NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

A SYSTEMATIC ANALYSIS OF ROBOTIC SECURITY AND INVESTIGATION

Yash Patel, Parag H. Rughani

School of Doctoral Studies & Research,
National Forensic Sciences University,
Gandhinagar, India
yash.phdcs20@nfsu.ac.in

Ph.D.
School of Cyber Security and Digital Forensics,
National Forensic Sciences University,
Gandhinagar, India
parag.rughani@nfsu.ac.in

***Abstract*—Robotics as being one of the growing fields is expected to change the life of humans in coming years. Rapid changes are being performed in the field of robotics to increase the usage of robots. They are mainly designed to replace human efforts and to be operated automatically. There are various types of robots used in different industries. Similar to other technologies, this technology also has a risk factor. Cybersecurity and digital forensic are the main aspects for researchers in robotics. Researchers have applied several tools and techniques to understand security aspects of robots and to acquire digital artifacts from the compromised robots. In this article we aim to study the work done in the areas of security and forensic investigation of robots. The article discusses basics of Robots and Robotics followed by analysis of work done by the researchers in the fields of security and forensics of robotics. The study suggests that a standard digital forensic framework is required for robots. The analysis also indicates that security and investigation of robots is still in its initial phase and requires a lot of research to be done in these fields.**

Keywords—Robotic; Robotic Security; Robotic Forensic; Cyber Security; Digital Forensics; Robot Operating System; ROS; Robots.

I. INTRODUCTION

In general, robotics is the combination of three major branches: computer science, electronics, and mechanical engineering. Robots are programmable machines that can work on demanding tasks and can replace humans in the real world. Initially, the robots were designed to perform monotonous tasks like manufacturing, shipping, handling, etc. Nowadays, the field of robotics is expanding, whereas they can work in every sector. Robots are growing in intellectual and mechanical compound capabilities in this field. Recently, they have become intelligent, flexible, and efficient machines.

Isaac Asimov was a famous fictional author. He has used the term robotics for the first time in the world. Asimov discussed three laws of robotics in his novel "Runaround" [1]:

Law 1 - Robots must never injure or harm humans.

Law 2 - Robots must obey the instruction of humans, without busting law 1.

Law 3 - Robots must defend their own existence, without busting law 1 and law 2.

Robots are created and manufactured in various shapes and sizes to perform specific tasks. They have immense opportunities in every field. Robots require hardware, software, and machine cognition [2]. Various types of robots are available such as pre-programmed, humanoid, autonomous, teleoperated, and augmenting robots. 1) Pre-programmed robots can perform monotonous tasks, which work in controlled environments. 2) Humanoids are robots that look and behave like humans. They can perform all the activities that humans can do. 3) Autonomous robots are independent robots, which operate on their own. Humans are not required during operational tasks. 4) Teleoperated robots are wirelessly connected robots and can be operated through remote places. These robots work in critical conditions where humans can not reach. E.g. Defusing bombs is a risky task, where augmenting robots can be used.

This article consists of seven sections as follows: Section 2 briefly presents the background of robots in cybersecurity and investigation. Brings out the various domains of robotics, problems and case studies related to cybersecurity of robots, several attacks based on the target layer of robots and others. Section 3 describes the fundamentals of robot operating system frameworks and analyzing the various vulnerabilities present in them. Section 4 highlights the overall security concerns of robots. Section 5 discusses existing forensic investigation techniques for robots. Section 6 discusses the future research path for the security and investigation of the robots. Section 7 concludes the article.

II. BACKGROUND

Robots play crucial roles in various industries such as defense, production, transportation, agriculture, academia, healthcare, hospitality, and many more. Robotics is a growing field in which many changes are taking place.

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

Nowadays, robots can interact with humans. However, recently many robotic related crimes (we call it robotic crimes) were noticed. Robots are not fully secure and have many known vulnerabilities as they are built upon existing software/hardware. These vulnerabilities, if explored, can cause cyber-attacks which could be dangerous to humans. Thus, the need to secure robots is realised by many researchers and industries.

Robots are critical assets of an organization. They need a secure and safe environment. So far, the robots were in the initial phase and had very limited use in the real world. Now, robots are everywhere and are capable of performing complex tasks with a high level of precision. Cyber threats for robotics are growing as systems are connecting digitally.

A. Domains of Robotics

In the robotics field, there are few highlighted fields in which robot application requires security and investigation. Nowadays, there are a variety of robot applications in various domains. The tasks given to robots in different fields are growing. The responsibility and dependency of robots in human lives are increasing. The latest robots can perform highly challenging tasks including space and water exploration. They have become smarter with the help of advanced artificial intelligence techniques like Deep Learning. Some of the major domains of Robotics are discussed below.

1) Military: The military domain is one of the critical domains as it involves risks to human lives and the economy. Nowadays, many agencies are developing highly advanced robots which can replace human soldiers. In general, the Unmanned Aerial Vehicles (UAVs) are used in Military for different purposes. These UAVs can be equipped with advanced weapons for defending attacks and for counter attacks. In one of the research carried out by Santiago Morante, et. al. [3], the authors have mentioned that communication between unmanned aerial vehicles (UAV) and computers is not encrypted. Whereas, any communications with these vehicles should be encrypted for compliance [4]. As per one of the reports, only 30% of military UAVs are using secure transmission which suggests that communication of around 70% of military UAVs can be easily intercepted by the unauthorized users [5]. However, in future, the military Robots can play a crucial role in search and rescue. They can be designed to search for explosives, miners, nuclear weapons, biological weapons, chemical weapons, etc. They can also be programmed to deactivate minefields and diffuse the bombs. Robots can easily fit in the space where humans can't go. Military robots may not only be used in defense but can also be used to attack. Robots may be made capable of identifying the target and attacking it.

2) Industry: The industrial domain uses programmable and armed robots that are stationary in the real world scenario. Armed robots are capable of moving through the axis for transferring goods. Industrial robots are utilizing applications such as welding, assembling, painting, material removing, transferring parts, machine tending, and collaborative tasks. They have cost-saving benefits and are very precise in the work. Collaborative robots are one of the types of industrial robots, which work together with other robots. Industrial robots can reduce workforce efforts by transferring assets from one place to another and can also work in a synchronized manner. They are used in critical environments where human lives are in danger and they do perform critical tasks [6]. Painting robots can reduce waste material and amount of time. They can paint in large areas as well as small areas of the products. The processes like assembling windshield and wheel mounting in vehicles are being automated with the help of robots. In small fabrication, robots can assemble pumps and motors at high speed. Robots are used everywhere and in every place of the world in this domain. Demand for industrial robots is increasing day by day as they can efficiently work in cutting, polishing, and trimming materials. Robots can accelerate the production process of the industry with higher speed and accuracy. Robots can also be used to perform tasks such as pouring molten metals, transferring metal strips, and loading Compressed Natural Gas (CNG).

3) Healthcare: Another major domain where robots are frequently used is healthcare where they can be used for nursing and surgical/medical treatment [7]. The Healthcare domain uses telemedicine [8], virtual care, and remote treatment. Collaborative robots are majorly evolving in operation rooms for highly precise surgical treatment and probably robot assisted surgery is one of the most demanding fields in robotics. Other than surgery, robots can assist in telepresence, medical transportation, sanitation, etc. Medical device packing is another application where collaborative robots (cobots) are used in packing medicines. Sterilization is a crucial task in which human contact is dangerous and if humans perform this task then, there is a high risk of contamination. Cobots make this simple for human life and eliminate the risk factor of humans. Lab automation is another application where blood sample testing in a lab requires more time and effort. A Lab in Copenhagen University Hospital performed 3,000 blood tests in a day manually while the same number of samples were tested in one hour with the help of a robot. Neurosurgery - one of the most complex branches of medical surgery relies on microscopes hence the robots are not capable of performing it. They can only be used to closely view the organ / part of the body to be operated due to the flexibility of moving them. Another example of use of robots in the medical domain is a robot called Kuku, which is equipped with a laser for cutting the bones. Kuku is the world's first robot that uses cold laser technology. It has no human contact while cutting the bones. Similarly, massage robots are designed for use in physiotherapy. This requires two Universal Robots (UR) for giving a full body massage to humans. The tele-operatable robots are remote-controlled and it reduces high risk of infection [9]. Some of the applications of robots for the healthcare domain are ARMAR III, Care-O-Bot 3, Cody, PR2, RIBA, Robotic Nursing Assistant, Hair-Washing Robot, ASIMO and ROSE [10].

4) Domestic: Domestic robots are also known as household robots. They are designed to help humans in day-to-day life. These robots can assist in vacuum cleaning,

pool cleaning, lawn mowing, floor cleaning, windows cleaning, entertainment, cooking, education, social interaction, security, and surveillance. They can also be designed to work in restaurant kitchens for cooking and chopping vegetables. This application of robots is used in Japan. Care-O-bot is a robotic assistance in homes [11]. Which has several features such as microphones, camera and 3D Sensors. The massive amount of data is collected through these sensors, which requires a safe environment to protect [12]. Nowadays, home robots have increased in the real world. Another useful category of domestic robots include elderly-care. The robot can check the health status and in case of emergency, it will notify the hospital or a family member. It can also schedule the medication time [13]. Vacuum cleaners are known as domestic cleaning robots and are connected to internet service. It will navigate the path of the floor while it will identify obstacles on the route through sensors. These robots have voice command functionality in which robots can work on a single command. Nowadays, robots are also used in providing home security and surveillance. They are designed to take care of residences and commercial properties in the absence of human beings. The artificial intelligence given to these robots allow them to notify an unauthorized access to the admin in case a malicious actor attempts to gain their access. Users can remotely operate robots and can check home at any time from any place using a robot camera. Latest robots are voice command enabled, so children can easily communicate with robots. Robots can also be used in teaching as they can assist the teachers in routine teaching.

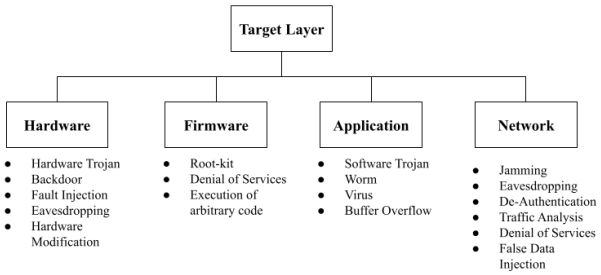
B. Cyber Security Threats in Robots

Like other technologies, robots are also vulnerable to cyber attacks. Robotic ecosystem has various attack surfaces for cybersecurity which consists of hardware, software, operating system, firmware, mobile application, internet services, network, cloud services. In one of the research carried out by Cesar Cerrudo, and Lucas Apa [14], the authors have found approximately 50 cybersecurity vulnerabilities from the robots ecosystem. Some of the vulnerabilities were common and others were a bit complex. The author's goal was to check how insecure robots are today. The author claims that their securitytesting was not at a high level. Some of the cybersecurity problems in robots are:

- Insecure Communications - Robots are connected with computers and mobiles using internet services. In many cases it has been observed that the communications between robots and computers are not encrypted. Attackers can easily intercept such insecure communications.
- Authentication Issues - In majority of implementations username and password are not required to access robot services which make it possible for anyone with sufficient technical skills to access it. It was also observed that if robot services require authentication then also it is not secure enough and can be easily bypassed.
- Weak Cryptography - Proper encryption is mandatory for Robots from cache sensitive data such as passwords, email, user social media, etc. Most of the robots are not using encryption in their ecosystem and a few use weak cryptography.
- Weak Default Configuration - It has also been observed that manufacturers and programmers are using the default password and common configuration mechanism in robots for easy access. Which makes it easy for anyone to review the functionality of robots by entering the default password and using common configurations.
- Vulnerable Open Source Robot Framework and Libraries - There are many open-source robot frameworks and libraries present in the world. However, these open-source solutions have many cybersecurity vulnerabilities. These vulnerabilities exist as the open source community is not able to update and patch the solutions with the pace by which the new vulnerabilities are discovered.

C. Cyber Attacks based on the Target Layer

The transformation of robotics is in rapid development. The range of robotics has changed from remote-controlled robots to humanoid robots. However, the advanced robotic technology being developed has a vast amount of risk. In this section, cyber attacks targeting different layers of the robotics system are identified and classified. Figure 1. Depicts threats corresponding to different layers of the robotic system.



1. Target Layer with their Threats

1) Attacks on Hardware Layer: Hardware trojan [15], hardware backdoor, fault injection, eavesdropping and hardware modification are few attacks which can target a hardware. Though these attacks are observed in almost all computer hardware, the hardware used in robots is also not an exception. An attacker can install a hardware-level backdoor in the robotic system to access the robots. During the maintenance process, high chances are there for attacking robots. Attackers can manipulate the hardware component by installing malware on robots or through the side-channel attacks or fault injection attacks which can result in loss of sensitive data. If the hardware used in a robot is vulnerable then the robot can be easily exploited through that vulnerable hardware.

2) Attacks on Firmware: Robots can update operating systems remotely using an internet connection. The code of the embedded system is held in flash memory [16]. Whenever the robot's operating system or firmware is

updated, zero-day cybersecurity vulnerabilities can take place, which leads to a growth in cybercrime. Robotic firmware has various attacks such as root-level access to a system, denial of services, and execution of arbitrary code. Whenever a robot is facing cybercrime on firmware, the attacker can access the embedded system and can install the malware on the robots, and the machine behaves like a bot.

3) Attacks on Robotic Software/Applications: Robotic software applications are vulnerable to security attacks as robots depend on application software for various tasks. Software applications of robots can be attacked by several attacks such as software trojan, worms, viruses, and others. Malware can be installed in robots using malicious code, which can collect sensitive data of users or can control operations of the victimized robot. Vulnerability in robot software application systems leads to compromised robots. The robots also possess ransomware [6] threat, a ransomware can encrypt sensitive data of the robot and can make it inaccessible.

4) Communication Attack on Robots: Robots communication can be prone to various attacks on security aspects like confidentiality, integrity, and authentication. Some of the attacks on robot communication include jamming, deauthentication, traffic analyzing, eavesdropping, false data injection, denial of service, man in the middle, etc. Jamming attacks target the availability of data and systems on robots. This attack can affect both the types of communication: robot-to-robot and robot-to-human. Robots are generally connected through internet connection. A deauthentication attack on robots can lead to broken connections between robotic devices. In such cases, anyone can join the internet connection and intercept and analyze the robot's traffic. The worst thing happens when the traffic is not encrypted as it happens in the majority of robotic communications. The man-in-the-middle attack can also be performed to take control of the robot [6].

D. Case Studies of Compromised Robots

The economy and human safety are the major issues in robotic technology. The main reason behind the robotic threat to humans is that the security of robots is not a priority while designing and manufacturing robots. A high range of attack vectors is available in the various layers of the robot. There are several consequences whenever robots are compromised. A few case studies surveyed are discussed in the following section:

In one of the incidents related to a home assistant robot for senior citizens, the robot named elder care was compromised [13]. In this, an elderly person living alone was assisted by the robot. The robot was designed to perform different tasks like medical care, household tasks, communication, cleaning the house and many more. The robot included a microphone, speaker, and camera communication features to become effortless for senior citizens. Whenever, there is an emergency situation, or for medical status the robot will notify the family member of the elderly person. Attackers targeted the network layer and compromised the robot by using wireless networks. After the attacking phase, the total control over the robot was with the attacker. Attackers could gain access to the sensitive data from the robots such as credit card data, banking information, etc and monitor the elderly person's activity via camera.

In another instance that happened in the automotive industry [17], where the autonomous car was compromised in a real life scenario. The production of autonomous cars was growing rapidly, and was entirely automated using some of the major features like intelligent keys, driverless driving, hands-free door lock, anti-collision proof, etc. These cars were designed to be self-driven on the roads. The wireless communication networks were used for operating sensors. However, the sensors of the cars were attached through internal networks. Here, attackers intercepted radio signals which were used on the car door system, but the signals were encoded. They used several tools for decoding the radio signals. Afterward, the attackers were able to access the internal network of the cars, and could disable breaks, monitor roads, and operate every sensor used in the cars.

In one of the similar instances that happened in the military domain [13], where an operation of the military of one country was using drones for surveillance on another country's military activities. In these drones, the design and manufacture of the components were from the country which was being monitored. After investigation, it was found that there were hardware backdoors by the manufacturing company. The kill switch was enabled in components, wherever a certain range of GPS coordinates intercept. Attackers could gain access to the drone after intercepting GPS coordinates.

In another incident that happened in the healthcare domain [17], where a teleoperated robot that can be used in surgery, named Raven II [18] was compromised by the attackers. These robots can perform telesurgery autonomously which have eight motion axes, including wrist 1 actuation, wrist 2 actuation, elbow join, shoulder join, insertion tool, roll tool, and grasping tool. Using these robots the infection spread in the hospital was eliminated and doctors, nurses and patients were protected. The surgery robots were using a robot operating system for performing tasks. Robots were connected to a public network, the attackers gained access to the surgery robot from the public network. In this scenario, the attackers performed a Denial of service attack on the robots when a critical surgery of the human was going on.

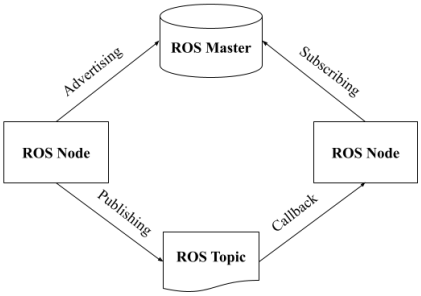
Above are a few incidents where the robots in different fields were compromised. The list can go on as the use of robots is being increased in different levels.

III. THE ROBOT OPERATING SYSTEM (ROS)

Like computers, the robots also need an operating system to function. One such operating system called Robot Operating System (ROS) has been in use since 2007 and is one of the most popular Robot Operating Systems till date. It is mostly used for industrial and academic purposes. Robotic technology is using robot operating systems for the development of robotic ecosystems, and it is a meta operating system framework that connects robot-to-human and robot-to-robot interaction. It can be used as a middleware on Linux and Windows platforms. Being highly focused on mechanical robots, security has never been a focused area in the robot operating systems [19]. In 2014, the ROS version was modified to ROS 2. The robot operating

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

system has a peer-to-peer network connection, which consists of ROS master, nodes, topics, messages, and services. ROS has a publisher/subscriber model for transferring messages. This system has several independent nodes, which are interconnected with each other for communication. An ROS model is explained in Figure 2.



2. ROS Model

- ROS Master - This node is the head communication hub of the robotic system. It has the responsibility of managing name services and providing connections between nodes. Whenever a new node is installed, it informs the master node about topics and publishing/subscribing. ROS master node will track the offered services and topics of the robot system, it maintains internal communication. If there will be no master node, then the nodes can not find each other for communication.
- ROS Nodes - This node has a process to perform the computation of robotic systems. Each and every node has its own name, which is recorded in the ROS master. ROS nodes can receive information from other nodes, and send information to nodes. ROS nodes have to communicate with each other and report to ROS master nodes.
- ROS Topic - Topic is a primary form of communication in robotic systems. Messages are communicated in the robotic system through the ROS topic. To identify the content of the messages ROS topic is used. ROS node will publish the message to the ROS topic. ROS topic will callback to the receiving node and transfer the information to another node. Topic names should be unique in the namespace, and content for ROS topics will state information, sensor data, motor commands, etc.
- ROS Messages - Nodes are sending and receiving messages with each other. ROS Messages are information that a node will dispatch to other nodes. It is a data structure that can hold data in it. Messages will be in data type such as integer, floating-point, and boolean. The data type can be built-in or customized.
- ROS Services - The node can advertise services in robotic systems. Services can be used to send a request and handle a reply. It represents an action that has defined the starting and ending. Services are in pairs; requesting form a node or responding to a node.

A. Vulnerabilities of Robot Operating System

The robot operating system is the most adopted framework used in various industries and academia for the development of robotic ecosystems, which have security related issues in it. Researchers have found several vulnerabilities in ROS. If an attacker can take control of ROS nodes, then it is possible to compromise ROS-based robots. In this article, some common vulnerabilities of robot operating systems are discussed [20][21].

- Application Programming Interface (API) misuse
- Data manipulation
- Data acquisition
- Flow Control
- Race Condition
- Security issues
- Unvalidated input

The listed vulnerabilities have the potential to compromise robots. These vulnerabilities are executed using attacks such as application programming interfaces misuse which can be faced through denial of service, evasion, and insertion. Data manipulation can be performed through eavesdropping and data alteration which leads to modification of the data of ROS-based robots by the attackers. Traffic sniffing will come under data acquisition, by intercepting the packets from an internet connection, where the attacker can analyze the traffic. Flow control includes buffer overflow of the ROS. Race conditions can be executed with denial of service and side channel attacks. Access control, authentication, authorization, and cryptography are security issues present in the ROS. The validation of parameters is not present in ROS. So, attackers can steal sensitive information using unvalidated input vulnerabilities [22].

IV. Security of Robots

In Robots, there are various target levels for compromising them and they can be attacked through remote places. Users or attackers can control, operate, monitor, and analyze robots from remote places. This section discusses research done by various authors in the field of robotic security.

Cesar Cerrudo, and Lucas Apa [14] discovered cybersecurity issues related to robots from various vendors. Several vulnerabilities had been pointed out in this research. Some of the robots were compromised using critical vulnerabilities. Similarly, Ishaani Priyadarshini [17] determined the cybersecurity risks involved in robots. The author highlighted the current situation of the robotic era, which is vulnerable to too many risks. Some of the case studies related to robots attempting the crime were discussed in this research. Several mitigation strategies are discussed to avoid cybersecurity risks on robotic systems.

Laura Alzola Kirschgens, et al. [23] discussed some case studies on robot safety. The authors also mentioned that not protecting robots will cause human loss, injuries, data theft, privacy issues, and destruction of the organization's reputation. They suggested that safe operational tasks are required for robots and for that security-first approach must take place. Wojciech Dudek & Wojciech Szynkiewicz [24] conducted a survey on the implementation of cybersecurity functions on robots. The authors suggested detection,

prevention, and reaction steps for securing robotic systems and evaluating the mobile service robot system for finding the complex threat

Jarrod McClean, et al. [25] assessed cyber-physical security of the robot operating system. The authors performed an experiment where ROS was kept between the hardware and software of the honeypot. The authors could intercept the ROS messages which were transferred from one node to another node using Wireshark. The wireshark data revealed that the communication was done in plain text. Several other common vulnerabilities and authentication solutions were also discussed in the research. Similarly, Santiago Morante, et al. [3] identified the security needed in robots and important issues related to robot cybersecurity. As per the authors, robots are not mature in terms of cybersecurity. There have been many problems in different industries, which were stated in the research. One of them is communication in robotics, which is usually done in plain text.

Munkenyi Mukhandi, et al. [26] demonstrated a process for securing robot communications based on MQTT protocol. They have designed the architecture and implemented the MQTT protocol for ROS communication. Experiments were to analyze response time, message throughput and rate with security and without security. After evaluation of the result, there was a negligible delay in time, throughput, and rate. The authors suggested that it is better to use it with security rather than without security communication. Bernhard Dieber, et al. [27] proposed a secure channel architecture and key management system for ROS. The authors evaluated the overhead performance of secure communication channels of ROS.

Abdul Hadi Abd Rahman, et al. [28] analyzed the robot communicates using CrptoROS. CrptoROS provides peer-to-peer communication on the ROS nodes. The authors compared performance with and without CrptoROS by communicating 100, 250 and 500 messages. Computation time for with and without CrptoROS were having negligible differences. The authors concluded that CrptoROS was protecting the messages from unauthorized users without affecting performance. Jongkil Kim, et al. [19] identified the security and performance issues related to the ROS2 system. The authors tested latency and throughput performance on wired and wireless networks. The test was based on communication security using various forms such as no security, cryptographic algorithm, and SSL/TLS. The results showed that it is better to use SSL/TLS communication security for ROS2.

Victor Mayoral-Vilches, et al. [29] demonstrated the flow of ransomware attacks on Robots which included cyber intrusion system, lateral movement, and control phase. In an experimental trial, Universal Robot - an industrial robot was used for testing against ransomware attacks. The authors created their own ransomware for industrial robots, named Akerbeltz. They installed ransomware into a robot which led to the user interface compromising phase. The data on the robot was encrypted by the ransomware and the legitimate user could not access the robot.

Similarly, Alberto Giaretta, et al. [30] assessed the humanoid robot called Pepper. The focus of their research was on manual and automated analysis of Pepper. In automated assessment, port scanning using Nmap and vulnerabilities scanning techniques were used. In manual assessment, ARP spoofing & traffic analysis using Wireshark, SSH dictionary brute force using hydra, simple animated messages, man-in-the-middle attack and remote control without authentication techniques were used. Mitigation of the vulnerabilities assessment through automated and manual analysis were also discussed in their research.

Sean Rivera, et al. [31] proposed a reconnaissance and exploitation tool for ROS called ROSploit which is similar to Nmap and Metasploit. Authors demonstrated some attack vectors possible on a robot application such as unauthorized publishing (injections), unauthorized data access, and denial of service on specific ROS nodes. Matt Kinzler, et al. [32] examined the security of two humanoid robots named NAO and JD. These robots can be used in local networks, in which anyone can connect with it. Packets captured through Wireshark were found to be in plain text. The authors also observed that default root account credentials were used in both the robots. The authors compared NAO and JD robots in terms of robotic cybersecurity.

Rafael R. Teixeira, et al. [33] identified that ROS-based robots can be successfully compromised. An autonomous robot called DoRIS was used in this experiment. The authors used Nmap for finding the IP address and ports of the robots. The malicious packets of ARP were sent to the server for eavesdropping on the communication. Attackers could easily take control over the data collected through ROS nodes. The authors used Man in the middle attack and ARP poisoning in their experiment.

Sofiane Lagraa, et al. [34] performed a security assessment of robot cameras using ROS and determined an intrusion detection system to detect abnormal flows on ROS. They identified several security flaws in robot cameras. In their experiment the authors performed attacks such as new image insertion using a black or white image, blurry image, flooding black image, modified images, etc. After compromising ROS camera nodes, the attacker could perform remote supervision, fake flow modification, and injection.

Bernhard Dieber, et al. [21] proposed a security architecture for ROS at the application level. In their experiment, the authors used an industrial domain robot named KUKU iiwa. Authors used an authorization server for communication to prove that secure communication between ROS nodes is possible with such servers and robots can be secured from false commands injection. Khalil M. Ahmad Yousef, et al. [35] assessed PeopleBot mobile robots. They identified the wireless communication risk between the robot and the user. In this experimental trial, the authors performed a DoS attack using IPv6 RA flood and another DoS attack using deauthentication of a wifi network.

Bernhard Dieber, et al. [36] proposed a security architecture for mobile manipulator robots. In this experiment several attack vectors, such as physical access, remote access via an external network, and access via hardware module were

executed. The results of the experiment suggest that use of chimera security architecture can prevent infection in other nodes even if a node is compromised. The authors concluded that the rate of risk of robots getting compromised is low after using chimera security architecture. Kacper Wardega, et al. [37] proposed a multi-agent path-finding through the observation plan against the masquerade attacks in multi-agent robots. Multi-agent robot systems consist of similar types of robots. The authors proposed that the observation plan can help in detecting a compromised robot from such systems.

Yamin Hu & Wenjian Luo [38] proposed an architecture of the robotic immune system similar to the biological immune system. The proposed architecture can protect a robotic system from external data or network. It has a multi-layer immune system such as environment, spam filtering, information fusion and response. The authors used innate and adaptive techniques in their proposed robotic immune system. The innate technique uses a rule-based method and the adaptive technique uses a self-learning approach.

V. Forensic Investigation of Robots

Though, not many cyber crimes pertaining to robots are reported, there is a need to consider the investigation aspects. We could find a very small number of articles related to forensic investigation of robots, some of them are discussed in this section.

Victor Mayoral Vilches, et al. [39] proposed a volatility plugin called ros_volatility which can be used to detect an attack on ROS. The application of the plugin was demonstrated by the authors with a scenario where unauthenticated registration of ROS nodes was attempted and the ros_volatily plugin was able to identify the attacker.

Giuseppe Vaciago & Francesca Bosco [40] proposed the need of a framework for the acquisition of digital evidence for robots. The authors suggested that best practices of rules and procedures for acquiring digital evidence from robots should comply with national or international bodies. The authors also emphasized on the need to have rules and procedures for protecting robots against possible cyber attacks.

Mawj Mohammed Basheer & Asaf Varol [41] reviewed security and digital forensic of robot operating systems. The authors suggested that the studies in the field of robotic forensic are extremely limited and it is a premature area of research.

VI. Discussion

The evolution of robotics in the real world is adopting rapidly. There have been several risk factors in the development of robots. Cyber safety in robots required more focus for the elimination of cybercrime. Most of the robots in the various industries are not prepared for security attacks and have been deployed in a hurry. Robots have started committing crimes such as killing humans, injuring humans, damaging themselves, destroying things, etc. The ecosystem of robots has security flaws at various target levels. Several robots have been tested for security assessment and almost similar vulnerabilities were identified. The rate of computation with and without security on robot communication has been discussed by many authors and the negligible difference of time was also observed.

The robot operating system (ROS), which is one of the most frequently used in robots, was developed in 2007. The studies on the digital investigation of this system are extremely limited. There has been major importance on the regulation governing framework of digital forensic and cyber security for robotics technology. Whenever a robot has attempted any crime, the first approach should be the digital forensic investigation of that system. Several existing techniques can be used on ROS for the investigation of the incidents, however dedicated tools and techniques to investigate robots are not yet available.

VII. Conclusion

Robotic technology is an emerging technology in the world. Robots have been acquired in several fields such as military, industrial, healthcare, domestic and others. This review article was aimed to study security and investigation of robots. Based on the review of work done so far, we could identify several research gaps in the field of security and investigation of robots. As per one of the observations we could see that the majority of researchers are more concerned about security aspects and only a few have worked on the investigation of robots. It has also been observed that researchers were using different types of robots but the result was almost similar. Since, a very limited work with the traditional approach is done in this field, we recommend novel research in both the domains: robotic security and investigation.

References

[1] George A. Bekey, Autonomous Robots- From Biological inspiration to Implementation and Control, MIT Press, Cambridge Massachusetts, London, England, Chapter-1, pp. 01-02, 2005.

[2] HUTTUNEN, J. KULOVESI, W. BRACE et al., Liberating Intelligent Machines with Financial Instruments, in “Nordic Journal of Commercial Law”, 2010, n. 2, available at http: //ssrn.com/abstract=1633460.

[3] Morante, Santiago & Victores, Juan & Balaguer, Carlos. (2015). Cryptobotics: Why Robots Need Cyber Safety. Frontiers in Robotics and AI. 2. 10.3389/frobt.2015.00023.

[4] Javaid, A. Y., Sun, W., Devabhaktuni, V. K., and Alam, M. (2012). “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” in 2012 IEEE Conference on Technologies for Homeland Security (HST), 585–590. doi:10. 1109/THS.2012.6459914.

[5] Most U.S. Drones Openly Broadcast Secret Video Feeds: http://www.wired.com/ 2012/10/hack- proof-drone/

[6] Yaacoub, JP.A., Noura, H.N., Salman, O. et al. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. Int. J. Inf.

Secur. (2021). https://doi.org/10.1007/s10207-021-00545-8.

[7] Azeta, Joseph & Bolu, Christian & Abioye, Abiodun & Oyawale, Festus. (2018). A review on humanoid robotics in healthcare. MATEC Web of Conferences. 153. 02004. 10.1051/matecconf/201815302004.

[8] Kadir, M.A.: Role of telemedicine in healthcare during covid-19 pandemic in developing countries. Telehealth Med, Today (2020).

[9] Riek, L. D. Healthcare Robotics. (2017). Retrieved from http://arxiv.org/abs/1704.03931.

[10] K. Doelling, J. Shin, and D. O. Popa, "Service robotics for the home: a state of the art review,"in Int. Conf. on Pervasive Technologies Related to Assistive Environments. ACM, p. 35. (2014).

[11] Hans, M., Graf, B., and Schraft, R. (2002). "Robotic home assistant care-o-bot: past- present-future," in Proceedings of the 11th IEEE International Workshop on Robot and Human Interactive Communication, 2002, 380–385. doi:10.1109/ROMAN. 2002.1045652.

[12] King, H. H., Tadano, K., Donlin, R., Friedman, D., Lum, M. J., Asch, V., et al. (2009). "Preliminary protocol for interoperable telesurgery," in the International Conference on Advanced Robotics, 2009. ICAR 2009, 1–6. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5174711&isnumber=5174665

[13] Clark, G.W., Doran, M.V., & Andel, T.R. (2017). Cybersecurity issues in robotics. 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), 1-5.

[14] Cerrudo, Cesar & Lucas Apa. (2017). Hacking Robots Before Skynet. IOActive, 1.

[15] Wang, X., Mal-Sarkar, T., Krishna, A., Narasimhan, S., Bhunia, S.: Software exploitable hardware Trojans in embedded processors. In: 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp. 55–58. IEEE (2012).

[16] Elmiligi, H., Gebali, F., El-Kharashi, M.W.: Multi-dimensional analysis of embedded systems security. Microprocessor. Microsyst. 41, 29–36 (2016).

[17] Priyadarshini, Ishaani. (2017). Cyber Security Risks in Robotics. 10.4018/978-1-5225-2154-9.ch022.

[18] Hannaford, J. Rosen, D.W. Friedman, H. King, P. Roan, L. Cheng, D. Glozman, J. Ma, S.N. Kosari, and L. White. Raven-II: An Open Platform for Surgical Robotics Research. IEEE Transactions on Biomedical Engineering, 60(4):954–959, 2013.

[19] Kim, Jongkil & Smereka, Jonathon & Cheung, Calvin & Nepal, Surya & Grobler, Marthie. (2018). Security and Performance Considerations in ROS 2: A Balancing Act.

[20] Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass and P. Schartner, "Security for the Robot Operating System," Journal of Robotics and Autonomous Systems. vol. 98, 192-203, 2017.

[21] Dieber, S. Kacianka, S. Rass and P. Schartner. (2016). Application-level security for ROS-based applications. 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 4477-4482. doi: 10.1109/IROS.2016.7759659.

[22] V. DiLuoffo, W. R. Michalson and B. Sunar, "Robot Operating System 2: The Need for a Holistic Security Approach to Robotic Architectures," International Journal of Advanced Robotic Systems vol. 15, 2018.

[23] Laura Alzola Kirschgens and Irati Zamalloa Ugarte and Endika Gil-Uriarte and Aday Muniz Rosas and Victor Mayoral Vilches (2018). Robot hazards: from safety to security. CoRR, abs/1806.06681.

[24] Dudek, Wojciech & Szynkiewicz, Wojciech. (2019). Cyber-security for Mobile Service Robots – Challenges for Cyber-physical System Safety. Journal of Telecommunications and Information Technology. 2. 29-36. 10.26636/jtit.2019.131019.

[25] Mcclean, Jarrod & Stull, Christopher & Farrar, Charles & Mascareñas, David. (2013). A Preliminary Cyber-Physical Security Assessment of the Robot Operating System (ROS). 874110. 10.1117/12.2016189.

[26] Mukhandi, Munkenyi & Portugal, David & Pereira, Samuel & Couceiro, Micael. (2019). A novel solution for securing robot communications based on the MQTT protocol and ROS. 10.1109/SII.2019.8700390.

[27] Dieber, Bernhard & Breiling, Benjamin. (2019). Security Considerations in Modular Mobile Manipulation. 10.1109/IRC.2019.00019.

[28] Abd Rahman, Abdul Hadi & Sulaiman, Rossilawati & S Sani, Nor & Adam, Afzan & Amini, Roham. (2019). Evaluation of Peer Robot Communications using CryptoROS. International Journal of Advanced Computer Science and Applications. 10. 10.14569/IJACSA.2019.0100786.

[29] Victor Mayoral Vilches and Lander Usategui San Juan and Unai Ayucar Carbajo and Rubén Campo and Xabier Sáez de Cámara and Oxel Urzelai and Nuria Garcia and Endika Gil-Uriarte (2019). Industrial robot ransomware: Akerbeltz. CoRR, abs/1912.07714.

[30] Giaretta, A., Donno, M., & Dragoni, N. (2018). Adding Salt to Pepper: A Structured Security Assessment over a Humanoid Robot. Proceedings of the 13th International Conference on Availability, Reliability and Security.

[31] S. Rivera, S. Lagraa & R.State. (2019). ROSploit: Cybersecurity Tool for ROS. 2019 Third IEEE International Conference on Robotic Computing (IRC), pp. 415-416. Doi: 10.1109/IRC.2019.00077.

[32] Kinzler, Matt, Miller, Justin, Wu, Zhou, Williams, Andrew, & Perouli, Debbie. (2019). Cybersecurity Vulnerabilities in Two Artificially Intelligent Humanoids on the Market. 40th IEEE Symposium on Security and Privacy. https://par.nsf.gov/biblio/10099177.

[33] Teixeira, Rafael & Maurell, Igor & Drews Jr, Paulo. (2020). Security on ROS: analyzing and exploiting vulnerabilities of ROS-based systems. 1-6. 10.1109/LARS/SBR/WRE51543.2020.9307107.

[34] S. Lagraa, M. Cailac, S. Rivera, F. Beck and R. State. (2019). Real-Time Attack Detection on Robot Cameras:

A Self-Driving Car Application. 2019 Third IEEE International Conference on Robotic Computing (IRC), pp. 102-109. doi: 10.1109/IRC.2019.00023.

[35] Ahmad Yousef, Khalil & Almajali, Anas & Hasan, Roa'a & Dweik, Waleed & Mohd, Bassam. (2017). Security Risk Assessment of the PeopleBot Mobile Robot Research Platform. 10.1109/ICECTA.2017.8251984.

[36] Breiling, Benjamin & Dieber, Bernhard & Schartner, Peter. (2017). Secure Communication for the Robot Operating System. 10.1109/SYSCON.2017.7934755.

[37] Kacper Wardega, Roberto Tron, and Wenchao Li. (2019). Masquerade Attack Detection Through Observation Planning for Multi-Robot Systems. 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019), Montreal, Canada, May 13–17, 2019, IFAAMAS, 3 pages.

[38] Hu, Yamin & Luo, Wenjian. (2018). Robotic Immune Systems: An Architecture. 1098-1103. 10.1109/SSCI.2018.8628619.

[39] Vilches, V., Kirschgens, L.A., Gil-Uriarte, E., Hernández, A., & Dieber, B. (2018). Volatile memory forensics for the Robot Operating System. ArXiv, abs/1812.09492.

[40] Vaciago, G., & Bosco, F. (2014). New Challenges in Robotics. Cyber Security and Digital Forensics.

[41] Mohammed, Mawj & Varol, Asaf. (2019). An Overview of Robot Operating System Forensics. 1-4. 10.1109/UBMYK48245.2019.8965649.