

“Formal Verification of the Secure Boot Feature in a Mobile Trusted Module”

The Mobile Trusted Module¹ (MTM) is an adaptation of the Trusted Platform Module, a hardware-based root of trust for personal computers, to mobile phones. Although both of these modules were developed by the Trusted Computing Group² (TCG), a non-profit standardisation organisation for interoperable hardware-enabled security that covers hardware and software building blocks and interfaces across different platforms, the MTM aims specifically to meet the needs of the mobile and wireless environment. In particular, the MTM enables standardised security solutions for, among others, platform integrity, device authentication, SIM-lock and secure device personalization, protection for downloadable content and software, mobile payments and ticketing, and user data protection and privacy.

The TCG's secure platforms are built on the assumption that these 'trusted modules' are indeed trustworthy; that is, that they can be relied on to perform their security functions as specified, even in a hostile software environment, where attackers may attempt to break a system, for instance, using unusual timings and unintended call sequences. Formal verification can provide a higher degree of assurance, in this context: that of mathematical correctness (in a particular model). Ideally, the entire MTM specification should be verified and a correspondence between the verified model and the actual implementation should be established using formal methods, but the scale of such an undertaking far exceeds the realm of a Master's project. Nevertheless, verification of very basic trust extension mechanism of the MTM during secure platform boot appears feasible. This is also an area, where the traditionally more controlled mobile platforms differ from the fully open world of the PC in that the MTM does not only record-keeping, but performs actual verification of each software component loaded during boot.

Proposed content:

- 1 Model the 'secure boot' feature of the MTM specification and implement the model in a theorem prover (such as Isabelle³).
- 2 Identify suitable security goals and formalize them as security specifications.
- 3 Determine a feasible proof strategy and incrementally refine a proof that the security requirements hold in the theorem prover.

Expected results:

Formal models and a report on the points listed above.

Required competence:

- Computer Science/Engineering, with a specialization in formal methods and/or security.
- Ability to learn quickly, work independently, and identify problems and solutions with relative ease.
- *Prior experience in working with a theorem prover or a trusted module is a plus!*

¹ <https://www.trustedcomputinggroup.org/specs/mobilephone/>

² <https://www.trustedcomputinggroup.org/home>

³ <http://www.cl.cam.ac.uk/research/hvg/Isabelle/>