

探秘 ROS 安全系列（二）

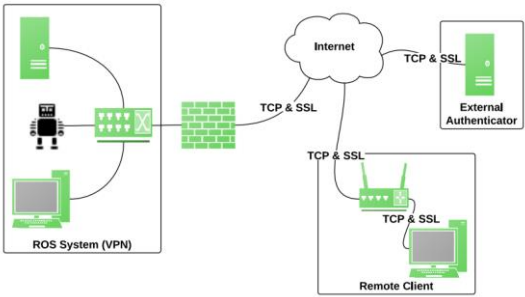
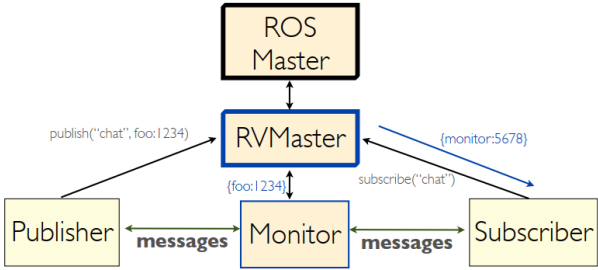
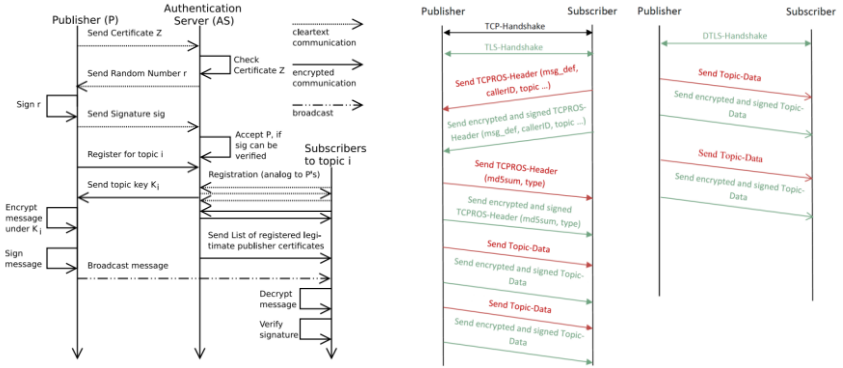
机器人操作系统 ROS 安全方案及趋势

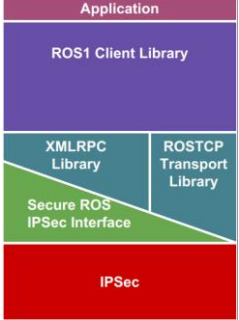
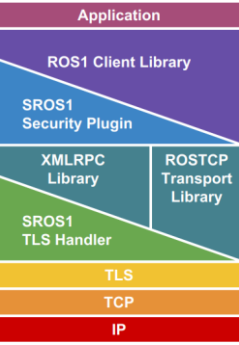
1. ROS 安全方案	2
1.1. ROS 1.0 安全方案	2
1.2. ROS 2.0 安全方案	3
2. 机器人安全趋势	4
2.1. 安全标准	4
2.2. 安全方案	5

1. ROS 安全方案

1.1. ROS 1.0 安全方案

在上一期文章中，我们介绍了 ROS 安全研究的多个阶段。在第二阶段，ROS 1.0 的安全风险充分暴露，业界涌现了众多安全方案，主要解决身份认证、加密通信、访问控制等风险。在各方案中，SROS 安全特性相对全面，同时具备较好的易用性（部署工具/脚本），是 ROS 社区推荐方案。（需要说明的是，因 ROS 本身演进规划，ROS 1.0 无官方安全方案。ROS 社区未来更多聚焦在 ROS 2.0）

方案	特点	架构图
rosauth	<p>【目的】解决远程客户端访问 ROS 身份认证问题</p> <p>【实现】ROS 系统运行在隔离网络域内；远程客户端在通过 SSL 在外部 Authenticator 进行身份鉴权并获取 token；远程客户端使用 token，通过 SSL 访问 ROS；ROS 校验 token，允许或拒绝访问。</p> <p>【不足】未解决身份认证后的 Authorization 问题</p>	
ROSRV	<p>【目的】实现 ROS 通信实时监控管理</p> <p>【实现】ROS Runtime Verification 使用 Man-in-the-Middle 技术，通过增加 RVMaster 节点，实时监控 ROS 1.0 内部消息，同时可配置访问控制策略进行访问控制。</p> <p>【不足】访问控制基于 IP，RVMaster 中心化设计在节点数过多时的 scalability 问题</p>	
Secure ROS Transport	<p>【目的】解决 ROS 通信安全与访问控制</p> <p>【方案 1】应用层方案，使用外部 Authentication Server 实现 publisher-subscriber 之间的身份认证与加密通信。优点是无需改动 ROS，缺点是应用层实现，无法阻止类似 DoS 攻击。</p> <p>【方案 2】通信层方案，使用证书+TLS 解决节点间身份认证、加密通信、访问控制问题。缺点是没有解决 master 节点安全问题。</p>	

Secure ROS	<p>【目的】解决 ROS 通信安全与访问控制</p> <p>【方案】基于 IPSec 实现身份认证与加密通信，使用系统配置文件实现集中式访问控制。优点是安装方便，不足是访问控制等基于 IP 粒度。</p>	
SROS	<p>【目的】解决 ROS 通信安全与访问控制</p> <p>【方案】基于 TLS+证书机制解决身份认证、加密通信、访问控制问题。使用经过证书签名的配置文件进行集中式访问控制，细粒度。不足是需要源码安装及相关配置。</p>	

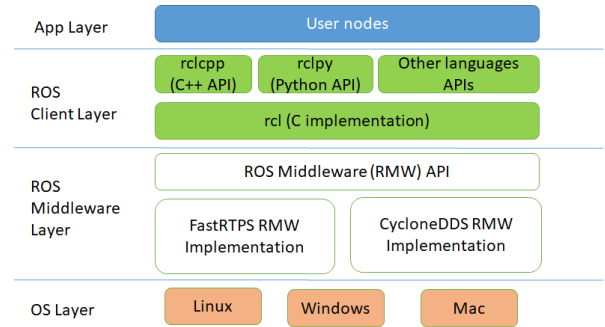
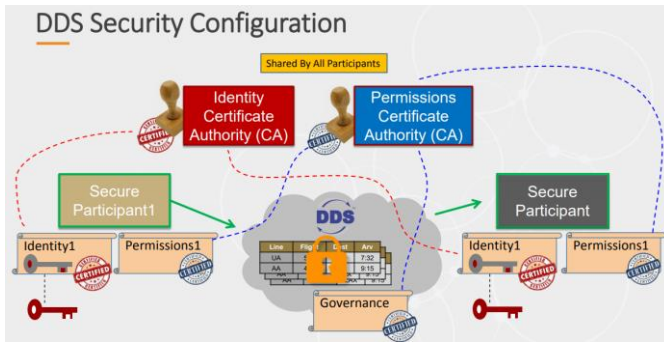
1.2. ROS 2.0 安全方案

ROS 2.0 阶段，因组件 DDS 自带安全特性原因，安全方案有了统一框架，并形成 [SROS 2](#)。命名 SROS 2 是为继承和区分 SROS 方案，但不同于 SROS，SROS2 是 ROS 2 官方标准并集成在主线中。

SROS 2 具体来说，指在 ROS 2 基础上为使能 DDS-Security 所做的特性适配和工具集，故

$$\text{SROS 2} = \text{ROS 2} + \text{DDS-Security Enable}$$

ROS 2 适配修改主要有两个，一个是 RCL (ROS Client Library) 层修改，一个是 SROS 2 utilities 工具集。RCL 修改主要是安全特性开关和策略配置，具体如 `ROS_SECURITY_ENABLE` (true/false)、`ROS_SECURITY_STRATEGY` (Enforce/Permissive)、`ROS_SECURITY_KEYSTORE` (key files directory) 等参数实现和支持。SROS 2 utilities 工具主要解决 PKI 密钥证书和控制策略文件的管理，具体如 CA 和 KEYSTORE 根目录管理、节点公私钥和证书创建部署、访问控制策略文件 (Governance/Permission) 创建部署等。



如上图所示，SROS 2 通过 PKI 机制，解决节点间通信安全，包括身份认证、加密通信；通过策略配置文件（Governance、Permission，证书签名），实现集中式访问控制。

关于访问控制，首先，Governance 文件限制 domain 域的整体访问控制策略，如节点访问控制（是否允许未授权节点访问，是否允许被发现），以及 domain 内部 topic 访问控制（是否允许被发现、是否允许未授权读写）等。其次，每个节点的 Permission 限制自己的访问权限，如是否允许对某 topic 读写。

因 DDS 是标准规范且有开源、商业不同实现，ROS 2 增加了 DDS 抽象适配层 RMW，如上图所示。

2. 机器人安全趋势

ROS 是目前最主流的机器人操作系统框架，ROS 安全经过多年研究和发展，在风险分析和安全方案维度已有不小进步，ROS 2 中已有了基于 DDS 的统一安全框架。但是对于 ROS 甚至整个机器人系统来说，在安全标准与规范、DDS 标准与实现差异、DDS 安全与性能、全系统方案等维度，还有很多工作可以改进。

2.1. 安全标准

自动驾驶领域已经有相对完整、成熟的安全标准，包括功能安全（Functional Safety）标准 ISO 26262、网络安全（Cyber Security）标准 ISO 21434。但在机器人领域，现有工业机器人标准 ISO 10218、ISO 20218、ISO/TS 15066、服务机器人标准 ISO 13482、ISO 23482 等主要面向功能安全，尚无权威的网络安全标准。但是，随着服务机器人应用推广、机器人网络安全研究、及产业联盟的推动，机器人网络安全标准是必然趋势。

2.2. 安全方案

在安全方案维度，针对现有方案的问题或盲点，后续可见的研究趋势有：

一是 DDS 本身的成熟度演进。一方面，当前开源或商业 DDS 实现与 DDS 标准规范还存在差异，例如 DDS-Security 标准规定了 5 大安全特性（Authentication、Access Control、Cryptographic、Logging、Data Tagging），而多数方案仅实现前 3 种强制特性；另一方面，开源 DDS 实现目前还存在性能、稳定性问题，质量成熟度不高。

二是基于 DDS-Security 安全方案的性能调优。一方面，在安全研究第三阶段，已有很多论文对 DDS-Security 方案的性能进行过深入分析，如加密算法对通信性能影响、DDS-Security 使能及 Governance 配置对整体性能影响等，但仍缺乏相对全面、精细的性能调优实践、指导。而 ROS 系统中不同节点、不同消息的安全需求并不完全一致，面向性能优化的安全策略对方案实施有积极意义。另一方面，社区中 DDS-Security 使能对应的 demo 样例相对简单、对应安全文档匮乏，用户学习和配置困难，不利于方案推广。

三是安全研究从 ROS 框架扩展到机器人全系统。在 SROS/SROS2 聚焦解决 ROS 本身安全问题后，作为 ROS 执行环境、存储载体的 Host OS 的安全和风险受到更多关注。例如 SROS 2 中密钥证书默认明文存储在 Host OS 指定目录下，无额外安全措施。业界 libddssec 方案通过 TEE 技术（ARM Trustzone）解决密钥证书安全存储问题，为机器人系统提供了可信计算和可信根能力，提升系统整体安全性。除软硬件安全能力应用外，一些研究倾向借用传统安全方案如 IDS（Intrusion Detection System）部署缓解 Host 风险，一些研究倾向于在机器人全系统中实施零信任方案，如 [Zero Trust in Robotics](#)。