Cybersecurity Analysis of Intelligent IIOT Robots

Zhang Yuehong
Shanghai Technical Institute of Electronics & Information
Shanghai, China
zhangyuehong@stiie.edu.cn

Abstract—This paper studies the possible threats to the damaged robots. By analyzing the security problems of intelligent robots, the purpose is to strengthen the safety of robots and prevent the possible serious damage to enterprises, consumers and their surrounding environment after the vulnerabilities are maliciously exploited by attackers. (Abstract)

1. Introduction
Large investments are being made in robotic technology in both public and private sectors. Worldwide spending on robotics and related services will grow to more than $188 billion in 2020, according to the newly updated Worldwide Commercial Robotics Spending Guide from International Data Corporation (IDC)[1].

In the near future, robots will be everywhere. Because many of these "intelligent" machines are self-propulsion. Being not easy to be attacked by hackers are very important. Otherwise, they can become dangerous tools, causing serious damage and causing substantial damage to the surrounding environment and the people they serve.

Robot ecosystem is usually composed of physical robot, operating system, firmware, software, remote control application, supplier Internet service, cloud service, network, etc. The whole ecosystem presents a huge attack surface, and has many kinds of network attack modes. In this paper, we addressed the cybersecurity vulnerabilities identified. Our goal is to make robots more secure and prevent vulnerabilities from being used by attackers.

2. Risks Analysis
These risks go beyond data breaches and production delays [2]. Cyberattacks targeting robotic ecosystems come with serious safety concerns. Nearly 50 network security vulnerabilities have been found in robot ecosystem components, many of which are common problems. Here is a list of these network security issues.

2.1 Unsafe Communication
Unsafe communication is an important part of robot ecosystem, through which users and ecosystem components can interact seamlessly. But most robots use unsafe communication. Mobile and software applications connect to robots via the Internet, Bluetooth, Wi-Fi, etc., but the communication channels are not properly protected. They send critical information in clear or weak encryption. Some robots also send data in plaintext to the provider service cloud platform without any protection.
2.2 Authentication Issues
It is important to correctly identify the users who have right to access the robot system. Only valid users can program robots or send commands to them. Failure to guard against unauthorized access means that attackers can easily use certain functions remotely without a valid user name and password, enabling them to basically control the robot.

Most robots provide one or more services, which can be accessed remotely through computer software, mobile applications, internet services, etc. These services include complex and critical functions. No user name and password authentication is required to use robot services, which will allow anyone to remotely access these services. In some cases, even if some services use authentication, there are ways to bypass authentication and allow access without the correct password. This is a very serious vulnerability, indicating that anyone can easily attack a robot remotely.

2.3 Privacy Issues
Robot ecosystems can include access to a large amount of information, depending on the intended use of various types of robots. Some of this information should be kept confidentially and should not be shared with anyone except the owner of the robot. Privacy information may include personal identity, health or financial data, or data related to the robot ecosystem itself. Users should have complete control over this information and what to share with whom and when.

Some mobile applications of robots send privacy information to remote servers without the consent of users, including mobile network information, device information and current GPS position. Without the user's knowledge, this information can be used for monitoring and tracking purposes. The robot can also remotely disclose private information without authentication, allowing anyone to access it.

2.4 Vulnerable Open Source Robot Framework and Library
The development of robots mostly uses open source frameworks and libraries, among which the most popular is the robot operating system (ROS), which is used in a variety of robots from multiple vendors. There are many known network security problems in ROS, such as plaintext communication, authentication and weak authorization scheme. All these problems make robots unsafe.

A common problem in robotics: researchers and enthusiasts use the same or very similar tools, software, and design practices around the world. This leads to poor network security defense capability, because research robots and prototype robots are often designed and manufactured without protection measures.

3. Control measures

3.1 Defense In Depth
The “defense in depth” concept is a hallmark of cybersecurity best practices. In this strategy, multiple layers of security exist so if a layer fails, subsequent layers can provide the necessary security defences. At the very least, a defense in depth strategy will delay the attacker and allow time for detection and response measures.

Within the robot itself, there’s usually an embedded operating system. Then there’s the application code that runs on that robot. A big area is all the communications code that will take and process commands to the robot. It’s usually connected to systems that are more PC-based. Those systems might have databases on them, or configurations relevant to the robot, and then their own operating system. Then we have the cloud servers and their software that communicates to the devices, to the robots, and to the users over the web interface. We essentially want to build security into each layer of control system architecture.

3.2 Penetration Testing
Penetration testing is one of the common methods to improve security capability, which can guarantee security by simulating real attacks. According to PTEs, the process of penetration testing includes
interaction, information collection, modeling, vulnerabilities analysis, and later development. Penetration testing aims to improve the security of the system, not to destroy it, and will not affect the usability of the target system.

More and more companies and organizations begin to use this method to identify and solve the potential vulnerabilities in the system, in order to prevent major flaws in the future. However, most of IOT security research focuses on analyzing, defending or attacking specific devices.

Testing applies to more than just the device itself. It involves the entire ecosystem [3]. This includes the device enclosure and the hardware, user and network interfaces; any data deployed to the device, such as third party libraries and custom source code for the device’s smart application; any mobile applications that connect to the device; and any systems the device communicates with that may be housed either in the cloud or on the corporate network. As shown in Figure 1.

![Figure 1. IOT penetration testing](image)

### 3.3 Secure By Design

Cybersecurity for robotics is still an immature field. The robotics industry is starting to understand its importance and how to implement security from the initial design all the way through to robot implementation[4].

Safety design for IIoT robotic system and what design factors must be considered? At present, there are various industry guidelines, such as IIC’s IOT security architecture and its manufacturing overview, or NIST’s cybersecurity framework. The first task of the development engineer is to determine how to apply the security policy or security architecture to the design and life cycle management of all or part of the devices of IIOT endpoint. The high-level objectives of IIOT security solutions include the following: product endpoint certification (including equipment, sensors, control systems), providing trace-ability of the product manufacturer, date of manufacture, and any other relevant information. Product endpoint configuration and usage control: provides endpoint security management and configuration control, with various permissions and usage mode control or restriction. Endpoint maintenance: includes secure software updates. Secure communication between the control system and the endpoint, and ensure the security of the control system data in storage.

Defence in depth and collaboration are needed to secure these functions. To ensure the cybersecurity for IIoT robotic systems, we need a multi-step approach. As shown in Figure 2.

![Figure 2. A multi-step approach to secure the IOT robotic system](image)

### 3.4 Cybersecurity Standards for Automation

The ISA/IEC 62443 standard provides guidance to those that create products, integrate systems, and operate industrial automation and control systems.

Part 62443-1-1 mainly introduces the security objectives, defense in depth, security context, risk assessment, security program maturity, security level life cycle, reference model, asset model, area and
pipeline model, and the relationship between models. It also includes seven foundational requirements (FR) and security assurance levels (SAL).

FR 1-Identification and authentication control: Identify and distinguish all subjects (people, processes, and equipment) and allow access to objects (systems or assets). The purpose is to protect unauthorized access to the device or information on it;

FR 2-Use control: The authorized subject carries out the access to the object according to the assigned permission level. The purpose is to protect the unauthorized operation of the device and avoid misuse of the operation;

FR 3-Data integrity: To ensure the integrity of information, the purpose is to prevent unauthorized users from tampering with data, authorized users to modify beyond their authority, and maintain the internal and external consistency of data;

FR 4-Data confidentiality: Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure;

FR 5-Restricted data flow: The system is segmented by region and pipeline to limit unnecessary data flow transmission between regions. The purpose is to protect information and prevent attackers from deliberately bypassing the system;

FR 6-Timely response to events: Continuously monitor the operation status of the system, report the information security incidents, provide conclusive evidence, and take timely and correct actions after the causes are determined. The purpose is to inform the authority of information security violations and report the relevant evidence collected;

FR 7-Resource availability: To ensure the availability of system and assets in the production process, the purpose is to protect the whole system resources from denial of service attack.

It has been seven years since the establishment of IEC / TC65 / WG10 working group in 2005. With the development of industrial control system and the integration with traditional IT system, the standard framework and content have changed. How to use FR and SAL to realize IIOT information security and conduct security assessment has also become a focus issue.

4. Summary

Cyber security here includes the functions, limitations and inherent risks that need to be defined at each step of the implementation of the system[5]. As society increasingly relies on robots, this industry must improve its safety practices to avoid possible serious consequences. Many network security problems can be prevented by implementing well-known network security practices. Hackers may attack these robots in a variety of ways. It is necessary to understand these threats and put the key security issues in the priority position for mitigation. New technologies are often prone to security problems, as vendors of robots give priority to time to market rather than security testing. This is usually due to the fact that network security is not considered at the beginning of the robot product's life cycle; after the product is released and sold, repairing vulnerabilities becomes complex and expensive. Fortunately, since the adoption of robots is not yet mainstream, there is still time to improve the technology and make it safer.

References
[1] Clark G W, Doran M V, Andel T R. Cybersecurity issues in robotics[C]// 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), IEEE, 2017.
[2] Jeong-Min Lee, Bum-Seok Park, Yong-seok Lee, et al. The development of 6 D.O.F. robot manipulator with human-friendly design[A]. IEEE/ASME International Conference on Advanced Intelligent Mechatronics[C]. Switzerland, 2007: 1-6.
[3] Sinan Kilicaslan, M. Kemal Ozgoren, S. Kemal Ider. Hybrid force and motion control of robots with flexible links[J]. Mechanism and Machine Theory, 2010, 45 (1) : 91-1
[4] Hang Libin, Zhou Dehong, Li Yuxia. Comprehensive evaluation and empirical analysis of industrial robot human-computer interaction system [J]. Ordnance Industry automation, 2018, 37(03):91-96.
[5] Zeng Yantao. Research routes of manufacturing robots in the United States in the next 15 years [J]. Robot technology and Application, 2013, 3: 1-5