A Perspective of Security for Mobile Service Robots

Gary Cornelius[1], Patrice Caire[1], Nico Hochgeschwender[2], Miguel A. Olivares-Mendez[1], Paulo Esteves-Verissimo[1], Marcus Völp[1], and Holger Voos[1]

[1] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, L-1359 Luxembourg, Luxembourg,
name.surname@uni.lu
[2] Bonn-Rhein-Sieg University, Sankt Augustin, Germany,
name.surname@h-brs.de

Abstract. Future homes will contain Mobile Service Robots (MSR) with diverse functionality. MSRs act in close proximity to humans and have the physical capabilities to cause serious harm to their environment. Furthermore, they have sensors that gather large amounts of data, which might contain sensitive information. A mobile service robot's physical capabilities are controlled by networked computers susceptible to faults and intrusions. The proximity to humans and the possibility to physically interact with them makes it critical to think about the security issues of MSRs. In this work, we investigate possible attacks on mobile service robots. We survey adversary motivations to attack MSRs, analyse threat vectors and list different available defence mechanisms against attacks on MSRs.

1 INTRODUCTION

Mobile service robotics is currently a fast moving sector with first devices already on the market, for example, the Robomow lawnmower or the Roomba vacuum cleaner [1]. One example of more sophisticated MSRs are autonomous self-driving cars which are planned to broadly appear on our streets in the years to come. Another example of a MSR is the Care-O-Bot[3] built by Fraunhofer Institute in Germany. This mobile robot assistant aims at actively supporting humans in their daily life. The Care-O-Bot consists of many sensors and actuators. This gives it the ability to sense its environment and act accordingly, which helps its autonomous behaviour [2]. One can imagine that these MSRs with a size of 158cm and a weight of 140kg are not toys and are potentially as dangerous as industrial robots, which may sometimes cause accidents such as in [3]. Some MSRs are actually equipped with standard manipulators such as KUKA LWR, Schunk and so forth.

In order to meet the safety requirements [4], Care-O-Bot is equipped with three laser scanners and several emergency stops. Furthermore, with its set of sensors and mobility the Care-O-Bot can collect large amounts of information which must be protected [6]. Other well known examples of MSRs are ARMAR, PR2, Pepper and Herb. To illustrate the consequences of an improperly secured robot imagine, for example, a home care robot that hands out medication to a patient in the wrong doses, disrupting the patients treatment or worse.

[3] http://www.care-o-bot-4.de/

Back in the days, robots were mostly used in industrial environments where the approach was to build security measures around them to separate robots from humans. Engineers were mainly focusing on the engineering side of the problem and security was always seen as something that could be added later in the process [4]. For industrial manufacturing robots this might be an acceptable solution, but clearly this will not work in the case of MSRs which are cyber-physical systems (CPS) build to interact and help humans with their daily tasks.

A MSR can be separated into two main parts, the hardware and the software. First, we have the hardware that provides a set of capabilities. Second, we have the software which is used to control the hardware to fulfil certain operations. A MSR is equipped with various sensors and actuators which allow it to sense its environment and act in it safely. The robot's main system has to interconnect with all its hardware devices and has to ensure their concurrent functioning. The requirement of reliable, concurrent hardware access with real time constraints makes the design and implementation of such systems an extremely hard task [5].

A few years ago MSRs were designed for a special purpose and did mostly not have any network interface. Today a robot's physical capabilities are controlled by networked computers, which are susceptible to fault and intrusion. With MSRs being developed to become part of our every day environment it is urgent to be aware of the security gaps of MSRs. Awareness should be raised on the fact that MSRs are an interesting target, not only for casual attackers.

In summary, we make the following contributions: i) Adversary motivations were surveyed. ii) A basic representation of a MSR was provided and four threat vectors that apply to this model were identified. iii) These threat vectors were ranked by prevalence and hazard risk. Furthermore, concrete examples of tools and defence measures that apply to each threat vector were listed.

The remainder of the paper is structured as follows. In section 2, we describe the environment of a MSR and give concrete examples describing an attacker's motivation. A basic MSR representation and list of threat vectors that apply to this representation is provided. In section 3 threat vectors are ranked according to prevalence and hazard risk. An extensive list of tools that are used to exploit these treat vectors together with applying defence mechanisms is provided. Section 4 contains the conclusion of this work.

2 A new Target for Adversaries

MSRs are a particularly interesting target for adversaries because they are cyber-physical systems built to sense and act upon their environment. A successful adversary is able to cause significant privacy issues and serious trouble in the robot's physical environment. MSRs act in a physical environment which includes humans, animals and other objects. MSRs inside a home environment can, for example, be attacked to gain information about the owner [6–9]. An infected MSR can, for example, listen to sensitive private conversations and the adversary will use this information to blackmail the owner.

In a concrete scenario, the infected robot can be used by an adversary that wants to know if the owners are at home to plan/execute a burglary. The adversary can also

use the robot to cause serious damage inside the robot's environment, which includes the robot itself. An infected robot could, for example, physically harm people or destroy property. Furthermore, the robot can be used to cause psychological harm to the owner by transmitting a frightening audio message or by performing terrifying actions. In another more futuristic example, we can imagine a cyber-warfare attack which simultaneously infects a large amount of robots. This attack spoofs the battery status of many robots simultaneously and puts them into charging mode, which might overload the power grid. We identified the following motivations to be particularly interesting:

- **Data Theft** : The robot's sensors collect large amounts of sensitive data, which can be accessed by an attacker which gained access to the robot. (Blackmailing, Espionage, planned burglary, etc.)
- **Destruction of Environment** : An attacker which gained control of the robot can cause serious hazards in the robot's environment. This includes i.e. physical damage to the robots environment and psychological damage to humans. (Vandalism, Terrorism, etc.)

The listed motivations show that MSRs do not only attract the attention of casual hackers, but they are also potential targets for state-level adversaries like intelligence agencies. In our model, attackers are not only limited to cyber attacks, but can also perform physical and environmental attacks on a robots sensing abilities. In Fig. 1, we illustrate

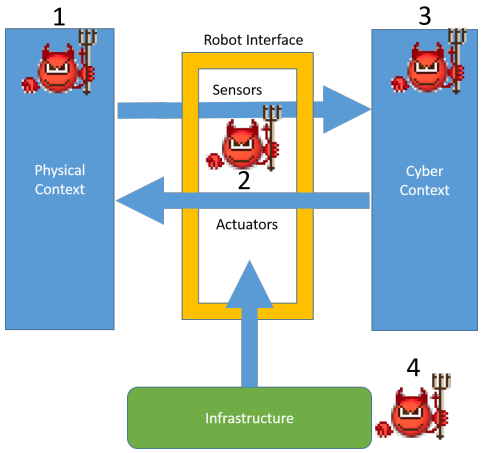

Fig. 1: Basic representation of a MSR with the physical Context on the left, cyber-context on the right and external infrastructure on the bottom. They are connected through the robot interface.

the basic representation of a MSR. The figure reads as follows, the physical context on the left and the cyber context on the right are linked through the robot interface. Sensors give feedback to the cyber system and actuators act in the physical context. The robot can also be connected to external infrastructures like laptops, smart-phones

or the cloud. A MSR is a system which has sensors and actuators that act as a bridge between the cyber context and the physical context. These devices are embedded inside the robot and the robot can therefore be seen as an interface between the physical and the cyber-world. The numbers represent the 4 threat vectors that we identified based on this representation. The threat vectors are: Attacks on Sensor Data(1), Attacks on Hardware(2), Attacks on Software(3) and Attacks on Infrastructure(4). In the case of threat vectors, the cyber context means everything related to software and the physical context means everything related to the external environment measurements, namely sensor data which is recorded from the environment.

3 Threat Vectors and Protective Measures

A threat vector is a path or means by which an attacker might get access to a system. Advanced adversaries might be able to combine multiple of these threats to abuse a vulnerability, which enables him to achieve his goals and motivations. We can imagine, for example, an attacker abusing the sensor data channel to install Malware on the system by exploiting a buffer overflow in the control software.

In Table 1, we assign different values to the prevalence and hazard risk of the threat vectors described in the following sub-sections. Attacks on software and infrastructure are the most critical, because these attacks have severe consequences, but do not necessarily require a sophisticated attacker. Furthermore, these attacks can be executed by any external adversary with a connection to the robot, whereas attacks on sensor data and attacks on hardware typically require physical access to the robot either during development, production, or usage. The table reads as follows, prevalence is ranked from

	Prevalence	**Hazard Risk**
Attacks on Sensor Data	Medium	High
Attacks on Hardware	Low	High
Attacks on Software	High	High
Attacks on Infrastructure	High	High

Table 1: Prevalence and Hazard Risk of threat vectors

low to high and is reversely correlated to the attacker's effort. Hazard Risk is ranked from low to high, where high means that an attack can have serious consequences. In Table 2, we provide examples for the tools that can be used to attack a MSR and also provide an overview of the countermeasures applying to these threats.

3.1 Threat Vector #1: Attacks on Sensor Data

Sensors and actuators are the bridge between the physical and the cyber world. Sensors sense the environment and send data to control units which manipulate actuators in the real world. Safety mechanisms were implemented to ensure that sensors and actuators could be reliably used to protect the robot and its environment. Typically, these safety

Threat	Tools	Defence Mechanisms
Attacks on Sensor Data	Side-Channel attacks (active&passive) [24,15,6,25,16,26,13,16] Hardware Attacks [13,17] Man In the Middle [27]	Anti-Virus Intrusion Detection System Redundancy, Diversity Electro-Magnetic Shielding Encryption Authentication
Attacks on Hardware	Physical Manipulation [20] Hardware Trojan [28,19]	Device Signatures Authentication Hardware Testing Formal Verification
Attacks on Software	Malware [9,22,23] Denial of Service [23,24] Phishing [22]	Anti-Virus Hardening (IDS,Firewall, etc.) No external hardware interfaces Vigilance Software Testing Security Updates Authentication & Access-Control
Attacks on Infrastructure	Standard Password [9] Man In The Middle [6,9]	Anti-Virus Authentication & Access Control Encryption

Table 2: Examples of tools and defence mechanisms for our Threat Vectors

mechanisms do not take into account active attackers [5] and manufacturers are negligent or might not be aware of the fact that side-channel attacks [23] also apply to robots. These attacks have the potential to leak sensitive information and can even cause environmental harm. Therefore, robots need effective prevention and detection mechanisms against side-channel attacks.

Well known Intrusion Detection Systems (IDS) like Snort are able to protect cyber-physical systems on the network level, but are not suitable for the sensor channel. This is because they were designed for analysing network traffic and cannot be directly used for traffic over the sensory channels. A new type of IDS is needed to tackle these gaps [10].

To introduce attacks on sensor data, imagine an autonomous security robot which is used in public spaces to prevent crimes and alert emergency services in case of a potentially dangerous situation. Attacking the sensors of this autonomous MSR could lead to privacy issues or to accidents like in [11] where a safety failure resulted in an accident which included a child. We picked four of the most interesting active-side channel sensor attacks and refer to the literature for passive side-channel attacks and more examples [5, 22, 23, 29, 30].

– **Laser Sensors** Many robots contain a Light Detection and Ranging (LiDAR) system which determines distances by measuring the brightness of targets illuminated with laser light. MSRs use LiDAR technology to perceive their environment or recognise objects. It has been shown that these systems are susceptible to active attacks. In [12], Petit et al. show effective replay, relay and spoofing attacks on a LiDAR system using a 60$ setup. They show that signals detected from other ve-

hicles could be replayed effectively. Furthermore, they were able to spoof the laser signals and make the LiDAR system believe that it could sense objects that were 50-200m away, trough a wall.

- **Gyroscope Sensor** A gyroscope sensor measures changes in tilt, orientation, and rotation based on angular momentum. Therefore, it is highly used in the area of UAVs. In [13], Son et al. show that it is possible to cause faulty sensor readings by using consumer-grade audio speakers. Furthermore, they demonstrate that they could crash drones using this sound-wave based attack.
- **GPS Sensor** In [22], Kerns et al. demonstrate GPS spoofing attacks on an Unmanned Aircraft (UAV). These attacks can result in robot kidnapping or might even cause unrecoverable navigation errors which may cause damage to the robot and its environment.
- **Hall Effect Sensors** Hall effect sensors detect fluctuations in magnetic fields and can be used for wheel rotation sensing. In [5], Akdemir et al. show that generating an electromagnetic (EM) pulse with similar attributes than the Hall effect sensors, an attacker could alter the feedback signals. An attacker could for example make the robot believe that it is going at low speeds, making him speed up and crash.

Securing hardware from side-channel attacks is a difficult and important problem. Especially for robots, where control-loops typically rely on the correctness of input sensor data [5]. Aside from clever prevention and detection mechanisms, a fail-safe mode should be implemented if the ongoing attack is found to be too severe. This fail-safe mode could either partly shut down the system by only disabling one type of sensors, or completely shut down the system.

To protect against attacks on proximity sensors like ultrasound range sensors, randomised pulse redundancy could be used [12].

Another effective approach is fault tolerance through sensor redundancy by replication or diversification of sensors. In the case of sensor replication, the robot could recognise an ongoing attack on one or several of its sensors, which measure the same environmental variable, due to differences in sensor readings. In case of diversification, sensors from different manufacturers could be used to protect against known security flaws in one of these sensors. To mount a successful attack, the attacker would have to invest more resources.

In [14], Bezzo et al. propose a state estimation algorithm to recognise active attacks by using multiple measurements. Their work shows similarities with the functioning of an Intrusion Detection System (IDS). They show that they were able to detect ongoing attacks using differences in the noise signatures coming from the sensor.

To prevent information leakage from EM radiation, Akdemir et al. propose EM shielding [5] which can be applied to the whole robot or only to individual components. Furthermore, solutions known from other cryptographic devices such as noise generators, masking techniques, etc., can be applied [15].

To prevent from Man in the Middle attacks, sensor data should only be sent encrypted. Furthermore, sensors should provide authentication mechanisms to prevent sensor replacement attacks.

3.2 Threat Vector #2: Attacks on Hardware

An adversary with physical access on the robot during development, manufacturing, or usage has enough time to plan and execute a physical attack on a robots hardware. The difference between *Attacks on Sensor Data* and *Attacks on Hardware* is that in the first the faulty measurements result from the manipulation of the environment but not from a direct attack on the robot's hardware. Therefore, we decided to separate these two threat vectors.

- **Hardware Trojan** An adversary with access to the design process of a computing chip, for example, can insert a Hardware Trojan Horse (HTH) into the chips circuit. Thereby, he would make all the devices that use this chip vulnerable [16].
- **Physical Attack** An adversary could replace a robots hardware with hardware that is not following the robots specifications. An adversary could, for example, replace a robots actuators with stronger ones, which causes safety issues.

Protection mechanisms against Hardware Trojan Horse (HTH) attacks have to be implemented already starting from the from production chain [25]. Defence mechanisms include, for example, side-channel device signatures. In [16], Tehranipoor et al. provide a classification of HTH together with a survey about detection mechanisms. Furthermore, reliable hardware authentication mechanisms are needed to mitigate physical replacement attacks [17].

3.3 Threat Vector #3: Attacks on Software

Available mobile service robots reuse most of the hardware components known from current computer generations. Furthermore, robots like the Care-O-Bot, or the PR2, rely on commonly used Linux operating systems. Typically, these systems cannot be manually updated and therefore, updates and critical security patches are not applied. Therefore, mobile service robots inherit all the security vulnerabilities known from current computer systems.

One example of a cyber attack on a CPS is the Stuxnet Virus [18]. Stuxnet is different from other computer worms. It does not aim to steal information from a hijacked computer, but it was built to cause destruction on equipment of Iranian nuclear power plants. Robot software runs on top of an Operating System (OS) which acts as a bridge between the application layer and the low-level hardware layer. Security, and the lack thereof, have an important impact on the systems overall security, including applications running on top of the OS. The lack of proper control and containment mechanisms for applications in an OS may lead to attacks from one application to another application. Once an adversary breaks into the kernel of an OS, he has the means to bypass any software level access control mechanism. This allows him to take complete control of the robot.

To our knowledge, no attempt has been made to give an overview of how cyber threats apply to the domain of mobile service robots. As a starting point, we take the most common computer security threats according to Symantec Norton [19] and analyse how they apply to mobile service robots.

- **Virus** A virus is a Malware which can replicate itself and infect a computer without the permission or knowledge of the user. A virus can only spread when it is deliberately sent by a user over the network or through other channels such as removable devices (i.e. USB-Stick). A virus makes changes to the system which are not wanted by the user. A virus on a service robot could delete files, reformat the hard disk or cause other damage to the system. Another goal of a virus could be for example to replicate itself to spread a text-file. This does not cause any damage to the system, but may take up memory or cause other unwanted system behaviours. Furthermore, a virus could put a robot out of order or cause environmental damage by sending commands to its actuators. The robot could also be used to cause psychologically harm to its owner by playing a scary audio file.
- **Spoofing and Phishing** Mobile service robots are used as personal assistants and one of their tasks could be to personally assist it's owner by, for example, scheduling events for its owner. This human robot interaction is naturally trusted by the user and believed to be personal, but in case of a phishing attack it is not. An attacker could for example trick the owner of a MSR into a fake conversation that is cheating the person into sharing private information with the robot.
- **Spyware** The goal of spyware is to gather information about a user without his knowledge. This information is usually sent back to the attacker over a network connection. A mobile service robot is a mobile platform full of sensors. Spyware programs can collect various types of personal information. An attacker might for example listen into your most private conversations or even watch what you are doing using the robots internal camera. Take for example long-term autonomy projects such as STRANDS[4] which aim to develop personalised MSRs that are capable, for example, to learn certain spatial patterns of their users like he is likely to not be in the office between 11:30 and 12:30. Such data is important to have for personalised robots, but could be also misused in one or another way.
- **Adware** On a robot we can imagine adware being installed together with an application that a user installs on the robot. Adware automatically displays advertising on a robots tablet device or might even access a robots actuators to play an advertisement. Robots open many more possibilities for adware developers. This malicious program might control the whole robot for advertising purposes, which is a critical safety issue. Furthermore, adware might contain spyware (see Spyware).
- **(Ro-)Botnet** A Botnet is a collection of Internet-connected devices which communicate and coordinate their actions through a command and control server or by sending messages to one another in a peer-to-peer fashion. Researchers observed that the increased appearance of IoT devices with default passwords lead to a huge increase of infected machines of the LizardStresser Botnet which has the capacity to launch DDoS attacks of 400Gbps upwards [20]. Mostly a Botnet steals computing resources and the robots performance may degrade as a result. More serious consequences may be caused by the programs that run on Botnets (see Trojan/Worm).
- **Worm** A computer worm is a self-replicating Malware. A worm does not need to be attached to a program, but uses for example 0-day exploits to spread itself through a network or the Internet, which differentiates it from a virus. Mobile service robots

[4] http://strands.acin.tuwien.ac.at/publications.html

are especially prone to worms, because they are connected devices that typically dont provide regular system updates. Worms can degrade network performance due to their replicating behaviour and they can also install back-doors on a system that allow the attacker to get complete control. The infected system can then be used to send spam or launch DDoS attacks as part of a bigger Botnet. Having complete control over the robot also results in privacy and safety issues.

– **Denial-of-Service attack (DoS)** A Denial-of-Service or DoS attack is an attempt to make a computer resource unavailable to users. If the attack is successful, the target machine cannot respond to legitimate traffic or responds slowly. DoS attacks are typically launched by Botnets, also known as Distributed DoS (DDoS) attacks. A DoS attack might slow down or completely crash a robots system. In [21], Vuong et al. show that using a multi-threaded TCP SYN floods on a robots network interface clearly impacted the robots movement and reaction time. DoS attacks might also be used to exploit buffer overflow vulnerabilities in software.

Countermeasures include the use of **microkernels** which minimise the codebase and are typically more secure and reliable. One example of such a micro-kernel is the seL4 [27]. The drawbacks of microkernels are a slight increase of controller latency and porting overhead for legacy code.

Furthermore, an OS can be secured, or **hardened**, by applying kernel patches, closing open network ports, installing Intrusion Detection Systems (IDS) and establishing firewall rules. As can be seen already in the smart-phone sector today, robots will have their own **Anti-virus** software that detects and eliminates known Malware.Some robots might provide application stores which allow users to download and install certain behaviours on the robot. Quality controls need to be established to avoid Malware coming from a robots application store.

To avoid infections trough removable-devices, it is encouraged to disallow any form of removable-device interfaces such as USB [6]. Softbank Robotics, for example, allows USB-Sticks to be plugged into its NAO robots, which are heavily used in research centres around the word. However, they do not directly provide any removable-device interface on their new Pepper robots, which are mainly designed for family and commercial use.

Robots should always be **updated** with the latest security updates because Malware spreads by exploiting vulnerabilities on the software and operating system level.

In case of Phishing attacks, the most effective way to handle this threat is through **vigilance**. Phishing, as a form of social engineering, relies on tricking users rather than on advanced technology. Well designed robot-human interfaces are needed to tackle this issue.

3.4 Threat Vector #5: Attacks on Infrastructure

The goal of this publication is to analyse the security of a mobile service robot itself. However, most MSRs are not only connected to the Internet, but also provide human-robot interfaces which allow remote control, either trough a website or special applications available for computers and smart phones. Therefore, we also need to consider this attack vector.

- **Standard Passwords** Most MSRs allow the user to authenticate using a predefined standard password [8]. These passwords can be changed manually by the user, which usually never happens. An attacker with network access to the robot can then easily access most of the robot's data. As can be seen in the Internet of Things (IoT) domain, standard passwords set by manufacturers should be avoided at all cost.
- **Passive and Active Eavesdropping** In [6], Denning et al. show that most mobile household robots do not provide any form of encryption. They show that Login credentials are send plain-text to the robot. Audio-visual streams of some of these robots did not require any authentication at all and allow everyone with network access to the robot to watch this stream.
- **Infected Machines** Other infected network devices could be used to attack and exploit any of its cyber vulnerabilities.This issue is not directly related to the robot itself, but nevertheless stays important. Especially regarding the use of standard passwords. Attacks on other devices are related to Thread Vector #3 : Attacks on Software.
- **Cloud Computing** Future mobile service robots might rely on cloud solutions to outsource storage, data sharing, collaborative planning and computationally expensive tasks like, for example, image recognition.

Homomorphic encryption schemes can, for example, be used to solve privacy issues related to the outsourcing computation to the cloud. Simple protection mechanisms such as authentication, access-control and encryption should be implemented to protect the robot and its data from unauthorised access, both locally and for remote connections.

Even though the robot is secured, a connection from an infected machine might lead i.e. to data theft. This might for example happen with the help of a keylogger which grabs the login credentials from the keyboard input of the infected machine. This attack however does not depend on the security of the robot itself. The user has to be aware of this and the same defence mechanisms that were mentioned in *Thread Vector #3 : Attacks on Software* should be applied.

4 CONCLUSIONS

In this work the security challenges introduced by Mobile Service Robots (MSR) are described. This work raises awareness on the different attacks that apply to robots by defining the adversary's motivations together with extensive list of threat vectors applying to MSR and tools that can be used to exploit these threats.

MSRs act in close proximity to humans and have the physical capabilities to cause serious harm to their environment. Furthermore, they have sensors that gather large amounts of data. Their physical capabilities are controlled by networked computers, which are susceptible to faults and intrusions inherited from current computer systems. Due to the characteristics of cyber-physical systems, cyber attacks can have severe consequences in the physical world and vice versa. We argue that MSRs are a prime target for casual hackers as well as state-level adversaries, partly because manufacturers seem to be negligent of security issues [6].

With this work we hope to raise awareness of the global threat plane of the specific threat vectors applying to MSRs. Security for MSRs is still a recent field and work is being done in many areas related to robotics, but mostly not applied. The robotic community should focus on being aware of and implement/fix well known security issues in robots. Security by design, is the right approach to follow if you design a robotic system. This means that the platform should be designed from the ground up to be secure. Privacy by design was out of the scope of this work, as the focus was on the security aspects of MSRs. Nevertheless it is a very interesting area and allows to provide a certain amount of privacy after the robot was hijacked [28].

Our future work will focus on real world experiments looking in greater detail at robotics frameworks like the Robot Operating System ROS, where recent work shows that there is great room for improvements [26].

ACKNOWLEDGMENT

Supported by the Fonds National de la Recherche, Luxembourg (Project ID:11609420)

References

1. Reuters: Demand for service robots seen at breakthrough: industry body (accessed 2017-01-03), https://goo.gl/pbTLLHL.
2. Fraunhofer Institute - Care-O-bot 4 - Technical data sheet, 2015.
3. Robot kills worker at Volkswagen plant in Germany (accessed 2017-01-03), https://goo.gl/wGOPwf.
4. E. Mitka, A. Gasteratos, N. Kyriakoulis, and S. G. Mouroutsos, "Safety certification requirements for domestic robots", Safety Science, vol. 50, no. 9, pp. 1888 1897, 2012.
5. Akdemir K.D., Karakoyunlu D., Padir T., Sunar B. (2011) An Emerging Threat: Eve Meets a Robot. In: Chen L., Yung M. (eds) Trusted Systems. INTRUST 2010. Lecture Notes in Computer Science, vol 6802. Springer, Berlin, Heidelberg.
6. Denning, T., Matuszek, C., Koscher, K., Smith, J.R., Koh no, T.: A spotlight on security and privacy risks with future household robots: attacks and lessons. In:Proceedings of the 11th international conference on Ubiquitous computing, pp.105114. ACM, 2009.
7. Knell, T., "Domestic robots: A case study on security in ubiquitous computing", 2014.
8. Yong, S.; Lindskog, D.; Ruhl, R.; Zavarsky, P., "Risk Mitigation Strategies for Mobile Wi-Fi Robot Toys from Online Pedophiles", Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom) , vol., no., pp.1220,1223, 2011.
9. Lee, M.K., Tang, K.P., Forlizzi, J. and Kiesl er, S. , "Understanding users' perception of privacy in human-robot interaction", In Proceedings of 6th International Conference on Human-robot Interaction, Lausanne, Switzerland, ACM, 181-182, 2011.
10. A. Uluagac, V. Subramanian, and R. Beyah. "Sensory channel threats to Cyber Physical Systems: A wake-up call", In Conference on Communications and Network Security, pages 301-309, 2014.
11. Fusion: Security robot accidentally attacks child (accessed 2016-07-15), https://goo.gl/uGLJto
12. J. Petit, B. Stottelaar, M. Feiri, F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR", Blackhat.com,p. 113,2015.

13. Son,Y., Shin,H., Kim,D., Park,Y., Noh,J., Choi,K., Choi,J., Kim,Y. "Rocking drones with intentional sound noise on gyroscopic sensors". In 24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, 2015. (2015), J. Jung and T. Holz, Eds., USENIX Association, pp. 881896.
14. N. Bezzo, J. Weimer, M. Pajic, O. Sokolsky, G. Pappas, and I. Lee, "Attack resilient state estimation for autonomous robotic systems", in Intelligent Robots and Systems (IROS 2014), 2014 IEEE/RSJ International Conference on,2014,pp.36923698.
15. Fan, J., Guo, X., De Mulder, E., Schaumont, P., Preneel, B., Verbauwhede, I.: State-of-the-art of Secure ECC Implementations: A Survey on Known Side-channel Attacks and Countermeasures. In: HOST, pp. 7687. IEEE Computer Society, Los Alamitos, 2010.
16. M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection",IEEE Des. Test Comput., pp. 1025, 2010.
17. S. Smyers : Hardware authentication mechanism for transmission of data between devices on an IEEE 1394-1995 serial bus network, Patent US5948136 A, 1999.
18. Wired: An Unprecedented Look at Stuxnet, the Worlds First Digital Weapon (accessed 2017-01-04), https://goo.gl/3tTDll.
19. Symantec: The 11 most common computer security threats (accessed 15 June 2016), https://goo.gl/Vo6fCE.
20. LizardStresser botnet targets IoT devices to launch 400Gbps attacks (accessed 30 June 2016), http://goo.gl/SBa9zW
21. T. Vuong, A. Filippoupolitis, G. Loukas, D. Gan, "Physical indicators of cyber attacks against a rescue robot", in IEEE International Conference on Pervasive Computing and Communications, pp. 338343, IEEE, 2014.
22. A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphrey s,"Unmanned aircraft capture and control via GPS spoofing", Journal of Field Robotics, 2014.
23. FX. Standaert : Introduction to Side-Channel Attacks, 2006.
24. Computerworld: Playing NSA, hardware hackers build USB cable that can attack (accessed 2016-08-01), http://goo.gl/kgBqrg.
25. Computerworld: Security researchers create undetectable hardware trojans (accessed 23 July 2016), https://goo.gl/PyuCXo.
26. F. J. R. Lera, J. Balsa, F. Casado, C. Ferandez F. M. Rio, V. Matean, "Cybersecurity in autonomous systems: Evaluating the performance of hardening ROS", alaga, Spain-June 2061, p. 47, 2016.
27. G. Klein, K. Elphinstone, G. Heiser, J. Andronick, D. Cock, P. Derrin,D. Elkaduwe, K. Engelhardt, R. Kolanski, M. Norrish, T. Sewell, H. Tuch, S. Winwood, "seL4: Formal Verification of an OS Kernel",2009.
28. D. J. Buttler, et al "Using Video Manipulation to Protect Privacy in Remote Presence Systems", 2015.
29. Guerrero-Higueras, A. M., DeCastro-Garcia, N., Rodriguez-Lera, F. J., Matellan, V. (2017). Empirical analysis of cyber-attacks to an indoor real time localization system for autonomous robots. Computers Security.
30. Psiaki, M. L., Humphreys, T. E. (2016). Protecting GPS from spoofers is critical to the future of navigation. IEEE Spectrum, 10.