ROS2 SECURITY

WORKING GROUP MEETUP

Ray Cole
coleray@amazon.com
Engineer, Amazon

Agenda

1. Introductions
2. Simplifying Security
3. Logging and Auditing
4. Secure Development
5. Learning and Guidelines
6. Amazon’s Plans
7. Future Roadmap

ROS2 Security: Simplify

1. Secure by default
2. “1-click” to secure
3. Introspect and configure
4. Encompass best practices
    a. *File system security*
    b. *Signed configuration*
    c. *Network security*

ROS2 Security: Logging/Auditing

1. DDS-Security logging plugin
2. Pre-defined logging topic
    a. *DDS:Security:LogTopic*
3. Need parity among DDS implementations
4. Bake configuration into RMW
5. On/off-device logging/audit

ROS2 Security: Development

1. Tooling
    a. *Static code analysis*
2. Secure Test-Driven Development
    a. *Security-centric integration tests*
3. Secure builds
4. Code security

ROS2 Security: Learning / Guidelines

1. Education for the community
2. Best practices
3. White papers
4. Design recommendations
5. Examples and tutorials
6. Tooling

ROS2 Crystal Security Tasks: Amazon

- ROS2 Threat model
- Security integration/regression tests
  - FastRTPS & RTI Connext
- Security File Generator
- CMake target for generating security configuration
- Snapshot tool to generate access control for production
  - ”secure my system”
- Recommendations for secure file system
- Security logging for audits

ROS2 Security: Future Roadmap?

1. SCADA/IIoT security
2. ARM TrustZone support
3. Hardware Security Module (HSM) support
4. Other crypto libraries (s2n, mbedTLS, etc)
5. Secure site master
6. Anomaly/outlier detection
7. TLA+ formal verification
8. Dynamic Fuzz Testing
9. Enterprise Management: Key generation, distribution, rotation

ROS2 Security: What else?

Who's working on it?