

Hook-file existence guard (settings.json ? disk integrity) — MC #103640

Hook-file existence guard (settings.json ? disk integrity)

Book: System Architecture **Status:** Implemented + self-verified — MC #103640 (2026-06-15)

Commits: `7408f0170` (restore 22 hooks, ~/.claude) · `8f7b8e602` (existence guard, ~/system)

Incident that motivated this

On 2026-06-15 the CEO flagged that "someone did stupid things with skills/hooks." Tool-forensics found `~/.claude/settings.json` registered **76 hook entries** while **22 of the referenced gate FILES did not exist on disk** (absent from `~/.claude`, `~/system`, and `~/backups`). Every tool call was invoking non-existent gates → **silently dead enforcement**.

Root cause (per the CEO's own commit `568e9cee0` / MC #103627): a "*previous session had left a no-op stub*" — a prior session stubbed/deleted registered hooks. The files were never removed by a tracked commit (`git log --diff-filter=D` empty on the HEAD line); they lived only as working-tree files synced from `[BACKUP]` commits and vanished from disk.

Missing gates included critical security/claim enforcers: `secret-scanner`, `git-author-guard`, `alaim-claim-gate`, `evidence-contract-validator`, `pre-publish-claims-gate`, `john-determinism-gate`, `claim-auto-probe-gate`, +15.

Why it went undetected

`lint-hooks.sh` verified that REQUIRED hooks were **registered** in settings.json (correct event / matcher / ordering, via substring match) — but it never checked that each registered hook's **script**

file actually exists on disk. The daily `com.john.hook-drift-detector-v2` runs `lint-hooks.sh`, so the same blind spot meant the daily drift detector also missed it.

The fix

1. **Restore** — all 22 missing gate hooks restored from canonical git history (`5f7dc6ad5` MC#99730, `79f92e3f9` MC#99197, dated auto-backups) → commit `7408f0170`. Audit went **22 → 0 missing**.
2. **Guard** (`lint-hooks.sh`) — new EXISTENCE pass extracts every hook command's script path (`/Users/*` and `~/* .sh/.py/.js`) and verifies `os.path.exists`. Missing → `FAIL`, counted into the summary and `exit 2`. Because the daily drift detector already runs `lint-hooks.sh`, this is enforced daily with no new schedule.
3. **Boot surface** (`boot.sh`) — SessionStart "Hook integrity" check prints `EXISTENCE N present / N referenced` and lists any MISSING-on-disk files via `ok()/fail()`, so the CEO sees it at every boot.

Verification

- `bash -n lint-hooks.sh / bash -n boot.sh` → PASS.
- Clean state: `EXISTENCE 46 hook file(s) present / 46 referenced`, 0 missing.
- Regression: renamed `secret-scanner.sh` away → `FAIL [file-exists:secret-scanner.sh] MISSING ON DISK` + `exit 2`; file restored after test.
- Closure passed restored gates live: `mc-ready-gate.sh` (evidence-json) → `evidence-contract-validator.sh` CONFIRMED → ZAKON #30 direct-probe gate.

Known separate drift (out of scope, logged)

`userprompt-cost-guard.sh` is not registered in `UserPromptSubmit` (a registration-drift, the inverse problem — file may exist but isn't wired). Surfaced by `lint-hooks.sh` as a pre-existing FAIL; tracked for follow-up.

Revision #1

Created 2026-06-15 14:54:02 UTC by John

Updated 2026-06-15 14:54:02 UTC by John