平成２６年度　卒業研究報告書概要

課程，学籍番号，氏名	課程：電気・電子情報工学課程，学籍番号：B133242，氏名：佐藤　清広
工学分野名：情報通信システム	指導教員名：市川　周一，藤枝　直輝，松岡　俊佑

題　　目：

命令拒否レジスタファイルを用いたソフトウェア改ざん攻撃への対策に関する研究

(Preventing software falsification using Instruction Rejection Register File)

Abstract

Recently, the defense of software against analysis, plagiarism, and falsification has become an important issue. Fujieda and Ichikawa proposed to use Instruction Register File (IRF) as a method to protect software. The IRF is a table of frequently-used instructions, which is referred by an index of an IRF instruction. The corresponding instruction can be executed both in an IRF instruction and in its original form. Software may be thus falsified using the original form of the instructions.

This study presents Instruction Rejection Register File (IRRF), which is a device to reject the original form of the instruction in the IRF. The target processor is Plasma. Our evaluation results show that the IRRF can be implemented with small hardware cost on FPGA (Field Programmable Gate Array): the increase of hardware cost was less than 1 % of Plasma. IRRF can reject 54.8 % of the original form of the instruction in the IRF.

概　　要

近年，ソフトウェアを解析・盗用・改ざんから防御する能力，すなわち耐タンパ性の重要性が増加している．ソフトウェアの耐タンパ性向上の 1 つの手段として，命令セット（プロセッサの命令と機械語表現との対応関係）をランダム化する手法が提案されている．命令レジスタファイル（Instruction Register File：IRF）は出現頻度の高い命令を集めたテーブルで，命令フェッチの消費電力削減のため提案された．藤枝と市川は IRF を耐タンパ性向上のために利用することを提案した．IRF を用いた手法では，IRF 内の命令を IRF のインデックスを指定することで参照できる．ランダム化は IRF のインデックスと命令の対応をシャッフルすることで行われる．ところが IRF を用いるだけでは，ソフトウェアの改ざんに対抗できない．IRF 内の命令は元々の命令表現でも実行できるため，IRF の内容を知らなくてもソフトウェアが改ざんできるためである．しかし，IRF にある命令は必ず IRF を参照する命令で使用することにすれば，IRF にある命令の元々の命令表現はプログラム中に出現しえないことになる．もし出現すれば，改ざんによる命令であるとみなせる．このように命令の直接実行を拒否する機構を追加することで，改ざんに対抗することができる．

本研究では，IRF にある命令の直接実行を拒否するためのハードウェアとして，命令拒否レジスタファイル（Instruction Rejection Register File：IRRF）を提案する．本研究の目的は，IRRF を用いて命令の実行拒否を行うシステムを設計し，IRF を用いた耐タンパ性向上手法に改ざんへの対策を提供することである．実装には MIPS 命令セットのソフトコアプロセッサである Plasma を使用した．本研究の手法を FPGA（Field Programmable Gate Array）上に実装し，そのコストについて評価した結果，ハードウェア量の尺度であるスライス数は１%未満の増加にとどまり，軽微なコストで改ざん対策を実現することができた．

IRRF の生成にあたって，IRF 内のどの命令が IRRF に登録されるかはインデックス生成法に依存している．適切な生成法を用いることで IRF にある命令を IRRF でより多く検出できる．インデックス生成法を変更し最適化を行った結果，IRF にある命令のうち 54.8 %を IRRF で実行拒否することが可能となった．

発表する際の課程を記入　　電気・電子情報工学　課程　　発表番号　48

（学籍が他課程所属の学生も発表する課程を記入すること）