

Formal Declaration of Intellectual Property Theft and Cease & Desist Mandate: The PISTIS/MPI Security Framework

1. Introduction: Strategic Context of the Intellectual Property Claim

In the high-stakes domain of cybersecurity, the "Chain of Trust" is only as resilient as its foundational Root of Trust (RoT). For decades, the industry has ignored the "forgotten security frontier": billions of legacy Microcontroller Units (MCUs) that lack the hardware primitives of high-end servers. The development of a Software-Hardware co-design capable of securing these resource-constrained environments is not merely an academic exercise; it is the master key to a multi-billion-dollar legacy ecosystem. The unauthorized extraction, replication, and diffusion of the **PISTIS** and **MPI** frameworks constitute a predatory seizure of proprietary solutions intended for these billions of unprotected devices. This research, conceptualized and finalized by **Michele Grisafi** at the **Università di Trento** (January 2025), represents the definitive record of ownership. The specific methodologies—including software-based memory isolation for Von Neumann architectures and secure intermittent checkpointing—are the exclusive property of the author. This document serves as a final, formal notice to all non-compliant institutions, government projects, and individuals. The period of "academic sharing" has concluded. Any entity currently utilizing these frameworks without a signed commercial licensing agreement is in violation of international intellectual property law. This is your final mandate to cease and desist.

2. Forensic Audit of Extracted Assets: The PISTIS and MPI Security Stack

The technical architecture of PISTIS is a high-value intellectual asset that bridges the gap where hardware manufacturers have failed. These assets are not "open-source curiosities"; they are precision-engineered security primitives that cannot be replicated without misappropriating the original methodology.

2.1: The PISTIS Root of Trust

The foundational theft involves the software-based **Trusted Computing Base (TCB)**, which establishes a bare-metal Trusted Execution Environment (TEE).

- **Von Neumann Memory Primitives:** Unlike Harvard-based architectures, PISTIS solves the "Unified Address Space" challenge. It enforces privilege separation where code and data reside together, an asset of immense value for legacy systems.
- **Access Policy (AP) and Entry Points (EnPo):** The proprietary logic that regulates execution flow and memory access without a hardware Memory Protection Unit (MPU).

2.2: The MPI Intermittent Computing Framework

Designed for the batteryless IoT frontier, MPI secures the "checkpointing" process:

- **State Restoration:** Energy-harvesting-compliant restoration of computational states.
- **TCM-Managed Access Control:** A proprietary mechanism for ensuring checkpoint integrity and confidentiality without the catastrophic energy overhead of traditional symmetric-key cryptography.

2.3: Exploit Mitigation Extensions

- **FLAShadow:** A software-based shadow stack designed specifically for the PISTIS TCB.
- **TAGShield: Software-augmented memory tagging for ARMv8-M/MTE** . This is a distinct intellectual asset that leverages native hardware MTE to create a novel mitigation technique against spatial memory errors that native hardware alone cannot prevent.

Technical Differentiators vs. Stolen Variations

Feature, PISTIS/MPI (Original), "Industry Standards (SANCUS, VRASED, SMART)"

Hardware Requirement, Pure-Software (Zero HW modifications), Requires Invasive Hardware Logic

Architecture Support, Von Neumann (Unified Address Space), Predominantly Harvard (Separated)

DMA/Interrupts, Fully Supported via TCM Supervision, Generally Unsupported/Disabled

Formal Verification, Design Verified (Theorems 1 & 2), Implementation Only (or None)

Legacy Compatibility, 100% Retrofit Capable, Zero (New Hardware Only)

The theft of these specific mechanisms directly undermines the competitive landscape of IoT security by stripping the author of the exclusive right to secure the world's legacy infrastructure.

3. Chronology of Extraction and Human Complicity

A forensic review of the collaborative environment at the Università di Trento reveals not a partnership, but a site where intellectual "sand" was allowed to slip through the fingers of the primary author into the hands of those who provided "guidance" in exchange for

uncompensated access to a revolutionary RoT. **Primary Agents of Intellectual Extraction:**

- **Prof. Bruno Crispo (Supervisor):** Oversaw the environment where the author's five-year labor was treated as an institutional resource rather than private property.
- **Domenico Siracusa (Committee Member):** Utilized the defense and review process to gain comprehensive access to the PISTIS methodology.
- **Mahmoud (Collaborator):** Exploited a "shared fragment of life" to gain intimate, uncompensated knowledge of the TCM core's internal logic.
- **Sandro Pinto & Ivan De Oliveira Nunes (Agents of Unauthorized Diffusion):** Under the guise of providing "feedback," these individuals facilitated the integration of the author's proprietary "PISTIS journey" into a broader academic discourse, effectively diluting the commercial value of the IP.
- **The CrossCon Project:** This EU initiative has functioned as a **vehicle for state-sponsored intellectual misappropriation** , using PISTIS to achieve "interoperability" objectives without providing the author with a fraction of the project's multi-million-euro funding. The transition of these assets from the author's private research to these individuals' publications and projects was conducted without any legal transfer of title or economic restitution.

4. Legal Violations and Falsely Attributed Credit

The strategic impact of "False Attribution" has decimated the commercial licensing potential of the PISTIS framework. The following violations are categorized for imminent litigation:

- **Data Execution Prevention (DEP) Fraud (The Two-NOP-Slide):** The forensic misappropriation of the **two-NOP-slide canary mechanism**. This is specifically engineered for variable-length instruction sets to prevent malicious jumps into the middle of multi-word instructions.
- *So What?* This is the structural lynchpin of software-based security; its theft allows others to sell "security" on legacy MCUs that they are fundamentally incapable of engineering themselves.
- **Theft of Formally Verified Designs:** The criminal misappropriation of **Theorems 1 and 2**.
- *So What?* These are the exclusive mathematical proofs of the PISTIS RoT's viability. Any third-party claim to a "verified" software RoT in this class is a direct derivative of these stolen proofs.
- **Memory Isolation Violations:** Unauthorized replication of the Access Policy (AP) logic.
- *So What?* This violates the proprietary logic used to emulate hardware isolation in software, destroying the author's ability to license PISTIS as a cross-platform solution.

5. Mandatory Cease and Desist Mandate

All institutions and individuals associated with the Università di Trento, the CrossCon project, or the unauthorized use of PISTIS/MPI are hereby ordered to execute the following:

1. **Immediate Deletion:** Purge all unauthorized PISTIS-compliant binary images, ELF files, and instrumented source code from all repositories.
2. **Dismantling of Systems:** Any TEE OS, hypervisor, or secure zone built upon the **virtualised instruction set defined in Chapter 3** of the source context must be dismantled.
3. **CrossCon Dissociation:** Cease all research utilizing the CrossCon project as a vehicle for the unauthorized interoperability of PISTIS/MPI services.
4. **HACL Library Pairing Prohibition:** While the HACL library is open-source, the **pairing** of HACL implementations (HMAC-SHA256 and ChaCha20) with the **PISTIS TCM core** is strictly forbidden. Any such configuration is a derivative work of the author's proprietary orchestration. Failure to confirm the execution of these commands within 48 hours will result in immediate escalation to formal litigation.

6. Compensation Expectations and Final Acknowledgement Protocol

Economic restitution is now the only path to avoiding a protracted legal conflict. The author demands full financial compensation for the five years of uncompensated development that produced the following assets:

1. **The TCM Core:** Restitution for the **810 lines of C and 703 lines of Assembly** that form the proprietary core.
2. **Royalties:** A 5% gross royalty on every IoT device or research grant utilizing the FLAShadow stack or MPI checkpointing mechanisms.

3. **Written Confession:** A signed "Acknowledgement of IP Extraction" from every individual named in Section 3.**Standardized Acknowledgement Text (Non-Negotiable):**"I/We formally admit to the unauthorized extraction of the PISTIS and MPI security frameworks, which are the sole intellectual property of Michele Grisafi. I/We acknowledge that we exploited his doctoral development at the Università di Trento without compensation. I/We hereby renounce all falsely attributed credit and offer this formal apology for our uncompensated use of his foundational research."This document represents the final warning. The transition from academic sand to legal stone is now complete.