

RIoT Secure AB

Redefining IoT Security and Scalability for the Future

In today's hyperconnected world, the Internet of Things (IoT) has become a cornerstone of digital transformation across industries—from smart manufacturing and logistics to healthcare and consumer electronics. Yet, as opportunities grow, so do the challenges. The journey from a promising prototype to a secure, large-scale IoT deployment remains one of the toughest hurdles for developers. Scalability, lifecycle management, compliance, and above all, security often slow down innovation and expose organizations to risk.

This is where RIoT Secure steps in. The company's groundbreaking approach provides developers with a robust foundation that bridges the gap between innovation and deployment without forcing them to compromise on security, scalability, or performance. By embedding security directly into the hardware architecture and combining it with a suite of proprietary technologies, RIoT Secure empowers developers to focus on what they do best: building transformative IoT applications.



Aaron Ardiri
CEO & Founder

**Bridging the
Prototype-to-Deployment Gap**

At the heart of RIoT Secure’s mission is the recognition that creating a prototype is rarely the problem; it’s turning that prototype into a secure, maintainable, and scalable product that challenges most IoT builders. The company solves this by introducing a dedicated microcontroller for security and communication, completely separated from the customer’s application microcontroller. This design philosophy ensures developers can devote their energy to AI at the edge, process automation, or industrial control, while RIoT Secure manages the heavy lifting around secure communication, compliance, and lifecycle management. By eliminating the traditional bottlenecks of scaling, RIoT Secure clears the path for thousands of devices to be securely deployed across geographies.

**Security as a Lifecycle
Responsibility**

Unlike many providers who treat IoT security as a one-time event, RIoT Secure views it as a lifecycle responsibility. Devices must remain secure from boot-up to end-of-life, including during updates and communication exchanges. RIoT Secure’s platform is built around a patented communication transfer layer, integrating key handling and OTA (over-the-air) updates directly into its architecture. This not only protects against

external threats but also enables customers to manage devices years after deployment—a capability many competitors lack.

**Trust Through Client-Server
Architecture**

RIoT Secure’s asymmetric trust model is another cornerstone of its platform. Resource-constrained devices handle only minimal local operations, while a dedicated RIoT Secure server manages trust anchors, identity, and policy enforcement.

This reduces the computational burden on edge devices, allowing even low-power microcontrollers to maintain secure communications. The result is a system that combines scalability, efficiency, and reliability—without the need for expensive enterprise-grade hardware.

**microTLS (µTLS): Security Without
Complexity**

Traditional TLS libraries are too heavy for constrained IoT devices. RIoT Secure’s answer is microTLS (µTLS)—a lightweight, optimized reimplementation designed specifically for microcontrollers. With a simplified API, developers can quickly integrate µTLS while maintaining compliance with industry-standard cryptography. A patented technology (US Patent 11,997,165 B2) reduces data payloads by up to 95%, significantly cutting communication costs and ensuring compatibility with devices that have limited flash and RAM.

**Shield: Protecting Firmware and
Intellectual Property**

In IoT, firmware is both IP and a gateway to the network. RIoT Secure’s Shield technology defends this critical asset through encrypted storage, secure boot validation, and runtime obfuscation. Unlike conventional protection methods, Shield remains active throughout the device’s lifecycle—preventing reverse engineering and unauthorized access long after deployment.

**Brawl WASM Runtime:
Bringing Web Assembly
to IoT**

RIoT Secure’s Brawl runtime introduces WebAssembly (WASM) to the world of IoT. Designed for microcontrollers, Brawl allows developers to run compact bytecode instead of heavy native firmware builds.

The result: reduced firmware size with near-native execution speeds. This not only enables multi-language development (C, Rust, and more) but also leverages a standardized execution format, opening new possibilities for IoT development.

Future-Proof Through Adaptability

The IoT ecosystem evolves rapidly, and RIoT Secure’s modular architecture ensures long-term relevance. Its stack—µTLS, Fusion, Oasis, Brawl, and Shield—adapts seamlessly to emerging standards such as Matter, OPC UA, and

industrial protocols, safeguarding customers’ investments for

**Meet Aaron Ardiri, Founder of RIoT
Secure**

Aaron Ardiri brings over 25 years of expertise in working with resource-constrained systems. His journey began in the late 1980s with low-level assembly coding and has since spanned to modern microcontroller-driven IoT solutions.

Over the years, he has developed everything from Game Boy emulators on PalmOS to secure communication stacks for Cortex-M0 devices. This unique background pioneering innovation under tight technical limitations inspired the vision behind RIoT Secure: enabling developers to focus on building breakthrough solutions while the platform manages the critical complexities of communication, security, and lifecycle management.

