マルチメディア通信と分散処理　106－26
コンピュータセキュリティ　16－26
（２００２．２．１５）

ダイナミックフィルタリングを利用したパーソナルファイアウォールの設計

小林文彦　西山裕之　溝口文雄
東京理科大学 理工学部

概要

常時接続環境が普及したことでセキュリティの弱いコンピュータが外部にサービスを提供し,不正侵入の危険にさらされている.パケットフィルタで守る方法が一般的だが許可したパケットには無防備である。そこで本論では,従来の静的なパケットフィルタリングではなくダイナミックフィルタリングを利用し,サービスを利用したいときだけ,適時ポートを開くことによりセキュアなサービスを提供するシステムの設計について述べる.

Design of Personal Firewall using Dynamic Filtering

Fumihiko Kobayashi Hiroyuki Nishiyama Fumio Mizoguchi

Science University of Tokyo

By the continuous connection Internet service, the weak computers of security aloways opens services to Internet and it is exposed to the danger of an unlawful access to its. In this paper, design of system which offers secure service is stated by opening a port to use service not the conventional static packet filtering but dynamic filtering.

1　はじめに

現在インターネット利用者は増大の一途を辿り,インターネットの常時接続サービスが以前よりも安価に実現できるようになり中小企業や,一般家庭にも広く普及し始めている.

安価な常時接続環境が整うことは,ユーザーにとって使用料金,利便性の面で喜ばしいことである.しかし,インターネットに常時接続するということは,常時外部からの危険にさらされるということでもある.インターネットでは,常に様々なスキャンや不正アクセスが行われており,何の対策もなしにインターネットにマシンを接続している状況は,危険な行為である.

このような不正アクセスの対策として,一般的にはファイアウォールを構築し,運用することでセキュアな状態を保つのだが,コスト面や,その導入,運用には専門的な知識を必要とする.ユーザーへのセキュリティ教育 [1] の研究も進められているが,現時点では一般家庭ユーザーの導入,運用には問題がある.

このため対象を絞ったパーソナルファイアウォールと呼ばれる製品が市販されている.本格的なファイアウォールシステムと異なり,一定のセキュリティルールに基づいて不正侵入を検出,警報を発するための仕組みとパケットフィルタリングによる不正なパケットを排除,ログ記録機能を持つ.パケットフィルタリング機能としては,常時接続に使用する ISDN ルーターやブロードバンドルーターにもフィルタ

リング機能があり,最低限のセキュリティを構築することになる.一般的には,ルーターのフィルタリング機能を使用してフィルタリングを行い,使用するサービスによってポートを空けている.しかし,このサービスは,常に外部からの不正アクセスを受けることになってしまうことになる.

本研究では,常時接続環境を対象に,この問題を解決するため,外部からアクセスできるサービスに対してユーザーがフィルタリングの設定などを意識することなく,セキュアにサービスを提供できる動的フィルタリングシステムと不正アクセス対策を提案する.

2 本研究の背景と目的

本研究では, 現在著しく増加している一般家庭の常時接続環境を想定する.ISDN やADSL,CATV など常時接続環境で,DHCP によるグローバル IP アドレス,また固定の IP アドレスを提供され,ISDN ルーターやブロードバンドルーターなどでマシンをNAT もしくは,静的 IP マスカレードでサービスを特定のマシンに割り当て,ローカルサーバーを公開しているものとする.外部との接続には,Windows2000 Professional もしくはWindows2000 Server を使用する.これは,多くのユーザーが Windows を使用していることから選択した.

外部に公開する FTP サービスや NetMeeting など使用したいサービスがあるとき,そのサービスが使用するポートは常に外部からの不正アクセスの危険にさらされることになる.例えば,ポートスキャンでポートが開いていることを知られ,そのサービスには既知のセキュリティホールがあると管理者権限を奪われる,トロイの木馬を仕掛けられるなど不正アクセスされる可能性は高くなる.インターネットには,簡単に不正アクセスが可能なスクリプトをダウンロードできるサイトがあるため,詳しい知識のないユーザーでも不正アクセスが可能である.不正アクセスされるのは,企業や政府機関のマシンだけではない.個人のマシンには,外部の人間にとって有用な情報がないから不正アクセスなどされないと考えているユーザーも多いが,不正アクセス者は最終目的となるマシンだけを狙うわけではない.多くの場合,不正アクセスの形跡が残らないように踏み台として多くのマシンを経由し,攻撃を仕掛ける.ここで,セキュリティの弱い一般家庭のマシンは格好の踏み台として狙われているのである.加えて,DDoS(分散サービス妨害) 攻撃と呼ばれるサーバーアタックのために使用される場合も増加している.

2.1 企業レベルの対策

企業では,パケットフィルタファイアウォールよりもセキュアなアプリケーションプロキシファイアウォールやステートフルパケットインスペクションなどを導入し,セキュアにサービスを提供しているが,コスト,運用面を考えると一般家庭で導入できるものではない.

加えて,ファイアウォールだけでなく,不正侵入を検知する侵入検出システム [2][3] もファイアウォールと併用して運用する企業も増加している.システム管理者によっては,サービスを使用する時間帯だけそのポートを開けるといった運用をしている.これは,不正アクセスされる可能性を減少させるためである.システムログを監視し [4] 不正がないかのチェックも行なっているだろう.しかしながら,一般家庭には専門のシステム管理者がいるわけではないのでこのようなシステム管理,運営は現実的ではない.

2.2 パーソナルファイアウォール

現在個人に特化したファイアウォールが市販されている.パーソナルファイアウォールとしては,Norton Internet Security2001 や BlackICE Defender などがある.BlackICE Defender は侵入検出に特化したパーソナルファイアウォールであり, ポートスキャン,SYN FLOOD などの不正アクセスを検出すると警告を促すなどの機能と簡易的なフィルタリング機能を有する.

Norton Internet Security では,パケットフィ

ルタリング,Web フィルタリングのフィルタリングを持ち, 不正侵入やプライバシー保護に関わる典型的な攻撃に対応するフィルタルールがセットされており, セキュリティレベルを「低レベル」,「中レベル」,「高レベル」などと大まかに設定されたレベルを選ぶだけで, すぐに利用できるようになっている. パケットフィルタリングでは,IP, ポート, プロトコルなどで許可, 遮断が設定可能である. しかし, フィルタルールでアクセス可能としたポートに対して, パーソナルファイアウォールは何も動作しない. 危険のあるサービスは使用せず, フィルタリングしておくことがセキュリティ面を考慮した場合適切であるが, それではサービスを受ける, 提供することはできない.

そこで, 本研究では動的パケットフィルタに着目し, サービスを使用するときだけ必要なポートへのアクセスを可能にするフィルタルールを自動的に設定することで不正アクセスの可能性を減少させる. また不正アクセス対策としてポートスキャンを検出し, 動的フィルタリングに反映させることで, ポートスキャン元からの攻撃を遮断することを目的とする.

3 システム構成

本システムでは, ルーターの NAT または静的 IP マスカレードで外部公開されたマシンにおいてルーターとは別途に次の機能を有する.

- 動的パケットフィルタリング
- 不正アクセス検出

3.1 動的パケットフィルタリング

Apache,Ftp など多くのサービスでは, 許可するホスト, 拒否するホストを指定し,IP によるフィルタリングを施しているが, これはサービスを利用するユーザーの IP を事前にしらなければならない. 現状の IPv4 ではグローバルアドレスの枯渇問題があるため多くのユーザーは固定 IP ではない. よって動的にパケットフィルタリングを行なう必要がある. 本システムでは, 外部公開するマシンに Windows2000 を想定している. Windows2000 には, 標準で RRAS(ルーティングとリモートアクセスサービス) の機能として, パケットフィルタリングが利用できる. Windows2000 Professional では,Server で提供されているＧＵＩによる設定, 一部機能がないもののフィルタリング機能は利用できる. RRAS では, 次のときにフィルタリングルールのチェックを行なう.

- input：パケットが入ってくる時
- output：パケットが外に出ていく時

RRAS は, netsh.exe コマンドを使用し, インターフェースに対するフィルタリングルールをフィルタタイプ（input,output）毎に設定し, フィルタの制御を行なう. RRAS のパケットフィルタの動作を簡単に示すと次の 2 点による組み合わせになる.

- フィルタ・ルールがないときのデフォルトルール
- デフォルトルールとは異なる動作をさせるための例外ルール

デフォルトルールとは, パケットを全て通過させるか, それとも全てブロックするかのどちらかを決めるものであり, 例外ルールとは, パケットを選択するためのパターンの集まりであり, これにマッチしたパケットがフィルタリング動作の対象となる. パターンにマッチした場合の動作はデフォルトがどちらであるかに依存する.

- デフォルトが全てのパケットをブロックさせる場合, 例外ルールにマッチしたパケットは通過し, どの例外ルールにもマッチしないパケットはブロックされる (図 1 に示す)
- デフォルトが全てのパケットを通過させるの場合, 例外ルールにマッチしたパケットがブロックされ, どの例外ルールにもマッチしないパケットは通過する.

フィルタは基本的には, インバウンドの TCP 接続要求をデフォルトですべて禁止し, 内部から外部へのアウトバウンドパケットは許可する. インバウンドの UDP についても必要なもの (DNS など) 以外は全てブロックする. ここで必要なものとは,DNS の応答パケット (ソースポート番号 53),DHCP の応答パケット (ソース・ポート番号 67, 宛先ポート番号 68) の 2 種類は許可しておく. 内部から外部へのアウトバウンドパケットは許可.ICMP についてもこれらを許可する理由は特にないので, すべてブロックし,ping の応答だけは許可するものとする.ping パケットでは,ICMP Echo(type=8,code=0),Echo Reply(type=0,code=0) を使用するのでこれを許可.

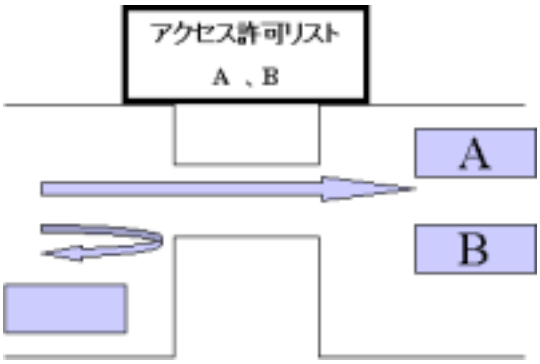

図 1: パケットフィルタ

ここへ, 使用したいサービスによって随時フィルタを追加, 削除していくことになる. 本システムでは, サービス指定でそのサービスが使用するポートへのインバウンドコネクション要求を許可する. あらかじめ, 使用するサービスとそのサービスが使用するポートを指定しておく. 既知のサービス, 例えば FTP やファイル共有などはあらかじめ使用するポートの設定を提供する.

- FTP : TCP 宛先ポート番号 21 へのインバウンド TCP 接続要求を許可
- ファイル共有: ポート番号 137-139

しかし, 外部からマシンのフィルタルールを自由に設定されてしまうと本システムが重大なセキュリティホールとなってしまう. そこで, 使用するサービスのアクセス権限を与える (フィルタにルール追加を依頼) ために, サービスアクセス認証を行う. このサービスアクセス認証は, ローカルマシン上で動作させ, 外部またはローカルマシンから, サービスを利用したいユーザーの認証を行い, 正規のユーザーであればそのユーザーに許されたサービスを掲示し, ユーザーが選んだ利用したいサービスに対してインバウンド接続可能となるフィルタルールを生成し, 適用する. このシステムで動的にフィルタリング可能なものは, 予め指定したサービスの中から, 各ユーザーに権限の与えられたサービスのみとなる.

ユーザー B に FTP と NetMeeting の使用権限が与えられていたとすると, ユーザー B は FTP か NetMeeting を使用可能にするフィルタルールしか実行できない (図 2).

図 2: サービスアクセス認証

3.2 接続許可フィルタルールの生成

認証に成功したユーザーが接続してきたコンピュータの IP とサービスを元に、このユーザーの IP からだけ指定されたサービスに接続できるフィルタルールを生成し、RRAS に設定することで認証を行なったユーザーにだけサービスを提供する。

ユーザー B が FTP を選んだとすると、FTP のサービスに必要なポート番号 21 と、ユーザー B がアクセスしてきた IP を使いこのようなフィルタを生成し、設定する。[add filter name=”インターネット

接続” filtertype=input srcaddr=ユーザー B の IP srcmask=0.0.0.0 dstaddr=0.0.0.0 dstmask=0.0.0.0 proto=tcp srcport=0 dstport=21]。この設定により、今まで閉じられていた TCP 21 番ポートが開き、ユーザー B がサービスアクセス認証でアクセスしてきた IP だけは FTP サーバーに TCP 接続が可能となる。

3.3 接続許可フィルタルールの削除

接続許可用に設定したフィルタルールはそのまま放置しておくと IP 詐称による攻撃を受ける可能性があるため、必要がなくなったフィルタルールは削除しなければならない。本システムでは、この削除のタイミングを 2 種類設けている。

- ユーザーから接続要求を確認し、接続が完了した場合
- 一定時間確立された接続にパケットが確認されない場合

接続完了時にフィルタルールを削除する場合には、サービスの中で一回の接続で接続状態を保ち処理を行なうようなものに適している。これは、一度接続確立状態になると新たな接続要求をサーバーが受け取る必要がないため接続要求を許可するフィルタルールが必要なくなることを意味する。例えば、ユーザー B が使用していた IP アドレスから FTP サーバー (TCP 21 番ポート) に接続要求がくるかどうかを監視し (ローカルホスト上に出入りするパケットの監視)、接続要求が来た場合には、TCP 接続が確立され、先ほど設定したフィルタは不要となるため削除する。[del filter name=”インターネット 接続” filtertype=input srcaddr=ユーザー B の IP srcmask=0.0.0.0 dstaddr=0.0.0.0 dstmask=0.0.0.0 proto=tcp srcport=0 dstport=21]。これにより、サーバーがコネクション要求を期待している僅かな時間しかインバウンドコネクション要求を許可しないので、不正アクセスを受ける可能性は極めて低くなる。クライアントの不具合などにより、期待しているコネクション要求がこない可能性もある。このためコネクション要求を許可するフィルタにはタイムアウト時間を設定し、定められたタイムアウト時間を過ぎても要求がこない場合には、フィルタルールを削除する。

サービスによっては接続と切断を繰り返すこともある。例えば FTP の制御用ポートなどであるが、コマンドを送るたびに接続要求を行なう。このためサービスごとにフィルタ削除の設定を行なっている。上述した接続要求がきたところでフィルタ削除する方法と、その通信においてパケットが一定時間確認されなくなったところでフィルタを削除する方法である。既知のサービスにおいてはこの設定はあらかじめ用意するものとする。その他のサービスに関してはユーザが使用するポート、フィルタ削除のタイミング（デフォルトで一定時間使用されていない場合）を設定する。

3.4 ポートスキャン検出

不正アクセスとしてポートスキャンを検出する [5]. ポートスキャンは不正アクセスを行なうための調査行為であり, ポートスキャンを受けた後は不正アクセスとなる攻撃を受ける可能性が極めて高い. ローカルホストに出入りするパケットを監視するのだが, ここで取得するパケットは,RRAS でフィルタする前のパケットである. このため閉じているポート, 例えば, 外部に開いていると危険な 137,138,139 番ポートなどを調べるパケットも取得可能である. ルーターでこれらのパケットを遮断, または静的 IP マスカレードで送られてくるパケットが制限されているときはポートスキャンを検出することはできない可能性もある. ポートスキャン検出には、フリーの侵入検出システム SNORT Version1.7-WIN32 を使用している。

- SNORT のログファイルから攻撃元の IP を抽出
- サービスアクセス認証のときにチェック
- 不正アクセス IP は認証許可しない

この動作で不正アクセスを防ぐ．ここまで説明したシステムの構成図を図 3 に示す.

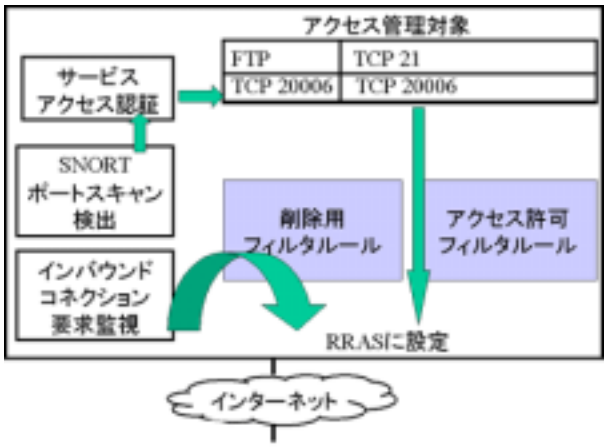

図 3: システム構成

4 関連研究

RPC(Remote Procedure Call) を利用するグループウェア等のインターネット対話型処理では,RPC のセキュリティ問題により不正侵入等の可能性がある. そこで, セキュアな RPC を実現するためのコールバック型コネクション確立方式が提案されている [6]. この方式では, ファイアウォールが外部へのアウトバウンドコネクション要求は許可するが, 内部へのインバウンドコネクション要求は許可しないことを前提に, サーバーからクライアントにコネクション要求を発行する. このコネクション要求はサーバーからクライアントに対するものなので, サーバー側からのファイアウォールは通過するが, クライアント側ファイアウォールは通過しない. この問題を解決するためにクライアント側ファイアウォールにポート指定でインバウンドコネクション要求を一回のみ許可する機能を追加している. このことで, 不正アクセスを受ける確率を極めて低くできるのだが, アプリケーションが使用している RPC をコールバック型コネクション確立方式 RPC に変更しなければならないため既存のアプリケーションは使用できない. 本システムでは, サービス特有のポートを使用するためコールバックコネクション型の RPC よりもセキュリティは劣るが, 既存のアプリケーションをそのまま使える利点がある.

5 まとめ

本論では, 常時接続環境下のセキュリティの問題点を述べ, 現状のパーソナルファイアウォールソフトの問題についても指摘した. この解決のために, 静的なパケットフィルタリングではなく動的フィルタリングを用いてサービスを使用したいときだけポートを開けるシステムを検討した. 使用するときだけポートを開くため, ポートスキャンによってポートが開いていることを知られる可能性が低く, ネットワーク全体に無差別に攻撃するワーム等に攻撃される可能性も極めて低くなる. これにより, ユーザーが適時フィルタリングルールを作成し, 適用することがなくなり, セキュリティ知識のないユーザーでもセキュアなサービスを提供可能なパーソナルファイアウォールの有用な機能を提案した.

参考文献

[1] 武田　圭史, 溝江　宏真, 武藤　佳恭,"ネットワーク侵入検出手法の比較と脅威に応じた動的な検出", 情報処理学会第 59 回全国大会論文集,pp.399-400,1999.

[2] 吉井　崇行, 平石　広典, 溝口　文雄,"侵入検知のためのデータマイニング技術を利用したプロファイル生成", コンピュータセキュリティシンポジウム 2000 論文集,pp.249-254,2000.

[3] 平石　広典, 溝口　文雄,"ログデータ分析用ビジュアルブラウザの設計", コンピュータセキュリティシンポジウム 2000 論文集,pp.277-282,2000

[4] 溝口　文雄, 井上　勝隆, 西山　裕之, 平石　広典,"ネットワーク配信型のセキュリティ教育システムの設計", コンピュータセキュリティシンポジウム 2000 論文集,pp.139-144,2000.

[5] Giovanni Vigna and Richard A. Kemmerer.NetSTAT: A Network-based Intrusion Detection Approach, 14th Annual Computer Security Applictions Conference, Phoenix, Arizona, pp.25-34, December 7-11, 1998.

[6] 平山　英昭, 本多　弘樹, 弓場　敏嗣,"セキュアな RPC のためのコールバック型コネクション確立方式",IC2000(http://www.csl.sony.co.jsp/ic2000/)