A web browser can be loosely thought of as an HTTP client that executes an HTML (and JavaScript) interpreter. When it receives requests from an HTML page, it must make security decisions on whether or not to allow the request. The set of rules that it is meant to enforce are collectively referred to as the Same Origin Policy, but they have never been fully formalized, and partial formalizations [FKS14, BBDM14] arguably leave out too many details to be considered a good basis for security proofs. Our goal is to produce the first formal specification of the Same Origin Policy, and the first verified browser security policy engine that meets this specification. Based on this verified browser core, we aim to develop the first end-to-end proofs of security for a web application.

The proposed internship is part of an ambitious multi-year project in collaboration with researchers at INRIA, Imperial College London, and Microsoft Research. As a first step, we are building a formal specification of HTML5 security in the F* programming language [SHK+16]. Our goal is to eventually cover all the security-critical parts of the standard specifications for HTML5, Content Security Policy, Cookies, and Cross Origin Resource Sharing. Unlike previous web security models [FKS14, BBDM14] our goal is to support interoperability testing, so we can know that our model is not too restrictive, as well as automated verification using F*, so that we can verify our implementation of these specs as well as web applications that use them.

We seek brilliant students who are interested in learning novel verification techniques, in writing and testing formal specifications, and in applying these techniques to real-world web security problems. The intern will be expected to tackle a well-defined sub-problem within the project and to work in collaboration with senior researchers towards a publication in a prestigious conference. Students with a background in programming languages, formal verification, or web security are strongly encouraged to apply.
References

