ROS Security WG

SOUTHWEST RESEARCH INSTITUTE®

David Anthony

Distro A. OPSEC #4584

What I’ve Been Working On

- Porting large ROS 1 codebase to ROS 2
  - Runs on multiple ground platforms
  - Large legacy application
  - Still under active development and experimentation
- Investigating using security with ROS 2
- Trying to introduce security practices into development workflow

Example Systems

- Large ground vehicle
  - 6 computers
  - 100+ nodes
  - 500+ topics
  - Multiple DDS domains
  - Need to restrict access between systems and network interfaces
- UAV Swarm
  - Dozens of UAVs with one or more onboard computers
  - One or more ground control stations
  - Need to both isolate and connect UAVs internally and externally

Issues Encountered in Security Deployment

- Security does not integrate well into development workflow
- Command line tools are challenging with complex systems
- Hard to verify system is properly configured
- Note: many of the developers on this project are not security experts and may be new to ROS and robotics

Existing Command Line Tools

- Developer experience
  - Felt like an all or nothing setting. Either everyone is encrypted and connected, or it took a lot of effort to configure
  - Integrating multiple DDS domains was very challenging and involved lots of hand editing of config files
  - Hard to replicate environments and reproduce configurations across a team
  - Hard to verify that the system was configured as expected. Lots of Wireshark time and using system tools to check configuration
  - Integrating into our normal development efforts is going to be tough

Wishlist

- Graphical tool for configuring and inspecting encryption, governance, and policy settings
  - Introspect running system to view security settings
  - Enable developers to easily integrate new code, nodes, and topics into secure system
  - Easily secure existing, unsecure system
- Better integration into our CI/CD pipelines and deployment
  - For example, can all configuration be set through yaml or other files?
  - Less dependence on environment variables so config options are explicitly and programmatically set
- Node introspection
  - Could “ros2 node info” show enclaves and pub/sub settings?
  - Could “ros2 topic info” show encryption setting?
- Key management