Electronic Communications of the EASST
Volume 080 (2021)

Conference on Networked Systems 2021 (NetSys 2021)

Hacking planned obsolescense in robotics, towards security-oriented robot teardown

Víctor Mayoral-Vilches[1,3], Alfonso Glera-Picón[1], Unai Ayúcar-Carbajo[1], Stefan Rass[3], Martin Pinzger[3], Federico Maggi[2], Endika Gil-Uriarte[1]

4 pages

Guest Editors: Andreas Blenk, Mathias Fischer, Stefan Fischer, Horst Hellbrueck, Oliver Hohlfeld, Andreas Kassler, Koojana Kuladinithi, Winfried Lamersdorf, Olaf Landsiedel, Andreas Timm-Giel, Alexey Vinel

ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Hacking planned obsolescense in robotics, towards security-oriented robot teardown

Víctor Mayoral-Vilches[1,3], Alfonso Glera-Picón[1], Unai Ayúcar-Carbajo[1], Stefan Rass[3], Martin Pinzger[3], Federico Maggi[2], Endika Gil-Uriarte[1]

[1] [victor|alfonso|unai|endika]@aliasrobotics.com
Alias Robotics, Venta de la Estrella 3, Pab. 130
Vitoria, 01005 Spain
[2] Federico_Maggi@trendmicro.com
Trend Micro Inc., Italy
[3] [Stefan.Rass |Martin.Pinzger |v1mayoralv]@aau.at
Universität Klagenfurt, Universitätsstraße 65-67,
9020 Klagenfurt, Austria

Abstract:

As robots get damaged or security compromised, their components will increasingly require updates and replacements. Contrary to the expectations, most manufacturers employ planned obsolescence practices and discourage repairs to evade competition. We introduce and advocate for *robot teardown* as an approach to study robot hardware architectures and fuel security research. We show how our approach helps uncovering security vulnerabilities, and provide evidence of planned obsolescence practices.

Keywords: teardown, robotics, security, repair, safety

1 Introduction

Robotics is the art of system integration [MHK+17]. A robot is a network of networks, with sensors, actuators, and dedicated computing resources, according to its application. A robotic manipulator, for instance, include the arm's mechanics (which generally include actuators and sensors), the human-machine interface (HMI), the controller (the main compute substrate for reasoning), and any additional safety mechanism. Most industrial robots of this kind range from tenths to hundreds of thousands of Euros. Accordingly, it is only reasonable to consider the need for repairing robots.

Unfortunately, most robot manufacturers follow planned obsolescence practices nowadays and organize approved distributors and integrators into private networks, providing repair parts only to *certified* companies. Among the most recent examples we observe the case of Teradyne, which robots are advertised as collaborative (i.e., designed to safely work in close contact with humans), while research unveils that they lack of safety measures [MJC+19] and a concerning cybersecurity [AZG+18] landscape.

Given these premises, we promote robot teardown as a systematic *process* to repair robots, improve robot hardware and research its security. In the long run, we argue that the more researchers and practitioners will get used to systematically teardown robots, the more this practice

will impact the quality assurance of hardware in robotics, putting pressure on manufacturers to produce robots with better hardware security measures, thereby safer.

2 Robot teardown

A *robot teardown* is the process of analyzing a robot's hardware architecture to model its functional behavior and physical components, through systematic disassembling. We identify three key purposes in robotics: a) dissection and analysis to evaluate the status of a product, b) competitive benchmarking against similar products, and c) gain engineering experience and knowledge. We focus on a) and c) through three case studies on the robots from Universal Robots (UR) and Mobile Industrial Robots (MiR), which have tenths of thousands of units sold and operating in close contact with humans (as collaborative robots), and have been already shown lacking security measures [MJD+19] from these two manufacturers.

Due to space limitations, we leave the complete walk-through of these case studies to an extended version of this paper, focusing now only on the outcome.

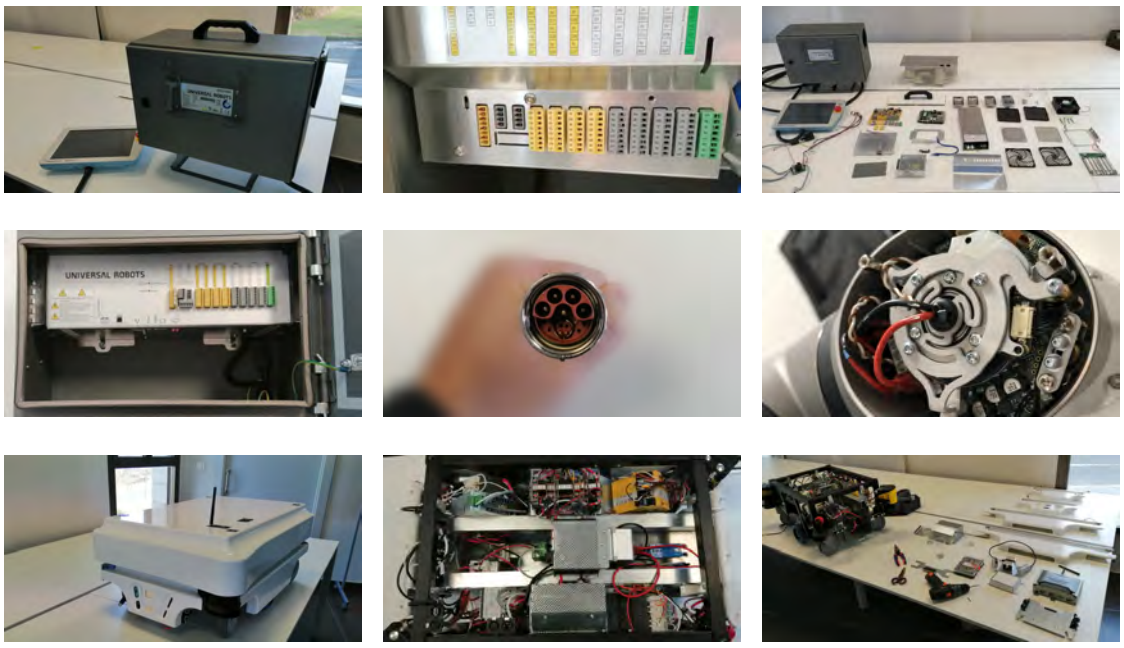

Figure 1: Teardown of three industrial collaborative robots: UR3 CB series (first three), UR3e e-Series (fourth to sixth) and MiR100 (last three).

2.1 Case Study 1: Teardown of an industrial collaborative robot

The safety logic of the UR3 CB-Series collaborative robot runs on a NXP LPC4437JET256 microcontroller, which datasheet[1] highlights that the microcontroller is not suitable for safety-critical systems according to the silicon vendor. This leads us to question the quality and reliability of the safety implementation within these robots. Therefore, through teardown, we were able

[1] https://www.nxp.com/docs/en/data-sheet/LPC435X_3X_2X_1X.pdf

to identify and pinpoint hardware components that don't meet the quality standards for the safety situations the robot may have to face, leading to an overall improved scenario for end-users.

2.2 Case Study 2: Teardown of a next-gen industrial collaborative robot

Following the CB-Series, we proceeded and disassembled one of the latest releases from Universal Robots, the UR3e, an e-Series. While the external look remains similar, the internals have changed significantly: 1) The e-Series controller integrates a single power supply unit (PSU), while the CB-series had two, 2) while the CB-Series presented two boards containing compute, power, and safety logic, the e-Series presents only one single printed circuit board (PCB) featuring a Xilinx Artix-7 series field-programmable gate arrays (FPGAs), widely used for implementing safety logic in a variety of automotive and control domains, 3) the base filter PCB—which helps interface power and RS485 communications from the controller (e-Series) to the robot arm mechanics—is similar to the one present in the CB-series, 4) the arm's mechanics connector changed in the e-Series but the power and communications lines remain coherent (through the base filter board) and 5) the electronics within the arm's mechanics do not present relevant changes from an interoperability perspective, which should facilitate re-purposing and reuse.

2.3 Case Study 3: Teardown of a mobile industrial robot

The MiR-100 is a popular mobile robot manufactured by the Danish Mobile Industrial Robots (MiR), also owned by the US Teradyne. The first impression is that various components of the robot could be improved from a safety perspective. Also, the teardown helped understand how this robot presents multiple (internal and external) networks and how each one of the sensors and actuators are connected across these networks, forming the data layer graph. The robot itself is powered by Robot Operating System (ROS) [QGC+09] and gaining further understanding of the ROS computational graph requires understanding also its underlying hardware mapping (from which one derives the data layer graph). The teardown exercise supplies exactly this and allows to produce a data layer graph represented in the form of a hardware schematic which can then be used in combination with the computational graph to gain further understanding of the robot.

3 Teardown to research security and identify planned obsolescence

Teardown supports Kerckhoffs' principle in revealing all the details and weaknesses of a security system, excluding volatile secrets such as keys or credentials stored in memory. Overall, the history of proprietary systems violating Kerckhoffs' principle by pursuing security-by-obscurity is rich of failure cases (with the military domain as the sole exception). As part of this research, our group identified more than 100 security flaws across the three robots described above over a period of two years. Most of the flaws were cataloged as vulnerabilities and 17 obtained new CVE IDs, all of which was publicly disclosed at the Robot Vulnerability Database (RVD) [MJD+19]. In most cases, these robots present few or no security measures, allowing adversaries to easily exploit the flaws of internal components (e.g. as demonstrated in RVD#2558, RVD#2561 or RVD#2562), so compromising the robot behavior or taking full control of it.

We argue that robot teardown is key for security research, as proper knowledge of the hardware helps determine potential attack vectors and which additional elements can help mitigate security

issues when the manufacturer does not react. As an example, our group introduced an additional commercial off-the-shelf hardware firewall within MiR's internal network between the main controller and the SICK's safety PLC mitigating RVD#2558, without having to modify any parts of the firmware.

Throughout this work, we found planned obsolescence particularly evident in the robots from Universal Robots. From an electrical point of view, these two robots present a similar layout for interfacing with the robot arm. The manufacturer however introduced subtle changes meant to make this particular intent harder. Our work showed how through teardown, we learned how to bypass these limitations using commercial off-the-shelf components with a total BOM price under 30 Euros.

4 Conclusions

We are concerned about the growing trend in robotics to create private networks of *certified* groups, a common practice shown by manufacturers like MiR or UR, both owned by Teradyne. We presented robot teardowns as an approach to study robot hardware architectures, obtain repairing capabilities, uncover planned obsolescence, and research its security. We advocate for a '*Right to Repair*' in robotics and encourage end-users to reflect their needs into their supply chains and into the original upstream robot manufacturers.

Bibliography

[AZG+18] L. Alzola Kirschgens, I. Zamalloa Ugarte, E. Gil Uriarte, A. Muñiz Rosas, V. Mayoral-Vilches. Robot hazards: from safety to security. *ArXiv e-prints*, June 2018.

[MHK+17] V. Mayoral-Vilches, A. Hernández, R. Kojcev, I. Muguruza, I. Zamalloa, A. Bilbao, L. Usategi. The shift in the robotics paradigm—The Hardware Robot Operating System (H-ROS); an infrastructure to create interoperable robot components. In *Adaptive Hardware and Systems (AHS), 2017 NASA/ESA Conference on*. Pp. 229–236. 2017.

[MJC+19] V. Mayoral-Vilches, L. U. S. Juan, U. A. Carbajo, R. Campo, X. S. de Cámara, O. Urzelai, N. García, E. Gil-Uriarte. Industrial robot ransomware: Akerbeltz. *arXiv preprint arXiv:1912.07714*, 2019.

[MJD+19] V. Mayoral-Vilches, L. U. S. Juan, B. Dieber, U. A. Carbajo, E. Gil-Uriarte. Introducing the robot vulnerability database (rvd). *arXiv preprint arXiv:1912.11299*, 2019.

[QGC+09] M. Quigley, B. Gerkey, K. Conley, J. Faust, T. Foote, J. Leibs, E. Berger, R. Wheeler, A. Ng. ROS: an open-source Robot Operating System. In *Proc. of the IEEE Intl. Conf. on Robotics and Automation (ICRA) Workshop on Open Source Robotics*. Kobe, Japan, May 2009.