨어 취약점	프로토콜 취약점

Ⅳ. 결 론

본 논문에서는 ROS2 대상 공격 기술의 동향에 대해 알아보았다. 보안 기술의 부재로 인한 ROS1 공격 기술들과 달리, ROS2 공격은 DDS 프로토콜 구현에서 발생하는 취약점을 이용하기 때문에 ROS2 기반의 다양한 서비스가 공격 대상이 될 수 있다. ROS2 환경에 대한 보안을 높이기 위해서는 ROS2를 구성하고 있는 다양한 모듈에 대한 취약점 분석 및 이에 대한 보안 기술연구가 필요하다.

참 고 문 헌

[1] 박정민, 고동범, 김정준, “고신뢰 스마트팩토리를 위한 자율컴퓨팅 기술”, *한국통신학회*, 33(11), pp. 16-22, 2016년 10월

[2] OPC UA, https://opcfoundation.org/about/opc-technologies/opc-ua/

[3] S.Profanter, A.Tekat, K.Dorofeev, M.Rickert, A.Knoll, “OPC UA versus ROS, DDS, and MQTT: Performance Evaluation of Industry 4.0 Protocols”, *IEEE International Conference on Industrial Technology*, pp.955-962, Feb. 2019

[4] ROS Based Robot Market by Robot Type and by Application – Global Opportunity Analysis and Industry Forecast 2022-2030

[5] M.Quigley, B.Gerkey, K.Conley, J.Faust T.Foote, J.Leibs, E.Berger, R.Wheeler, “ROS: An open-source robot operating system”, *Workshops at the IEEE International Conference on Robotics and Automation*, May. 2009

[6] J.McClean, C.Stull, C.Farrar, D.Mascareñas, “A preliminary cyber-physical security assessment of the Robot Operating System(ROS)”, *Proceedings of the SPIE- The International Society for Optical Engineering,* May. 2013

[7] “Data Distribution Service”, OMG1.4, Mar 2015

[8] “DDS Interoperability Wire Protocol“, OMG2.3, Apr 2022

[9] https://docs.ros.org/en/foxy/Concepts/About-Different-Middleware-Vendors.html

[10] "DDS Security", OMG1.1, Jul 2018

[11] https://canonical.com/blog/what-is-sros-2

[12] T.Yen, F.Maggi, E.Boasson, V.Mayoral-vilches, M.Cheng, P.Kuo, C.Toyama, “The Data Distribution Service (DDS) Protocol is Critical: Let’s Use it Securely!,” *Black Hat Europe,* Nov 2021

[13] F.Maggi, R.Vosseler, M.Cheng, P.Kuo, C.Toyama, T.Yen, E.Boasson V.Vilches, “A Security Analysis of the Data Distribution Service (DDS) Protocol”, *Trend Micro Research,* Apr 2022

[14] G.Deng, G.Xu, Y.Zhou, T.Zhang, Y.Liu, ”On the (In)Security of Secure ROS2“, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security,*pp.739-753, Nov. 2022

〈저 자 소 개〉

허 재 웅 (Jaewoong Heo)

2021년 2월 : 한림대학교 융합소프트웨어학과 졸업
2021년 9월 : 숭실대학교 정보보호대학원 소프트웨어학과 석사 과정
<관심분야> 자동차 보안, ROS 보안, IoT 보안

이 예 지 (Lee Yeji)

2020년 3월 : 서울여자대학교 정보보호학과 학사 과정
<관심분야> 자동차 보안, ROS 보안, IoT 보안

조 효 진 (Hyo Jin Jo)

종신회원

2009년 2월 : 고려대학교 산업공학과 졸업
2016년 2월 : 고려대학교 정보보호대학원 정보보호학과 박사
2016년 6월~2018 8월 : University of Pennsylvania 박사 후 연구원
2018년 9월~2020년 8월 : 한림대학교 소프트웨어융합대학 조교수
2020년 9월~현재 : 숭실대학교 소프트웨어학과 조교수
<관심분야> 자동차 보안, IoT 보안, 프라이버시