平成 27 年度 卒業論文概要			
所　　属	機械情報工学科	指導教員	光來 健一
学生番号	12237012	学生氏名	猪口 恵介
論文題目	クラウドにおける VM リダイレクト攻撃を防ぐ安全なリモート管理		

1　はじめに

近年，急速にクラウドコンピューティングの普及が進んでいる．クラウドコンピューティングのサービス形態の一つである IaaS 型クラウドでは，ユーザに仮想マシン（VM）などのインフラを提供し，ユーザは VM に OS やアプリケーションをインストールして利用することができる．ユーザは VM（ユーザ VM）を管理する際に，まず管理 VM と呼ばれる VM にネットワークを介して接続し，管理 VM 経由でユーザ VM にアクセスを行う．例えば，ユーザは管理 VM においてユーザ VM の起動や終了を行ったり，ユーザ VM 内部のシステムにログインして管理を行ったりすることができる．

しかし，管理 VM を管理しているクラウドの管理者は必ずしも信頼できるとは限らない．そのため，クラウド管理者によって管理 VM の権限を悪用されて様々な攻撃を行われる可能性がある．そのような攻撃の一つに，ユーザがアクセスする VM を変更される攻撃が考えられる．本研究ではこのような攻撃を *VM* **リダイレクト攻撃**と呼ぶ．VM リダイレクト攻撃によって悪意ある管理者が用意した VM にアクセスさせられた場合，VM 内部にインストールされたスパイウェアなどによってユーザの情報が盗まれる恐れがある．

本研究では，クラウドにおいてユーザ VM を管理する際に，管理 VM における VM リダイレクト攻撃を防ぐ *UVBond* を提案する．

2　VM リダイレクト攻撃

管理 VM はユーザ VM を管理するために用いられる VM であり，ユーザ VM に対して様々な権限を持っている．例えば，ユーザは管理 VM においてユーザ VM の起動や停止を行ったり，バックアップを作成したり，他のホストへのマイグレーションを行ったりすることができる．また，管理 VM 内に作成されるユーザ VM の仮想デバイスに直接アクセスすることで，ネットワークを用いずにユーザ VM 内のシステムにログインしてアクセスすることもできる．

管理 VM はクラウドのシステム管理者によって管理されているが，クラウドの管理者は必ずしも信頼できるとは限らない．実際，Google の管理者がユーザのプライバシを侵害するという事件が発生している．また，サイバー犯罪の 28% は内部犯行であり，管理者の 35% は機密情報に無断でアクセスしたことがあるという報告もある．このように，クラウドのサービスプロバイダ自体は信頼することができるとしても，クラウド内に管理権限を悪用する管理者がいないことを保証するのは難しい．

悪意あるクラウドの管理者は管理 VM の権限を利用してユーザ VM に対して容易に様々な攻撃を行うことができる．

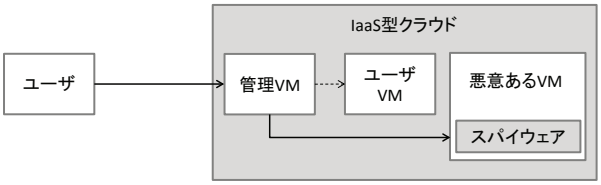

図 1　VM リダイレクト攻撃

本研究では特に，VM リダイレクト攻撃と呼ぶ攻撃に着目する．VM リダイレクト攻撃は図 1 のように，管理 VM においてユーザがアクセスする VM を変更する攻撃である．クラウドの管理者は，スパイウェアなどをインストールした悪意ある VM を作成しておき，ユーザをその VM にアクセスさせることで様々な攻撃を行うことができる．例えば，システムのログインプログラムを改ざんしたり，キーロガーを仕掛けたりすることで，ユーザが VM 内のシステムにログインする際にパスワードを盗むことができる．

3　UVBond

本研究では，VM のディスクを介してユーザと VM を強く結びつけることで VM リダイレクト攻撃を防ぐ *UVBond* を提案する．UVBond ではディスク暗号化を用いることにより，ユーザの指定したディスクイメージから VM が起動されたことをユーザ自身が確認することができる．VM が正しく起動されていれば，UVBond はユーザに暗号化された VM 識別子を返す．ユーザはこの VM 識別子を用いて VM にアクセスすることで，管理 VM においてアクセス先の VM を変更されることを防ぐことができる．

クラウドの信頼できない管理者が VM のディスク暗号化や VM 識別子の管理に干渉できないようにするために，UVBond は信頼できるハイパーバイザを用いる．ハイパーバイザは VM の下で動作する基盤ソフトウェアであり，VM の実行を制御する．本研究では，クラウドプロバイダは信頼できるものとし，クラウド内のハイパーバイザは TPM と呼ばれるハードウェアを用いたセキュアブートで正常に起動されることを仮定する．

3.1　暗号化ディスクを用いた VM の起動

UVBond では，図 2 のようにユーザ VM によるディスクの読み書きをハイパーバイザが捕捉し，データの復号化および暗号化を行う．ユーザにより暗号化されたディスクイメージは従来と同様に管理 VM に格納される．そして，ユーザ VM は管理 VM と通信することによりディスクへのアクセスを行う．従来のハイパーバイザはこの通信を中継するだけであったが，UVBond では通信の内容を解析することでディスクから読み

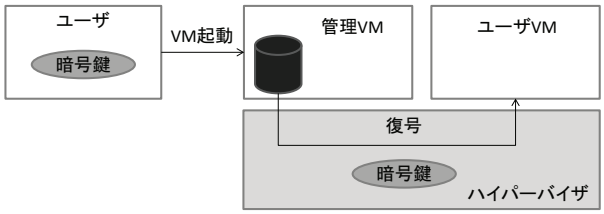

図 2　暗号化ディスクを用いた VM の起動

込むデータの復号化，および，ディスクに書き込むデータの暗号化を実現する．

ディスクイメージの暗号化に用いられる暗号鍵は VM の起動時にユーザによってハイパーバイザに登録される．信頼できない管理者に暗号鍵を盗まれないようにするために，暗号鍵はハイパーバイザの公開鍵で暗号化されてハイパーバイザに渡される．ハイパーバイザの公開鍵はあらかじめ信頼できる鍵サーバに登録しておく．この暗号データを受け取ったハイパーバイザだけが自身の秘密鍵を用いてディスクの暗号鍵を復号することができる．

UVBond は VM の起動時に，指定されたディスクイメージがハイパーバイザに登録された暗号鍵で暗号化されたものであるかどうかを確認する．そのために，ハイパーバイザ内でディスクのブートセクタのチェックを行う．ブートセクタは VM の起動時に必ず読み込まれ，固有のマジックナンバが格納されている．ハイパーバイザがブートセクタを復号して正しいマジックナンバを確認することができれば，暗号鍵に対応するディスクを使って VM が起動されていることを保証できる．

さらに，UVBond は暗号化ディスクと暗号鍵の組がユーザによって用意されたものであるかどうかとを確認する．これは，信頼できない管理者が用意した暗号化ディスクと暗号鍵の組を使ってユーザの意図しない VM が起動されることを防ぐためである．そのために，ハイパーバイザは登録された暗号鍵を用いて特定の文字列を暗号化し，ユーザに送信する．ユーザが自身の持つ暗号鍵でそれを正しく復号できれば，ハイパーバイザにも同じ暗号鍵が登録されていることになり，ユーザの VM が起動されたことを保証できる．

3.2　VM 識別子を用いたリモート管理

管理 VM 上の信頼できない管理者がユーザ VM に対して不正な操作を行えないようにするために，UVBond では，ユーザが VM を操作する際には VM 識別子を用いる．VM 識別子はハイパーバイザ内で特定の VM に結びつけられており，ハイパーバイザからユーザに暗号化されて送信される．ユーザは VM を操作する際に，図 3 のように VM への操作命令とともに暗号化した VM 識別子およびカウンタ値を管理 VM 経由

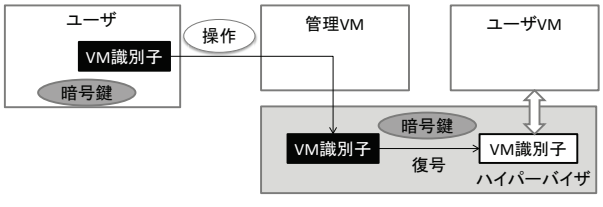

図 3　VM 識別子を用いたリモート管理

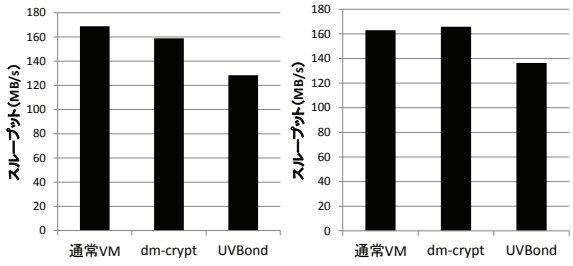

図 4　ディスク読み込み性能　　図 5　ディスク書き込み性能

でハイパーバイザに送信する．ハイパーバイザは VM 識別子が結びつけられている VM に対して指定された操作を実行するため，管理者が別の VM を操作するように変更することはできない．また，カウンタ値を 1 ずつ増加させることにより，暗号化された VM 識別子を保存しておいて後で再利用するリプレイ攻撃を防ぐことができる．

4　実験

まず，UVBond において正しい VM 識別子を指定した場合にだけ VM が操作できることを確かめる実験を行った．実験には Intel Xeon E3-1290 の CPU，8GB のメモリを搭載したマシンを使用した．ハイパーバイザとして Xen 4.4.0 を動作させ，ゲスト OS には Linux 3.13 を用いた．VM には 2 つの CPU と 1GB のメモリを割り当てた．本実験のために，VM 識別子を指定して VM の一時停止と再開を行う操作命令を作成した．実験の結果，ユーザから操作命令とともに暗号化した VM 識別子およびカウンタ値を送信した場合には VM が正常に操作できることを確認した．一方，正しい VM 識別子を指定しなかった場合は VM が操作できないことも確認した．

次に，UVBond を用いてディスクが暗号化されたユーザ VM に対して，bonnie++ を用いて性能測定を行った．比較として，暗号化を行わない通常 VM および，dm-crypt を用いて OS が暗号化を行う VM を用いた．それぞれの VM で 10 回ずつ計測した読み込み性能と書き込み性能の平均値を図 4，図 5 に示す．読み込み性能については，通常 VM と比較して dm-crypt でも 6% 性能が低下しているが，UVBond では 24% 低下することが分かった．これは，UVBond では管理 VM とユーザ VM 間の通信の内容を解析しているためだと考えられる．一方で，書き込み性能については，dm-crypt ではオーバヘッドがないのに対して，UVBond では通常 VM から 16% 性能が低下した．これについても，読み込みの場合と同様の原因が考えられる．

5　まとめ

本研究では，ユーザと VM を強く結びつけることで VM リダイレクト攻撃を防ぐ UVBond を提案した．UVBond では暗号化ディスクを介してユーザと VM を結びつける．信頼できるハイパーバイザがディスクの暗号化・復号化を行うことでユーザの VM が正しく起動されることを保証し，VM 識別子を用いることでユーザの VM への安全なアクセスを実現する．現在の実装では単一 VM にしか対応していないため，複数 VM へ対応することが今後の課題として挙げられる．