情報処理学会論文誌　プログラミング　Vol.7　No.3　51 (July 2014)

発表概要

逆方向実行可能言語によるエンコーダとデコーダの同時実装

田中 哲[1,a)]

2014年1月14日発表

本発表ではプログラムを逆方向にも実行可能なプログラミング言語 Conservation を提案し，例として X.509 証明書のエンコーダとデコーダを記述する．また応用として，エンコーダを修正して間違った証明書を生成し，既存の暗号ライブラリに対してファジングを行う．通信プロトコルやデータフォーマットなど，データをプロセスの外部で表現するためにはデータをバイト列にエンコードし，また，逆にバイト列をデータにデコードすることが欠かせない．エンコードとデコードは対になる処理であるが，通常は別々に開発するため，正しく対応がとれた実装になるとは限らない．本発表ではプログラムを逆方向にも実行可能なプログラミング言語によりエンコードとデコードをひとつのプログラムとして記述可能とする．それにより常に正しく対応のとれたエンコーダとデコーダが開発できる．また，開発における利点だけでなく，ファジングにも利用できることを示す．

Implementing Encoder and Decoder at Once in a Reversible Programming Language

Akira Tanaka[1,a)]

Presented: January 14, 2014

This presentation proposes a reversible programming language: Conservation. We implemented encoder and decoder for X.509 certificates as an example program. Also, we modify the encoder to generate wrong certificates and fuzz existing cryptographic library. Implementation for communication protocols and data formats needs encoder (converter from a data structure to a sequence of bytes) and decoder (converter from a sequence of bytes to a data structure). Usually they are implemented individually and not guaranteed to be inverse functions of each other. This presentation explains the language can be used to implement a pair of encoder and decoder with single program. The program can run forward to work as an encoder and run backward as a decoder. The behaviors are guaranteed to be inverse functions. This means correct program can be implemented with less effort. The program can also be used for fuzzing by modifying the encoder.

[1] 独立行政法人産業技術総合研究所セキュアシステム研究部門
Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Ibaraki 305–8568, Japan
[a)] tanaka-akira@aist.go.jp