Name propositions

- **secdom**: security domains.
- **spansec**: security span.
- **scspan**: side-channels span or security context span.
- **uspan** / **mspan**: microarchitecture spans.
- ...

Charter proposition

Timing covert channels are used to exfiltrate confidential data using microarchitectural states as a medium for communications. These channels are particularly relevant in the context of microarchitectural attacks such as Spectre and Meltdown.
The security domains task group (proposed short name: secdom TG) will define a small ISA extension to prevent malicious covert channels. More precisely, we will introduce a notion of security domains. Covert channels must be prevented across security domains by adapting the microarchitecture. Security domains allow the application logic to formally define microarchitectural isolation constrains that must be enforced by the hardware.
The TG will develop an ISA specification, a security guide, an implementation guide, a proof-of-concept implementation including both a prototype RISC-V core and compiler, and a test suite for common covert channels.

Performance counters

Performance counters can serve as the basis of architectural covert channels. This can be mitigated by scoping them in the security domain.

Should we consider performance counters in the scope of the TG ?