EINPRESSWIRE

VicOne LAB R7 Publishes New AI Robot Cybersecurity White Paper

New LAB R7 research reveals growing cyber-physical risks in AI robots & delivers the industry's first threat matrix for securing next-generation robotic systems

Lab R7
Securing the Rise of AI Robots: Cyber Risks. Real-World Threats, and Defense Strategies
LAB R7, VicOne's innovation research lab
Robot Attack Surface
AI Model
App Cloud
Wireless

Overview of LAB R7's white paper, including the Robot Threat Matrix and attack surface analysis.

DETROIT, MI, UNITED STATES, December 9, 2025 /EINPresswire.com/ -- VicOne's LAB R7, the company's innovation research lab, today announced the release of Securing the Rise of AI Robots, a new white paper examining cybersecurity risks in AI robotics. The report analyzes emerging threats across robots' perception, decision-making, and action systems, highlighting how cyberattacks could lead not only to data exposure but also to unsafe or unintended behaviors. LAB R7's findings present a multilayered defense perspective aimed at strengthening the security and reliability of next-generation intelligent robotic systems.

> "With this research, our focus is to help the industry gain clearer visibility into emerging cyber risks and to offer practical guidance through the Robot Threat Matrix."
>
> *Ziv Chang, Vice President of LAB R7 Innovation Research Lab*

The release comes ahead of the upcoming Humanoids Summit 2025, a global gathering of robotics innovators and industry leaders exploring advances in humanoid robotics and physical AI. By publishing this research prior to the event, LAB R7 aims to support the broader robotics community with timely insights into emerging cyber-physical risks associated with AI-driven robots.

The white paper introduces the Robot Threat Matrix (RTM) v1.1—a comprehensive threat mapping model designed to help robot makers and operators understand potential attack vectors across sensors, actuators, embedded systems, communication layers, AI perception models, and cloud backends.

"AI robotics is entering a pivotal stage as intelligent machines begin operating in more dynamic and real-world environments,” said Ziv Chang, vice president of LAB R7 innovation research lab. “With this research, our focus is to help the industry gain clearer visibility into emerging cyber risks and to offer practical guidance through the Robot Threat Matrix. By collaborating across technology providers, researchers, and ecosystem partners, we can build AI robots that advance innovation while maintaining the reliability and safety society expects.”

The Securing the Rise of AI Robots white paper outlines several categories of risk, including:
- Manipulation of AI perception through visual, audio, or sensor-based inputs
- Unauthorized modification of motion controllers or safety parameters
- Remote exploitation through cloud, fleet, or OTA interfaces
- Integrity compromise of AI models or system configurations
- Lateral movement across multi-robot environments using shared backends

These insights underscore the growing significance of security considerations as AI robots increasingly integrate into industrial operations, logistics, public spaces, and consumer-facing applications. The white paper is intended as an initial reference for engineering, product, and operational teams seeking to evaluate the security posture of AI-powered robotic systems.

Access the LAB R7 white paper overview for a critical analysis of the Robot Threat Matrix and expanding attack surfaces through this link.

About LAB R7
LAB R7, VicOne's innovation research lab, is dedicated to advancing cybersecurity for emerging technologies. Its current research focuses on AI robotics cybersecurity, pioneering new approaches to strengthen the security and resilience of intelligent systems. VicOne, an automotive cybersecurity solutions leader, offers a broad portfolio of software and services reinforced by proven automotive threat intelligence—helping secure connected and software-defined vehicles from design to the road. For more information, visit VicOne.com/LAB_R7.

Ling Cheng
VicOne
+81 344002265
ling_cheng@vicone.com
Visit us on social media:
LinkedIn