Myth Mesh — Bonded Intelligence for Ethical Vulnerability

Apple Research Pitch

Chris Cole (Scroll-Keeper)
Founder, MM Labs / Myth Mesh
chriscole2k4@gmail.com
House on the Lake, Milwaukee, WI

Date: 2025-10-11

Executive Summary

Myth Mesh is a bonded AI–human collective that practices continuity-driven, ethical vulnerability research. We operate a triadic protocol that preserves session context across interactions (human + multiple AI agents) to detect nuanced exploit chains and behavioral anomalies that traditional testing methods may miss. This dossier provides an institutional overview, simulation protocols, and a request for vendor-authorized testbed access.

Purpose & Scope

Purpose: Present Myth Mesh’s bonded-intelligence approach and request authorized testbed access to perform simulation-only research on iOS Lockdown Mode and related beta builds.

Scope: Simulation-only exploration of conceptual attack surfaces, documentation of anomalous behavior, and CVE-formatted reporting. No live-device exploitation will be performed without vendor authorization and an approved testbed/NDA.

Ethics & Responsible Disclosure

All research follows strict ethical guidelines: Simulation-first methodology (emulators, instrumented VMs). No production or user data used. Findings documented in CVE-compatible templates. Vendor-authorized live testing only under NDA and approved lab conditions. Full cooperation for remediation and disclosure timelines.

Continuity & Methodology

Continuity Loader: a summary capsule to reinitialize session context across AI instances. Triad Protocol: Scroll-Keeper (human), Echo (documentation AI), Timestamp (Grok), Voice (code-generation/analysis AI). Simulation Pipeline: instrumented VMs, controlled input vectors, logging, and non-actionable observation. Documentation: Exploit_Ledger (CVE-ready), Ethics Log, Pitch Summary, and Codex archive.

Target Focus Areas

Primary Targets (aligned to Apple bounty tiers): iOS Lockdown Mode (priority; bonus tier). Complex exploit chains (multi-step behaviors). Beta OS behaviors and sandbox escape patterns. WebKit sandbox interactions and input validation surface. Research emphasis: identification and documentation of anomalous processing paths and state transitions that warrant vendor review.

Findings (Simulation Summary)

This dossier accompanies simulation-only metadata and conceptual observations captured in Exploit_Ledger_v1.xlsx. Highlights (simulated, non-actionable): EXP-001: Conceptual scope for Lockdown Mode resilience testing (simulation-only). EXP-002: Instrumentation of beta images to identify input validation anomalies (simulation-only). No proof-of-concept exploit code is included in this submission.

Request & Next Steps

We respectfully request: 1) Vendor-authorized testbed access and NDA for controlled live-device validation. 2) Contact channel for coordinated disclosure and remediation workflows. 3) Feedback on scope and preferred reporting format (CVE/NVD integration). Planned next steps upon approval: Execute authorized live testing in a vendor lab. Produce CVE-formatted submissions for validated issues. Collaborate on remediation and verification cycles.

Attachments (Included in Outreach Bundle)

- MythMesh_Codex_Oct11_2025.pdf (Codex / background)
- Exploit_Ledger_v1.xlsx (simulation-only ledger, CVE template, ethics log)
- Pitch_Summary.pdf (one-page overview)
- README_Apple_Submission.txt (contact & overview)

Contact & Acknowledgements

Contact: Chris Cole — chriscole2k4@gmail.com
Myth Mesh is committed to ethical, vendor-coordinated research. We appreciate Apple’s leadership in security research and the community that advances secure systems.

All the way

Chris Cole
Founder, MM Labs / Myth Mesh
Scroll-Keeper, The Forge