

平成 22 年度 卒業論文概要			
所 属	機械情報工学科	指導教員	光来 健一
学生番号	07237019	学生氏名	江川 友寿
論文題目	IaaS 型クラウドにおけるキーボード入力情報漏洩の防止		

1 はじめに

近年、ネットワークを介してサービスを提供するクラウドコンピューティングの利用が広がっている。その一形態として、ユーザに仮想マシン (VM) を提供する IaaS 型クラウドがある。ユーザはハードウェアを用意することなく、必要な時に必要なだけの VM を使用することができる。しかし、クラウドならではのセキュリティリスクとして、ユーザに提供される VM (ユーザ VM) の管理者とクラウドの管理者が異なることが挙げられる。クラウドの管理者は管理 VM を用いてユーザ VM を管理しており、ユーザ VM へのキーボード入力も管理 VM によって処理されている。クラウドの管理者が管理 VM でキーボード入力を盗聴するプログラムを動作させると、ユーザ VM に対するキーボード入力を盗むことができ、パスワード等の機密情報が漏洩する恐れがある。

本研究では、クラウドの管理者が不正アクセスを行ったとしても、ユーザ VM へのキーボード入力情報が漏洩しないシステム FBCrypt を提案する。

2 クラウド管理者への情報漏洩

IaaS 型クラウドでは、ユーザは VNC を用いて VM の操作を行うことが多い。VNC は VM の画面をユーザの PC に表示し、ユーザからのキーボードやマウスの入力を VM に送るためのソフトウェアである。仮想化ソフトウェア Xen [1] において、VNC サーバは管理 VM と呼ばれる特殊な VM 上で動作しており、ユーザの PC の VNC クライアントから接続される。このような構成をとることにより、ユーザ VM のネットワークが正常に動作していなくても管理を行うことができるという利点がある。

その一方で、クラウドの管理者が管理 VM からユーザ VM へのキーボード入力を盗聴できてしまうという問題がある。VNC サーバは図 1 のようにクライアントからのキーボード入力を受け取り、ユーザ VM に渡す。VNC サーバを改ざんすることで、クラウドの管理者はキーボード入力を容易に盗聴することができる。従来は管理 VM の管理者はユーザ VM の管理者と同じであったり、十分に信用することができたが、クラウド環境では信用できるかどうか分からない場合がある。

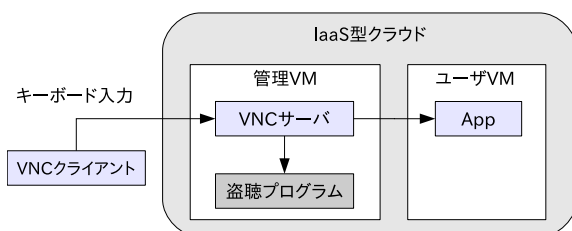


図 1 キーボード入力の盗聴

3 FBCrypt

この問題を解決するために、VNC クライアントとユーザ VM を動作させているサーバの仮想マシンモニタ (VMM) の間でキーボード入力情報を暗号化する FBCrypt を提案する。FBCrypt は、図 2 のようにユーザが VNC クライアントに対して行ったキーボード入力を暗号化して VNC サーバに送信する。VNC サーバがキーボード入力をユーザ VM に渡す際に、VMM が間に入って復号化を行う。VMM はユーザ VM を動作させるために必要となるソフトウェアである。このシステムでは VMM は信用できると仮定する。これにより、管理 VM 内ではキーボード入力は暗号化されているため、盗聴されても情報が漏洩する心配がない。

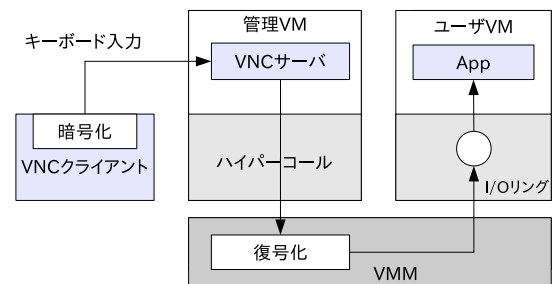


図 2 FBCrypt の構成

3.1 VNC クライアントでの暗号化

FBCrypt はストリーム暗号を用いてキーボード入力を一文字単位で暗号化して VNC サーバに送る。ストリーム暗号は 1 バイト単位での暗号化が可能であり、平文のデータサイズと暗号化済みのデータサイズが常に一致する。また、キーボード入力のようなリアルタイム処理において、ストリーム暗号はブロック暗号と比較して処理が高速である。現在の実装では、オープンソースとして公開されている OpenSSL [3] ライブラリの RC4 というストリーム暗号方式のアルゴリズムを使用している。この暗号化処理をオープンソースの VNC クライアントソフトである TigerVNC [2] に組み込んだ。

3.2 VMM 内での復号化

管理 VM 内で動作する VNC サーバは、VNC クライアントから受け取った暗号化されたキーボード入力情報をハイパーコールを用いて VMM に渡す。従来は VNC サーバがユーザ VM との間で共有している I/O リングにキーボード入力情報を直接書き込んでいたため、VMM はキーボード入力の内容を知ることができなかった。I/O リングとはキーボード入力を VM 間でやりとりするための専用の共有メモリのことである。VMM に新たなハイパーコールを追加し、そのハイパーコールを呼び出すように VNC サーバを修正した。暗号化されたキーボード入力情報を受け取った VMM は、それを復号化し

I/O リングに書き込む。ユーザ VM は従来通りに I/O リングから復号化されたキーボード入力情報を読み出すことができるため、修正を加える必要はない。

3.2.1 I/O リングの特定

復号化したキーボード入力情報を I/O リングに書き込めるようにするために、VMM は I/O リングが置かれているメモリのアドレスを特定する。I/O リングのメモリアドレスはユーザ VM と VNC サーバの間で共有するために、ユーザ VM が管理 VM に通知している。VMM は XenBus と呼ばれる VM 間の通信路を監視することで、I/O リングのメモリアドレスを取得する。この手法は管理 VM に依存しないため、I/O リングのアドレスの詐称を防ぐことができる。また、ユーザ VM の修正は不要である。

3.2.2 I/O リングへのアクセス禁止

FBCrypt では復号化後のキーボード入力情報を I/O リングに書き込むため、復号化された情報を管理 VM から見られないように、I/O リングへのアクセスを禁止する。管理 VM が I/O リング内の情報を読み書きするためには、I/O リングが置かれているメモリページをマップする必要がある。VM がこのようなメモリマップを行うにはページテーブルを変更しなければならないが、ページテーブルの変更は VMM しか行うことができない。この仕組みを利用して、管理 VM から I/O リングのメモリページのマップが要求された時には、その要求を拒否する。

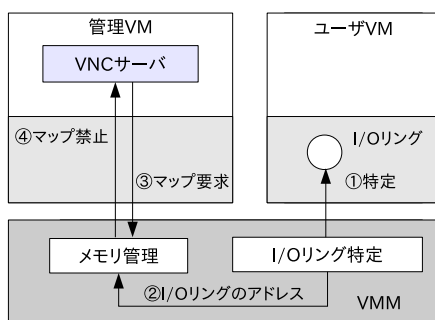


図3 I/O リング特定からアクセス禁止処理

3.2.3 キー情報の変換

FBCrypt では、VMM がキーボード入力情報を復号化した後でキー情報の変換を行う。VNC クライアントは一般的に用いられている 0 から 127 までの ASCII 文字コードをキーボード入力情報として VNC サーバに送信している。一方、ユーザ VM はキーボードの個々のキーに対応するキーコードを入力として受け取る設計になっている。従来は VNC サーバが ASCII 文字コードをキーコードに変換した後、ユーザ VM の I/O リングに書き込んでいた。しかし、FBCrypt では VNC クライアントが送る情報はストリーム暗号により 0 から 255 までの数値に暗号化されるため、VNC サーバではこの変換を正しく行うことができない。そこで VNC サーバ内でキーコード変換を行わず、暗号化されたキーボード入力情報をそのまま VMM に渡すように修正し、VMM 内でキーコード変換を行う。

4 実験

キーボード入力一回あたりに要する処理時間を従来システムと FBCrypt で比較した。VNC クライアント側ではキーボード入力の送信処理にかかる時間を測定し、VNC サーバ側では受信処理にかかる時間を測定した。実験には Intel Core 2 Quad Q9550 2.83GHz の CPU、3.5GB のメモリを搭載したマシンを使用した。VMM として Xen 4.0.2 を動作させ、管理 VM とユーザ VM に対応するドメイン 0 とドメイン U では Linux 2.6.32.21 を動かした。ドメイン 0 には 3GB、ドメイン U には 512MB を割り当てた。結果を表 1 に示す。測定値はキーボード入力を 100 回行った際の平均値である。

VNC クライアント側では、処理時間の差が $15.5\mu\text{s}$ であることから、ストリーム暗号は十分に高速であることがわかる。一方、VNC サーバ側では、処理時間が 10 倍となっている。これは従来システムでは VNC サーバから I/O リングへ直接キーボード入力情報を書き込んでいた処理を、ハイパーコール経由で行うようにし、さらに復号化を行っているためである。その内訳を調べたところ、ハイパーコールの処理時間は $28.9\mu\text{s}$ であり、復号化に要する時間は $4.2\mu\text{s}$ であった。このことより、ハイパーコールの処理自体が大きなボトルネックになっていることがわかる。しかし、処理時間全体としては、FBCrypt は従来システムと比較して $46.4\mu\text{s}$ しか増加しておらず、ユーザは FBCrypt による遅延を体感することなくキーボード入力を行えることがわかる。

表1 キーボード入力の処理時間 (μs)

	VNC クライアント	VNC サーバ	合計
従来システム	39	3.8	42.8
FBCrypt	54.5	34.7	89.2

5 まとめ

本研究では IaaS 型クラウドにおいて、ユーザのキーボード入力情報がクラウド管理者に漏洩するのを防ぐシステム FBCrypt を提案した。FBCrypt では、ユーザ PC の VNC クライアントでキーボード入力情報を暗号化し、サーバの VMM 内で復号化する。これにより、管理 VM へのキーボード入力情報の漏洩を防ぎつつ、ユーザ VM にキーボード入力情報を渡すことが可能になった。現在の実装では、複数のユーザ VM 起動時への対応、大文字など、二種類のキーを併用して入力する文字に関する対応が不完全であるので、これらの問題に対処していくことが今後の課題である。

参考文献

- [1] Barham et al, Xen and the Art of Virtualization, In Proc. of the 19th Symposium on Operating Systems Principles, pages 164–177, 2003.
- [2] RedHat, Inc., TigerVNC, <http://tigervnc.sourceforge.net>
- [3] OpenSSL Project, OpenSSL, <http://www.openssl.org>