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	09237033	学生氏名	重田 一樹
論文題目	クラウドにおける仮想マシンの安全な監視機構		

1　はじめに

近年、急速に普及している IaaS 型クラウドはネットワークを介してユーザに仮想マシン（VM) を提供し、ユーザは必要な時に必要なだけ VM を利用することができる。一方で、IaaS 型クラウドはインターネットに接続されているため、攻撃者によって攻撃を受ける可能性がある。そのため、侵入検知システム（IDS) を用いて VM を監視することが重要である。この IDS を安全に実行できるようにするために、VM を用いた IDS のオフロード手法が提案されている。この手法は監視対象のシステムを VM 上で動作させ、IDS だけを別の VM で動作させる。これにより、IDS が攻撃を検知する前に攻撃者によって無力化される事態を防ぐことができる。しかし、IaaS 型クラウド内の VM に IDS オフロードを行うと、IDS が正しく動作していることを保証できないという問題が生じる。クラウド内で IDS オフロードを行ってもそのクラウド自体が信用できるとは限らないためである。

本研究では、監視対象の VM が動作しているクラウドの外に IDS をオフロードし、ネットワーク経由で VM を監視できるシステム RemoteTrans を提案する。

2　IaaS 型クラウドにおける IDS オフロード

VM を用いた IDS のオフロードは、図 1 のように、監視対象のシステムをサーバ VM と呼ばれる VM を用いて動作させ、IDS だけを IDS-VM と呼ばれる別の VM で動作させる手法である。監視対象であるサーバ VM に攻撃者が侵入してもサーバ VM 上には IDS が存在しないため、IDS を攻撃されることはない。一方、IDS-VM 上では IDS 以外のシステムをできるだけ動作させないようにすることで、攻撃を受けにくくすることができる。オフロードされた IDS はサーバ VM のメモリを解析して情報を取得することで、サーバ VM のプロセス等の監視を行い、攻撃を検知することができる。

IaaS 型クラウドによって提供される VM を利用する場合には VM の監視はより重要になる。しかし、IaaS 型クラウド上の VM を用いて IDS オフロードを行うとセキュリティ上の問題が生じる。IaaS 型クラウドにおいては、クラウドを利用しているユーザ、または、そのユーザが所属する組織がクラウド自体を管理しているわけではない。そのため、利用しているクラウドが常に信用できるものとは限らない。ユーザにはクラウド内の IDS が正しくサーバ VM を監視しているかどうかを確認する手段もない。また、悪意のあるクラウドの管理者によってサーバ VM と IDS-VM が同時に攻撃される可能性もある。このことから、従来の IDS オフロード手法を IaaS 型クラウドに適用するのは難しい。

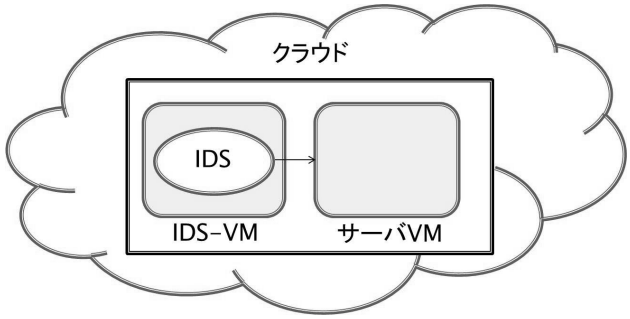

図 1　IDS オフロード

3　RemoteTrans

本研究では、監視対象の VM が動作しているクラウドとは別のホストに IDS をオフロードし、ネットワーク経由でサーバ VM を監視できるようにするシステム RemoteTrans を提案する。RemoteTrans は IDS に対して透過的にリモートのクラウド内の VM を監視する機構を提供する。RemoteTrans は図 2 のように、監視ホスト側にある RemoteTrans ランタイムとクラウド側にある RemoteTrans サーバによって構成される。RemoteTrans サーバは RemoteTrans VM と呼ばれる IDS-VM と同等の機能を持った VM 上で動作させる。このように、IDS をユーザが管理している監視ホスト上で動作させられるようにすることで、IDS の正常な実行を保証することができる。

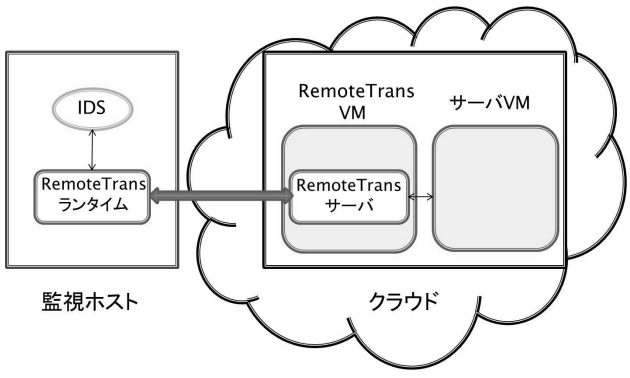

図 2　RemoteTrans のシステム構成

3.1　カーネルデータの監視

RemoteTrans は IDS が必要とするデータをサーバ VM のカーネルメモリから見つけ出し、得られたデータを IDS に提供する。IDS がはまず、カーネルデータのアドレスとサイズを RemoteTrans ランタイム経由で RemoteTrans サーバに送る。RemoteTrans サーバは、アドレスからだけでは取得するデータのサイズがわからないため、データサイズも一緒に送る必要

がある。次に、RemoteTrans サーバは送られてきたアドレスからデータが含まれているサーバ VM のメモリ領域を見つけ出す。RemoteTrans VM とサーバ VM は異なる VM であり、隔離されているため、このメモリ領域を RemoteTrans VM 上にマップしてアクセスできるようにする。マップしたメモリ領域からアドレスに対応するデータを見つけ出し、データサイズの分だけを RemoteTrans ランタイムに返す。RemoteTrans ランタイムは得られたデータを IDS に返すことで、IDS はカーネルデータの監視が可能になる。

3.2 データの整合性チェック

IDS 自体をクラウドの外で実行できるようにしたとしても、クラウドが信用できるとは限らないため、RemoteTrans サーバが返すデータはクラウド内で改ざんされる恐れがある。例えば、RemoteTrans サーバが改ざんされた場合、サーバ VM のメモリ上のデータではなく、別のデータを返すことができる。その結果、サーバ VM の侵入の痕跡を隠すことも可能になる。

クラウド内での改ざんを検出するために、RemoteTrans は送信されたデータが正しいかどうかをチェックする。そのために、クラウドでは仮想マシンモニタ（VMM) の中でデータのハッシュ値を計算する。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り、3.3 節で述べる機構を用いることにより、クラウド内の VMM を信頼できるようにする。信頼できる VMM 以外は正しいハッシュ値を計算できないようにするために、VMM が保持している秘密鍵をハッシュ値の計算に含める。

データの整合性チェックを含めた監視の流れは図 3 のようになる。監視ホストの RemoteTrans ランタイムからデータのアドレスとサイズを受け取った RemoteTrans サーバは、ハイパーコールを用いて VMM を呼び出す。VMM は指定されたアドレスが含まれる VM のメモリ領域をマップし、対象データのハッシュ値を計算して RemoteTrans サーバに返す。RemoteTrans ランタイムはデータのハッシュ値を RemoteTrans サーバから受け取ると、VMM と共有している秘密鍵を用いて受信したデータのハッシュ値を計算する。その値が受信したハッシュ値と一致していればデータは改ざんされていないことがわかる。

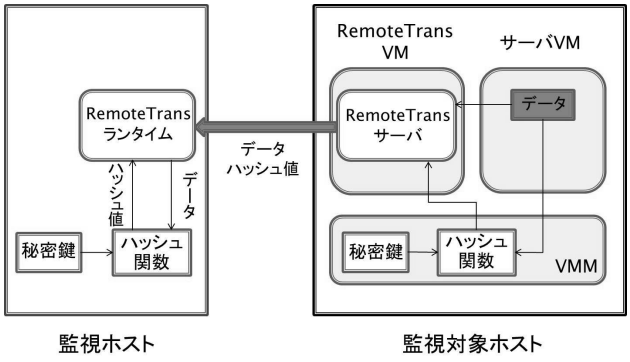

図 3　安全なカーネルデータ監視の流れ

3.3 VMM の完全性チェック

正しい VMM が動作していることを確認するために、リモートアテステーションと呼ばれる技術を用いる。サーバの起動時に VMM のハッシュ値を計算し、クラウドの外の検証サーバに送ってその値を検証することで、VMM が改ざんされていないことを確認する。計算したハッシュ値は TPM と呼ばれるセキュリティチップに格納されるため、ハッシュ値の改ざんはできない。

4 実験

VM 内のプロセス情報を取得する IDS（ps-vm) を RemoteTrans 上で実行し、その実行時間を測定した。比較のために、ps-vm を従来システムの IDS-VM 上で実行したときの実行時間も測定した。監視対象ホストには、Intel Core i7 の CPU、16GB のメモリを搭載したマシンを使用し、VMM として Xen 4.1.3 を動作させた。RemoteTrans VM の OS は Linux 3.2.0、サーバ VM の OS は Linux 2.6.27.35 を用いた。監視ホストには、Intel Core i7 の CPU、8GB のメモリを搭載したマシンを使用し、OS は Linux 3.2.0 を用いた。これらのホストはギガビットイーサネット・スイッチで接続した。

実験結果を表 1 に示す。実行時間は 87 個のプロセス番号とプロセス名を取得するのにかかった時間を 10 回計測した際の平均値である。RemoteTrans を用いてプロセス情報を取得すると、従来システムよりも 20 秒以上時間がかかった。これは、一つのプロセス情報を取得するたびに、データのアドレスとサイズを送っているため、監視ホストと監視対象ホストの通信回数が多くなっていることが原因と考えられる。また、現在の実装ではプロセス番号とプロセス名も別々に取得しているので、２つのデータをまとめて取得するようにすれば、データ取得時間を短縮できると考えられる。

表 1　プロセス情報取得時間（秒）

	実行時間
従来システム	0.04
RemoteTrans	20.88

5 まとめ

本研究では、監視対象の VM が動作しているクラウドの外に IDS をオフロードし、ネットワーク経由で VM を監視できるようにするシステム RemoteTrans を提案した。RemoteTrans は IDS が必要とするデータの情報を RemoteTrans サーバに送り、その情報を基に必要なデータを RemoteTrans ランタイムに返す。データの整合性は VMM 内でハッシュ値を計算することによって保証する。改ざんされていないデータを用いてクラウドの外で監視を行うことにより、安全に監視を行うことができる。今後の課題は、情報を取得するときの通信のオーバヘッドを減らし、RemoteTrans と Transcall[1] を併用して VM を監視できるようにすることである。

参考文献

[1] 飯田貴大、光来健一. VM Shadow: 既存 IDS をオフロードするための実行環境. 第 119 回 OS 研究会、2011.