5X-06

VMセキュアプロセッサにおける暗号化方式の検討
Data Encryption Methods for VM Secure Processor

嶋 紘之 † 宮永 瑞紀 † 千田 拓矢 † 岡本 拓也 † 五島 正裕 § 坂井 修一 †
Hiroyuki Shima Mizuki Miyanaga Takuya Chida Takuya Okamoto Masahiro Goshima Shuichi Sakai

1 はじめに

ネットワークやハードウェア技術の発展により，Amazon EC2などの仮想サーバを提供するクラウドサービスが普及している [1]．クラウドプラットフォームを利用する場合，利用者自身がサーバ筐体を保有・運営する必要がなく，利用に当たっては最低限の接続環境を用意するだけでよいため導入・運営コストなど様々な面で優れている．

その一方で，近年クラウドサービスのセキュリティ面のリスクが指摘されている．クラウドプロバイダ内部の管理者・オペレータに悪意がある場合，クラウド利用者の機密情報の悪用をされることが想定される．Googleの技術者が自社サービスのユーザの個人情報を盗む事件 [2] も発生しており，このようなリスクは無視できない．従来のソフトウェアによる対策に留まらず，強い権限によるアクセス制御， すなわちOSや端末の管理者に与えられるアクセス権限をもハードウェアレベルで制限する手法が必要になっている．

本稿では，クラウドサービスにおける悪意あるクラウド管理者による情報漏洩・改竄の問題の解決を目的として，我々が提案しているVMセキュアプロセッサ [3] の概要を説明し，そこで用いる暗号化方式の検討及び評価を行なう．

2 悪意のあるクラウド管理者の脅威

クラウドユーザの機密情報への脅威は大きく2つに分類できる．

2.1 管理者権限の悪用

クラウド管理者が権限を悪用することによる，クラウドのユーザが使用する仮想マシン (ユーザVM) 内の機密情報の漏洩・改竄によるリスクが指摘されている．クラウドのユーザはクラウドで使用する機密情報を自身のユーザVM内に保存していることが一般的だが，クラウド管理者の仮想マシン (管理VM) やハイパーバイザ (仮想マシンモニタ) はユーザVMに対して一般に強い権限をもっており，これを悪用されユーザVM内の情報を窃取・改竄される危険性がある．管理者権限の悪用はソフトウェアによる暗号化やアクセス制御で対応可能である．

2.2 ハードウェアに対する物理的な攻撃

管理者権限の悪用に対してソフトウェアを用いて対処したとしても，ハードウェア (メモリ，データパス，NICなど) に対する攻撃が行われた場合，ユーザVM内の情報の漏洩・改竄を防ぐことが出来ない．クラウドサービスではハードウェア本体はユーザから見て遠隔地にあるため，悪意ある管理者によってハードウェアを利用した情報の不正取得がなされる危険性がある．攻撃手法としては，デジタル回路の信号を解析できるロジックアナライザでハードウェアを直接解析するなどが挙げられる．クラウドにおいては，ソフトウェアレベルの攻撃だけではなくハードウェアに対する攻撃も防ぐ必要がある．

3 セキュアプロセッサ

管理者権限の悪用及びハードウェアに対する物理的な攻撃への解決策として，これまで以上に強い権限によるアクセス制御，すなわち管理者権限をもハードウェアレベルで制限する手法が研究されている．不正な手段を用いてコンピュータ内の情報を窃取・改竄する攻撃対策のハードウェアレベルの研究としてAEGIS [4]，Ascend [5]， L-MSP [6] などのセキュアプロセッサが挙げられる．セキュアプロセッサはプロセスを悪意のあるOSや他のプロセスから守ることを目的としている．セキュアプロセッサではプロセッサ内部のみ信頼し，プロセッサ外部に情報を書き出す際プロセスに対して透過的に暗号化することでプロセスの挙動や情報をOSや他のプロセスから秘匿する．

セキュアプロセッサの実用化への大きな障害として，OSとユーザプロセスの強い結びつきが挙げられる．既存OSをセキュアプロセッサに用いるにはプロセス管理に関する根幹部分の改変が必要になる．

4 VMセキュアプロセッサ

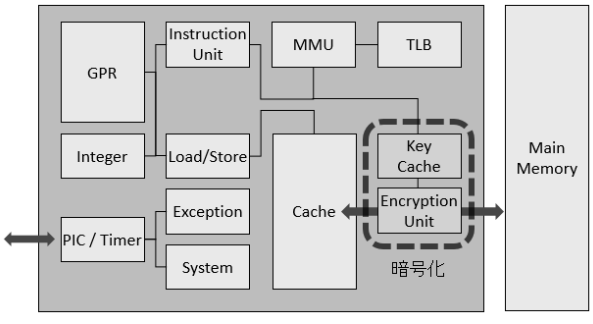

図 1: VMセキュアプロセッサ

クラウドサービスでユーザVM内の機密情報へのタンパの対策として，我々はセキュアプロセッサを仮想化に対応させたVMセキュアプロセッサを提案している．悪意あるクラウド管理者からユーザVMを保護することを目的とし，クラウド管理者の管理者権限の悪用とハードウェアに対する物理的な攻撃を想定してい

†東京大学, The University of Tokyo
§国立情報学研究所, National Institute of Informatics

る．セキュアプロセッサでは保護対象はユーザのプロセスだったが，VM セキュアプロセッサではユーザ VM を保護対象としている．これにより OS のプロセス管理を改変するセキュアプロセッサと比べ改変の負担は軽減される．VM セキュアプロセッサにおいてはハイパーバイザの改変のみで済む．

4.1 プロセッサによる暗号化・復号

VM セキュアプロセッサでは，悪意あるクラウド管理者による物理的な攻撃を想定して，プロセッサ内部のみ信頼し，プロセッサ外部は信頼できないものとする．プロセッサ外部であるメモリ上の情報は暗号化によって機密性を確保する．通常のプロセッサの構成に図 1 で枠線で囲んだ暗号化・復号ユニットを追加している．プロセッサからメモリにデータを書き込む際に暗号化を行い，メモリからデータを読み込む際に復号を行う．暗号化・復号には共通鍵暗号方式を用いる．これにより，プロセッサ外部ではユーザ VM の情報は暗号化されているため，悪意あるクラウド管理者に物理的にハードウェアを解析されても情報が盗み出されることはない．

4.2 アクセス制御

VM セキュアプロセッサは，プロセッサ内部のレジスタの機密性を確保するためにアクセス制御を行う．仮想化環境では VM ごとに仮想化されたプロセッサが割り当てられるが， 物理的なプロセッサは異なる VM 間で共有していることがあるため，ユーザ VM 以外の VM からプロセッサ内部のメモリにアクセスされることがある．したがって，VM セキュアプロセッサではキャッシュに VM ごとに固有の識別子を割り当て，識別子と同一の VM のみにアクセスを許可する．これによって，クラウド管理者の管理者権限を用いてもユーザ VM の情報を盗むことが出来ない．

5 VM セキュアプロセッサに適用する暗号化方式

VM セキュアプロセッサ内においてのみブロック単位で暗号化・復号するため，共通鍵暗号方式のブロック暗号を用いる．暗号強度や設計の平易さを加味して AES を採用する．

6 評価

6.1 評価環境

Alpha21164A という命令セットアーキテクチャのプロセッサシミュレータ「鬼斬弐」[7] にて，AES によるメモリ暗号化を行う場合の性能評価を行った．評価には SPECCPU 2006 に含まれる全 29 本のベンチマークプログラムを用いた．入力データセットには ref を用い，最初の 1G 命令をスキップし直後の 100M 命令の評価を行った．

6.2 評価モデル

メモリアクセスにかかる時間が 200cycles の場合と，AES によるメモリアクセスにおける遅延が 21cycles 加わった場合の 221cycles の場合で評価し，遅延挿入による相対 IPC を求めた．AES による遅延は AES のソースコードを元に現実的な値を算出した．

6.3 遅延挿入による相対 IPC

評価結果を図 2 に示す．遅延挿入による性能低下は最大で 6%で平均は 0.5%であった．実用に耐える性能低下の範囲内で AES を用いて外部メモリを暗号化・復号出来ると言える．これにより，VM セキュアプロセッサにおいて AES の採用が妥当だと言える．

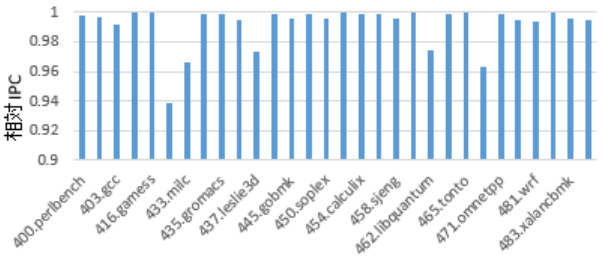

図 2: 遅延挿入による相対 IPC

7 おわりに

クラウドサービスにおける悪意あるクラウド管理者による情報漏洩・改竄の問題の解決を目的とした，VM セキュアプロセッサにおける暗号化方式の検討及びプロセッサシミュレータ「鬼斬弐」による評価を行った．AES によるメモリアクセスにおける性能低下は実用の範囲内であり，VM セキュアプロセッサにおける AES の採用は妥当であると言える．今後はオープンソースのプロセッサである Open RISC [8] への AES の実装を行う予定である．

参考文献

[1] Amazon Web Services. 国内のお客様の導入事例 Powered by AWS クラウド, http://aws.amazon.com/jp/solutions/case-studies-jp/, 2014.

[2] New York Media LLC. ”Elite Google Engineer Used Google Data to Spy on Four Teens ” New York Media LLC. , America, 2014

[3] 山田剛史, 千田拓矢, 山口利恵, 五島正裕, 坂井修一. VM を保護するセキュアプロセッサとそれを用いたアプリケーション認証手法. 2014 年 暗号と情報セキュリティシンポジウム予稿集, 3F3-3, 2014.

[4] G. E. Suh, Charles W. O’Donnell, and Srinivas Devadas. Aegis: A single-chip secure processor. *Design & Test of Computers, IEEE*, Vol. 24, No. 6, pp. 570–580, 2007.

[5] Christopher W. Fletcher, Marten v. Dijk, and Srinivas Devadas. A secure processor architecture for encrypted computation on untrusted programs. pp. 3–8, 2012.

[6] 橋本幹生, 春木洋美, 川端健. オープンソース os と共存可能なセキュリティプロセッサ技術 (特集情報セキュリティ技術–安心・安全な社会へのソリューション), 2005.

[7] 塩谷 亮太, 五島 正裕, 坂井 修一: プロセッサ・シミュレータ「鬼斬弐」の設計と実装, 先進的計算基盤システムシンポジウム SACSIS 2009, pp. 120-121 (2009).

[8] Damjan Lampret, Chen-Min Chen, Marko Mlinar, Johan Rydberg, Matan Ziv-Av, Chris Ziomkowski, Greg McGary, Bob Gardner, Rohit Mathur, and Maria Bolado. Openrisc 1000 architecture manual. *Description of assembler mnemonics and other for OR1200*, 2003.