様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１０日現在

機関番号：１５１０１
研究種目：若手研究（Ｂ）
研究期間：2009 ～ 2010
課題番号：２１７００００９１
研究課題名（和文）　マシン間協力による不正侵入被害拡散防止モデルの実現

研究課題名（英文）　Research on the cooperative model for the prevention of the propagation of Compromised Machines
研究代表者
高橋　健一（Kenichi Takahashi）
鳥取大学大学院・工学研究科・准教授
研究者番号：３０３９９６７０

研究成果の概要（和文）：不正侵入への対策として IDS や IPS などの技術が研究開発されているが、攻撃者に対して防御者が後手に回っているのが現状である。このため、侵入を完全に防ぐことは難しいという前提の下で新たな対策手法を考える必要がある。そこで、不正侵入したマシンを踏み台として攻撃に利用し難くすることで不正侵入被害の拡散を防止するための仕組みを提案した。本提案システムをシミュレーションにより実験した結果、踏み台マシンの削減効果を確かめることができた。

研究成果の概要（英文）：It is still difficult to detect and/or prevent intrusions. Thus, we should assume that our machines can be compromised anytime for a next generation security framework. In this research, we proposed a new intrusion detection methodology based on the notifications from other machines. Our simulation results show our proposed system is effective to reduce compromised machines. Moreover, the proposed model will suppress the propagation of compromised machines.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,700,000	510,000	2,210,000
２０１０年度	1,500,000	450,000	1,950,000
総　計	3,200,000	960,000	4,160,000

研究分野：ネットワークセキュリティ
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：侵入検知，ネットワークセキュリティ，コミュニケーション

１．研究開始当初の背景

インターネットの広がりと共に不正侵入による被害が深刻になってきている。IPA/ISEC の「コンピュータ不正アクセスの届出状況」によればサーバへの不正アクセスによる被害が毎月報告（2008 年 9 月: 32 件、8 月: 23 件）されている。侵入による被害はサーバの破壊や保管されている情報の盗難だけでなく、踏み台として他のマシンの攻撃に利用され、その企業・団体の信用を失うと共に加害者としての損害賠償を求められる可能性もある。そのため不正侵入に対する十分なセキュリティ対策を施す必要がある。

このような不正侵入への対策として IDS や IPS などの技術が研究開発されているが、基本的にこれらの技術では既知の攻撃にしか対応することができず、攻撃者に対して防御者が後手に回っているのが現状である。例えば、代表的な不正侵入検知手法としてシグネチャやパターンマッチングを基礎とする手法があるが、ポリモーフィックワームやスピア攻撃などに対する効果はほとんど期待できない。また、ゼロデイ攻撃やプログラムコードの肥大化などの要因も重なると不正侵入を完全に防ぐことは難しいと考えるべきである。そこで、侵入を完全に防ぐことは

難しいという前提の下で新たな対策手法を考える必要がある。

２．研究の目的

攻撃者が不正侵入したマシンを踏み台として利用し難くすることで、不正侵入被害の拡散を防止するための仕組みを実現する。本提案ではそれぞれのマシンは通信ポリシを持つ。通信ポリシはそれぞれのマシンの管理者によって正常な通信がルールとして定義される。このとき、あるマシンＡが他のマシンＢに通信を試みた場合、マシンＢによってマシンＡの通信ポリシが確認される。通信ポリシに定義されていない通信であった場合、その通信がマシン Ｂ によって拒否されると共にマシンＡの管理者に通知される。これによってマシンＡからマシンＢへの攻撃の拡散を防ぐことができ、またマシンＡの管理者が予期していない通信が発生したことを知ることができる。攻撃者は不用意に踏み台マシンから他のマシンを攻撃するとその攻撃活動が検出され踏み台マシンも失うことになり、結果として侵入者の行動を抑制し不正侵入被害の拡散を防止する効果が期待できる。

そこで本研究では提案システムの実現に向けて、通信ポリシの定義方法や不正通信検出時の管理者への通知方法、通信ポリシの改竄検出・防止手法を具体化すると共に、シミュレーションによる侵入被害の拡散防止効果を明らかにする。

３．研究の方法

本研究では攻撃者が不正侵入したマシンを踏み台として利用し難くすることで、不正侵入被害の拡散を防止するための仕組みを実現する。本仕組みを実現するためには以下の課題に取り組む必要がある。

（１）通信ポリシの定義：本提案ではマシンの管理者が設定した通信ポリシを利用する。実用性を考えるとマシンの管理者が簡易で効果的なポリシの設定方法について検討する必要がある。

（２）不正通信検出時の管理者への通知方法：本提案ではマシンＡからマシンＢへの通信が発生したときに、それが通信ポリシに合致しない場合、そのことがマシンＢからマシンＡの管理者に向けて通知される。しかし、本提案ではマシンＡが侵入されていることを前提としているためにマシンＡを経由しての通知は侵入者によって破棄されてしまうことが考えられる。すなわち、マシンＡを経由しない通知方法をマシンＢに対して知らせる必要がある。

（３）通信ポリシの改竄検出・防止手法：本提案ではマシンＡがすでに侵入されていることを前提としているために、通信ポリシ自体が侵入者によって改竄されてしまうことが考えられる。このため、通信ポリシの完全性、正当性を保証するための仕組みを検討する必要がある。

（４）シミュレーション実験による効果の確認：複数台マシンにより本提案システムの効果をシミュレーションすることで有効性を検証する必要がある。具体的には本仕組みを備えたマシンが全マシン中のどれ位あれば、どれ位の割合で、どれくらいの時間で不正侵入が検出可能かを検証する。

４．研究成果

ネットワーク上の他のマシンが不正通信を検知し、それを通知することで不正侵入検知の契機とするための仕組みを提案する。通知を受け取った管理者は自分が管理するマシンの調査を開始し、マシンの復旧および新たなセキュリティ対策を施すことができる。図１にシステムの概要を示す。

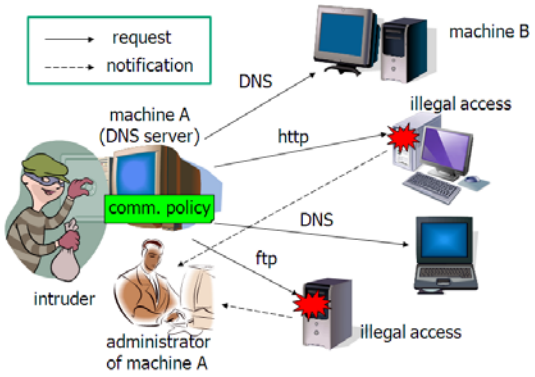

図１．提案システムの概要

本提案システムにおいて各マシンはそれぞれの通信ポリシを持つ。通信ポリシはデフォルトとしてすべての通信を拒否するものとし、そのマシンから他のマシンに対して発生する可能性がある通信をルールとして記述する。あるマシンＡから他のマシンＢへの通信が発生した場合、まずマシンＢはマシンＡの通信ポリシを確認する。その通信が通信ポリシに定義されている通信であった場合、マシンＢはその通信をマシンＡからの正常な通信として受け入れる。しかし、定義されていなかった場合、マシンＡの管理者が期待しない通信がマシンＡから発生しているものとして、その通信を拒否すると共にマシンＡの管理者に通知する。これによって、その通信が侵入者による攻撃活動だったとしても、マシンＡからマシンＢへの攻撃の拡散を防ぐことができる。また、マシンＡの管理者は自分が期待していない通信がマシンＡから発生していることを知り、その対策を施すことができる。すなわち、攻撃者は不用意に踏み台マシンから他のマシンを攻撃すると、その攻撃活動が他のマシンによって検出され踏み台

マシンを失う可能性がある。このため、攻撃者は踏み台マシンを使って無差別に他のマシンを攻撃することができなくなり、結果として侵入者の行動を抑制し不正侵入被害の拡散を防止する効果が期待できる。

例えば、管理者が DNS サーバを立ち上げたとする。DNS サーバは他の DNS サーバと DNS 通信（53/TCP、UDP）を行うことでドメイン名を IP アドレスに変換する。このため、管理者は DNS 通信を正常な通信として通信ポリシに記載する。このとき、その DNS サーバが侵入により踏み台マシンとして利用され、侵入者が HTTP での通信を試みたとする。しかし、HTTP は DNS サーバの通信ポリシで許可されていないため、通信先のマシンから DNS サーバ管理者に向けての通知が発生する。その通知によって、DNS サーバ管理者は HTTP での通信が発生したことを知ることができ、不正侵入の可能性を調査する契機にすることができる。

（１）通信ポリシ

本提案システムでは通信を受けたマシンが通信ポリシによって正常な通信であるかを判定する。正常な通信でなかった場合、そのマシンはそのことを通信元マシンの管理者に通知する。このため、通信ポリシには正常な通信を定義するための許可ルールと通知方法を示すための通知ルールが必要になる。図２に通信ポリシを示す。

```
<communication>
  <rule prot = protocol name or port
        [dest = IP addresses] />
</communication>
<notification>
  put the tag for a notification way
</notification>
```

図２．通信ポリシ

許可ルールではそのマシンから他のマシンに対して発生する可能性がある通信を記述する。現時点ではプロトコルと通信相手から構成される単純なものを許可ルールとして採用している。図２中、communication タグで囲まれた部分が許可ルールであり、prot にはプロトコル名またはポート番号を記述し、dest には通信先アドレスを記述する。dest はオプションであり、明記されていない場合、すべてのアドレスへの prot での発信を許可することを表す。

通知ルールでは不正な通信が発生したことを通信元マシンの管理者に通知するための方法を記述する。notification タグで囲まれた部分が通知ルールであり、通知方法をタグで指定する。ここで、その通信ポリシを持つマシン経由の通知方法を指定すると、その通知自体が侵入者によって破棄される危険性がある。このため、その通信ポリシを持つマシンを経由しない通知方法を指定することが望ましい。

（２）通信ポリシの改竄対策

本提案システムでは通信ポリシを持つマシンが侵入されていることを前提としている。このため、通信ポリシ自体が侵入者によって改竄される可能性がある。このため、通信ポリシの改竄を検知できるための仕組みが必要となる。しかし、侵入者がウイルス対策ソフトなどを無効化できる可能性を考えると、通信ポリシを持つマシンだけで改竄防止対策を講じることは難しい。そこで、通信ポリシを持つマシンとは別に安全に管理された管理用のマシンが存在することを仮定する。管理用マシンを安全に管理するためには可能な限り攻撃される危険性を排除する必要がある。そこで、管理用マシンの安全性を確保するために、管理用マシンは他のマシンに向けてデータを送信することはできるが、他のマシンからの要求を一切受け付けないといった仮定を置く。

管理用マシンの存在を仮定すると、管理用マシンが定期的に通信ポリシを確認し、通信ポリシの改竄を検知する方法が考えられる。しかし、侵入者が管理用マシンからの要求（だけ）に改竄前の通信ポリシを提示する可能性が考えられ、この場合には有効に機能しない。また、管理用マシン経由の通信を行わせることで、他のマシンではなく、管理用マシンで通信ポリシの確認を行い、不正な通信の発生を検出する方法が考えられる。しかし、管理用マシンが他のマシンからの要求を受け付けていることになり、管理用マシンの安全性を保証できなくなる危険性が存在する。また、管理用マシンに通信ポリシ確認の負荷が集中するといった問題も存在する。

通信ポリシの改竄を検知するための方法として、認証局が発行する公開鍵証明書による電子署名を利用する方法がある。しかし、公開鍵証明書を利用するための手続きや認証局の安全性を十分に保証しなければならないといった問題がある。そこで、適当な他のマシン（このマシンを協力マシンと呼ぶ）に通信ポリシの改竄を検知するための情報を持たせ、協力マシンからの情報で通信ポリシの改竄を検知するための仕組みを実現する。図３に通信ポリシの改竄検知のための仕組みを示す。

マシン A の管理者は管理用マシンを利用して、通信ポリシの改竄を検知するための通信ポリシチェック情報（PCI: Policy Check Information）を作成し、協力マシンに向けて送信する。通信ポリシを持つマシン A から、

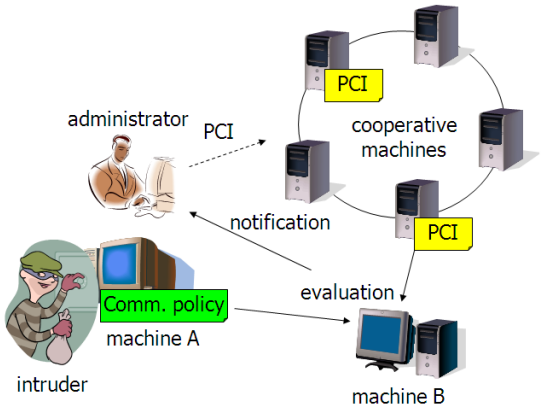

図３．通信ポリシの改竄対策

あるマシン B への通信が発生した場合、マシン B はマシン A から通信ポリシを受け取ると共に協力マシンからマシン A の PCI を受け取る。PCI によって通信ポリシを評価することで通信ポリシの改竄を検知することができる。また、侵入者がマシン A の機能を無効化することで、マシン A がマシン B に対して通信ポリシを渡さない場合も考えられる。このときはマシン A の PCI を協力マシンが管理しているか確認することで、マシン B はマシン A の機能が無効化されている可能性を検知できる。通信ポリシの改竄や機能の無効化が検知された場合、マシン B はそのことをマシン A の管理者に通知する。このことで、マシン A の管理者は通信ポリシが侵入者によって改竄されたことや機能が無効化されたことを知ることができる。

（３）シミュレーション実験による提案モデルの評価と考察

本提案システムの不正侵入に対する効果を確かめるために、本提案システムを備えたマシン PM（Proposed Machine）と備えていないマシン OM（Ordinaly Machine）をエージェントシステムとして実現しシミュレーション実験を行った。本シミュレーションでは AM を 16 台、PM と OM の合計で 2048 台分のエージェントを準備し、その内の 32 台に 1 台(3。125%）が踏み台マシンとなっている状態を初期状態とした。

AM は 6 時間の内のランダムな任意の間隔をあけて、すなわち、1 日に平均 8 回、4 つのプロトコルの中からランダムに選択したプロトコルを使った攻撃指示を侵入済みの OM または PM(踏み台マシン)に対して行う。PM、OM は AM からの指示を受けると、指定されたサービスに対して最新の脆弱性を突いた攻撃を他のマシンに対して一回行う。ただし、AM が侵入したマシンを持たない場合は、踏み台マシンを使わずに AM が直接攻撃を行う。また、PM と OM は p×2 日の内のランダムな間隔をあけて、すなわち、平均 p 日に一度、マシンの検査、および最新の脆弱性パッチを適用する。マシンの検査によってすべてのマシンは侵入されていない状態になり、脆弱性パッチの適用によって、それまでに既知のすべての脆弱性がなくなる。また、v×2 日の内のランダムな間隔をあけて、すなわち、平均 v 日に一度、新たな脆弱性が発生し、新たな脆弱性発生と同時に最新の脆弱性パッチが作成される。

OM が攻撃を受けた場合、攻撃に利用されたプロトコルを使ったサービスを提供しており、更に最新の脆弱性パッチが適用されていなければ侵入された状態となる。PM が攻撃を受けた場合、その通信元マシンの通信ポリシを確認する。その攻撃が通信ポリシに違反したものであれば通信元マシンに通知する。このとき、通知を受けた通信元マシンは検査、および最新の脆弱性パッチの適用により侵入されていない状態に復旧する。一方、通信ポリシに違反したものでなく、かつ OM の場合と同様に、攻撃に利用されたプロトコルを使ったサービスを提供しており、更に最新の脆弱性パッチが適用されていなければ侵入された状態となる。

ここでは、PM が 12.5%の割合で存在すると仮定し、p を 12、v を 6 としたときの本提案システム導入効果を図４に示す。

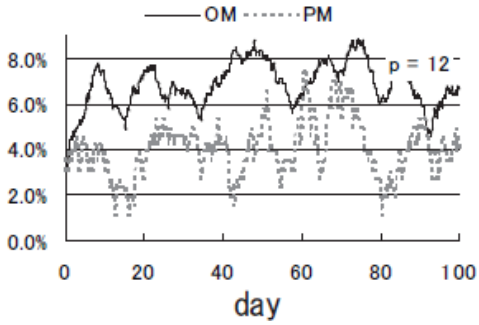

図４．本提案システムの導入効果

脆弱性パッチ適用頻度が多いほど、最新の脆弱性パッチが頻繁に適用され、マシンの検査により侵入状態から復旧するため、侵入されたマシンの割合が少なくなる。また、PM では平均 p 日に一度の脆弱性パッチ適用以外に、他者からの知らせによる侵入状態からの復旧、および脆弱性パッチ適用の機会が発生する。このため、侵入されたマシンの割合は OM に比べて PM の方が少なくなる。12 日目から 100 日目まで（初期の踏み台マシンの数の影響が大きいため 12 日目までを省いた。）の侵入されたマシンの割合は、OM が平均 7.01%に対して PM が平均 4.03%となっており、侵入されている PM の割合は OM の 6 割程度であった。また、侵入されている時間（復旧時間 － 侵入された時間）の平均は OM で 7.12 日、PM で

4.41 日となっており、侵入されている時間も OM に比べて PM の方が短く、OM の 6 割程度の時間で復旧できていることがわかった。
　また、PM の割合や p、v の値を変更したシミュレーション結果についても、同様に提案システムの有効性を確かめることができた。

（4）まとめ
　本研究では外部からの通知により不正侵入被害の拡散を防止するための仕組みを提案した。本提案システムでは各マシンが通信ポリシを持ち、その通信ポリシに違反する通信を受けたマシンがそのことを通知する。通知を受けたマシンの管理者は自分が想定していない通信が発生したことを知り対策を施すことができる。このため、侵入者が踏み台マシンから他のマシンを攻撃すると、それが検知され踏み台マシンを失う可能性があるため、踏み台マシンを使って無差別に攻撃することができなくなり、結果として不正侵入者の行動を抑制する効果が期待できる
　シミュレーションにより評価した結果、提案システムを導入したマシンが多ければ多いほど攻撃者が踏み台マシンを失いやすく、攻撃の幅が狭める効果が見込めることが分かった。また、本提案システムは既存の IDS や IPS といった技術と競合する仕組みではなく、両者を併用することで不正侵入に対してより効果的な対策を立てることができる。

５．主な発表論文等

〔雑誌論文〕（計１件）
（1）高橋健一, 藤井雅和, 櫻井幸一: 他者からの知らせによる不正侵入被害拡散防止モデルの提案と評価, 電子情報通信学会論文誌, Vol.J93-D, No.7, pp. 1114-1124, 2010 年, 査読あり

〔学会発表〕（計２件）
（1）高橋健一, 松崎隆啓, 峯恒憲, 櫻井幸一: ルールレポジトリを用いたユーザがカスタマイズ可能なデータ保護方法の提案, Computer Security Symposium 2010, pp. 149-154, 2010 年 10 月 10 日, 高松
（2）高橋健一, 藤井雅和, 櫻井幸一: 第 3 者通知による侵入検知手法のシミュレーションによる評価, 2010 年暗号と情報セキュリティシンポジウム, 1E1-1(CD-ROM), 2010 年 1 月 19 日, 香川

〔図書〕（計０件）
なし

〔産業財産権〕
○出願状況（計０件）
なし

○取得状況（計０件）
なし

〔その他〕
なし

６．研究組織
(1)研究代表者
高橋　健一（Kenichi Takahashi）
鳥取大学大学院・工学研究科・准教授
　研究者番号：３０３９９６７０

(2)研究分担者
なし

(3)連携研究者
なし