Introduction

1. Overview

Robotic technology serves a diverse range of industries, including healthcare, entertainment, logistics and military applications. The robotics market features a broad spectrum of robots, including industrial robots, service robots, medical robots, agricultural robots, and autonomous vehicles.

2. Importance of Cybersecurity

Today's and future robots will operate in closer proximity to humans, making it essential to understand their vulnerabilities and potential threats to ensure the safety of both humans and robots. Despite their primary role in enhancing human life quality, robots can be involved in unfortunate and harmful incidents. Consequently, the implications of security issues in robotic systems can be severe and multifaceted. Additionally, it is crucial to protect these sophisticated and expensive machines from such threats to maintain their functionality and integrity.

Problem Statement

Modern robots are typically designed to be open, robust, and user-friendly, facilitating straightforward operation and maintenance. However, many of these systems lack adequate security measures, especially considering their frequent accessibility via the internet for remote operation, which significantly enlarges the attack surface.

Operating system attacks exploit weaknesses in support software such as Linux-based operating systems (ROS) which constitute the heart of several robots. Analyzing a total of 176 threats collected from the robot vulnerability database showed that 92.6% are mainly software-related.

MANUFACTURING NET

VIDEO ADVERTISE NEWSLETTER SIGNUP PODCAST Sign In

Aerospace AI Automotive Cybersecurity Energy Gen Z Industry 4.0 Operations Software Supply Chain

Massive Industrial Robots Vulnerable To Being Hacked

In one case, researchers were able to reconfigure a robot's programming to make it draw a line two millimeters off from the intended target.

By — Meagan Parrish

May 3, 2017

(AP Photo)

Imagine what you could do if you controlled the 220-pound arm of an industrial robot. That's exactly what researchers set out to do in an experiment that revealed security vulnerabilities in robots that manufacture everything from phones to cars.

Latest in Industry 4.0

SPONSORED

5 Most Common Small Manufacturing Challenges According t...
August 1, 2024

New Semi-Automated Pallet Shuttle Technology Optimizes Material...
July 17, 2024

Massimo to Launch New Automated Vehicle Assembly Robot Line
July 17, 2024

4,000-Ton Crane Sets Record While Lifting 800-

Accreditation & Quality Compliance Center

News & Analysis | CMS Compliance Crosswalk | OSHA Program Manuals | Resources | Memb

NEWS & ANALYSIS

Home > News & Analysis > Cybersecurity company finds vulnerabilitie

Cybersecurity company finds vulnerabilities in hospital robots

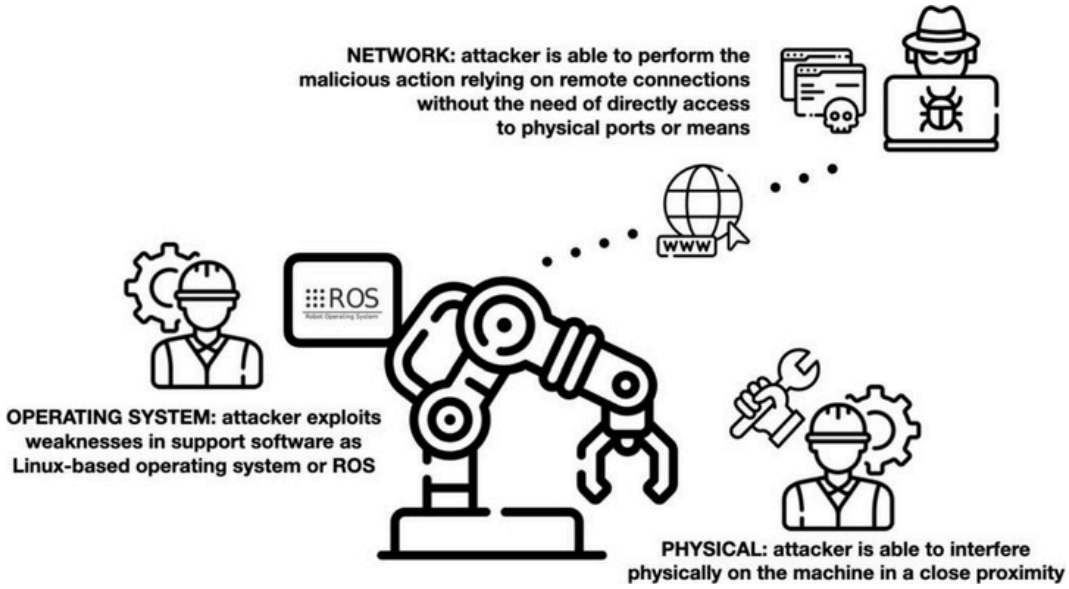
April 26, 2022 | Accreditation & Quality Compliance Advisor - Volume 16 Issue 17

Next »

By Eric Wicklund

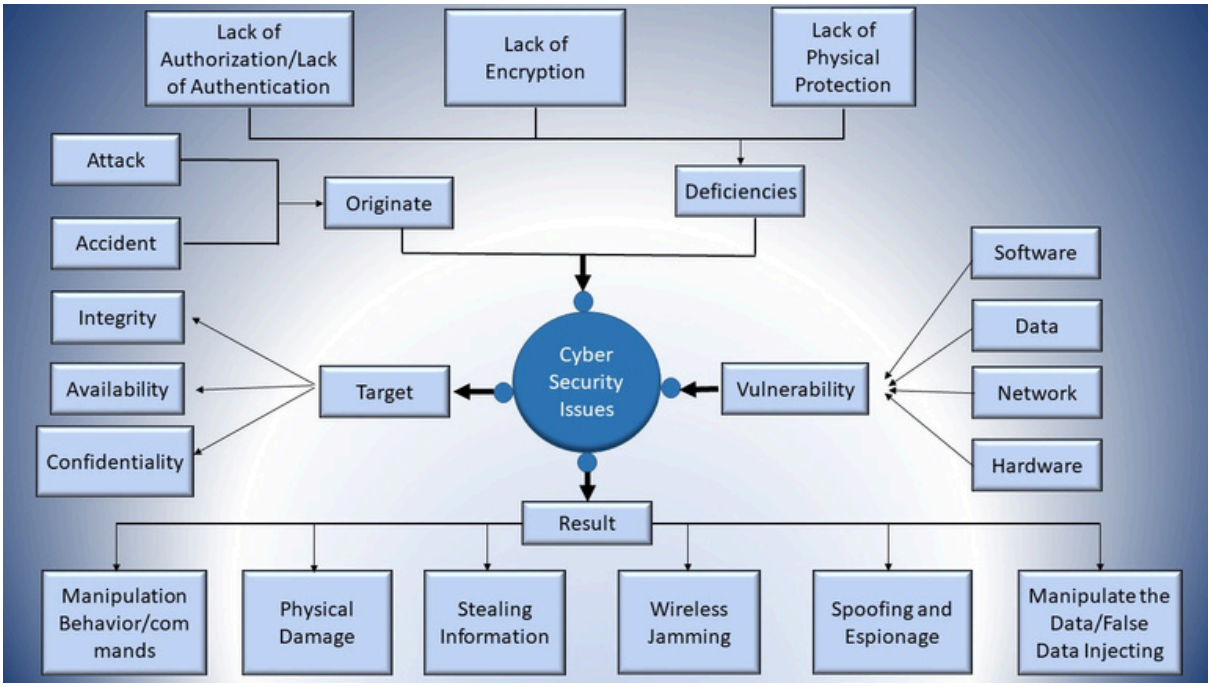
An autonomous robot commonly used in hospitals to transport medication and other supplies from room to room could be hacked and used to spy on patients and staff, according to a New York-based healthcare IoT security company.

The cyber attacks include Ransomware, APT, DoS (Denial of Service), MITM (Man-in-the-Middle) and attacks on ROS (Robot Operating System) nodes. These attacks can target different areas including physical components, network infrastructure and operating systems.



Ofcourse, There is also an APT. Advanced Persistent Threats (APTs) represent a sophisticated and prolonged form of cyberattack, often targeting specific organizations or institutions with highly customized strategies. Rootkits are a common tool used in APTs due to their ability to deeply integrate into an operating system, compromising its core components while remaining undetected.

Analysis

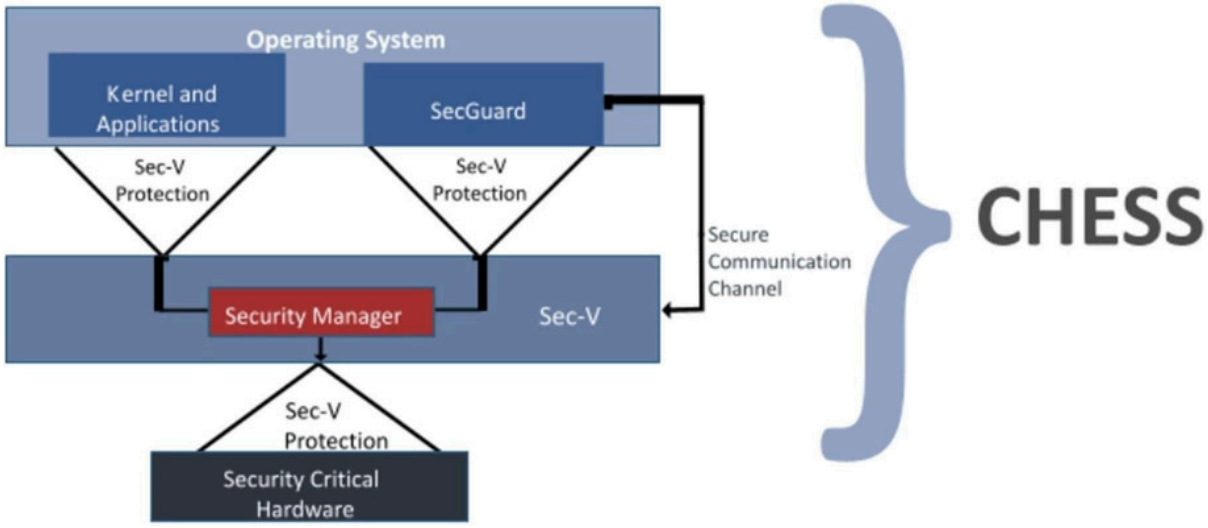


The above figure simplifies the main cyber security issues of robots. Security risks can emerge accidentally during the development of robot platforms , applications, hardware and sensors while even untrained users can cause unwanted security problems for robots accidentally. On the other hand, cyber security problems can be caused by attackers (Wang et al., 2021). Hackers aim at being able to spy or use critical data of robots and information to damage or even to destroy robots.

Some limitations in fact as lack of authorization/authentication, encryption and physical protection play a critical role in making the robots weak against cyber security issues and their implementation needs to be upgraded

Solution and Implementation

Robotics security does not have a single, definitive solution. Instead, the most effective approach is to implement defense in depth (DiD), which combines multiple layers of protection to safeguard these systems. To address Critical and Zero-day cyberattcks, SecurWeave has developed a Secure hypervisor. Which protects the robotic systems from Advanced threats e.g. APT, rootkit.



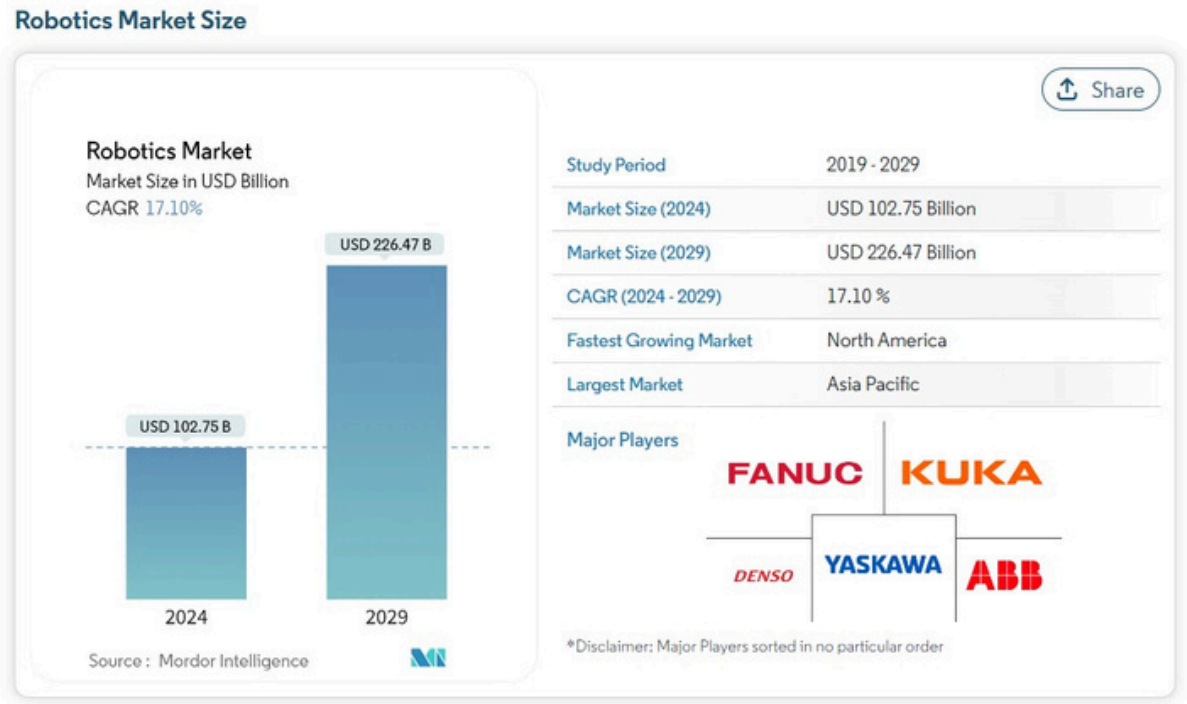
The key components in **CHESS** are detailed below.

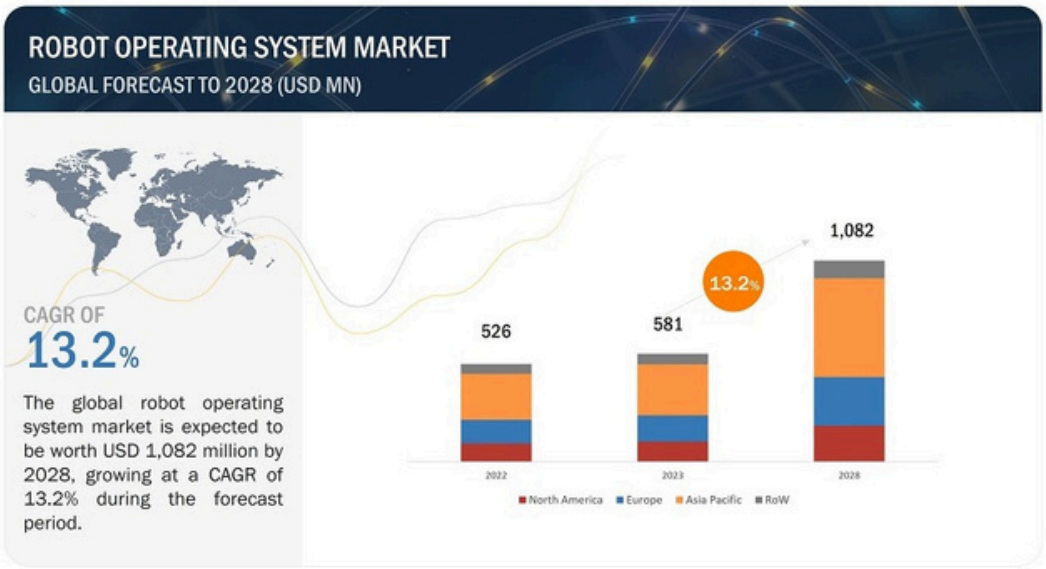
SecGuard
SecGuard is CHESS's User Interface for alerting, policy configurations, secure update etc. SecGuard will provide RESTful APIs for configuration and management purposes.

Sec-V the Security Hypervisor
Sec-V is a purpose-built security hypervisor targeted to detect, contain and analyze kernel mode APTs. The surge in APTs with kernel mode components.

SecurWeave's CHESS secure hypervisor operates at a privilege level higher than that of the OS kernel, providing it with a strategic vantage point to monitor and manage system activities. This elevated privilege allows CHESS to effectively identify and mitigate attacks originating from the kernel or I/O devices, which are often critical vectors for security breaches in robotic systems. By leveraging this unique position, CHESS ensures that even if the operating system or peripheral devices are compromised, the core security and functionality of the robotic system remain intact and secure.

Market Size





Robotics and ROS markets are growing at a CAGR of 17.1% and 13.2% respectively.

Cybersecurity in Robotics Market Size (2024) - USD 4.2 billion

Cyber Security in Robotics Market

Attributes	Details
Cyber Security in Robotics Market CAGR (2023 to 2033)	11.7%
Cyber Security in Robotics Market Size (2023)	USD 3.8 billion
Cyber Security in Robotics Market Size (2033)	USD 11.6 billion

Key Players

- McAfee
- TUV Rheinland
- Alias Robotics
- Exida
- DXC Technology
- Infosec

The Cybersecurity in Robotics market is projected to reach USD 4.2 billion by 2024. Studies indicate that embedded cybersecurity is crucial in safeguarding the future of operational technology, with hypervisor based security playing a vital role in enhancing security and safety in robotics and industrial automation.

Addressable Market

Intel Technology and ROS/Linux are widely used in various robotics systems across different sectors due to its powerful processors, advanced computing capabilities and open source operating system. Here are some top key players in the robotic industry.

1. Industrial Robots

- KUKA Robotics

-ABB Robotics

-Universal Robots

2. Service Robots:

- SoftBank Robotics

-iRobot

3. Autonomous Mobile Robots (AMRs):

- Fetch Robotics

-Clearpath Robotics

4. Drones:

-DJI - Intel Falcon 8+

5. Healthcare Robots:

- Intuitive Surgical

- Aethon TUG

6. Educational and Research Robots:

- TurtleBot - Robotic Operating System (ROS) based systems

7. Humanoid Robots:

- Honda ASIMO

8. Agricultural Robots:

- Blue River Technology

9. Consumer Robots:

-Sony Aibo

- Anki Cozmo

10. Autonomous Vehicles:

- Waymo

Conclusion

After reviewing the challenges, conducting thorough analysis and implementing solutions for robotic systems, we have also assessed the market size and addressable market for CHESS-P. It is evident that SecurWeave's CHESS is market-fit and provides a secure solution for robotic systems.

SECURWEAVE

securweave.com
info@securweave.com
+91-8790532463

Plot No 13/A, Laxmi Nagar Colony, Manikonda,
Rangareddy Telangana,
India 500089