Chapter 18

Conclusion and Outlook

I summarize my thesis in this conclusive chapter. In addition, I give an outlook for future research directions.

In this thesis, I investigated the security of browser-based identity federation. In particular, I considered several variants of standardized protocols, namely Security Assertion Markup Language (SAML) and WS-Federation. I chose a twofold approach to ensure their security: Firstly, I contributed vulnerability analyses and security measures that improved subsequent standard editions. Secondly, I created the first formal security proof for browser-based identity federation. My proofs govern static information flow, freshness, and channel authenticity of the WS-Federation Passive Requestor Interop Profile. I proved that the protocol is secure in a realistic setting with insecure and server-side authenticated secure channels. My proof holds against static adversaries with passive access to the browser. The proven specification is constraint-based, and so are the security proofs of this thesis. This bears the advantage that my results cover other protocol variants, which fulfill the proven constraints as well. In addition, I inferred a set of robustness criteria [80] for actual identity federation systems from my proofs. Yet, the constraint-based proofs have the drawback that they do not benefit from the composition theorem of the Reactive Simulatability (RSIM) Framework. I perceive this as an interesting open research question: to what extend can simulation-based proofs achieve the same grade of accuracy and the faithfulness to constraint-based standards? My initial assessment is that the accommodation of constraint-based specifications covering multiple protocol variants will escalate the complexity of the simulator.

I presented the first formal framework for rigorous security proofs of browser-based protocols. It builds on the Reactive Simulatability (RSIM) framework [14], to which I contributed a visual specification language for state-transition functions of I/O automata. In addition, I presented generic machines for browser and browsing behavior of users. The framework excels in the rigorous hand-written analysis of browser-based protocols and allows for an efficient graph-based assessment of static information flow. A canonical next step is the progression to tool-supported analysis, which
contains ample opportunities for future research: How can tool-supported formal methods faithfully analyze browser-based protocols while incorporating the necessary subtleties?

I explicitly excluded certain browser hazards from my framework, in which the restriction on active content is an important example. Whereas the consideration of scripted form POSTs and redirects is per se sufficient for the analysis of identity federation, other browser-based protocols can benefit from an active content model as well. Research covering a browser’s same-origin-of-code policy does an important first step into this direction. I perceive the exact modelling of active content and related browser hazards as an interesting topic for future research.

Whereas I presented a rigorous security proof of a POST-based WS-Federation protocol, there are various identity federation and browser protocols yet to be proven. My formal browser model also covers identity federation based on redirect of pseudo-random credential references as well as other techniques with POSTs and redirects. A rigorous security proof of the SAML 2.0 SSO Browser/Artifact Feature, for instance, seems well achievable in the browser model, but requires careful analysis. My browser model also seems to be suitable for a rigorous analysis of specific trust settings, such as two-factor authentication with secure devices or human interactive proofs.