ePDH online.com

Credit: 1 PDH

Course Title:

Cybersecurity of Robotics and Autonomous Systems

Approved for Credit in All 50 States

Visit epdhonline.com for state specific information including Ohio's required timing feature.

3 Easy Steps to Complete the Course:

1. Read the Course PDF
2. Purchase the Course Online & Take the Final Exam
3. Print Your Certificate

Chapter 5

Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety

Francisco J. Rodríguez Lera,
Camino Fernández Llamas,
Ángel Manuel Guerrero and
Vicente Matellán Olivera

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.69796

Abstract

Robots and autonomous systems in general are set to suffer similar cybersecurity problems that computers have been facing for decades. This is not only worrying for critical tasks such as those performed by surgical, or military robots but also for household robots such as vacuum cleaners or for teleconference robots compromise privacy and safety of their owners. What will happen if these robots are hacked? This study presents a survey on the cybersecurity attacks associated with service robots, and as a result, a taxonomy that classifies the risks faced by users when using service robots, distinguishing between security and safety threads, is presented. We also present the robot software development phase as one the most relevant ones for the security of robots.

Keywords: cybersecurity, privacy, safety, robots, autonomous systems

1. Introduction

Practically by definition, all robots are equipped with the ability to sense, process, and record the world around them [1]. In order to offer the best performance, they are continuously gathering information. Under these circumstances, if these robots are compromised, then a two-dimensional security problem arises: first, security issues regarding the virtual side of the robot (data, communications, and so on), and second, those problems associated with physical side that concerns both robot and user integrity. The state of the art present the "Cyber-physical security" term to encompass virtual and physical problems.

Cyber-physical attacks present several challenges that have to be faced [2]. In this study, we have focused in two particular cases: safety and privacy. On the one hand, safety problems cover the consciences associated with the physical integrity of the individuals. People are usually worried about the problems that robots can cause on people or their belongings, hacked robots aggravate these concerns. For instance, there are several commercially available surgical robots as Da Vinci work connected to communication networks allowing remote operations by specialists, what would happen if these robots or their communications would be hijacked? There have been claims of hacked military robots [3], but even service robots at home poses security problems, they could hurt toddlers or produce severe damages to homes (arson, bumping into cars, etc.).

On the other hand, privacy problems associated with robots are spreading in many areas. There are a wide range of service robots that been introduced in homes and retailing spaces. They can be used as mobile teleconference platforms, welcoming assistants, virtual pets, toys, etc. If these robots were hacked, they could provide a lot of private information about the users interacting with the robot or who simply passed by. This information can go from general data (age, size, etc.), private pictures, user routine information, economic, etc., which opens a new stage for cybersecurity of robotic systems [4].

The survey presented in this study overviews the state of the art of the security in mobile robots and it is organized as follows. Section 2 presents a general overview of cybersecurity threats to robots. Section 3 proposes a taxonomy for the risks. Then, in Section 4, the ones related with privacy are analyzed in more detail, whereas Section 5 analyzes the ones associated to safety. Section 6 faces the problems related with software development frameworks for robots. Finally, Section 7 summarizes the work faced in this chapter.

2. Modeling robot cybersecurity threats

Before analyzing in detail the risks generated by compromised robots, it is necessary to model the threads that define the cybersecurity scenario for robots. We propose a model defined overviewing Open Web Application Security Project (OWASP) [5] risk identification and different definitions of cyber-physical security on cyber-physical systems [6]. Our proposal generalizes the previous research, while trying to avoid specifying the taxonomy for any particular scenarios, such as autonomous cars, or social robots.

Figure 1 shows the elements that have to be taken into account to propose a model. We have group the security threads into five groups that will be described later. First, in the top layer, we present the origin of the threats [7, 8]. Threads can have three main origins, which are as follows:

1. Natural, associated to natural disasters.
2. Accidental, generated by the fact that there are no perfect situations as those planned in laboratories.
3. Attack, those events generated by external users with the aim to gain control over a resource of the robot.

http://dx.doi.org/10.5772/intechopen.69796

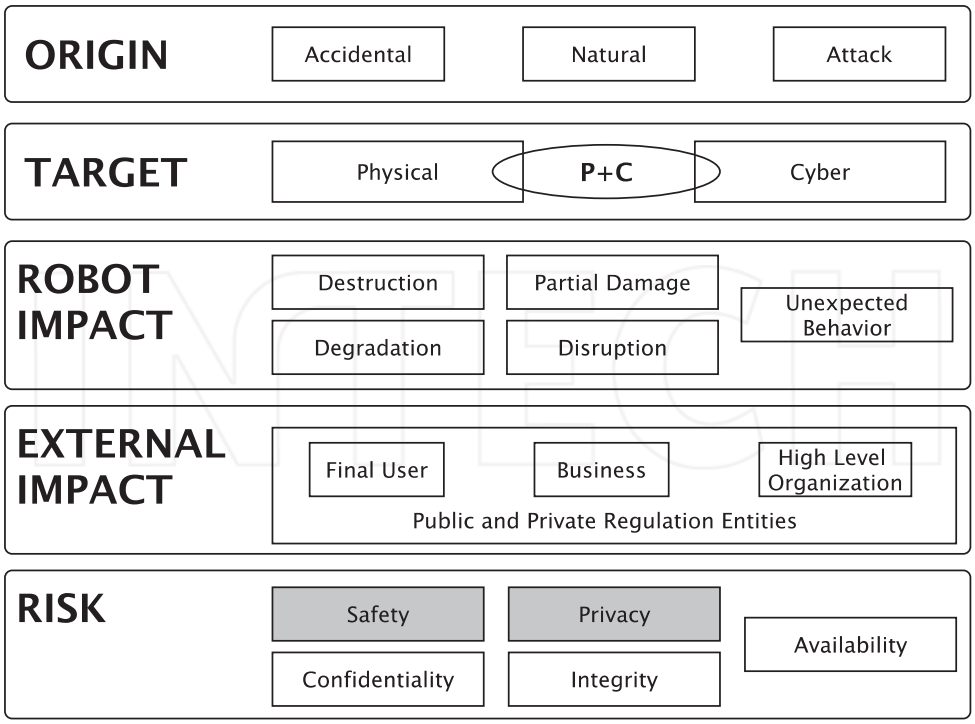

Figure 1. Modeling the robot cybersecurity scenarios.

These elements need to be faced beforehand a robot is deployed in a real environment, and a set of contingency plans should be executed in order to handle these situations.

These plans should consider the three possible targets identified in the second row of **Figure 1**, that is, the robot itself, data managed by the robot, and the combination of both components.

First, threats change the normal operation mode in a physical way. Threads could have been generated by natural conditions, accidental situations, or attacks and could cause five different impacts on the robot (third row in **Figure 1**), which are as follows:

1. Destruction, which implies nonoperability.
2. Partial damage, which involves malfunction of the robot.
3. Disruption, entails the interruption of a single, multiple, and total robot components.
4. Degradation, meaning that the range or capability of any robot component decreases along time.
5. Unexpected behavior, which could be considered as a degradation of the whole robot, not just a component.

Second, cyberthreats can affect the normal operation mode in a virtual way, that is, threads can modify the information gathered, stored, or transmitted by the robot. These threads have more impact on external entities than in the robot itself. In this way, we have organized the impact caused by cyber threats into three groups (corresponding to the fourth row in **Figure 1**), which are as follows:

1. Issues associated to robot manufacturers or open source developers (drivers and core software).
2. Issues associated to third party solutions (libraries) needed by robot manufacturer applications.
3. General vulnerabilities associated with the overall software components of the robot.

Software security issues can be intentionally or unintentionally presented in the software components of the robot. They can be categorized according to [9] into software flaws, security configuration issues, and software feature misuse.

According to existing taxonomies in software vulnerabilities [10], these issues could be added in the analysis, design, implementation, deployment, or maintenance phases. The last one also includes misconfigured robots due to final user adjustments, which allow attackers to get control over the robot.

Third, cyber-physical threats represent the sum up of both previous threads (represented by C+P ellipse in **Figure 1**). From our point of view, it can be illustrated when a sensor or an actuator is compromised. It can be performed by substitution or modification of the hardware, changing them physically or modifying the firmware. The overall system would work in the same manner but the threat would have added a new hidden functionality. The impact associated to an attack to this kind to cyber-physical threat is unexpected; the reason is that the original functional definition has been compromised.

So far, we have defined the robot impact associated with each type of target. Before explaining the risks associated with this model, it is necessary to define the actors that would be involved during or after a security threat happens. By "actors," we mean the set of people and legal entities involved in the deployment of a robotic system.

Our proposal considers four different types of actors: final users, that is, the people interacting with the robot; business users, who deploy a robot for a particular task; robot vendors, which manufacture robots and provide software; and independent software developers who create robot functionalities (individual developers or community developers) for different commercial robots. Additionally, public and private regulatory entities are also involved in the cybersecurity of robotic systems, although they do not use robots directly.

Next section analyzes risks associated with the use of a service robotic platform deployed in private or public scenario (bottom layer in **Figure 1**).

3. Modeling risks

Security risk analysis is usually based on two factors: likelihood of a successful attack against an asset, and the consequence of such an attack [11]. Literature presents several studies about the cybersecurity threats targeted to industrial environments [12]. On the contrary, there are a few studies about the risks associated with service robots at home.

Usual information security overviews classify cyber threats [13] into three fields: confidentiality, integrity, and availability of information. Extended versions for cyber-physical domains [14] add privacy, authentication, authorization, auditability, and nonrepudiation. On top of this, it is also necessary to add safety issues associated with the physical damages caused by a cyberattack.

This section models the risks associated with an attack in terms of the final user type. We identify three groups of final users of service robots such as domestic users, commercial ones, and high-level organization. We set out below the risks that hacked robots pose to these users:

Risks to domestic users can be classified as:

1. Economic risks, which can be quantified as the amount of money required to fix elements of the robot or the environment after an attack.
2. Physical, if any damage to humans happens.
3. Psychological, these risks include the loss of elements people can be attached to, or the dissemination of private information.

Commercial and business risks are related to:

1. Intellectual property, which could be accessed by competitors.
2. Reputation, which could be damaged by the publication of the attack.
3. Economic impact, including the fixing of damaged assets and the loss of profit caused by the damages and their repair.
4. Regulatory problems, if private information about clients or transactions is revealed.

Public Administration (and large very large corporations):

1. Political risks, associated with the loss of confidence by the citizens, not only on the institutions but also in the use of robots in general.
2. Economic damages.
3. National security problems, including the revelation of secrets or damages to strategic assets.

Table 1 summarizes our perception about these threats, which are identify using numbers 1–4 as in the previous description of risks that can be caused by attacks to the physical elements of robots.

The type of asset threatened depends on the different levels of physical attacks to the robot: destruction, partial damage, degradation, disruption, or substitution of their elements, which are presented in the rows of the table.

These assets also depend on the type of user. In **Table 1**, columns correspond to the three different types of users of service robots previously identified (domestic, commercial, or governmental).

Organizations proposed in **Tables 1** and **2** are not oriented to classify the relevance of different risks. They affect distinct actors in different ways, and users' perception about the relevance of these risks is also different. For instance, domestic users of service robotics are usually more worried about privacy issues, whereas corporative users are more concerned about the reputation of the company or its personal reputation in the company.

The same happens with the safety issues; domestic users are more concern about the economic damage that robots can cause in their belongings, whereas corporative users are more worried about reputational damages or potential lawsuits.

From our point of view, attacks on privacy are the one of most relevant risks that service robots could bring both to homes and to business, even more disturbing than the physical

Attack/users	Domestic/personal	Commercial/business	Public administration
Destruction	1, 2	2, 3	2, 3
Partial damage	1, 2, 3	2, 3	2, 3
Degradation	1	3, 4	2, 3
Disruption	1, 2, 3	2	2
Substitution	1, 2, 3	1, 2, 3, 4	1, 2, 3

Table 1. Physical risks for different types of users.

Origin of vulnerabilities/ type of users	Domestic/personal	Commercial/business	Public administration
Manufacturer	1, 3	1, 2, 3, 4	1, 2
Third party	1, 3	2, 3	1
General vulnerability	1, 3	1, 2, 3, 4	1, 2

This table uses the same taxonomy to characterize the risks caused by cyberattacks.

Table 2. Cybersecurity risks for different types of vulnerabilities.

ones. Service robots are usually not very large robots, so the physical damages they can cause are limited. However, the leak of information can cause severe damages. So, we will analyze focused on privacy characterization in the next section.

4. Privacy risks characterization

Robots can go places humans cannot go, see things humans cannot see, and do things humans cannot do. These characteristics have made them useful tools in many domains as space exploration, rescue missions, hazardous materials manipulation, etc. Their reliability and versatility have also made them very common in industrial environments, such as manufacturing, logistics, etc.

The increase of the computing power and the lowering of the prices of sensors have made possible the extension of robots into other domains. They are entering people's daily life as household robots, autonomous cars, or welcoming assistants in retail business.

It is not hard to imagine why service robots raise privacy concerns [15]. By definition, robots are equipped with the ability to sense, process, and record the world around them. These concerns about privacy problems can go as far as making robotic toys tools for pedophiles: "Because of their built-in cameras, microphones, speakers, and mobile capabilities, all of which can be controlled remotely, mobile Wi-Fi robot toys can pose a risk to families with children when used remotely, an attribute that can be exploited by online pedophiles who want to exploit young children online" [16].

This is not a distant disturbing possibility, it is happening right now. For example, the Wall Street Journal [17] reported that after an investigation into Cayla doll,[1] Germany's Federal Network has issued an order for all parents to find the doll and destroy her. Parents who ignore the order to destroy Cayla could face a fine of up to €25,000 and up to 2 years in prison. On its website, the agency posted a template for a destruction certificate that should be filled in, signed by a waste-management company, and sent to the agency as proof of destruction.

Cayla doll is just an example. Currently, there are many different commercial robots, from vacuum cleaners to social interactive robots that could cause similar problems. From our point of view, the most challenging from the point of view of privacy are the last ones. Social robots usually use cameras to identify users and try to profile them (sex, age, etc.) and also try to figure out their interests for entertaining the users in toys, or for commercial purposes in sales assistants. All this information is private information and any attack on the robot could compromise it.

In the next subsection, we classify the social robots regarding their function, and in the next one regarding the types of sensors they use.

[1] https://www.myfriendcayla.com/

4.1. Types of social robots regarding their use

We distinguish two types of social robots according to the number of potential users interacting with them. First, are the ones designed for personal use. There are two main types of personal robots: nonmobile social assistive robots usually designed as home assistants, as for instance QT[2] or Jibo[3] and mobile telepresence platforms as Beam[4] or Zenbo.[5] The interaction ratio of these robots is 1:*n*, where n is a small number, just the owner, her friends, and family. All of them share some characteristics of their cameras and microphones, the difference between them is the range of the sensors, which is larger in mobile platforms that can move around.

Second group is made up by platforms designed for commercial venues, as for instance, Aldebaran's Pepper. These robots are usually larger than first group ones and also the ratio of interaction in this type of robots is higher (1:*m*), where *m* is larger than *n*, that is, $m >> n$ because these robots interact with the visitors/clients of the venue.

The type of privacy problems is different between the two groups. Robots for home environments, could be listening to conversations or taking pictures of personal info around, or even while you change clothes… Robots deployed in public spaces could learn which are your interests, record conversations between bankers and clients, clone your identification methods, make market studies about your preferences, etc.

Privacy risks have to be classified and should be made explicitly communicated to the buyers of service robots. We propose to classify the privacy risks of service robot according to their sensors. According to this analysis, users should consider what type of robot they are ready to use, and also what kind of security and connectivity they are going to allow in their robots.

4.2. Privacy risks associated with sensors

Roboticists usually distinguish two basic types of robotic sensors: *Exteroceptive* sensors (i.e., lasers, range sensors, cameras, etc.), which provide information about robot workspace, and *Proprioceptive* sensors (i.e., wheel encoders, battery status), which give data about the robot itself. In addition, researches have addressed data fusion problem, that is, how to merge the overall information from robot sensors in just a single flow that could unify all sensors information in one channel.

Table 3 summarizes our proposal of classification for privacy risks, from 1 (very low) to 5 (very high), regarding the severity of the information leakage for the different types of sensors. According to this table, integration of data from various sensors is the most dangerous type of sensor because it can disclose full information about private activities of people, such as their location, images, etc. In an immediate lower level, are people images and conversations, which are the most sensitive leaks in the *exteroceptive* sensors. Finally, *extero-*

[2]http://luxai.eu/products/qt%20robot.html
[3]https://www.jibo.com
[4]https://www.suitabletech.com
[5]http://zenbo.asus.com/

Sensor	*Level*	*Presence*	*Personal information*	*Environment Information*	*Example*
Sensor fusion	5	Yes	Yes	Yes	Full disclosure of scenario activity
Exteroceptive		Yes	Partial	Partial	
Camera	4	Yes	Yes	Yes	Private images of owners
Microphone	3	Yes	Yes	Partial	Recording private conversations or acoustic signals
Range	2	Yes	No	Yes	Recording of private activities
Proprioceptive		No	No	No	
Localization	2	No	Yes	Yes	Maps of the private areas
Encoders	1	No	No	No	Recognize if the robot is moving or not

Table 3. Classification of sensors according to their risks to users' privacy.

ceptive sensors that measure ranges (lasers, ultrasounds, infrared, etc.) are less significant from the point of view of privacy, although some private information can be extracted from range readings. For example, age or sex can be concluded from gait patterns detected using a laser range scanner [18].

In summary, *exteroceptive* sensors are the most sensitive ones from the point of view of privacy if they got hacked. The type of information these sensors were gathering means the relevance of the problem in terms of privacy risks if the robot got compromised.

Information from *proprioceptive* sensors is sometimes considered less sensitive, however it can be used to get information about the current status of robots, which could be used in malicious activities (i.e., planning a housebreaking knowing that guardian robots have to recharge).

Another issue regarding sensors is to clarify where sensor data processing is made. Sensors provide raw data, images for instance. This data has to be transformed into information: detecting a face, identifying that face, or classifying it (age, race, etc.). Algorithms doing these processes are usually very demanding in terms of computer power and manufacturers to safe battery or for lowering prices of robots made this computation "in the cloud." This means that data are sent to remote computers, processed there, and the results sent back to the robot. This may be illegal in some jurisdictions (see previously mentioned Cayla example), but even being legal, these practices pose many risks in the communication (data and information can be intercepted), and also about the storing of this information and its use by the manufacturer or third parties.

Security issues regarding the use of cloud services in cyber-physical system have also been widely discussed [19] in the network community, and their recommendations can be directly applied to robotic systems.

5. Modeling safety issues

We have dealt with the security problems; cyberattacks to robots also raise safety concerns. We propose to classify the safety problems associated with robots attending to the behavior of robots observed by their users. We distinguish two basic behaviors: controlled or noncontrolled, that is, if the robot is having a responsive behavior or if it is acting randomly. This is an external and subjective perception, but we think that can be easily asset by any robot user.

In **Table 4**, we distinguish between two types of anomalous situations that a service robot can suffer and regular behavior of the robot. We propose that the situation has to be appraised by external observers and classified in one of these three categories: normal, abnormal, or under attack.

"Normal" behavior is the expected behavior of the robot according to the manufacturer specifications and user commands. By "Abnormal," we mean that the robot is not working as expected but it is not under attack. If the observed behavior of the robot is controlled, that is, responding to stimuli, the main problem is that the robot will not be able to fulfill its task. If

Situation	Behavior	Status	Threads
Normal	Controlled	Regular	
Abnormal	Controlled	Tasks are not performed in the designed way, but the robot reacts to stimuli	Lack of completion of actions commanded by legitimate users of the robot
	Noncontrolled	Tasks are not performed in the designed way and the robot behaves randomly	Potential damages to users/ environment. Lack of completion of actions commanded by legitimate users of the robot
Under Attack	Controlled	A new task is performed The same task is performed	The robot could be used as a weapon Lack of completion of actions commanded by legitimate users of the robot
	Noncontrolled	Tasks are not performed in the designed way and the robot behaves randomly	Potential damages to users/ environment. Lack of completion of actions commanded by legitimate users of the robot

Table 4. Classification of safety problems in robots associated to their behavior.

the robot is not responding, more severe damages can happen. In both cases, one usual solution is to reset robot using the mandatory reset physical button [20] available in every service robot.

The "under attack" case is the most difficult to assess by a user. It is difficult for an external observer to know what is happening inside the robot. Observers can verify whether the robot is "controlled," that is, it is responding to stimuli or not. If it is, but is doing a different task than expected, this could be an indication of an attack. But even if the robot is working as expected, it could have been compromised and the attacker could be hiding under the normal behavior of the robot.

Regarding the severity of the safety risks, the main features of robots that define the consequences of safety problems are based on physical dimensions of the robot, mainly size and weight of the robot; and also, the hazardous elements accessible by the robot, which can be components of the robot (batteries, effectors, etc.) or elements that can be reached by the robot (cargo being delivered, environment elements being manipulated, etc.).

Thus, we propose a classification of safety risks for robots based on the size of the robot. We propose a three-level classification of risks, which are as follows:

1. Low-level risks: Robots that can be carried out by users. This means that robots interacting with children or handicapped people should be small enough to be considered at low risk.
2. Medium-level risks: Robots that cannot be carried by users, but whose size is smaller than their users. This means that the robot cannot be handled by users, but they are not intimidated by them.
3. High-level risks: Robots which are larger than the users in any of the user dimensions like size, height, and speed.

5.1. Examples of attacks

There are different ways of attacking a robot, and different levels in the severity of the intrusions. **Table 5** shows some examples of cyberattacks to service robots indicating if it generates a privacy [1] or a safety problem [2].

"Stealth attacks" can be implemented in different ways. In this type of attack the attackers basically try to modify the sensors readings of the robot to induce an error. This can be achieved by modifying the environment, or interfering with the sensors. Some solutions could have been proposed to detect this kind of attacks for instance using the cumulative sum (CUSUM) [21] to detect errors in a range sensor readings, which could cause collisions in a mobile robot.

Another well-known attack is the "replay attack." If attackers are able to intercept the communications of the system, they can replay captured packages, even if they are encrypted. If the communication protocol is not prepared for this kind of attack, the system will consider these replayed packages as legitimate, and make mistakes in the decisions. This type of attack is also used as a precursor to discover the interiority of the system, looking for new weaknesses.

Attack	*Type*	*Example*
Stealth attack	2	Modification/Substitution of sensors readings
Replay attack	1,2	Attacker impersonating roles
Covert attack	1	Third party applications sharing personal data
False-Data injection	1,2	Medical robots
DoS attack	2	Robot not working at all
Remote access	1,2	Robot controlled by an attacker
Eavesdropping	1	Attacker monitoring robot-user messages

Table 5. Example of attacks to service robots.

There are other types of attacks to robots not related to their sensors. They can be targeted to the cognitive elements of the control system. For example, in a medical robot, if false information is given to the system about the condition of the patient, the robot could take wrong decisions that potentially could cause severe damages. This kind of "False-Data Injection" could also be used in other type of robots, for instance, providing false maps to a mobile robot to bring a collision, or fake information to a robotic shop assistant to mislead clients.

From the point of view of privacy, "Eavesdropping" is one of the most feared threads in computer systems. The same concern applies to robotic systems. If robotic systems exchange information with other off-board systems, this communication can be compromised and private information about the users can be obtained (this problem has been described in Section 4.2).

Denial of Service (DoS) is other classic type of attack. DoS attacks in robotics generally mean that the robot stops working, so damages are not suffered by robots, neither robots damage people or their environment. Damages are due to lack of the service provided by the robot. The severity of the attack depends on the criticality of the service to be supplied.

A worse case arises when the robot is not just stopped but hijacked. This is known as in cybersecurity as a "Remote Access." In this situation, robots pose safety problems, not just privacy ones.

Classifying the severity of the attacks is a challenging problem. It is very difficult to predict the consequences of the attacks. Even a small loss of data can have catastrophic effects on the reputation of a company. A single private image eavesdropped from a home robot can be used for blackmailing a tycoon. DoS attacks that only prevent the robot for doing its work could look less dangerous, but they are really important, for instance, in tele-surgical robotic systems [22].

6. Securing the development

As we have previously mentioned, most of the cybersecurity problems in robotics are due to the lack of awareness among developers of software for robots [4]. Software controlling robots

need to be secured, which means that the methodologies, tools, and development frameworks used have to be secured.

Different robotic development frameworks (RDF) have appeared in last years. RDFs simplify and speed up the development of robotic applications because they ease the portability of applications among different robots, favoring code reusability and reducing the cost of new developments.

Major contributions of RDFs are hardware abstraction, which hides the complexity of managing heterogeneous hardware by using standard interfaces; distribution of computing resources, which let programmers spread the computation of complex systems over a network; and the creation of "communities" of developers around them for sharing code, tools, etc.

However, contributions provided by RDFs have also brought security flaws to the robotics ecosystem. For instance, sharing code without the appropriate precautions open a door for *malware* infections. In the same way, using distributed computation means that data is being transferred among different computers, in many cases using public infrastructure (public Wi-Fi networks) where different types of attacks can happen, as we have previously described.

This is due to the youthfulness of the robotic community. In many cases, transference from research and university environments to commercial products is happening too fast. Mainstream RDFs do not have any security mechanism in their design.

For instance, robotic operating system (ROS), the "de facto" standard for robotic systems, was designed without taking into account almost any security protections. Malicious malware can easily interfere with ROS communications [23], read private messages or even supersede nodes.

Cybersecurity was not a requirement for ROS at its conception because it was designed mainly for research purposes, but now it has to be because it is being used in commercial products. The new version of this framework (known as ROS 2.0) which is currently in development (beta stage) is trying to solve these problems by using DDS as a standard middleware [24].

RDFs are based on software engineering principles, which means that they are suitable for adapting secure methodologies [25] used in more mature software development communities.

Using standard methodologies and secure tools is not a new issue, it has been proposed several times [26] but as robots use is expanding to homes and streets, with people increasingly trusting on them for more tasks of their daily life, this need is becoming imperative.

7. Conclusion

In this chapter, we have dealt with the security and safety problems potentially caused by cyberattacks to robots. As major contribution, we have proposed a taxonomy for the attacks to service robots. This classification takes into account different types of assets that can be compromised, which could be physical or immaterial (information, reputation, etc.) and could be useful when deciding whether to acquire a robot or not.

We have classified the different types of sensors that usually equip service robots and the relevance of the information they can gather in case of a cyberattack. This information could also be useful when configuring robots for different uses.

We have also analyzed the safety problems that arise when a robot is compromised. In this case, we propose a taxonomy of the problems based on the subjective perception of users about the behavior of robots and a classification of the risks depending on the size of the robots.

Finally, we have analyzed the role of the development frameworks used to program robots. In this case, we recommend the use of standard methodologies and good practices common in other software development environments. We also point out that some well-known middleware, as ROS, have severe security flaws that should be taken care of if it is going to be used for commercial products.

Acknowledgements

This work has been partially funded by INCIBE (Instituto Nacional de Ciberseguridad S.A.), a public company of the Kingdom of Spain and the Universidad de León under the Adenda 21 of the framework agreement between the two entities.

Author details

Francisco J. Rodríguez Lera[1], Camino Fernández Llamas[2], Ángel Manuel Guerrero[2] and Vicente Matellán Olivera[2]*

*Address all correspondence to: vicente.matellan@unileon.es

1 AI - RoboLab University of Luxembourg, Belval, Luxembourg

2 RIASC - Research Institute on Applied Sciences to Cybersecurity, Universidad de León, León, Spain

References

[1] Calo RM. Robots and privacy. In: Bekey P, Abney G, Lin K, editor. Robot Ethics: The Ethical and Social Implications of Robotics. Boston: MIT Press; 2011

[2] Humayed A, Lin J, Li F, Luo B. Cyber-Physical Systems Security - A Survey [Internet]. 2017. arXiv preprint. arXiv:1701.04525

[3] Rawnsley A. Iran's Alleged Drone Hack: Tough, but Possible [Internet]. 2011, Wired. Available from: https://www.wired.com/2011/12/iran-drone-hack-gps [Accessed: March 1, 2017]

[4] Apa L, Cerrudo C. Hacking Robots Before Skynet. Seattle: IOActive Inc.; 2017. pp. 1-17. https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf

[5] v.40, OWASP Testing Guide. OWASP Testing Guide.OWASP. [Online] [Internet]. 2014. Available fromhttps://www.owasp.org/images/1/19/OTGv4.pdf [Accessed: April 1, 2017]

[6] Alvaro A. Cardenas; Saurabh Amin; and Shankar Sastry. Secure control: Towards survivable cyber-physical systems. In: IEEE Distributed Computing Systems Workshop, 2008 (ICDCS'08); 2008. IEEE; 2008. pp. 495-500

[7] Gabriel J. Mission-centricity in cyber security: Architecting cyber attack resilient missions. In: 5th International Conference on Cyber Conflict (CyCon); 2013. pp. 1-18

[8] Conklin A, White GB. E-government and cyber security: The role of cyber security exercises. s.l:. 39th Annual Hawaii International Conference on System Sciences (HICSS'06); 2006. IEEE; 2006. pp. 76b–79b.

[9] LeMay E, Scarfone K, Mell P. The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities. National Institute of Standards and Technology (NIST); 2012. Interagency Report

[10] Piessens F. A taxonomy of causes of software vulnerabilities in internet software. Proceedings of the 13th International Symposium on Software Reliability Engineering; Los Alamitos, CA: IEEE Computer Society Press; 2002

[11] Byres E, Lowe J. The myths and facts behind cyber security risks for industrial control systems. Proceedings of the VDE Kongress. 2004;**116**:213-218

[12] Ten CW, Manimaran G, Liu CC. Cybersecurity for critical infrastructures: Attack and defense modeling.. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. 2010;**40**(4):853-865

[13] Cavelty MD. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review. 2013;**15**(1):105-122. DOI: 10.1111/misr.12023

[14] Yan Y, et al. A survey on cyber security for smart grid communications, s.l: IEEE. IEEE Communications Surveys & Tutorials. 2012;**14**(4):998-1010. DOI: 10.1109/SURV.2012.010912.00035

[15] Denning T, Matuszek C, Koscher K, Smith JR, Kohno T. A spotlight on security and privacy risks with future household robots: Attacks and lessons. s.l. In: 11th International Conference on Ubiquitous Computing (UbiComp '09); 2009. ACM; 2009. pp. 105-114

[16] Yong S, Lindskog D, Ruhl R, Zavarsky P. Risk mitigation strategies for mobile Wi-Fi robot toys from online pedophiles. s.l. IEEE International Conference on Privacy, Security, Risk and Trust 2011 and IEEE International Conference on Social Computing 2011. IEEE; 2011. pp. 1220-1223. DOI: 10.1109/PASSAT/SocialCom.2011.194

[17] Andrea Thomas, Germany issues kill order for a domestic spy - Cayla the toly doll. Wall Street. Wall Street Journal. [Online] [Internet]. 2017. Available from: https://www.wsj.com/articles/germany-issues-kill-order-for-a-domestic-spycayla-the-toy-doll-1492098755 [Accessed: April 28, 2017]

[18] Pallejà T, Teixidó M, Tresanchez M, Palacín J. Measuring gait using a ground laser range sensor. s.l: MDPI. Sensors. 2009;**9**(11):9133-9146. 10.3390/s91109133

[19] Yana Z, Zhangc P, Vasilakosd AV. A survey on trust management for Internet of Things. s.l.: Elsevier. Journal of Network and Computer Applications. 2014;**42**:120-134. DOI: 10.1016/j.jnca.2014.01.014

[20] ISO/TC 299 Robotics. Robots and Robotic Devices -- Safety Requirements for Personal Care Robots. Geneve: ISO, 2014. p. 79. Standard

[21] Sabaliauskaite G, Ng GS, Ruths J, Mathur A. Experimental evaluation of stealthy attack detection in a robot. s.l. In: IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE; 2015. pp. 70-79. DOI: 10.1109/PRDC.2015.33

[22] Coble K, Wang W, Chu B, Li Z. Secure software attestation for military telesurgical robot systems.. MIlitary Communications Conference (MILCOM 2010). San José, California: IEEE; 2010. DOI: 10.1109/MILCOM.2010.5679580

[23] Lera FJR, Balsa J, Casado F, Fernández C, Rico FM, Matellán V. Cybersecurity in Autonomous Systems: Evaluating the performance of hardening ROS: s.n. XVII Workshop en Agentes Físicos; 2016; Málaga (Spain). 2016. pp. 47-54

[24] Woodall, William. ROS on DDS. *ros.org*. [Online] [Internet]. 2016. Available from: http://design.ros2.org/articles/ros_on_dds.html [Accessed: Mayo 10, 2017.]

[25] Finnicum M, King ST. Building secure robot applications. In: Proceedings of the 6th USENIX Conference on Hot Topics in Security, HotSec'11. Berkeley, CA: USENIX Association; 2011. pp. 1-1. http://dl.acm.org/citation.cfm?id=2028041

[26] Tomatis N, et al. Designing a secure and robust mobile interacting robot for the long term. IEEE International Conference on Robotics and Automation (ICRA); Taipei, Taiwan. 2003. DOI: 10.1109/ROBOT.2003.1242256