SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

脆弱性自動検知に向けたバイナリプログラム解析ツールの開発
Development of a Binary Program Analysis Tool for Automatic Vulnerability Detection

泉田 大宗 * 橋本 政朋 † 森 彰 ‡
Tomonori Izumida Masatomo Hashimoto Akira Mori

キーワード バイナリプログラム解析, 脆弱性解析, ファームウェア解析

あらまし

筆者らは、IoT デバイスのセキュリティを自動的に分析・診断する手法として、ファームウェアの静的解析による脆弱性の自動検知技術に取り組んできた。本稿では、独自に開発したバイナリ静的解析ツールを既存の商用リバースエンジニアリングツールに統合することで、CPU アーキテクチャや OS やコンパイラに依存しない自動解析を実現した過程について説明する。そして、実際に報告された IoT ファームウェアの脆弱性を例に取り、典型的なメモリ破壊の脆弱性がどのように自動検知されるかについて解説する。

謝辞

この研究は、国立研究開発法人新エネルギー・産業技術総合開発機構（ＮＥＤＯ）の委託業務（JPNP16007）の結果得られたものである。

* IIJ イノベーションインスティテュート, 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム, IIJ INNOVATION INSTITUTE INC., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan, tizmd@iij.ad.jp
† 千葉工業大学, 千葉県習志野市津田沼 2-17-1, Chiba Institute ofTechnology, 2-17-1 Tsudanuma, Narashino, Chiba 275-0016,Japan
‡ 産業技術総合研究所, 大阪府池田市緑丘 1-8-31, National Instituteof Advanced Industrial Science and Technology, 1-8-31 Midorigaoka, Ikeda, Osaka 563-8577, Japan