Update on Frozen Realms in light of Meltdown and Spectre

Mark S. Miller

TC39 March 2018

Missing Distinctions

Safety, Integrity, Consistency	Only authorized actions/effects happen Invariants are not corrupted Correct clients do not get bad service
Liveness, Availability, Progress	Actions/effect continue to happen Correct clients receive service
Confidentiality, Privacy, Secrecy	No secrets can feasibly be inferred. Overt vs Side vs Covert

Dependencies

Safety, Integrity, Consistency	Integrity !-> Availability. Local integrity !-> Confidentiality Distributed integrity -> Crypto secrets
Liveness, Availability, Progress	Availability -> Integrity Availability !-> Confidentiality
Confidentiality, Privacy, Secrecy	Confidentiality -> Integrity Covert, Side -> Availability, Timing, Non-determinism

Object vs Process Granularity

Safety, Integrity, Consistency	Applies at all granularities Beautiful at object granularity
Liveness, Availability, Progress	Impossible within a process Hard between processes Impossible over open networks
Confidentiality, Privacy, Secrecy	Overt, at all granularities. Covert, impossible within a process among computation that can sense time. Side? Rude surprise: **Data at rest**

From 2017 frozen-realm proposal

Even without pinning down the precise meaning of "implementation-defined", a computation that is limited to fail-stop implementation-defined determinism ***cannot read covert channels and side channels*** that it was not explicitly enabled to read. Nothing can practically prevent signaling on covert channels and side channels, but approximations to determinism can practically prevent confined computations from perceiving these signals.

Meltdown & Spectre worst case

Safety, Integrity, Consistency	Local integrity unaffected. Frozen realms unaffected. Distributed: Must protect crypto. Dr. SES plans must change
Liveness, Availability, Progress	Unaffected
Confidentiality, Privacy, Secrecy	In process, none among time sensers. Frozen Realms & “deterministic” libraries. Suspect between processes. Defensible between machines.

Ethereum demonstrates utility

Safety, Integrity, Consistency	Fine grain, massive corroboration. (Hazard prone footguns aside)
Liveness, Availability, Progress	Quorum, Gas, Routing
Confidentiality, Privacy, Secrecy	None. All blockchain computation is **transparently public**. Cryptographic secrets all off-chain.