論文の内容の要旨

論文題目　Formal Verification of Low-level Software
（低レベルソフトウェアの形式的な証明）

マーティ・ニコラ

Formal verification of low-level software has become a trend in the formal methods community. This is justified by the fact that our lives rely on this software: brake systems of cars, flying controls of airplanes, vital medical devices, or security probes of power plants. Beyond the stakes, the difficulty also motivates the community. Indeed this software verification presents a challenge: they are complex, often written in different languages and they implement subtle control-flow.

In this thesis, we study the formal verification of a particular case of lowlevel software: operating system kernels. As a test-bed we have chosen Topsy, an embedded operating system for network devices. This kind of software has the particularity to run user applications, to provide them services and to make
the interface with the underlying hardware. Our main interest is about the interaction between the kernel and its user applications. Our study starts from an abstract view of the system, implemented as a
model of the hardware, the kernel and its applications in the SPIN model checker. We use this abstraction to verify properties about the message passing services and the protection of the kernel memory. For this latter property we identify some parts of the code that are sensible, such as the memory allocation and the context switching. The next step is to verify the source code implementing these facilities. For this purpose we model both a C-like language and the MIPS assembly, inside the Coq proof assistant, as well as a well-known extension of Hoare-logic: the separation logic. Using these implementations we verify the memory allocator and application context switching code of Topsy. Through this experiences, we come to investigate the automation of code verification. We also implement an original and certified verification function for separation logic triples inside of Coq. This function can be extracted as a stand-alone and certified verifier. We apply this verifier on the verification of a library for lists, which is a must have for operating system kernels, and to the thread creation function of Topsy.