VM のメモリ暗号化によるクラウド管理者への情報漏洩の防止

田所秀和[†] 内田昴志[††]
光来健一[††,†††] 千葉滋[†]

1. はじめに

ネットワークを介して様々なサービスを提供するクラウドコンピューティングが普及してきている。クラウドコンピューティングの一形態である、EC2[1] に代表される IaaS は利用者に仮想マシン (VM) を提供しており、利用者は必要な時に必要なだけ VM を使うことができる。しかしその反面、自分で管理していないクラウド内にあるサーバを利用しているためセキュリティが大きな課題となっている。例えば、クラウドの管理者が VM のサスペンドを行った場合、容易に利用者の VM から情報を盗み出すことができ利用者の機密情報が漏洩する恐れがある。本研究では VM からの情報漏洩の中でもメモリからの情報漏洩に着目し、これを防ぐことを目的とした。

2. クラウド管理者への情報漏洩

特権 VM は、ユーザ VM の起動や停止をしたり、ハードウェアへアクセスする権限を持った VM である。クラウド管理者は、この特権 VM を通して新たなユーザ VM の作成、サスペンド・レジュームなどの管理をおこなう。この管理のために、特権 VM はユーザ VM のメモリを読み書きできるようになっている。例えば、ユーザ VM のサスペンドは、特権 VM がユーザ VM のメモリをすべて読み取りその内容をディスクに保存することで実現されている。

クラウド管理者が、このようなユーザ VM のメモリを読む機能を悪用すると、ユーザ VM 内の情報を盗むことができてしまう。例えば、ゲスト OS のメモリ上のファイルキャッシュを見ることにより、ディスクを暗号化していてもファイルの内容を盗み見ることができる。また、メモリ上に一時的に格納されているパスワードなどの機密情報を盗むこともできるかもしれない。

† 東京工業大学
†† 九州工業大学
††† 独立行政法人科学技術振興機構, CREST

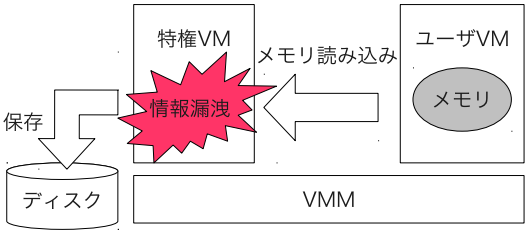

図 1 サスペンド時の情報漏洩

3. VMM によるユーザ VM のメモリ暗号化

この問題を解決するために、本研究では特権 VM がユーザ VM のメモリへアクセスするときに、仮想マシンモニタ (VMM) がメモリを暗号化することで情報漏洩を防ぐシステム VMCrypt を提案する。ユーザ VM のメモリを暗号化することで、特権 VM がユーザ VM のメモリにアクセスしても、メモリの内容を容易に盗み出せないようにする。例えば、特権 VM がユーザ VM のサスペンドを行う際、保存されるメモリの内容を自動的に暗号化してユーザ VM の状態をディスクに保存することができる。また、レジューム時にはディスクから暗号化されたユーザ VM の状態を読み込んだ後でメモリの内容を自動的に復号化することで安全にユーザ VM を復元できる。

VMCrypt では、どのメモリページを暗号化するかを VMM が判別する。これは特権 VM がアクセスする時に、単純にユーザ VM のすべてのメモリを暗号化するわけにはいかないためである。例えば、特権 VM はユーザ VM のサスペンド・レジューム時にユーザ VM の一部のメモリの内容を読み書きする必要がある。ただし、これらはユーザ VM 内の機密情報ではないため、特権 VM が内容を見ることができても情報漏洩は発生しない。

VMCrypt は特権 VM からの情報漏洩を防ぐために、VMM がクラウド管理者に改ざんされないと仮定している。VMM の起動時に Intel TXT[2] 等のハードウェアの機能を使うことで、起動する VMM が改ざ

んされていないことを保証することができる。また、起動後は VMM は特権 VM より高い特権で動くので、特権 VM から VMM を改ざんするのは難しい。

4. VMCrypt の実装

我々は VMCrypt を Xen を用いて実装した。Xen においては特権 VM はドメイン 0 と呼ばれ、ドメイン U と呼ばれるユーザ VM を管理している。現在の実装では、ゲスト OS として準仮想化 Linux を対象としている。

4.1 VMM での暗号化・復号化

VMM によるメモリ暗号化はドメイン 0 がドメイン U のページをマップする際に行う。メモリマップの検出は、ページテーブルを変更するハイパーコールを監視することで行う。ドメイン 0 がドメイン U のメモリページをマップする際には、必ずハイパーコールを発行してページテーブルを書き換える。

一方、ページの復号化はマップしたページをアンマップした際に行う。アンマップの検出は、ページフォールトを監視することで行う。ドメイン 0 は、マップしたページをアンマップするためにページテーブルエントリを書き換えるが、VMM はページテーブルを書き換え禁止にしておりページフォールトが発生する。このときに、ドメイン U のページをアンマップしようとしていたら、同時にページの復号化を行う。

4.2 暗号化除外ページ

準仮想化 Linux では、ドメイン 0 が読み書きするために暗号化してはいけないページが 4 種類ある。VMCrypt では、VMM がゲスト OS 中のこれらのページを認識し、暗号化しないようにする。

共有情報 (shared_info)

shared_info は、VMM とゲスト OS が情報を共有するために用いられるページである。shared_info には、後述する P2M テーブルの情報が含まれており、サスペンド時にドメイン 0 が読み込める必要がある。shared_info が存在するページは VMM も管理しているので、簡単にこのページを暗号化しないようにすることができる。

起動情報 (start_info)

start_info は、ドメイン 0 とゲスト OS が情報を共有するために用いられるページである。仮想コンソールを実現するためのページなどが含まれており、ドメイン 0 が設定するために書き込める必要がある。VMM は start_info として使われるページを管理していないが、このページはドメイン 0 が仮想 CPU のレジスタ経由でドメイン U に通知している。VMM はドメイン U の実行を再開するハイパーコール中でこのレジスタをチェックすることで、start_info のページを特定する。

ページテーブル

ドメイン 0 がドメイン U をサスペンドする際、ドメイン U のページテーブルを書き換えてから保存する。準仮想化 Linux では、ページテーブルは仮想アドレスからマシンフレーム番号への対応表であるため、ドメイン 0 はページテーブルのマシンフレーム番号を疑似物理フレーム番号に変換するためである。VMM はページテーブルに使われているページを管理しているため、サスペンド時にドメイン 0 がページテーブルをマップしようとしているかどうかは容易に判定できる。一方、レジューム時には、ドメイン 0 がページテーブル用にページを pin するハイパーコールを発行するため、判別することができる。

P2M テーブル

P2M テーブルは、疑似物理フレーム番号からマシンフレーム番号への対応を管理する木構造である。ドメイン 0 がドメイン U をサスペンドする際、P2M テーブルを保存するためにこの木をたどる必要がある。サスペンド時には、VMM は shared_info から取得した P2M テーブルをたどることにより P2M テーブルのページを判別できる。このとき、P2M テーブルの疑似物理フレーム番号をドメイン U の使われていないメモリに暗号化して記録しておき、レジューム時の判別に使う。レジューム時には、保存しておいた疑似物理フレーム番号からマシンフレーム番号を求め P2M テーブルの判定に使う。マシンフレーム番号を求めるために P2M テーブルは使えないので、ドメイン U が使うページ一覧と M2P テーブルを使う。

5. まとめと今後の課題

本稿では IaaS 環境において、クラウド管理者への情報漏洩を防ぐシステム VMCrypt を提案した。現在は VMM からの暗号化除外ページの判定が不完全であり、一部のページについては専用のハイパーコールで VMM に登録している。VMM だけで判別できるようにすることが今後の課題である。

参 考 文 献

1) Amazon Web Services: Amazon Elastic Compute Cloud, `http://aws.amazon.com/ec2/`.
2) Intel Corp.: Intel Trusted Execution Technology, `http://www.intel.com/technology/security/`.