社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（5）
2005－CSEC－28（5）
2005／3／22

ワームの拡散遅延を目的とした検知・遮断機構の提案

大宅裕史[†]　櫨山寛章[†]　門林雄基[†]

近年ワームの感染によりネットワークが不通な状態に陥る例が多数報告され問題になっている。通信不能な状態を回避するためには感染行為の初動で対処することが望ましい。しかしながらワームは爆発的に拡散するので人的対処をする前にネットワークが通信不能になってしまう。提案機構では、ワームが感染行為をする際のランダムアクセスに着目しワームのトラフィックを検知する。検知した後、感染に用いられている TCP/IP セッションを維持し引き延ばすことで他ホストに対するワームの感染を抑える。また、提案機構の近傍に感染したホストを確認した場合、そのホストをネットワークから遮断することでさらなる感染拡大を防ぐ。提案機構ではワームを検知すると共にワームの拡散の遅延をはかる。

A proposal of detection and blocking mechanism for retarding the spread of Internet worm

Yuji Ootaku,[†] Hiroaki Hazeyama[†] and Youki Kadobayashi[†]

In recent years, network congestion caused by worm traffic occurs frequently. Worm occupies wide bandwidth of the network when it tries to infect other hosts. Hence, it is important to respond to the congestion caused by worm in early stage of infection. It is hard to do so, however, because they spread on the whole network very quickly. In order to solve this problem, we propose a mechanism aimed to delay worm's proliferation. The mechanism determines worm traffic by monitoring the connection to the unused IP addresses. When the mechanism finds out the traffic, it deceives itself as targeted hosts and maintain the connections. When any infected host exists on the same subnet, the mechanism shuts down the affected network.

1. はじめに

近年、Blaster[1)]、Sasser[2)] 等のワームによる被害が増えてきている。これらのワームは、広く使われているシステムの脆弱性を利用して自動的に拡散すると言う特徴が挙げられる。これらのワームが拡散するときのトラフィックが輻輳の原因となり通信障害が発生する。ワームの発生を確認後、できるだけ早い段階での人的対処が通信障害を防ぐのに効果的である。しかしながら、ワームの拡散速度は非常に早いので人的対処をする前に通信障害が発生する規模まで拡散してしまうのが現状である。[3)] ワームからネットワークを守る手法として Firewall や Intrusion Detection System/Intrusion Prevention System(IDS/IPS) が挙げられる。これらの対策は外部から侵入してくるワームを防ぐには有効だが、内部でのワーム拡散を防ぐことはできない。そこで本稿ではワームの発生を検知しワームの拡散を遅延させる機構の提案を行う。

2. 関連技術

ワームからネットワークを守る技術として次のようなものが挙げられる。

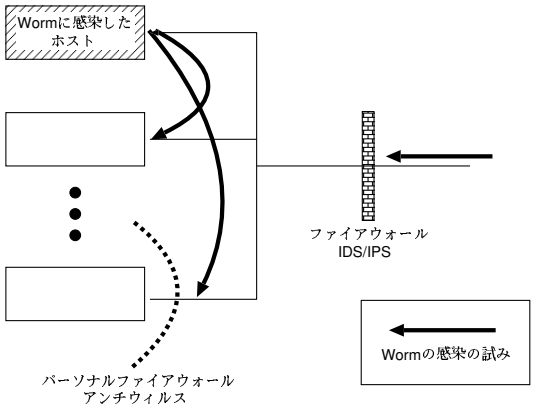

図 1　ワーム対策技術の模式図

† 奈良先端科学技術大学院大学
Graduate School of Information Science NARA Institute of Science and Technology

2.1 ファイアウォール

ファイアウォールは外部からの通信の可否をあらかじめ設定されたルールによって決める。ワームが利用する TCP 及び UDP のポートを閉じることによりワームの侵入を防ぐことができる。しかしながら、サービスの都合上、ワームが使用するポートを外部に公開している場合は、ファイアウォールが通信を許可してしまうので、ワームの侵入を防ぐことができない。また、感染ホストがファイアウォールの内側のネットワークに持ち込まれた場合には内部ホストの感染を防ぐことはできない。例えば、ワームに感染したノート PC がファイアウォール内部のネットワークに接続された場合、ファイアウォールは内側のネットワークに拡散するワームに対しては全くの無力である。つまり、ファイアウォールの外部からの感染を防ぐことは可能だが内部のホスト間の感染に対しては無効である。

2.2 IDS/IPS

IDS/IPS ではファイアウォールではとらえることのできないネットワークに対する攻撃を認識及び防御することができる。IDS/IPS の検知手法は不正検出と異常検出の 2 つに大別できる。現在一般的に普及している検知手法は不正検出である。不正検出ではあらかじめ登録されたシグネチャと呼ばれる通信のパターンと通信を照合することによって不正や異常を検知したり遮断したりする。ワームのシグネチャが存在するとワームの侵入を検知することができるが、未知のワームに対してはシグネチャが存在しないので検出できない。

2.3 パーソナルファイアウォール/アンチウイルスソフト

パーソナルファイアウォールやアンチウィルスソフトはネットワーク上での対策ではなく、個々のホストに導入することで、ワームからホストを守る技術である。これらを導入することにより、ホストにワームが侵入することを未然に防ぐ。しかしながら、現在普及しているアンチウイルスソフトはパターンマッチ方式を利用しているので、更新を怠って新しいパターンを導入していないとワームを検出できない。また、パターンにない未知の新しいワームも検出することはできない。

2.4 現在の関連技術の問題点

前節まで挙げた現在のワーム対策技術にはそれぞれいくつかの問題点がある。問題点を整理すると以下の様になる。

- ファイアウォール
  - ルールの設定によってはファイアウォールをすり抜けてしまう可能性がある
  - ネットワーク内部で拡散するワームに対しては有効ではない
- IDS/IPS
  - パターンマッチによる検知が主流なので、未知のワームに対しては無効である
- パーソナルファイアウォール/アンチウィルスソフト
  - パターンマッチで検知しているので、未知のワームに対しては無効である

現在の関連技術の問題点として挙げられるのは、ファイアウォールのようなネットワークを対象とした保護技術では、内部でワームが拡散するのを抑えることができない。また、全ての技術に共通するところとしてシグネチャやルールを用いたパターンマッチの手法を用いているので、新たに出てきたワームに対してのパターンができあがるまではこれらの技術は有効ではない。最近ではシステムの脆弱性情報が公開されてからその脆弱性をついたワームが出てくるまでの期間が短くなる傾向にある。未知のワームに対して必要な技術とは、ワームの発生を通信の中から発見し、かつ、そのワームをネットワーク内部で拡散することも防ぐことができる技術である。

3. ワームの検知・遮断機構の提案

2.4 節で述べたように、現在のワーム対策技術は内部でワームが拡散するのを抑えることができない。外部からのワームの対策ができていても、感染したホストが内部ネットワークに接続した時に対処できなければ、ネットワークの障害発生は防げない。

ワームの拡散を抑えるためには、現在の検知手法の主流であるパターンマッチを用いない方法でワームの発生を検知する必要がある。

また、検知したワームに対し何らかの方法で遅延をはかる必要がある。そこで提案機構では拡散の遅延をはかるために通信の引き延ばしと感染ホストの遮断を行う。

3.1 検 知 手 法

ワームを検知する手法としてワームが通信を行う際の特徴に着目した。

多くのワームに共通して挙げられる特徴は、不特定多数のアドレスに感染を試みる点である。

多くのワームはどのホストが脆弱性のあるサービスを実行しているかの情報を持たない。そのため感染を試みる際は適当に対象 IP アドレスを定める。どのように感染の対象アドレスを決めるかはワームによって

異なるが、一定の法則性を持って拡散を試みる際の対象をランダムに定める。ワームがランダムにアドレスを選定する際に、その IP アドレスが必ずしもホストが存在するアドレスであるとは限らない。

そのためワームが拡散を試みる際には未使用の IP アドレスに対する通信が増加する。よって提案機構では使用されていない IP アドレスに対する通信をワームの通信とみなし、拡散を遅延させるための行動をとる。

3.2 通信の引き延ばし

ワームが感染を試みる際に TCP を用いているワームが多いことに着目した。3.1 節で検出されたワームの通信が TCP を利用していた場合、TCP のコネクションを維持し続け通信を引き延ばすことで拡散の遅延をはかる。TCP のコネクションが維持され続けると結果として他の IP アドレスに感染を試みることができなくなる。多くのワームはスレッドを用いて同時並行でいくつもの IP アドレスに対して感染を試みるが、スレッドの数は有限なので提案方式は拡散の遅延に効果があると言える。

3.3 ワームに感染したホストを判別し排除

未使用の IP アドレスに対する通信が 1 ホストから連続すると、そのホストは確実にワームに感染したとみなせる。そこで、ワームに感染したとみなしたホストをネットワークから遮断することにより、拡散行動をとれないようにする。これにより、拡散行動をとるホストが減少すると、感染を試みる通信の量も減り、新しい感染ホストの増加量を抑えることができる。結果として拡散の遅延がはかれる。

この手法を用いることで感染行動に TCP を用いないワームの拡散も遅延をはかれる。

4. 実験による検証

3 章で述べた提案機構の有効性を検証するために提案機構を実装し、疑似ワームを用いた実験により評価した。提案機構を導入する前後でワームの拡散速度がどのくらい変化するかを確認した。

4.1 実 験 環 境

実験をした環境は次のとおりである。

- PC・9 台
  - CPU:PentiumIII 1.4GHz
  - Memory:1GB
  - OS:VineLinux 3.1(kernel 2.4.27)
- ネットワーク
  - スイッチ-マシン間:1GHz
  - スイッチ-スイッチ間:1GHz

マシン、スイッチのネットワークトポロジは図 2 のとおりである。

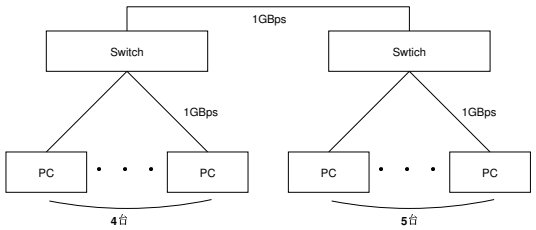

図 2 ネットワークトポロジ

4.2 想 定 環 境

次のような環境を想定して実験を行った。

サブネットマスクが/24 のアドレス空間において、全ての PC が同一サブネットに存在し、L2 ではフラットに配置されている。アドレスの使用率は 25%である。使用されている IP アドレスはランダムに決定した。64 台の存在するホストのうち 8 台が脆弱性を持っているとする。

4.3 疑似ワーム

実装した疑似ワームは本来のワームのようにシステムの脆弱性を利用して拡散するものではない。あらかじめ各ホストに疑似ワームを非活動状態で起動しておく。非活動状態の疑似ワームが感染命令を受けるとホストの探索を開始し、探索先に感染命令を送ることで活動状態のワームを増加させる。以上のような行動をさせることでワームの感染の通信を模倣した。感染対象のホストを探索する手法は過去のワームが用いた方法を模倣した疑似ワームを用いた。探索方法の詳細は以下のとおりである。

4.3.1 局所優先探索

局所優先探索とは、探索するアドレスを完全にランダムに決めるのではなく、一部に感染ホストの IP アドレスを使う探索手法である。そのため、感染ホストに近い IP アドレスを使用しているホストを優先的に感染対象とする。感染ホストの IP アドレスを A.B.C.D とする。X,Y,Z はそれぞれ 0 から 255 の間のランダムな数とする。疑似ワームは以下のような確率で感染対象とする IP アドレスを定める。

(1) $\frac{1}{8}$ の確率で完全にランダムに IP アドレスを定め感染対象とする
(2) $\frac{1}{2}$ の確率で A.X.Y.Z という IP アドレスを定め感染対象とする。
(3) $\frac{3}{8}$ の確率で A.B.X.Y という IP アドレスを定め感染対象とする。

4.3.2 逐次探索

逐次探索は起点となる IP アドレスを定め、その IP アドレスから順番に探索をしていく手法である。同一サブネットにいるホストが順番に探索されることになる。感染ホストの IP アドレスを A.B.C.D とする。疑似ワームは以下のような確率で感染対象とする IP アドレスを定める。

(1) 60%の確率で X.Y.Z.0 というアドレスを生成する。X は 1 から 253 の間の、Y、Z は 0 から 255 の間のランダムな数である。

(2) 40%確率で A.B.C.0 というアドレスを生成する。

(3) 生成されたアドレスの最後の一桁を 1 ずつ増加させて順々に感染対象とする。つまり、X.Y.Z.0 のアドレスが生成されたときは X.Y.Z.1、X.Y.Z.2、··· という順番で感染対象ホストを定めていく。

4.4 提案機構の実装

実験に用いた実装では使用中の IP アドレスのリストをあらかじめ生成することで、使用されている IP アドレスに対しての通信か否かを判断する。提案機構は Promiscous モードでパケットの受信をする。ARP Request が到着すると、問い合わせているアドレスを確認する。使用されている IP アドレスに対する問い合わせの場合はそのまま破棄するが、使用されていない IP アドレスに対する問い合わせの場合は ARP Reply を送信する。

IP パケットが届いたら、提案機構送信元アドレスと送信先アドレスをリストに保存する。同じ送信元から異なる送信先アドレスに 3 回以上通信の試みがあった場合は、ワームに感染したとみなしてホストを遮断する。今回はワームに対して停止命令を送ることで遮断の代わりとした。

ワームからの通信が TCP を用いていた場合にはスリーウェイハンドシェークを行う。その際こちら側のウィンドウサイズは 1 に設定しておく。その後データが送信された時には ACK 番号を増やさないパケットを送信し再送を要求する。

5. 実験結果

機構を導入する際は脆弱性のある全ホストに早い速度で感染したが、提案機構を導入した結果、拡散が広まる前にワームを遮断し、拡散を止めた。

5.1 提案機構導入前

機構を導入する前はワームの拡散を阻害するものが全く無いので全ホストに感染をした。表 1 に示す値は

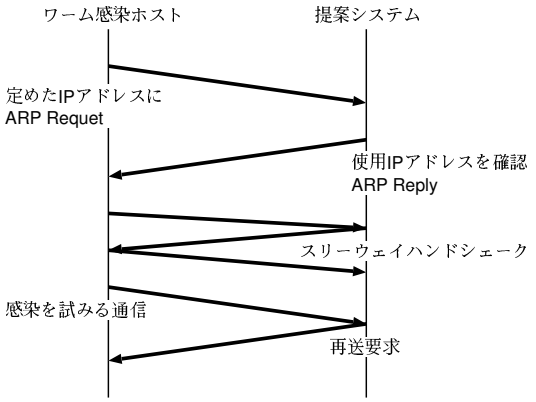

図 3 提案機構の通信の概要

ワームが脆弱性のある全てのホストに感染するまでにかかった時間である。実験は複数回行った。 上段が複数回行ったときの平均時間で下段が複数回の試行の中でもっとも早く全てのホストに伝搬するまでにかかった時間である。

	局所優先	逐次
平均時間 (秒)	7.6	6.4
最短時間 (秒)	5.6	5.2

表 1 脆弱性のある全ホストに伝搬するまでに要した時間

このように、ワームに対し何ら対策を講じない場合、早い速度で拡散するので拡散が少ない状態での人的対処は不可能である。

5.2 提案機構導入後

提案機構を導入した場合はワームが脆弱性のある全てのホストに広まる前に遮断された。逐次優先探索を行うワームでは感染したのは起点となったホストのみで、局所優先探索を行うワームでも多くて 2 台のホストが感染した時点で遮断された。

これは提案機構がワームの活動開始後短時間でワームの通信を検知し、遮断したためである。

6. 考　　察

5 章で示したように提案機構はワームの拡散を止める結果となった。つまり、起点のワームが活動を開始してから短時間で活動を停止させたためである。ワームの活動が停止したのは想定環境では外部からの感染通信の流入を考慮しなかったためである。

外部からの流入が少なかった場合は、今回の実験結果のように短時間で感染活動を停止させることができると考えられる。これは外部に対して送信された感染を試みる通信も短時間で抑えることができたと言える。このことから、他ネットワークに拡散するパケットの

数も抑えられ、ネットワーク全体に広まる速度を遅くできた。当初の目的であるワームの拡散の遅延に効果があると言える。

7. 今後の課題

今回の実験は限られた想定環境でのみ行われたので、他の想定環境での実験が必要である。提案機構では使用されている IP アドレスの数が検知に大きな影響を与える。提案機構がどの程度のアドレス使用率まで効果を発揮できるのかを検証する必要がある。また、脆弱性のあるホストの台数の変化による影響、外部からのワームの流入量による影響も検証する必要がある。

また、現在は提案機構が独立して動いているが、同じネットワーク内の異なるサブネットに配置された機構が連携をはかった場合より効果が期待できるので、今後検討していきたい。

参 考 文 献

1) Knowles, Douglas., Perriot, Frederic. and Szor, Peter. “Symantec Security Response: W32.Blaster.Worm” Symantec 26 Feb. 2004 <http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster .worm.html>
2) Nakayama, Takayoshi., and Ladley, Fergal. “Symantec Security Response:W32.Sasser.Worm” Symantec 27 Jul. 2004 <http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser. worm.html>
3) Staniford, Stuart., Paxson, Vern. and Weaver, Nicholas. “How to Own the Internet in Your Spare Time” Usenix Security 2002