セキュリティレベルの高いMTAの提案

4F－6

近藤岳大* 西野順二* 小高知宏* 小倉久和*
*福井大学工学部情報工学科

1 はじめに

近年、インターネットの発達が急激であり、その用途は多岐にわたっている。しかしながら、使用者・管理者のセキュリティに対する意識にはあまり変化が見られず、パスワードの剥奪やシステムの乗っ取りなど、セキュリティの脆弱性が顕著に表れてきた。この中で、電子メールのサーバを対象とした攻撃が頻繁に報告されている[1]。

本研究では、ネットワークセキュリティについて再検討をし、特にインターネット中で最も良く使われている電子メールサーバのセキュリティについて着目した。そして、セキュリティレベルの向上を目指したメール配送用プログラムを検討し、具体的なメールサービスシステムの実装を試みた。

2 既存のMTAの課題

文献[1]に紹介されているネットワーク上での攻撃例や、既存のメール配送エージェント(MTA:Mail Transfer Agent)の問題点を、表1にまとめる。表1が実際にあった攻撃例である。

これらの攻撃の中で電子メールサーバに関係するのが、

表1: 実際の攻撃の例

コンピュータウィルスの感染
サービス不能攻撃
ソフトウェアの脆弱性・設定ミスへの攻撃
SPAMメール、メールボム
違法なファイルのコピーサイト
ルート権限の乗っ取り
パスワードの剥奪
cgi-binプログラムへの攻撃
TCP/IPのバグへの攻撃
PINGによる攻撃

サービス不能攻撃、ソフトウェアの脆弱性・設定ミスへの攻撃、SPAMメール、メールボム、root権限の乗っ取りである。

現在もっともよく使用されているMTAソフトsendmailは、機能が豊富かつ柔軟である。しかし、同時に設定ファイルが独自の言語で書かれており、またそのファイルが非常に大きなものであるため設定が極めて困難である。これは設定ミスを引き起こしやすく、セキュリティホールが発生しやすいことが指摘されている[2]。

3 セキュリティレベルを上げたMTAの提案

3.1 概略

われわれが提案するMTAソフトウェアは、設定を可能な限り単純化にすることによって設定ミスを防ぎ、不必要な機能を削除することで、セキュリティホールの発生を押さえることを目的としている。また、管理者の負担を軽減できるのではないかと考えた。

現在では、qmailというsendmailをより簡潔にしたMTAソフトが注目されている。しかし、このqmailも実際に運用するときにはそれなりの専門知識を必要とし、誰もが簡単に導入できるものではない。本研究においては、ネットワークセキュリティを考慮しつつこのqmailよりもさらに単純化し、設定を簡潔にしたものを目指している。

3.2 仕様

本研究におけるMTAの仕様のポイントは以下の3つの点がある。

1. 大学の研究室やSOHOなど小規模ネットワーク向けを対象としている。
2. プロトコルはTCP/IP上のSMTPに限定する。
3. 機能ごとに複数のプログラム分割する。

まず、メールサーバへの攻撃が行われるのは、専門の管理者や十分な知識を持つ人がいないようなSOHOなど小規模ネットワークが多いということから[1]、専門ではない人でも運用ができるものにする。また、小規模ネットワーク向けにすることで、使われない機能を削除し設定を容易にする。

本研究ではTCP/IP上のSMTPに限定した。実際、senmailやqmailではUUCPによるメール配送もサポートしているが、このプロトコルは現在のところほとんど使用されていない。また、一体型のsendmailに対し、qmail同様機能ごとに複数のプログラムに分割し、それぞれを最小限の権限で動作させることにする。こうすることにより、セキュリティバグの発生箇所の削減と、障害発生時の原因追求を容易にしている。

The proposition of MTA with high security level.
Takehiro Kondoh* Junji Nishino* Tomohiro Odaka* Hisakazu Ogura*
*Faculty of Engineering, Fukui University

3.3 機能

特定する MTA で、機能を取捨選択することにより、設定を容易にすることができる。sendmail、qmail、本研究での MTA の機能を表 2 にまとめる。

この MTA の運用を小規模ネットワークと限っているため、他サーバから届いた自サーバのユーザ宛てのメール配送、自サーバから他サーバ宛てのメール配送は行うが、他サーバから他サーバへのメール中継は行わない。メールが届かなかったときのためのエラーメール配送、万が一のときの履歴を調べるためのログの保存は必要である。

メールの中継を行わないことにより、SPAM メールの踏み台サーバとされることを防ぐことができ、不正使用を試みようとしたことを、ログを保存しておくことにより追求することができる。

表 2: 機能比較表

		sendmail	qmail	今回の MTA
配送関係	自サーバ宛てのメール配送	○	○	○
	他サーバ宛てのメール配送	○	○	○
	ローカル配送	○	○	○
	メールの中継	○	○	
	エラーメール配送	○	○	○
	UUCP のメール配送	○	○	
管理	ログの保存	○	○	○
連送関係	forward による転送	○	○	
	エイリアス機能	○	○	
	仮想ドメイン	○	○	
	メーリングリストの運営	○	○	

3.4 提案する MTA の内部構造

データの流れは図3.4のようになっている。まず、SMTP 経由で送られてきたメールは、キュー管理のプログラム「queue」に渡される。その後、「send」は配送キューにおかれたメッセージを配送する。ローカル受信者当てのときには「lspawn」を使用し、リモート受信者あてのときには「rspawn」を使用する。また、メッセージが配送できないときには、キューに一時ためておき、後に再度配送を試みる。「lspawn」及び、「rspawn」はそれぞれ「local」「remote」を呼び出して配送を行う。

これらを独立したプログラムとすることにより、各々のプログラム上で使用者のチェックを行うことが可能となり、不正使用に対する防御壁をそれぞれに組み込むことができるようになる。加えて各々を最小限の権限で動作させることにより、誤った動作やクラッカーの介入によるファイルの添加・削除を防ぐことができる。

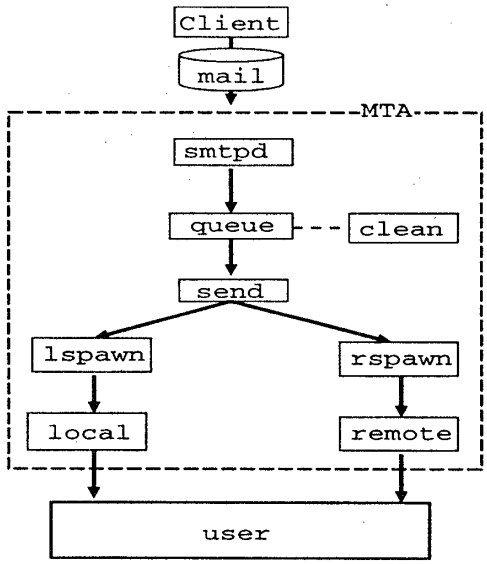

図 1: データの流れ

4 まとめ

本研究では、電子メールを利用したどのような攻撃が行われているか、どの部分でのセキュリティレベルを上げるべきかを調査・考察した。その結果、現行のメール配送用プログラムの設計方法に問題があることが分かった。そこで、できうる限り機能・動作・設定を簡単にした MTA を目指し、その仕様を設計した。

よく似た MTA として qmail があったが、qmail と異なる点は、標準入力からの処理を削除したという点である。現在、メールの読み書きは MUA(MailUserAgent) を使うのがほとんどであるため、標準入力からの処理は不必要である。また、攻撃の標的となるのは、SOHO などの小規模ネットワークが多いことに着目し、小規模ネットワークでも簡単に運用・管理ができる MTA を設計した。

参考文献

[1] インプレス:インターネットマガジン 97/12〜98/12 月号「インターネットセキュリティの現状」:インプレス:1997,98

[2] William Stalling 著:インターネットセキュリティのすべて:日経 BP 社:1997

[3] Jonathan B.Postel:SIMPLE MAIL TRANSFER PROTOCOL:1982

[4] David H.Crocker:STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES:1982