Ключевые слова

certified programming, robust web applications, cryptographic verification, programs translation

сертифицированное программирование, надежные веб-приложения, трансляция, верификация, криптографические протоколы

Аннотация

Полубелова Марина Игоревна. Компиляция сертифицированных F*-программ в робастные Web-приложения. Научный руководитель: к.ф.-м.н., доц. Григорьев С. В. Направление “Математическое обеспечение и администрирование информационных систем”, кафедра Системного программирования.

Одним из способов повышения надежности систем является использование сертифицированного программирования для создания и верификации программного обеспечения. В рамках данного подхода реализация выполняется на языке с богатой типовой системой, статически гарантирующей некоторые свойства программы. Такая программа впоследствие транслируется в исполняемый на целевом устройстве язык программирования. Такой подход используется, например, для верификации криптографических примитивов в проекте HACL*, выполненном на языке программирования F*. В данной работе целевым языком для трансляции F*-программ выбран язык JavaScript, поддерживаемый всеми современными веб-браузерами. В работе предложены правила трансляции из F* в JavaScript, сохраняющие аннотации типов. Благодаря этой особенности возможно использовать инструмент Flow для дополнительной проверки полученной в результате трансляции программы.

Количество использованных источников: 37.
Полубелова, М. И. Компиляция сертифицированных F*-программ в робастные Web-приложения: магистерская дис.: защищена 13.06.2017 / Полубелова Марина Игоревна. — СПб., 2017. — 36 с. — Библиогр.: с.34-36.

Marina Polubelova. Compiling verified F* programs to robust Web applications. Scientific supervisor: Associate Professor Grigorev Semen. Speciality: Software and Administration of Information Systems, chair of Software Engineering.

One way to improve the robustness of systems is by using certified programming to create and verify programs. For this approach, the language with a rich type system is used to guarantee some properties of programs statically. Then such programs are translated into the target language for further execution. This approach is used in HACL* project dedicated to the verification of cryptographic primitives. All code of the project is written and verified in F* programming language. In this work, the target language of the F* programs translation is JavaScript, which is supported by all modern Web browsers. Translation rules proposed in the work preserve type annotations for more efficient use of a type checker Flow.

The number of references is 37.

Polubelova M. Compiling verified F* programs to robust Web applications: a master’s thesis: thesis defence 13.06.2017 / Polubelova Marina — SPb, 2017. — 36 pages — Bibliogr.: pp.34-36