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

VMM を用いたプログラム実行時の証拠取得機能における取得対象の拡張と改ざん耐性の向上

Extension of Target Information and Improvement of Tamper Resistance for VMM-Based Evidence Collection Function of Program Execution

伊藤 寛史 * 中村 徹 †‡ 磯原 隆将 † 山内 利宏 §‡
Hiroshi Ito Toru Nakamura Takamasa Isohara Toshihiro Yamauchi

キーワード Virtual Machine Introspection，証拠保全，プログラム実行

あらまし

利用者が実行したプログラムについて，実行環境，実行過程，および実行結果の証拠を保全し，検証可能にすることは重要である．証拠に基づく検証により，脆弱性の悪用および改ざんされたプログラムやライブラリがプログラムの実行過程に含まれていないことを保証できる．ここで，プログラム実行の証拠を保全できていない場合，プログラム実行処理を検証することは困難である．

我々は，仮想計算機モニタ（以降，VMM）を用いて，プログラム実行の証拠を保全するシステム（以降，従来のシステム）を提案した [1]．従来のシステムでは，VMM を用いて，取得した情報を監視対象のゲスト OS から隔離する．これにより，取得した情報の改ざんを防止する．従来のシステムでは，ゲスト OS 上でのプログラム実行時に利用されたライブラリ情報について，取得方法および改ざん前に取得する方法は示されている．しかし，証拠として取得する情報のうちライブラリ以外の情報について，取得方法および改ざん前に取得する方法は検討されていない．また，ゲスト OS で取得した情報の改ざん防止のため，ゲスト OS からホスト OS への情報の転送方法は検討されていない．

本稿では，従来のシステムを拡張し，証拠として取得する情報のうちライブラリ以外の情報について，取得方法，および改ざん前に取得する方法を提案する．また，ゲスト OS からホスト OS への情報の転送方法を提案する．ライブラリ以外の情報の取得方法については，セマンティックギャップに対処するために，VMM から取得可能か調査し，情報ごとの取得方法を検討した．セマンティックギャップとは，OS 内で取得できる情報と VMM から取得できる情報について，OS によって意味付けされているか否かの差のことである．改ざん前に取得する方法については，情報の生成に関連するシステムコール処理時を取得の契機とした．ゲスト OS からホスト OS への情報の転送方法については，ゲスト OS での取得処理後にゲスト OS で VMM への遷移処理を行うことで，ゲスト OS からホスト OS へ情報を転送する．本稿では，拡張したシステムの実現方式を示し，取得する情報の例および情報取得によるオーバヘッドの評価結果を述べる．

参考文献

[1] Toru Nakamura, et al.: (Short Paper) Evidence Collection and Preservation System with Virtual Machine Monitoring, The 16th International Workshop on Security (IWSEC 2021), Lecture Notes in Computer Science (LNCS), vol.12835, pp.64-73 (2021).

* 岡山大学 大学院自然科学研究科, 〒 700-8530 岡山県岡山市北区津島中 3-1-1, Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama, 700-8530, Japan.
† KDDI 総合研究所, 〒 356-8502 埼玉県ふじみ野市大原 2-1-15, KDDI Research, Inc., 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan.
‡ 国際電気通信基礎技術研究所, 〒 619-0288 京都府相楽郡精華町光台 2-2-2, Advanced Telecommunications Research Institute International, 2-2-2 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0288, Japan.
§ 岡山大学 学術研究院 自然科学学域, 〒 700-8530 岡山県岡山市北区津島中 3-1-1, Graduate School of Natural Science and Technology, 3-1-1 Tsushima-naka, Kita-ku, Okayama, 700-8530, Japan.