SROS2 Demos
Overview

- **References**
  - Related IROS 2018 publications
  - Design of ComArmor & Keymint

- **Comarmor**
  - An extensible access control language
  - Write succinct, expressive policy profiles

- **Keymint**
  - Meta build tool for security artifacts
  - Automated generation and signing of PKI

- **Demos**
  - Hands on examples using SROS2
  - Deploying SROS2 onto the Turtlebot 3
Procedurally Provisioned Access Control for Robotic Systems

Verifiable policies
- Static analysis

Automated tooling
- Security at scale

See lighting talk and paper
- https://youtu.be/OzPgkhH139g

Current yaml Profile Policy

Profiles are Attached to subjects via URI (Namespace)

Attachment is an expression used to match a URI

Profiles are composed of object access Rules or nested profiles

Rules specify object type, attachment, and permissions the policy allows or denies
Alternative ComArmor Profile Policy

Profiles are Attached to subjects via URI (Namespace)

Attachment is an expression used to match a URI

Profiles are composed of object access Rules or nested profiles

Rules specify object type, attachment, and permissions the policy allows or denies
Keymint: automated cryptographic build tool

```
$ keymint create "/foo/bar/wheatley"
$ keymint build src/foo/bar/wheatley
$ keymint install build/foo/bar/wheatley
$ tree keymint_ws/
keymint_ws/
├── build/foo/bar/wheatley
│   ├── csr.pem
│   │   ├── key.pem
│   │   └── permissions.xml
│   │   └── governance.xml
│   └── install/foo/bar/wheatley
│       ├── cert.pem
│       │   ├── key.pem
│       │   └── permissions.p7s
│       │   └── governance.p7s
│   └── src/foo/bar/wheatley
│       └── keymint_package.xml
└── private
    └── identity.key.pem
    └── permissions.key.pem
```

```
Subject name: /foo/bar/wheatley
Issuer Name: Identity CA
Hash: SHA256
Type: RSA
Size: 4096
Valid: ~52k AD
```

```
Subject name: comarmor.d/* (example.xml)
Profile:
  Attachment: /foo/*/wheatley
#include <tunables/node>
  param /use_sim_time r,
  topic /chatter{,**} p,
  deny topic /chatter/foo p,
  deny topic /*/e-stop{,**} p,
  service /wheatley/get_loggers x,
  service /wheatley/set_logger_level x,
```

```
Subject name: /foo/bar/wheatley
Issuer Name: Identity CA
Hash: SHA256
Type: RSA
Size: 4096
Valid: ~52k AD
```

```
Signature
permissions.xml
<dds xmlns:xsi="..."
<permissions>
<grant_name="...
</permissions>
</access_rules>
<domain_rule>
```

```
Signature
governance.xml
<dds xmlns:xsi="..."
<permissions>
<grant_name="...
</permissions>
</access_rules>
<domain_rule>
```
Demos

Using docker to quickly reproduce the secure talker and listener example from the previous section.

- Demos
  - [github.com/ruffsl/ros2_docker_demos](https://github.com/ruffsl/ros2_docker_demos)

Using ComArmor and Keymint to deploy SROS2 to a more elaborate robotic application stack

- Turtlebot3 Example:
  - [github.com/ruffsl/IROS2018_SROS2_Tutorial](https://github.com/ruffsl/IROS2018_SROS2_Tutorial)