State-of-the-art in robot security

Bernhard Dieber

JOANNEUM RESEARCH

Institute for Robotics and Mechatronics

Klagenfurt, Austria

This work has been supported by the Austrian Research Promotion Agency in the program ”ICT of the Future” (grant no. 861264) and the Austrian Ministry for Transport, Innovation and Technology (bmvit).

Cyber threats in robotics

- Classically, robots have worked in isolation
- Modern robots work in highly interconnected environments
- Industry-grade robots are not harmless machines
- Robots pose risks to property and life
- Insecure robots may be manipulated remotely
- Industrial security is breached frequently [Byres et al., 2004, Cheminod et al., 2013, Stouffer et al., 2015, Karnouskos, 2011, Nelson, 2016, Fairley, 2016]

Security in ROS

- ROS has no built-in security [McClean et al., 2013]
- Missing authentication, authorization and confidentiality functions
- ROS is an easy target
  - Exploit XMLRPC-API used to interact with ROS master
  - Use stealth publisher attack to inject data or isolate subscribers
  - Use service isolation for DoS
  - Parameter manipulation

Attacks on ROS [Dieber et al. 2019]

- Stealth publisher attack
  - Isolate a node within the ROS application, feed with fake data
- Service isolation attack
  - Make the rest of the application think that a service is no longer available
- Malicious parameter attack
  - Modify rosparam server

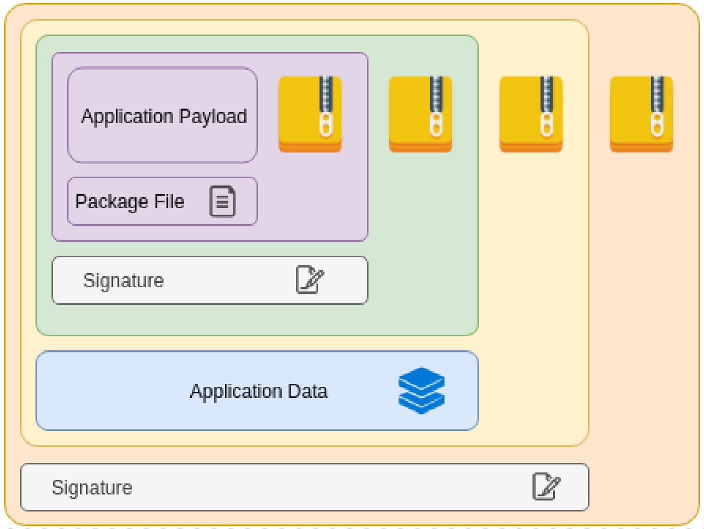
- Tools
  - roschaos
    - https://github.com/ruffsl/roschaos
  - RosPenTo
    - https://github.com/jr-robotics/RosPenTo

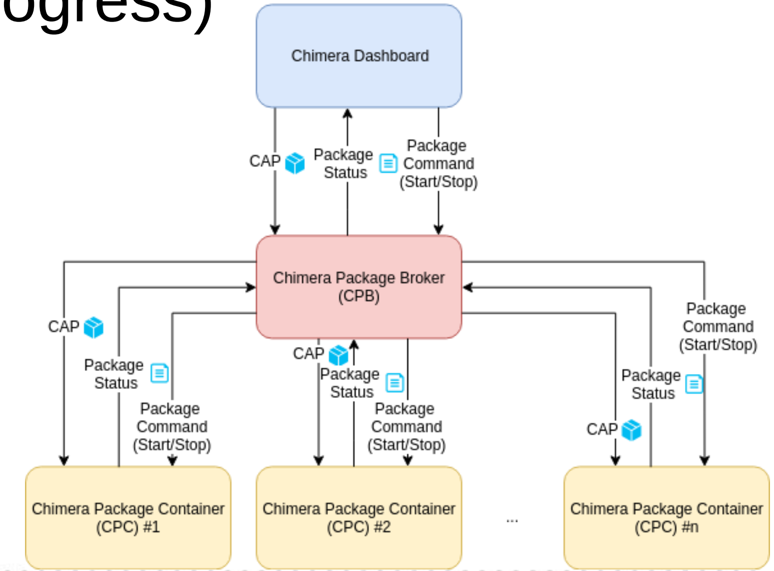
Countermeasures

- Application-level security [Dieber et al. 2016]
  - Use dedicated authentication server
- SROS1 [White et al. 2016]
  - Using TLS and AppArmor
  - Python only, TCP only
- Secure ROS core [Breiling et al. 2017]
  - Using TLS
  - C++, TCP and UDP
- SRI secure ROS [http://secure-ros.csl.sri.com/]
  - Uses IPSec

Security is more than applied cryptography

- Workflows for accessing secured devices [Dieber et al. 2017]
- Security architecture for mobile manipulators [Dieber and Breiling 2019]
- Secure deployment (work in progress)




Chimera Dashboard
CAP
Package Status
Package Command (Start/Stop)
Chimera Package Broker (CPB)
CAP
Package Status
Package Command (Start/Stop)
CAP
Package Status
Package Command (Start/Stop)
Package Command (Start/Stop)
Package Status
CAP
Chimera Package Container (CPC) #1
Chimera Package Container (CPC) #2
...
Chimera Package Container (CPC) #n

Security in ROS2

- ROS2 builds on DDS
- DDS has security mechanisms based on proven techniques
  - https://www.omg.org/spec/DDS-SECURITY/1.1/
- SROS2 project makes DDS security accessible to ROS2
  - https://github.com/ros2/sros2
- Access provisioning for SROS2 integrated in build process [White et al. 2018]

If everything else fails

- Storing forensically usable evidence on robot incidents
- Robot black box [Taurer et al. 2018]
  - Account for elevated security risks in autonomous systems
  - Separate device or dedicated software module
  - Cryptographic scheme to ensure CIA
- Work in progress of White et al.
  - Blockchain-based

Literature

- Byres, E., Dr, P. E., & Hoffman, D. (2004).The myths and facts behind cyber security risks for industrial control systems. In Proc. of VDE Kongress.
- Breiling, B., Dieber, B., & Schartner, P. (2017). Secure communication for the robot operating system. In *11th Annual IEEE International Systems Conference, SysCon 2017 - Proceedings*. https://doi.org/10.1109/SYSCON.2017.7934755
- Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. Industrial Informatics, IEEE Transactions on, 9(1), 277–293
- Dieber, B., Breiling, B., Taurer, S., Kacianka, S., Rass, S., & Schartner, P. (2017). Security for the Robot Operating System. *Robotics and Autonomous Systems*.
- Bernhard Dieber, Benjamin Breiling. Security considerations in modular mobile manipulation. IRC2019, 2019.
- Dieber, B., White, R., Taurer, S., Breiling, B., Caiazza, G., Christensen Henrikand, & Cortesi Agostino. (2019). Penetration testing ROS. In Anis Koubaa (Ed.), *Robot Operating System (ROS) - The complete reference vol. 4*. Springer.
- Fairley, P. (2016). Cybersecurity at u.s. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [news]. IEEE Spectrum, 53(5), 11–13.
- Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. In 37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011)(pp. 4490–4494).
- McClean, J., Stull, C., Farrar, C., & Mascareñas, D. (2013). A preliminary cyber-physical security assessment of the Robot Operating System (ROS). In *Proc. SPIE* (Vol. 8741, pp. 874110–874118). https://doi.org/10.1117/12.2016189
- Nelson, N. (2016). The Impact of Dragonfly Malware on Industrial Control Systems.Technical report, SANS Institute.
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015).Guide to Industrial Control Systems (ICS) Security. Technical report, National Institute of Standards and Technology. NIST Special Publication 800-82, Revision 2.
- Taurer, S., Dieber, B., & Schartner, P. (2018). Secure data recording and bio-inspired functional integrity for intelligent robots. In *Proceedings of the 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2018)*.
- R. White, H. I. Christensen, G. Caiazza and A. Cortesi, "Procedurally Provisioned Access Control for Robotic Systems," *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Madrid, 2018, pp. 1-9.
doi: 10.1109/IROS.2018.8594462

JOANNEUM RESEARCH ROBOTICS – Institute for Robotics & Mechatronics

JOANNEUM RESEARCH
Forschungsgesellschaft mbH
ROBOTICS – Institute for Robotics & Mechatronics

Lakeside B08a, EG
9020 Klagenfurt am Wörthersee
Austria

Tel.: +43 316 876-2000
Fax.: +43 316 876-2010

robotics-office@joanneum.at
www.joanneum.at/robotics

we challenge robotics!