



Home

Blog

Interview with Aaron Ardiri - CEO & Founder of RIoT Secure

Interview with Aaron Ardiri - CEO & Founder of RIoT Secure

**Shauli Zacks**

Published on: May 21, 2025

Content Editor

▼ This article contains

When it comes to IoT security, few leaders bring the same level of urgency and personal commitment as Aaron Ardiri. Following a tragic incident in Stockholm that highlighted the dangers of insecure connected systems, Ardiri founded RIoT Secure to protect what many overlook: the small, resource-constrained IoT devices powering critical infrastructure around the world. In this [SafetyDetectives](#) interview, he shares how his team is rethinking device architecture, optimizing secure communications, and helping developers embed security without compromising performance—or needing to become cybersecurity experts themselves.

Can you share the founding story of RIoT Secure and what inspired you to focus on securing resource-constrained IoT devices?

RIoT Secure was founded out of a strong sense of urgency and a deeply personal connection to the vulnerabilities we saw emerging in the IoT space. The tipping point came in 2017 after a terror attack in Stockholm, where a stolen vehicle was used as a weapon. We realized that had there been a secure, remote solution available to disable the vehicle, the tragedy might have been prevented. But such capabilities, if implemented without robust security, could easily be misused.

This incident crystalized the need to secure not just high-powered connected systems, but also the growing ecosystem of small, resource-constrained IoT devices that are becoming pervasive in critical infrastructure. Our mission since then has been to create a secure, scalable foundation for IoT that developers and businesses can rely on – without needing to become cybersecurity experts themselves.



RIoT Secure's hardware sandbox architecture is a key differentiator. How does this approach enhance security and optimize resource use compared to conventional methods?

Traditional IoT architectures typically rely on a single micro-controller that handles everything – from communications and security protocols to application logic. This setup introduces performance bottlenecks and security risks, as vulnerabilities in one component can jeopardize the entire system.

At RIoT Secure, we took a radically different approach with our hardware sandbox model. We split responsibilities across two dedicated micro-controllers: one handles security, communication, and lifecycle management, while the other is left entirely to the developer's application.

This physical separation ensures complete isolation of critical processes and allows developers to maximize resources for their applications without interference. Not only does this model reduce attack surfaces, but it also gives developers the freedom to choose any operating system, programming language, or runtime that best suits their use case – without compromising security.

Your patented communication protocol significantly reduces bandwidth and power requirements. Could you explain the challenges you faced in developing it and its impact on IoT device longevity and operational cost efficiency?

Creating a communication protocol that drastically reduces data transmission while maintaining end-to-end security was no easy task. The challenge was to move away from heavyweight protocols like HTTPS or DTLS that package messages like MQTT – which are inefficient for devices with limited bandwidth and power – and develop something lightweight, secure, and interoperable.

Our patented protocol reduces data overhead by over 90% compared to traditional methods, thanks to compact serialization, efficient state tracking, and adaptive payload handling. The impact is significant: devices can operate longer on smaller batteries, lower-cost connectivity plans become viable, and data integrity is maintained even under intermittent network conditions.



This dramatically lowers the total cost of ownership and extends the lifecycle of deployed devices, particularly in industries like logistics, utilities, and remote monitoring where every byte and every milliamp counts.

What are the biggest challenges in managing the security lifecycle of IoT devices?

The lifecycle of an IoT device is far more complex than just deployment. It involves secure on boarding and enrolment, real-time monitoring, firmware updates, vulnerability patching, and eventual decommissioning. Each of these phases presents its own security challenges.

One of the biggest obstacles is maintaining secure, scalable update mechanisms for fleets of devices – especially in environments where connectivity is unreliable. Another is enforcing consistent security policies across heterogeneous hardware and software environments. With RIoT Secure, we address these challenges head-on through a developer-first SaaS platform that automates lifecycle tasks, integrates seamlessly with existing ecosystems, and ensures firmware integrity throughout a device's operational life.

By embedding lifecycle management directly into the architecture, we reduce human error, simplify compliance, and help businesses meet cybersecurity regulations such as the EU Cyber Resilience Act.

How do you see the evolving IoT landscape influencing the future of security solutions?

The future of IoT security is being shaped by the growing convergence of edge computing, artificial intelligence, and regulatory pressure. As more intelligence moves to the edge, devices will need to make autonomous decisions – often in real-time and without reliable connectivity.

This amplifies the importance of localized security, secure execution environments, and verifiable firmware. Regulatory frameworks like the Cyber Resilience Act are also pushing manufacturers to adopt “secure by design” principles, which will become a competitive advantage rather than a compliance burden. At RIoT Secure, we see ourselves at the forefront of this evolution.

Our solutions are already enabling secure edge computing, and we're continually investing in research to support emerging use cases like predictive maintenance,



decentralized data processing, and zero-trust architectures in IoT networks.

Looking ahead, what are your top priorities for RIoT Secure's growth, and how do you balance innovation with the increasing complexity of cybersecurity threats in the IoT domain?

Our immediate priority is to scale our proven technology to a broader market. We've spent the last few years validating our platform through high-impact deployments, like at Stockholm Arlanda Airport with SAS Ground Handling. Now, we're focused on commercial expansion, on boarding new partners, and securing funding through our late Seed round.

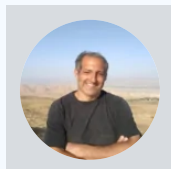
At the same time, we remain committed to pushing the boundaries of innovation. We're exploring next-generation technologies that address the rising demand for secure, lightweight compute environments and simplified IoT development – like our upcoming BRAWL and SHIELD platforms, empowering low size application firmwares. Balancing innovation with threat complexity requires a security-first mindset rooted in simplicity, automation, and modularity.

We don't just react to threats – we engineer our solutions to anticipate them, allowing our customers to stay ahead without needing to navigate the complexity themselves.

Share It:



About the Author



SHAULI ZACKS

Content Editor

PUBLISHED ON: May 21, 2025

Shauli Zacks is a content editor at SafetyDetectives.

He has worked in the tech industry for over a decade as a writer and journalist. Shauli has interviewed executives from more than 350 companies to hear their stories, advice, and insights on industry trends. As a writer, he has conducted in-depth reviews and comparisons of VPNs, antivirus software, and parental control



apps, offering advice both online and offline on which apps are best based on users' needs.

Shauli began his career as a journalist for his college newspaper, breaking stories about sports and campus news. After a brief stint in the online gaming industry, he joined a high-tech company and discovered his passion for online security.

Leveraging his journalistic training, he researched not only his company's software but also its competitors, gaining a unique perspective on what truly sets products apart.

He joined SafetyDetectives during the COVID years, finding that it allows him to combine his professional passions without being confined to focusing on a single product. This role provides him with the flexibility and freedom he craves, while helping others stay safe online.



978



904

Was this article helpful?



10 (12 votes)

Leave a Comment

Write a comment

Name

Email

☐ I agree to receive email updates about my comment.

SUBMIT

