GlobalLogic®

Advances in Robotics and Cybersecurity

by Bharat Bhooshan Tyagi

Abstract

Robotics has been in existence for nearly a century and continues to evolve with technological advancements in areas that include both software and hardware. A robot can be as small and simple as a remote control or as complex as a humanoid. Robots have become an integral part of human life, and their use cases range from household utilities to medical, defense, and space projects.

Robots are primarily computer systems with physical capabilities. In general, they suffer from security issues similar to what computers have faced for decades. If robots are compromised, two different types of security threats may arise:

- Virtual security risks such as breach of data, hacked communication, etc.
- Physical aspects which concern the integrity of the robot and its operator.

Thus, both the virtual and physical issues in robotics platforms are part of cyber-physical security.

Contents

Robots

The term robot comes from the Czech word robota, which means forced labor.

A robot can be defined as a controlled unit designed to perform tasks in a repeated manner with speed and precision. A robot may be controlled by a computer or a human operator.

Types of Robots

Pre-programmed Robots

These robots operate in a controlled environment where they perform non-complex, repeated tasks.

Humanoid Robots

A humanoid robot generally has a human appearance and imitates human behavior. Humanoids generally perform activities similar to humans, such as running, jumping, and talking.

Autonomous Robots

These robots operate independently of human operators and choose their actions based on the information they gather via sensors. They perform activities in open environments that do not require human supervision.

Tele-operated Robots

These are mechanical bots that are controlled by humans. These robots usually work in extreme geographical conditions, weather, circumstances, etc.

Augmenting Robots

These Robots are empowered with more capabilities or replace the abilities a human may have lost.

Generations of Robots

First Generation

The first-generation robots are simple mechanical arms that can perform precise motions at high speeds, repeatedly and continuously for days. These robots are mostly used in manufacturing industries.

Second Generation

The second-generation robots that were commonly used in the 1980s are loaded with a number of different sensors, such as proximity, pressure, and tactile sensors, as well as radar and vision systems. The controller device adjusts the operation of the robots based on the data collected by the sensors.

Third Generation

The third-generation robots are of two kinds and made with smart technologies: the autonomous robot and the insect robot. An autonomous robot is a sensor-based intelligent machine that can perform tasks mostly without supervision. Insect robots are collections of very small robotic devices, all under the control of a central computer. These machines work like bees in a hive or ants in anthills.

Fourth and Beyond

There are currently no robots in operation that can be identified as fourth-generation robots.

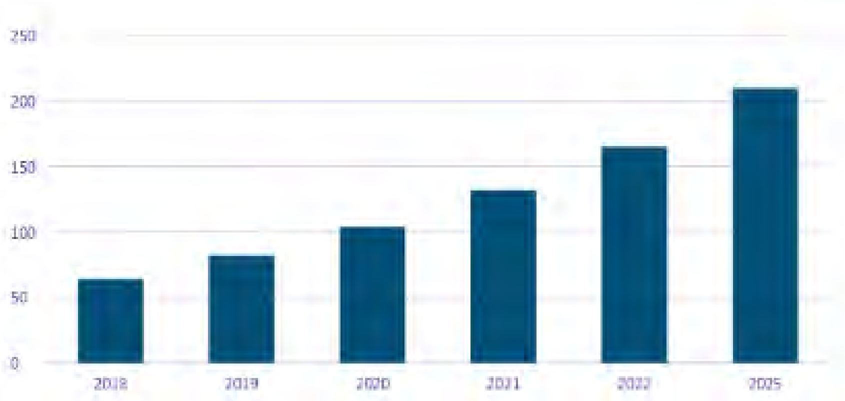
Robotics

Robotics is the study of robots.

According to Wikipedia, “Robotics is an interdisciplinary research area at the interface of computer science and engineering. Robotics involves the design, construction, operation, and use of robots. The goal of robotics is to design intelligent machines that can help and assist humans in their day-to-day lives and keep everyone safe. Robotics draws on the achievement of information engineering, computer engineering, mechanical engineering, electronic engineering, and others.”

Market Revenue

According to Statista, the global market for robots is expected to grow to just under 210 billion US dollars by 2025 at a compound annual growth rate of around 26%.



Robotic Platforms

Here are some of the robotic platforms that anyone can use to build and test robotic applications.

Robotics Benchmarks for Learning with Low-Cost Robots (Google ROBEL)

ROBEL is an open-source platform designed primarily to facilitate R&D for physical hardware in the real world. This category of robotic platform includes robots that are low-cost, modular, easy to maintain, and are reliable enough to open up the field of Reinforcement Learning.

Aerial Informatics and Robotics Simulation (Microsoft AirSim)

Microsoft's AirSim is an open-source robot simulation platform. Robots built on this platform can capture data for models from wheeled robotics and aerial drones to static IoT devices. AirSim can be used by designers and developers for seamless generation of training data and various computations in order to create real-world simulations.

Apollo Baidu

Apollo Baidu is an open, reliable, and secure software platform for designing and developing autonomous driving systems through on-vehicle and hardware platforms.

NVIDIA Isaac

NVIDIA Software Development Kit (SDK) is a developer toolkit for the creation and deployment of artificially intelligent robots.

AWS RoboMaker

RoboMaker is a cloud-based integrated robotics development environment created by AWS. It can help developers plan, deploy, and test robotics applications using cloud services.

ROSbot 2.0

ROSbot 2.0 is a development platform for autonomous robots. It has sturdy mechanics, strong computation, and state-of-the-art sensors like RGB-D (depth sensor) camera, Light Detection and Ranging (LiDAR) sensors, and expansion ports.

Risk Assessment of Robotic Platforms

The following are some of the common security problems facing robotics platforms.

Insecure communications

Most robotic platforms rely on wifi or Bluetooth technology to connect robotic devices to the internet. The data that is exchanged either has very weak encryption or sometimes is in plain text. This kind of insecure communication can easily lead to a cyberattack.

Authentication issues

Often, key robot services do not require authentication, allowing anyone to acquire remote access to those services. In some cases, where services use authentication, either it is very weak or can be bypassed easily.

Missing authorization

Most robots expose their functionality (including the installation of applications) and many other critical functionalities without sufficient authorization. This provides an easy opportunity for an attacker to install malware and gain full control.

Privacy issues

Robots often capture and send a user's private information through remote servers but without consent. This information may pertain to the device, service provider (network), or current geographic location, etc., along with other critical and sensitive private data.

Weak default configuration

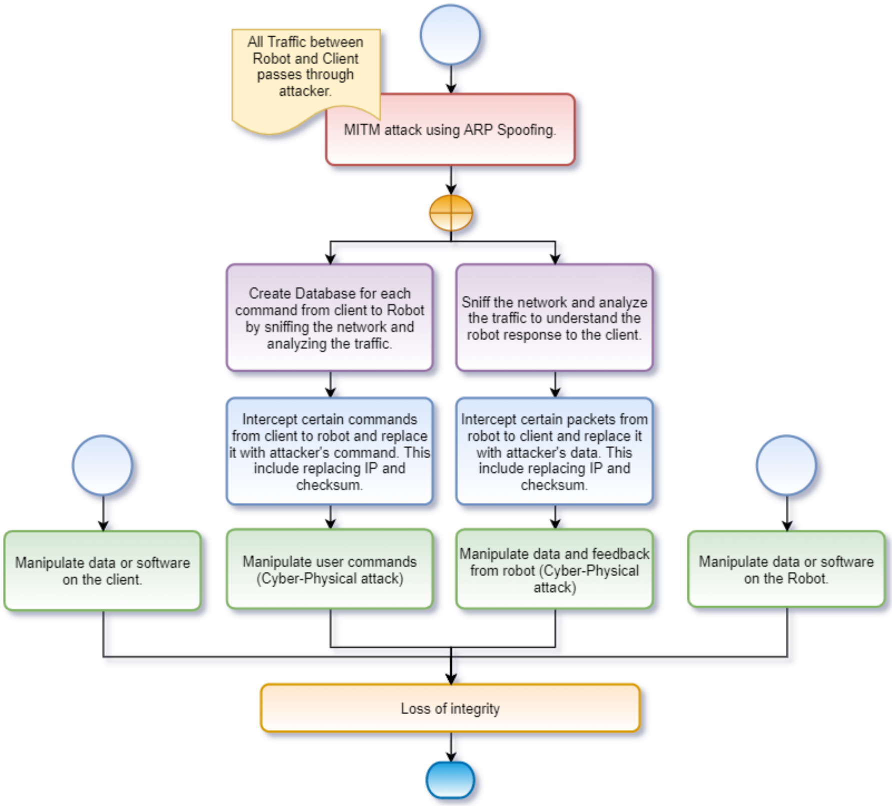
Most robotic devices have default configurations that are easy to guess, and attackers can take advantage of them. There have been instances when a default password configuration doesn't have a provision to protect the password or change it.

Types of Attacks on Robots

Integrity Attacks

The intention of the man-in-the-middle (MITM) attacker is to alter a robot's behavior or the response (statistical data, readings, video clips, etc.) it sends back to the client. The loss of integrity is achieved by altering/manipulating the communication between the client and the robot to cause cyber-physical impacts.

An integrity attack can be performed at different levels (depending on how close the attacker is to the target, i.e., robot or the controller), as shown in the following flowchart.



All Traffic between Robot and Client passes through attacker.
MITM attack using ARP Spoofing.
Create Database for each command from client to Robot by sniffing the network and analyzing the traffic.
Sniff the network and analyze the traffic to understand the robot response to the client.
Intercept certain commands from client to robot and replace it with attacker's command. This include replacing IP and checksum.
Intercept certain packets from robot to client and replace it with attacker's data. This include replacing IP and checksum.
Manipulate data or software on the client.
Manipulate user commands (Cyber-Physical attack)
Manipulate data and feedback from robot (Cyber-Physical attack)
Manipulate data or software on the Robot.
Loss of integrity

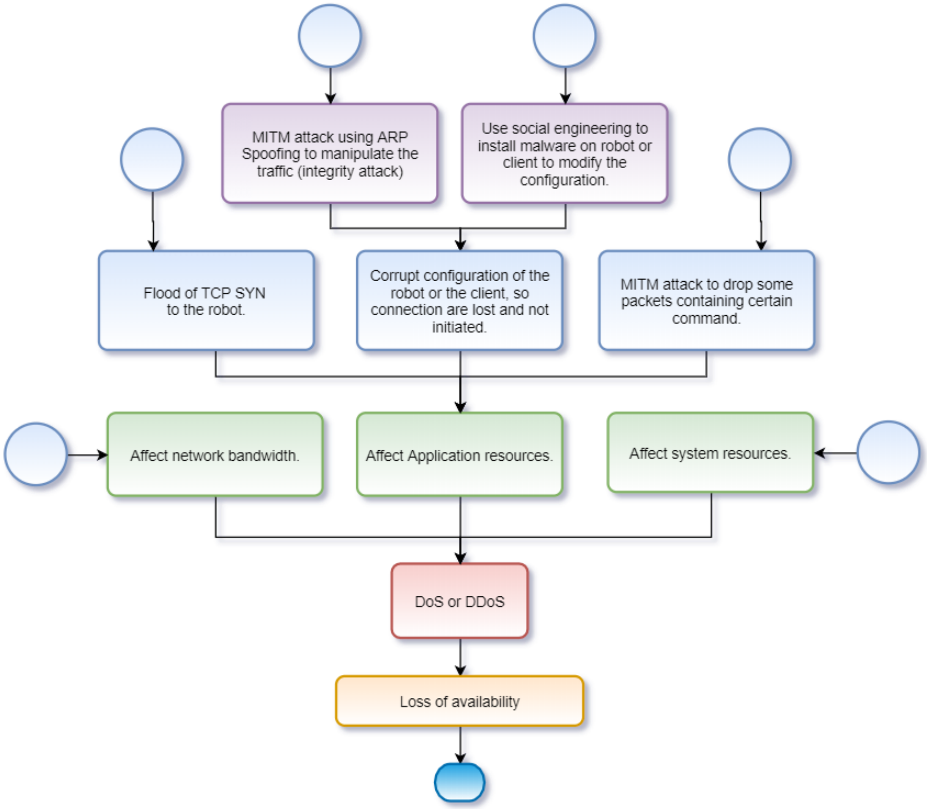
Consequences of Integrity Attacks

- Manipulates the robot's behavior
- Delays or prevents the robot from performing time-sensitive tasks
- Hijacks the robot physically
- Manipulates robot navigation to unintended or unauthorized place(s)
- Denies remote access service to the robot, whereby the robot becomes unavailable
- Physical damage or injuries as a result of a collision with humans or equipment
- Sensitive information is stolen from the robot
- Certain robot features are reduced or limited

Availability Attacks

The intention of such attacks is to deliberately affect the efficiency of a robot. The data packets are altered while the command message is in transition. Distributed Denial of Service (DDOS) attacks, when a message recipient is overwhelmed with traffic, is one of the major attacks in this category.

An availability attack can be performed at different levels, as depicted in the flowchart below.


MITM attack using ARP Spoofing to manipulate the traffic (integrity attack)
Use social engineering to install malware on robot or client to modify the configuration.
Flood of TCP SYN to the robot.
Corrupt configuration of the robot or the client, so connection are lost and not initiated.
MITM attack to drop some packets containing certain command.
Affect network bandwidth.
Affect Application resources.
Affect system resources.
DoS or DDoS
Loss of availability

Consequences of Integrity Attacks

- Denies remote access service to the robot
- Robot is unreachable or stolen
- Physical damage to the robot
- Physical damage or injuries as a result of a collision with humans or equipment

Confidentiality Attacks

The last type of security attack is the confidentiality attack. The intention here is to capture the information exchanged between the controller and the robot. As stated in the previous section, the fact that there is no end-to-end encryption of the information means that through a successful MITM attack, the attacker can capture all the traffic in plain text. This includes authentication details, if security configuration is not enabled on the server.

Consequences of Confidentiality Attacks

- Sensitive information stolen from the robot.
- Loss of intellectual property, design, and program code, and system breaches.

Cyber Attack Mitigation Strategy

With security breach techniques advancing each day and the domain of robotics being so vulnerable, the prevention of cyberattacks is extremely crucial and a must. Here are some cyberattack mitigation strategies that can be employed:

Secure Communication

Ensure a security layer is provided over the communication channels where information is being transmitted. The communication channel should be dedicated, with an authentication mechanism in place between controller and robot. The encryption of information being transmitted will restrict modification, manipulation, and hijacking attacks.

Use of Communication Buses

Secure communication can also be achieved by communication buses. Unlike traditional communication, communication buses are based on ethernet and hence can make use of features pertaining to TCP/UDP/IP.

IP Whitelisting

Only authorized controllers/administrative tasks should be able to reach the robot, which can be achieved through whitelisting.

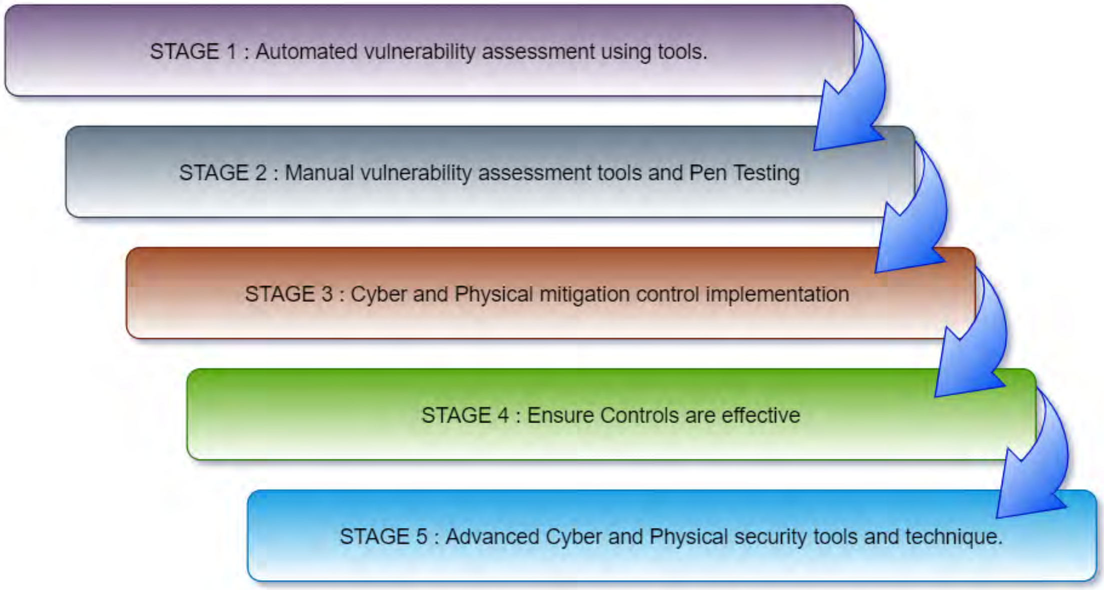
Data Distribution Service

Integrating data distribution service (DDS) as a transport layer will ensure authentication, access control, and cryptography.

Authentication Mechanisms

Public/private key exchange, certificate-based authentication, port monitoring, and arbitration may ensure proper encoding and decoding of transmitted data.

Cyber and physical security for robotic systems require a multistage testing approach, as depicted in the following diagram:



STAGE 1 : Automated vulnerability assessment using tools.

STAGE 2 : Manual vulnerability assessment tools and Pen Testing

STAGE 3 : Cyber and Physical mitigation control implementation

STAGE 4 : Ensure Controls are effective

STAGE 5 : Advanced Cyber and Physical security tools and technique.

Conclusion

Robotics is one of the fastest-growing technologies and is being modified continuously to meet the basic requirements of the future. Anticipating future demands, several inventions have already made their way into the field of robotics and several are underway. It is believed that several intelligent robots will be created to carry out various intrinsic operations and human-level manual tasks. The US Department of Defense plans to have completely autonomous robot soldiers by 2035.

With technology evolving at such a rapid rate, it will certainly lead to many security issues in the robotics sector. The future of the industry will be determined by how secure robotic platforms are. If security risks are not taken care of, artificial intelligence (which forms the very basis of robotics) may someday dominate humanity. To ensure that humans remain the masters of robots, the cybersecurity risks will need to be addressed as a priority and with the utmost attention in order to balance out any negative impacts.

References

What is Cyber Security? Definition, Best Practices & More

What is Robotics? What are Robots? Types & Uses of Robots.

Robot Generations - 21118 - Robotpark ACADEMY

7 Platforms You Can Use To Build & Test Robotics Applications

5 ways robots are vulnerable to cyberattacks

Analyzing Cyber-Physical Threats on Robotic Platforms

Robotics market revenue worldwide 2018-2025

Robotics (Wikipedia)

About the Author

Bharat Tyagi is a software architect, designer and developer with special interests in robotics and machine learning. Bharat has more than 15 years of experience in software development in different domains, including healthcare, finance and security.

GlobalLogic®

GlobalLogic, a Hitachi Group Company, is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating our strategic design, complex engineering, and vertical industry expertise with Hitachi's Operating Technology and Information Technology capabilities, we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the automotive, communications, financial services, healthcare & life sciences, media and entertainment, manufacturing, semiconductor, and technology industries.

www.globallogic.com