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

PIN 認証プログラムへの命令改変フォールト攻撃の形式的影響評価
How to Formally Evaluate the Effects of Instruction Manipulation Attacks on PIN Authentication Programs

林 俊吾 † 坂本 純一 †* 松本 勉 †
Shungo Hayashi Junichi Sakamoto Tsutomu Matsumoto

キーワード フォールト攻撃　命令改変攻撃

あらまし

動作中の機器に外乱を与えて故障を発生させ，機器内部の秘密情報の漏洩や不正な機能改変を引き起こす攻撃はフォールト攻撃と呼ばれており，組込み機器に実装された暗号機能やアクセス制御等のセキュリティ機能に対する脅威として認知されている．これまでに様々な故障注入方法によるフォールト攻撃により，プロセッサで実行される命令をスキップしたり，命令の機械語の一部を操作して別の命令に改変したりする攻撃が確認されている[1][2]．このような，実行される命令を別の命令に故障注入により改変するフォールト攻撃を，命令改変攻撃と呼ぶ．命令改変攻撃ではどのように命令を改変するかに応じて様々なモデルが定義できる．

本報告では,この命令改変攻撃がプログラムに与える影響を形式的に評価する手法を提案する．すなわち提案手法では，命令改変攻撃がなされた場合のプログラムの振舞いを記号的に解析し，攻撃者の目的が達成されるための条件あるいは達成されないための条件が真になるかを検証し，それらの結果をもとに命令改変攻撃がプログラムへ与える影響を分類する．また，攻撃成功の成否がプログラム実行時のプロセッサの初期状態に依存する場合は，追加評価を行うことにより攻撃成功の難易度を定量的に評価する．そして 1 回のレーザー照射を行い命令の機械語を操作するモデルの命令改変攻撃を想定し,この攻撃モデルの攻撃者がアクセス制御の一種である PIN 認証のプログラムに対して与える影響を評価する．評価対象とする PIN 認証プログラムは，フォールト攻撃評価用のコード集[3]のものを使用する．これにはフォールト攻撃対策を適用したいくつかの PIN 認証プログラムの実装があり，どの実装が効率的に今回のモデルの攻撃者に対する耐性を高められるかを評価し，命令改変攻撃に対して有効な PIN 認証プログラムの実装について検討する．

† 横浜国立大学 〒240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7
Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan
* 産業総合研究所 〒135-0064 東京都江東区青海 2-3-26
National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo 135-0064, Japan

本研究の一部は，内閣府が進める戦略的イノベーション創造プログラム（SIP）「ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティ」（管理法人：NEDO）によって実施されたものである．

参考文献

[1]Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, "An In-depth and Black-box Characterization of the Effects of Clock Glitches on 8-bit MCUs",Workshop on Fault Diagnosis and Tolerance in Cryptography, pp.105-114, 2011.
[2]Brice Colombier, Alexandre Menu, Jean-Max Dutertre, Pierre-Alain Moëllic, Jean-Baptiste Rigaud, Jean-Luc Danger, "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller", IEEE International Workshop on Hardware-Oriented Security and Trust, pp.1-10, 2019.
[3]Louis Dureuil, Guillaume Petiot, Marie-Laure Potet, Thanh-Hale, Aude Crohen, Philippe de Choudens, "FISSC: A Fault Injection and Simulation Secure Collection", International Conference on Computer Safety Reliability and Security, pp.3-11, 2016.