CANONICAL

ROS ESM

Security maintenance for your ROS environment

June 2021

Introduction

Over the years, several security breaches have been reported with severe monetary and data privacy repercussions. Disregarding the industry, robots and autonomous systems represent security threat vectors that can be exploited. As with any system, robotic security is not just about the platform itself, but the weakest link in the digital ecosystem where the robot resides. Therefore, robotics companies need to develop security mechanisms for securing their products from malicious actors as well as understand the risk that they bring and they are exposed to in any network.

Software updates for security maintenance represents the minimum requirement for reducing vulnerabilities. If a robot software in a manufacturing line or retail is not maintained, sooner or later attackers may gain a foothold on it and possibly use it to gain access to the device itself, and potentially to other corporate assets. Therefore, security maintenance is included in all cybersecurity frameworks such as Center for Internet Security (CIS) top 20 or National Institute of Standards and Technology (NIST) Cybersecurity Framework, and its application in robotics is as equally valid as any other computational system. All software needs to be constantly maintained and patched. But security patching is time-consuming and work-intensive, and as a result, it detracts companies from their robotics development. Security maintenance can also be costly and the challenges scale up as you manage a fleet of devices.

Consequently, it becomes imperative to provide adequate security maintenance for devices that interact not only with the virtual world, but with the physical world as well. It is also important to provide reliable tools for innovators that will make this work easier and allow them to focus on their groundbreaking work, while not overlooking critical cybersecurity controls. Tools that will help not only the companies but also their end users.

In this whitepaper, we will explore the security landscape and how security maintenance is a key aspect of robotics security compliance. We will also discuss the barriers and challenges of security maintenance in the Robot Operating System (ROS) environment. Finally, we will describe the advantages and features of Robot Operating System Extended Security Maintenance (ROS ESM), Canonical's security maintenance service for deployed robots.

The security landscape in robotics

Back in 2017, the headlines were all about a breach of the company Equifax. Equifax is one of the main personal credit checking firms in the US; they provide credit scores based on people's financial history. In 2017, they were breached, exposing the personal information of nearly 150 million people. The source of the breach was a single customer complaint portal that hadn't been patched. A fix for the Apache webserver vulnerability had been made available months before the attack, but this particular service was left unpatched. As a result, attackers landed on this server and were able to pivot from here to other servers. In 2020, the US Federal Trade Commission finally settled the case, which included up to $425million to assist people affected by the breach[1].

Security maintenance matters, and while it might not be the only defence layer, without it an organisation has a significant likelihood of having their computer systems compromised. With the development of the Industry 4.0 vision, robots are largely connected to the internet to access enterprise-management systems. Today, companies can automatically order any part needed to complete the scheduled production, reconfigure the robotised production lines, and track their operational status. This interconnection is critical, but offers a novel attack surface.

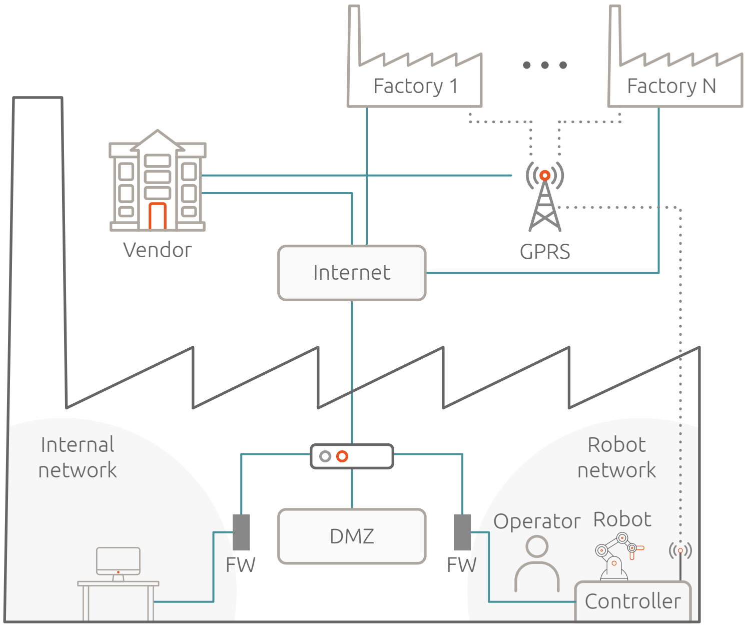

Figure 1. Robotics vulnerability architecture

Through vulnerable robots, organisations can leak sensitive information about its environment, or even cause physical harm if accessed by an unauthorised party[2].

Equipped with different sensors, such as cameras or motion sensors, robots can collect sensible data from its users and can even directly change its environment through actuators (Figure 2).

[1] Gressin. "The Equifax Data Breach: What to Do." Federal Trade Commission Consumer Information, 2017.
[2] DeMarinis, Nicholas, et al. "Scanning the internet for ros: A view of security in robotics research." 2019 International Conference on Robotics and Automation (ICRA). IEEE, 2019.

Existing work has assessed the state of industrial robot security and found a number of vulnerabilities[3]. This includes direct repercussions on operational downtime, outages and failures. Today, increasingly sophisticated multi-stage ransomware attacks are being used to target manufacturing firms. Other security vulnerabilities are also being exploited as breaches through HVAC credentials[4].

While 'security by obscurity' has been largely used to stay safe from prying eyes, ubiquitous connectivity has rendered this approach largely ineffective. Ubiquitous connectivity or pervasive computing devices are network-connected and constantly available, such as PC, laptops, tablets, smart watches. Pervasive computing can occur with any device, at any time, in any place and in any data format across any network. If a device can hand tasks or data from another device, it can be infiltrated[5]. Taking advantage of new interconnections to compromise devices originally designed to work in isolation is a pattern already observed in the automotive and industrial control system (ICS) sectors[6 7].

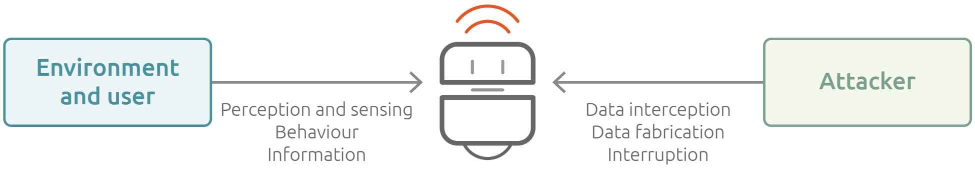

Figure 2: vulnerability architecture

Conversely, often robotics systems are placed in a separate, firewalled network enclave for protection not connected to the internet. However, robots typically still communicate with the corporate network for system monitoring and software updates, and this communication can be exploited. Take for instance Stuxnet, a malicious computer worm first uncovered in 2010. It is one of the first examples of vulnerability exposures from devices not connected to the internet. Stuxnet targets supervisory control and data acquisition (SCADA) systems and it's believed to be responsible for causing substantial damage to the nuclear program of Iran[8]. It is initially spread using infected removable drives such as USB flash drives.

After Stuxnet, other successful attacks have been recently observed. In 2014, an attack on a German steel mill caused the inability to shut down a blast furnace[9]. In 2015, 295 security incidents were reported to the U.S. ICS CERT, of which 22 reached the core of critical control systems[10].

But this does not only impact industrial robots. From healthcare to retail, from home robots, to research platforms. Robots offer solutions to many automation challenges, but while the applications change, the security risk is still there.

[3] Quarta, et al. "An Experimental Security Analysis of an Industrial Robot Controller." IEEE Symposium on Security and Privacy (SP), 2017.
[4] Winter. "Home Depot hackers used vendor log-on to steal data, e-mails." USA Today, accessed 31 Mar 2021.
[5] Quarta, Davide, et al. "An experimental security analysis of an industrial robot controller." 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017.
[6] Koscher, Karl, et al. "Experimental security analysis of a modern automobile." 2010 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2010.
[7] Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." USENIX Security Symposium. Vol. 4. 2011.
[8] Brunner, Martin, et al. "Infiltrating critical infrastructures with next-generation attacks." Fraunhofer Institute for Secure Information Technology (SIT), 2010.
[9] Quarta, Davide, et al. "An experimental security analysis of an industrial robot controller." 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017.
[10] Industrial Control Systems Cyber Emergency Response Team. "NCCIC/ICS-CERT Year in Review." Homeland Security, 2015.

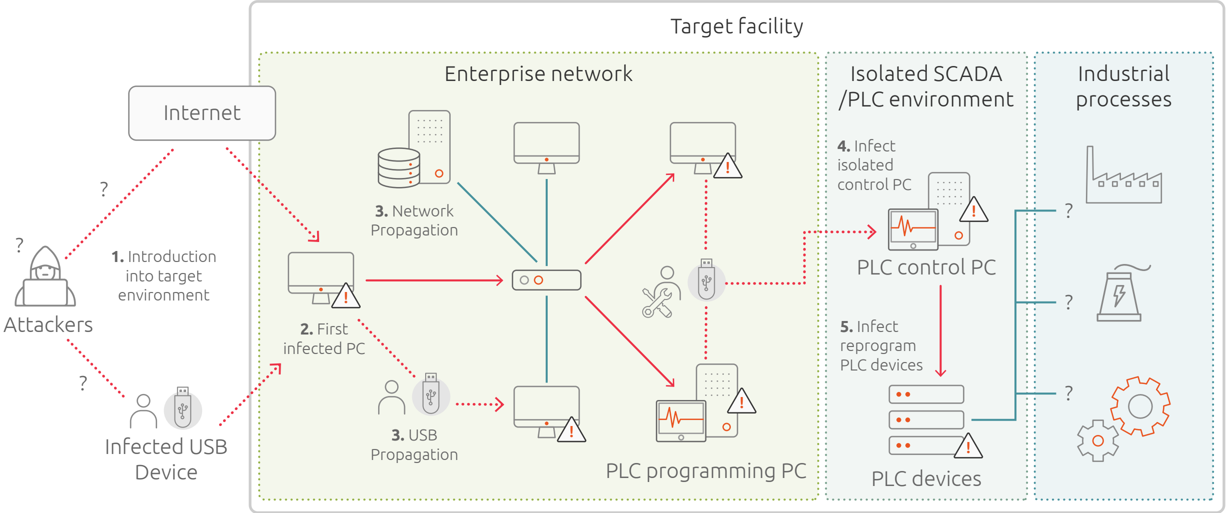

Figure 3: Points of attack in industries

The challenges of security maintenance

There is a structured way to significantly reduce risk. Just like any other computer in a warehouse, hospital, office or home, robots can follow common consensus of foundational security controls. This will not only reduce security risks, but will also guide developers during the early stages of conceptualisation and design of their robotics products. And this starts with security maintenance.

Take for instance the Center for Internet Security (CIS) Controls or the National Institute of Standards and Technology (NIST). Both organisations provide cybersecurity best practices that companies around the world rely on to improve their cyber defences. Both frameworks have controls that focus on security maintenance.

The first line of defence is to keep your OS and software up to date with security updates and CVEs fixes to avoid becoming an avenue of exploitation. It's the first step towards compliance and the first barrier of support. It is not difficult to be compliant, but it could be a challenge to keep your deployed robots security maintained.

Deploying service robots has become easier in the last years, mainly thanks to open source projects such as Robot Operating System (ROS). Actually, ROS low-level functionalities and tools allow roboticists to win modularity, abstraction, connectivity and agility. However, the robot systems themselves are becoming more complex, increasing maintenance challenges.

For instance, a human-robot interaction application could consist of ~ 65 software programs to balance face recognition, voice recognition, and navigation[11]. Autonomous driving vehicles or delivery robots have even more components for localisation, pedestrian detection, mission planning, motion planning, and more. ROS applications evolve and expand, and with them the complexity of the software components have become a more pressing issue for robotics companies.

[11] Wang and Christensen, "TritonBot: First Lessons Learned from Deployment of a Long-Term Autonomy Tour Guide Robot." 27th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN), 2018.

To ensure that all these components keep on performing as they should, robots need regular maintenance and frequent updates. Unfortunately, with each robot added, the monetary cost of paying for engineers to fix the product increases. Organisations also need to consider the implications of taking engineers away from developmental work , compromising long term sustainability. When organisations scale-up, they usually scale these problems with them.

Once deployed, robots are expected to last years on-site, meaning robotics companies either need to factor in OS and software upgrades into their maintenance plans, or run on unsupported software. This also affects those developing services for robots such as fleet management solutions, navigation or computer vision systems. Companies can either dedicate their time and resources to create those updates or wait for community members to address these issues. Neither is an optimal solution since both detract from your product and do not scale effectively. Furthermore, companies supporting customers in critical operations should not wait for the security patches to be available since the repercussions could be higher.

Another challenge is that upstream ROS updates and packages can break backward compatibility (API and ABI breakage). Without ABI compatibility between different patch versions, the released software that builds on top of that stack needs to be re-released for every patch version. In other words, any time the ROS stack releases a patch version, every other stack needs to be released as well[12]. With this there is no guarantee that the community can release binary versions of software or updates that will work with all future versions of a package, as long as it is only depending on stable stacks.

[12] Faust. "ABI Compatibility." ROS Org, 2010.

Enterprise security maintenance with ROS ESM

Security maintenance is the first line of defence and a control requirement in cybersecurity frameworks. However, there are several challenges for deploying and maintaining a security CI/CD infrastructure. Security patching is time-consuming and detracts from your robotics development. It can be costly as you manage a fleet of devices, and if done incorrectly it loses its purpose and it could interrupt the normal operation of devices.

Therefore, for ROS to increase its deployment in commercial products and services, there is a need for extending the security and support for ROS robots. Committed with our innovators, aiming to bridge the market gaps for robotic companies, Canonical developed ROS Extended Security Maintenance (ESM). As part of Ubuntu Advantage subscription, and delivered in partnership with Open Robotics, ROS ESM gives you a hardened and long-term supported ROS system for robots and its applications.

At Canonical, we develop security and update personal package archives (PPAs) for a number of service packages in the Ubuntu Main Repository and the Ubuntu Universe Repository. This includes available high and critical CVE fixes and security updates. For instance, we have more than 5,000 CVE fixes for Xenial alone at the time of writing. These fixes reside in our ESM repository and are available to any Ubuntu Advantage client through subscription tokens.

Since its inception in 2004, Ubuntu has been built on a foundation of enterprise-grade, industry-leading security practices. Canonical never stops working to keep Ubuntu at the forefront of safety and reliability. ROS ESM builds upon the world-class infrastructure used by Canonical to deliver security updates for the Ubuntu base OS and critical infrastructure components.

With ROS ESM, we have brought the same tested and maintained infrastructure to include security and update PPAs for core ROS packages. We will continue to backport critical security updates and bug fixes for ROS, for EOL and non-EOL distributions starting with ROS 1 Kinetic.

With ROS ESM companies can address several security maintenance challenges:

- Maintenance compliance
  ROS ESM supports ROS robots to be compliant with security maintenance controls from industrial cybersecurity frameworks such as CIS top 20 and NIST Cybersecurity Framework v1.1. Through ROS ESM, companies will be receiving critical security updates and common vulnerabilities and exposures (CVE) fixes for ROS, relevant dependencies (e.g. Python 2, OpenCV 3) and the Ubuntu OS.

- Exposure reduction
  With ROS ESM, companies no longer need to wait for a package maintainer to identify, fix and make patches available upstream. Canonical monitors and scans security issues, and creates the respective security updates.

- Stable packages and updates
  Updates go through a strict evaluation process before making them available to the ROS ESM users. All the updates are tested in Canonical's tested and maintained infrastructure. This includes unit tests, ABI tests, integration tests, distribution tests and smoke tests to make sure updates work end-to-end.

In addition, by enabling Canonical's ESM repositories you will get trusted and stable binaries for your ROS and Ubuntu base OS distribution with updates and packages that won't break your device API/ABI compatibility. ROS ESM provides developers with curated packages that meet Canonical's high standards for stability and interoperability.

- Easy to enable, easy to consume
  ROS ESM is easy to configure and enable in your ROS environment. To enable ROS ESM repositories companies only need a few commands in their Ubuntu terminal. To update and consume the security patches, companies only need to update/upgrade their system (either through the terminal or by using the Update Manager).

- ROS Enterprise support
  ROS enterprise support is also available for ROS ESM customers. Enterprise support represents a single point of contact for all the software in ESM, including ROS. Companies no longer need to try to figure out where to log a bug or propose a fix. This will allow companies to save engineering time and effort by contacting Canonical and Open Robotics. All in one place.

  ROS ESM customers can also access support to other open source software and infrastructure through their subscription to Ubuntu Advantage.

Conclusion

Overall, whether in production or deployment, robots are required to be constantly patched with security updates. This represents a challenge when we are talking about a fleet of devices that will inevitably live beyond the standard support lifecycle of the software powering it, depend on third-party package maintainers, and are supporting critical operations.

To support the deployment and security of ROS robots deployed on the field, Canonical proposes the Robot Operating System Extended Security Maintenance (ROS ESM) as the foundation for security compliance in different industries. From healthcare to agritech, ROS ESM provides security maintenance both for ROS applications and the Ubuntu OS. Through ROS ESM robots will receive backported security updates that have been tested and curated guaranteeing system stability. We aim to help ROS developers deploy more secure devices by easing security maintenance with ROS ESM.

Learn more

For more information about Canonical's ROS ESM, please visit our website.
You may also consider reading the following materials:

- ROS ESM - Frequently Ask Questions
- Webinar about Security and ROS ESM

To get in touch with Canonical about ROS ESM, click here.

Canonical Limited, Registered in England and Wales, Company number 110334C Registered Office:
12-14 Finch Road, Douglas, Isle of Man, IM99 1TT VAT Registration: GB 003 2322 47

Delivered by Canonical