平成 24 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	09237020	学生氏名	梶原 達也
論文題目	仮想シリアルコンソールを用いたクラウドの安全なリモート管理		

1　はじめに

近年，ネットワークを経由してユーザに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まっている．その一つの形態として，ユーザに仮想マシン（VM）を提供する IaaS 型クラウドがある． IaaS 型クラウドを使うことで，ユーザはハードウェアを用意することなく，クラウド上の VM を利用することができる．提供された VM（ユーザ VM）を管理するために，ユーザに対して仮想シリアルコンソールが提供されている．ユーザは SSH などを利用して管理 VM と呼ばれる VM にログインし，仮想シリアルコンソールに接続することでユーザ VM にアクセスできる．

しかし，クラウドにおいては，管理 VM を経由して仮想シリアルコンソールを利用すると情報漏洩の危険性が高まる．これは，ユーザ VM のキーボード入力を処理する管理 VM が必ずしも信頼できるとは限らないためである．例えば，管理 VM のセキュリティ対策が不十分であった場合には，外部から攻撃者に侵入される可能性がある．また，悪意を持ったクラウド管理者が攻撃を行う可能性も考えられる．このような場合には，管理 VM 内でキーボード入力を盗聴するプログラムを動作させるだけで，パスワード等の機密情報を簡単に盗まれてしまう．

本研究では，クラウドにおいて仮想シリアルコンソールを用いる際に，管理 VM へのキーボード入力の漏洩を防ぐ SCCrypt を提案する．

2　管理 VM への情報漏洩

仮想シリアルコンソールは， VM の仮想的なシリアルポートを用いて VM 内のシステムにアクセスするための機能である．仮想シリアルコンソール経由で VM へアクセスを行う場合，一旦，管理 VM にアクセスする必要がある．例えば，ユーザは SSH のようなリモート接続ソフトウェアを用いて管理 VM にログインし，管理 VM から仮想シリアルコンソールに接続する． SSH などで直接，ユーザ VM にログインする方法に比べて，VM のネットワークの設定ミス時や OS の起動時のように，ネットワークが使えない時でもアクセスが可能というメリットがある．

しかし，ユーザからの仮想シリアルコンソールへの入力が管理 VM を経由することになるため，クラウドにおいては管理 VM からの情報漏洩の危険性が高まる．従来の計算機環境では，管理 VM の管理者とユーザ VM の管理者が同一，もしくは，同一組織に所属していたが，クラウド環境ではこれらの管理者が異なるために十分に信用できるとは限らない．そのため，管理 VM のセキュリティ対策が不十分で攻撃者の侵入を許してしまうかもしれない．また，クラウド管理者自身が攻撃を行う可能性も考えられる．

SSH を利用して管理 VM にログインする場合，SSH サーバがクライアントからの入力情報を処理するため，図 1 のように SSH サーバを改ざんすることで容易にキーボード入力を盗聴できてしまう．SSH は通信の暗号化により，ネットワーク上での盗聴を防ぐことができる．また，公開鍵認証を用いることで通信相手のなりすましを防止することもできる．しかし，SSH により情報漏洩が防げるのは SSH クライアントとサーバ間の通信であり，SSH サーバからユーザ VM までの間は守られない．

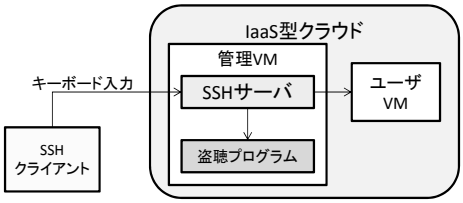

図 1　キーボード入力情報の盗聴

3　SCCrypt

本研究では，SSH クライアントと仮想マシンモニタ（VMM）の間でキーボード入力情報を暗号化する SCCrypt を提案する．VMM は VM を動作させるための基盤となるソフトウェアである．SCCrypt は，図 2 のように SSH 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 SSH サーバに送信する．SSH サーバがキーボード入力情報を仮想シリアルデバイスに渡すと，仮想シリアルデバイスの代わりに，VMM がユーザ VM 内の仮想シリアルドライバのキューに書き込む．その際に，VMM は入力情報の復号化を行う．仮想シリアルドライバに対するインタフェースは従来通りであるため，ユーザ VM 側への修正は不要である． VMM で復号化することにより，管理 VM 内では入力情報が暗号化されたままとなり，盗聴されても情報が漏洩することはない．

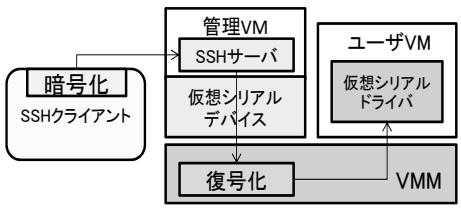

図 2　SCCrypt のシステム構成

クラウド内の VMM の完全性は，リモートアテステーションと呼ばれる技術を用いて保証する．リモートアテステー

ションでは， TPM と呼ばれるハードウェアを用いて VMM のハッシュ値を計算し，クラウド外の検証サーバで改ざんされていないことを検証する．

3.1 SSH クライアントでの暗号化

SCCrypt はキーボード入力を一文字単位で暗号化して SSH サーバに送信する．暗号化には暗号鍵との XOR 演算を行う XOR 暗号を用いた．現在の実装では，暗号化された入力情報に一定のパターンが存在するため，RC4 や AES-CTR などのストリーム暗号を用いることを検討している．

3.2 VMM 内での復号化

管理 VM 内の仮想シリアルデバイスは図 3 のように VMM を呼び出して入力情報を復号化する．VMM を呼び出すために新たなハイパーコールを追加した． VMM 内では SSH クライアントと同じ暗号鍵を用いて，暗号化されている入力情報を復号化する．その後で， VMM はユーザ VM 内のコンソールリングに復号化した入力情報を書き込む．コンソールリングは，仮想シリアルデバイスがユーザ VM にキーボード入力を受け渡すためのキューである．ユーザ VM 内の仮想シリアルデバイスは従来通りに，コンソールリングに書き込まれた入力情報を読み出すことができる．

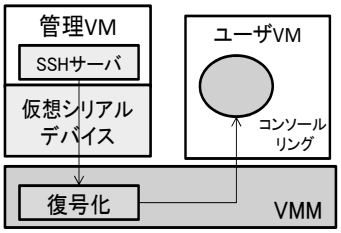

図 3　キーボード入力情報の復号化処理

VMM はユーザ VM 内のコンソールリングを VM の起動時に特定する．コンソールリングは管理 VM とユーザ VM 間で共有されるだけであり，従来の VMM は認識していなかった．そこで，SCCrypt では，VMM が VM の起動時に CPU レジスタに格納される情報からコンソールリングを見つけ出す．

3.3 仮想シリアルコンソールへの接続

SSH クライアントからユーザ VM にアクセスするには，SSH で管理 VM にログインし，ユーザ VM の仮想シリアルコンソールに接続するコマンドを実行する必要がある．しかし， SCCrypt では管理 VM に送られる入力情報はすべて暗号化されるため，入力したコマンドは暗号化されたまま実行され，意図したコマンドを実行することができない．また，この際に管理者権限が必要になるが，クラウドにおいて管理 VM の管理者権限をユーザに与えるのは非現実的である．

そこで，管理 VM にログインしてコマンドを実行するのではなく，図 4 のように，コマンドを指定して SSH クライアントを実行する．この方法を用いると，コマンドの文字列を通常のキーボード入力とは別に扱うことができるため，コマンドだけを暗号化せずに SSH サーバに送る．また，sudo コマンドを用いることで，ユーザには仮想シリアルコンソールに接続するコマンドを実行する時にだけ管理者権限を与える．

```
ssh -t tatsuya@192.168.0.67 sudo
/usr/lib64/xen/bin/xenconsole 1
```

図 4　コマンドを指定した SSH 接続

4 実験

SCCrypt がキーボード入力を正しく暗号化できているかどうかを確かめる実験を行った．サーバマシンには，Intel Core i7 870 2.93GHz の CPU，4GB のメモリを搭載したマシンを用いた．VMM として SCCrypt を実装した Xen 4.1.3，管理 VM とユーザ VM の OS には Linux 3.2.0.36 を，SSH サーバには既存の OpenSSH 5.9p1 を用いた．クライアントマシンには， Intel Xeon E3-1270 3.40GHz の CPU，8.00GB のメモリを搭載したマシンを用いた．OS に Linux 3.2.0.37 を用い，SSH クライアントとして SCCrypt を実装した OpenSSH 6.0p1 を用いた．

この実験では，SSH クライアントを用いてユーザ VM の仮想シリアルコンソールに接続し，キーボード入力を行った．その上で，管理 VM の仮想シリアルデバイスが実装されている QEMU に盗聴プログラムを組み込み，受け取った入力情報をファイルに保存するようにした．「あいうえお」と入力した時の盗聴結果は図 5 のようになり，入力情報が暗号化されていることがわかる．

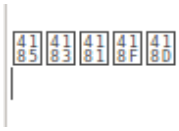

図 5　盗聴された入力情報

5 まとめ

本研究では，仮想シリアルコンソールを用いて IaaS 型クラウド内の VM をリモート管理する際に，キーボード入力情報の漏洩を防ぐシステム SCCrypt を提案した．SCCrypt は，SSH クライアントでキーボード入力情報を暗号化し，クラウド内の VMM で復号化する．その結果，管理 VM でキーボード入力情報が盗聴されたとしても機密情報が漏洩することはなく，ユーザ VM に安全にキーボード入力情報を送ることができる．

今後の課題は、ストリーム暗号のようなより安全性の高い暗号方式を使うことである．また，ユーザ VM からの仮想シリアルコンソールへの出力も暗号化できるようにする必要がある．

参考文献

[1] T. Egawa, N. Nishimura, and K. Kourai, Dependable and Secure Remote Management in IaaS Clouds, Proc. CloudCom 2012, 2012.