Paper Title

Diego Lupi, Pedro Nieto, and Huaira Gómez

FaMAF - Universidad Nacional de Córdoba, Córdoba, Argentina

Resumen Easycrypt[1] es una herramienta automatizada que soporta la construcción y verificación de pruebas de seguridad de sistemas criptográficos. Permite mejorar la confianza en sistemas criptográficos mediante la entrega de pruebas verificadas formalmente que resultan en sus metas propuestas. Provee una plataforma versátil que soporta pruebas automatizadas pero también permite al usuario realizar puebas complejas de manera interactiva entrelazando la verificación del programa con la formalización de las matemáticas, hecho fundamental al formalizar pruebas criptográficas.

Keywords: Easycrypt · Game-based cryptographic proofs · Probabilistic.

1. Introducción

Desde siempre las pruebas fueron propensas a errores, lo que naturalmente las puede llevar a ser erróneas. En particular las pruebas de seguridad criptograficas la correctitud es critica para mejorar la confianza en el sistema criptografico. Actualmente se tiede a generar mas pruebas de seguridad de las que se pueden verificar, se omiten detalles finos desde un analisis formal que pueden tener grandes efectos en la practica. Teniendo en cuenta que los sistemas criptograficos en el mundo real pueden ser vulnerados, es necesario hacer las verificaciones sobre los pruebas de los sistemas criptograficos para evitar un desastre en el area de la seguridad.

Easycrypt es una herramienta que permite de manera interactiva buscar, construir, y realizar comprobaciones en maquina a pruebas de seguridad de construicciones criptograficas usando la secuencialidad del codigo con un enfoque de juego. En Easycrypt los juegos cryptograficos se modelan como modulos, que consisten en procedimientos escritos en lenguaje imperativo. Por otra parte los adversarios se modelan como modulos abstractos, modulos cuyo codigo es desconocido y puede cuantificarse. Desarrollada inicialmente por IMDEA Software Institute, e Inria. Posteriormente se sumo al desarrollo la École Polytechnique (Escuela Politecnica). IMDEA software institute es un instituto para el estudio avanzado de tecnologias para el desarrollo de software asentado en Madrid, Espana. Inria es un centro de investigación francés especializado en Ciencias de la Computación, teoría de control y matemáticas aplicadas. Por ultimo, la École Polytechnique es una gran escuela de ingenieros francesa bajo la tutela del Ministerio de Defensa.

El primer prototipo de EasyCrypt fue lanzado en 2009. Luego en 2012 se le hizo una reimplementacion completa con el objetivo de superar varias de las limitaciones que revelo el protopipo. Actualmente se encuentra en la version 1.0 que fue liberada el 10 Octubre de 2017. Desde el inicio EasyCrypt se ejecuto por linea de comandos, requeria que el usuario escriba las especificaciones criptograficas en un lenguaje de expresiones tipadas propio de la herramienta, con fuertes similitudes con los modulos de OCaml[2]. Luego de su reimplementacion fue posible ademas usar una interfaz interactiva en la que el usuario puede simular paso a paso la verificacion de su especificacion, y tambien contar con la capacidad de verificar pruebas mas complejas. Para ello los desarrolladores permitieron que EasyCrypt pueda ejecutar scripts interactivamente en Proof General[3], tambien debian proveer las bases requeridas para llevar a cabo algunos razonamientos criptograficos estandares para lo cual implementaron cuatro logicas que pueden ser usadas para crear argumentos híbridos.

Un aspecto fundamental que presenta la herramienta es el de darle la posibilidad al usuario de elegir el enfoque por el cual quiere verificar su especificacion criptografica, ya que es posible elegir interactivamente una o mas tecnicas de reduccion, decidir si realizar chequeo fuerte o debil.

Referencias

1. Gilles Barthe, Juan Manuel Crespo, Benjamin Gregoire, Cesar Kunz, Santiago Zanella Beguelin. Computer-Aided Cryptographic Proofs. Third International Conference, 2012.
2. OCaml Website: (2013) https://ocaml.org.
3. Proof-General Website: (2016) https://proofgeneral.github.io.