2025

SWARM

CAMA

SECURITY

Lightweight Attestation PoC

Table of Contents

CAMA
SECURITY

INTRODUCTION

FOSTERING SAFE AND SCALABLE IOT SYSTEMS

OUR MISSION: TO SECURE CRITICAL INFRASTRUCTURE

While IoT devices promise unprecedented operational efficiencies, they often come with a hidden cost: security vulnerabilities. Current industry practices neglect to prioritize verifying microcontroller firmware, creating opportunities for malicious actors to exploit weaknesses and compromise device integrity. These weaknesses, increase the opportunities which malicious actors seek to exploit vulnerabilities, compromising not only device integrity but also lives and national infrastructure. As the IoT continues to expand into critical sectors, stringent security measures have become a matter of survival.

COLLABORATING FOR A SAFER IOT ECOSYSTEM

No single organization can overcome the IoT device security challenges alone. This is because these interconnected systems keep on expanding and, thus, require cooperation between industries, governments, and standards bodies to realize a much safer IoT ecosystem. We will together establish consistent security protocols, develop best practices, and share threat intelligence in keeping pace with the emerging risks. Our vision focuses on open communication, partnerships, and innovation where security goes hand in hand. Together, we can ensure that these devices serve to improve efficiency and convenience while continuing to underpin the trust and safety on which our critical infrastructure and everyday life depend.

THREAT LANDSCAPE AND CHALLENGES

INDUSTRY SHIFT TOWARD INTERNET OF THINGS

The rapid adoption of Internet of Things (IoT) devices across industries reflects a shift toward enhanced connectivity and convenience. However, this transformation has introduced significant risks, as many devices lack robust mechanisms to ensure firmware integrity, leaving them vulnerable to basic hardware-level attacks.

THE COST OF CONVENIENCE

This convenience comes with a price: IoT devices, comprising microcontroller units with very limited resources, use vulnerable code for their software. Interconnected, the risks increase: one breach could put entire systems at risk. To that end, advanced safeguards and innovation is needed to find vulnerabilities and secure IoT ecosystems.

CATASTROPHIC RISKS FOR CRITICAL INFRASTRUCTURE

Current industry practices of neglect in prioritizing the verification of microcontroller firmware create critical points of failure in essential systems. A single compromised embedded device could have catastrophic consequences, such as medical device malfunction, power grid failure, or disrupted emergency response systems in industries like healthcare, energy, and transportation. These weak points in devices create avenues for malicious actors to exploit vulnerabilities, affecting not only the integrity of the device but also putting lives and national infrastructure in peril. The more IoT finds its presence in critical sectors, the more stringent security measures become vital for survival.

CAMA
SECURITY

SWARM OVERVIEW

PRODUCT FEATURES

REAL-TIME WATCHDOG

Unlike traditional on-demand checks, our active system continuously monitors device integrity, enabling real-time automated patching where resources allow.

CRYPTOGRAPHIC FIRMWARE VERIFICATION

IoT devices securely store and provide cryptographic proofs of firmware integrity to verifiers, ensuring trust across interconnected systems.

ROOT OF TRUST INTEGRATION

Operates within the root of trust on the microcontroller unit (MCU), ensuring an immutable foundation for authentication and attestation.

HARDWARE COMPATIBILITY

Seamlessly integrates with off-the-shelf (COTS) hardware, simplifying deployment without requiring specialized components.

SCALABLE SOLUTION FOR IOT ECOSYSTEMS

Optimized for low-resource devices, SWARM provides robust security without compromising performance or efficiency, enabling widespread adoption across industries.

SECURE ATTESTATION MECHANISM

Ensures the stored secret and attestation functions are tamper-proof and inaccessible to other program memory, safeguarding critical operations.

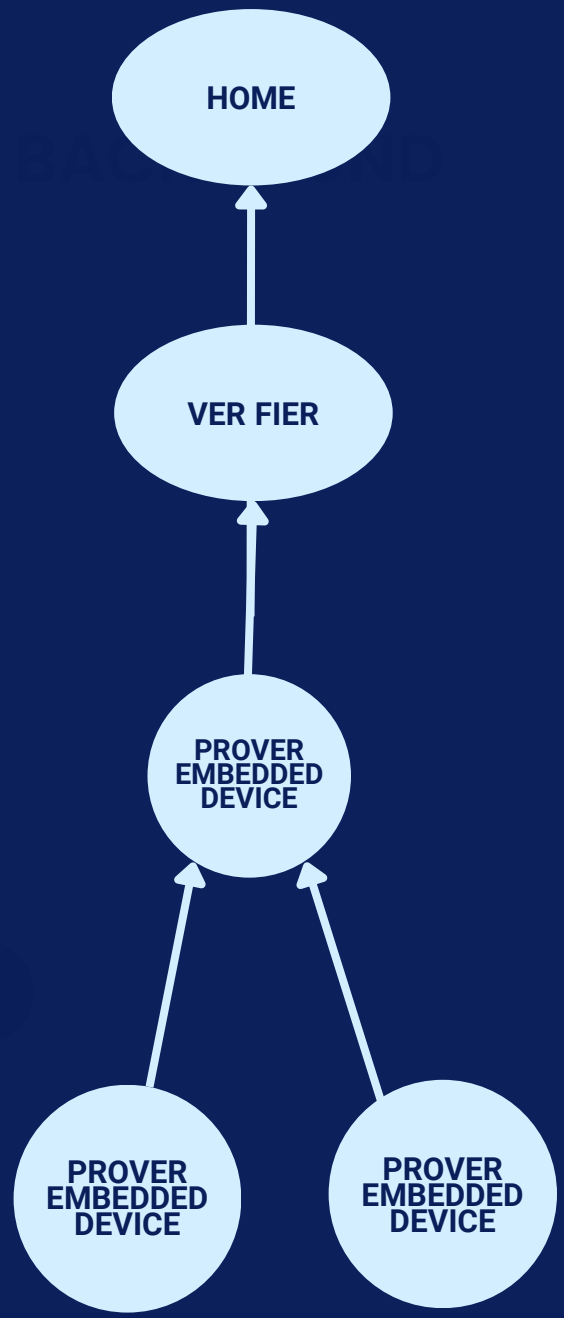
END-TO-END DEVICE INTEGRITY

Enables verifiers to confirm the unmodified status of device firmware, protecting against unauthorized changes and ensuring system reliability.

PROPRIETARY ATTESTATION PROTOCOL

SWARM leverages an in-house proprietary attestation protocol designed for efficiency, capable of running on resource-constrained devices like ARM Cortex-M series chips.

TOPOLOGY DIAGRAM



CAMA
SECURITY

CONCLUSION

SUMMARY

A COMPLETE RESILIENCE SOLUTION

We provide a full-spectrum resilience framework to lock down firmware, hardware, and operational integrity. What differentiates us, however, is that our solution is proactive. While others can only show that some issues exist after they have set in, our approach constantly monitors for, detects, and can stop such threats from taking hold in the first place. Unlike classic security models that depend on breach detection after an event has already occurred, we ensure embedded devices remain secure at all times and maintain system integrity and reliability.

PROACTIVE PROTECTION THROUGH CONTINUOUS VERIFICATION

More than breach detection, our solution finds the way to stop the threats before they set in. We achieve this through continuous cryptographic attestation in order to timely identify and mitigate any unauthorized change or anomaly. This proactive approach to defense collapses blind spots that more traditional, reactive approaches to security usually miss and reduces the risks of supply chain attacks, firmware tampering, and execution of unauthorized code.

Critical infrastructure requires this layer of security, where uninterrupted operations are a must, such as energy grids, chemical manufacturing plants, and fire response systems, since one compromised device can disrupt services, pose a safety hazard, or bring about a system failure. We provide a trustworthy base for critical infrastructure to operate securely, efficiently, and uninterruptedly by embedding security directly into device integrity, rather than just external monitoring.

THE FUTURE

ENCOURAGING WIDESPREAD ADOPTION FOR A SAFER FUTURE

Our goal is not exclusivity but widespread adoption. We believe that by making our solution accessible, we can contribute to a more secure IoT ecosystem, setting a new industry standard for embedded device integrity. As regulatory bodies and industry groups push for stronger security requirements, new standards for device integrity and attestation are emerging. By proactively aligning with and influencing these evolving standards, we ensure that our solution is not only effective but also future-proof, helping organizations stay ahead of compliance mandates and security best practices.

BETA DEPLOYMENT & PERFORMANCE OPTIMIZATION

Over the next year, we will conduct beta releases with select clients, testing our solution on real-world devices. This process will allow us to gather valuable feedback, refine implementation efficiency, and identify areas where mathematical operations may perform differently across hardware variations.

CUSTOM HARDWARE FOR MAXIMUM SECURITY & EFFICIENCY

Insights from our beta phase will guide the development of custom hardware optimized for seamless, high-performance security. By fine-tuning both software and hardware, we aim to deliver an industry-leading solution that balances efficiency, resilience, and verifiability, ensuring long-term trust and operational security.