保護ドメインを用いた権限分割による安全なメーラの設計

島田 佳広　品川 高廣　吉澤 康文
東京農工大学工学部情報コミュニケーション工学科

1 はじめに

近年のインターネット接続環境の普及に伴い，電子メールを利用してウィルスなどの悪意のあるコードを送りつけ，メールを受け取ったコンピュータに被害を及ぼすケースが増加している．

本研究では，ウィルスなどに感染して悪意のあるコードを実行してしまったとしても，その被害を最小限に抑えることができるメーラを設計する．本研究ではメーラを必要な権限ごとにコンポーネントに分割し，保護ドメインを用いてそれぞれのコンポーネントに必要最小限の権限のみを与えることによって安全なメーラを実現する．

2 本研究のアプローチ

従来のメーラはアクセス権限の分割がなされていないため，悪意を持つ者に乗っ取られた場合，メーラを起動したユーザの権限でアクセス可能な全ての資源が危険にさらされてしまう．例えばメーラが root 権限で動作していた場合，パスワードの変更も可能である．

バグのないメーラを作成すればよいという考え方もあるが，どのメーラにおいても脆弱性は発見されており，現実的には難しい．以下がその例である．

mozilla:悪質な POP サーバに接続すると任意のコードを実行できてしまう脆弱性[1]

Sylpheed:悪意のある SMTP サーバによって攻撃可能な脆弱性[2]

EdMax フリー版,Winbiff:HTML メールのリンククリックで攻撃者の記述したスクリプトが実行される[3]

アプリケーションのアクセス権限を制限することによって，不正アクセスの被害を最小限に抑えることを目的とした保護機構自体は，既に様々なものが提案されている[4,5,6]．しかしこれらの保護機構を実際に適用するためには，アプリケーション毎にどのようなアクセス権限が必要かを検証し，必要な権限ごとにアプリケーションを的確に分割して，それらの間の API を設計するといった作業が必要であり，既存のアプリケーションへの適用は容易ではないことが知られている．

そこで本研究では，メーラを例として取り上げ，実際にアプリケーションを適切なコンポーネントに分割してそれらの権限やコンポーネント間の API を定義することによって，一般に安全なアプリケーションを新しく設計する際，指針となる知見を得ることを目的としている．

A Proposal of Secure Mailer with Authority Division Using Protection Domains
Yoshihiro Shimada, Takahiro Shinagawa and Yasufumi Yoshizawa
Department of Computer , Information and Communication Sciences,Faculty of Engineering Tokyo University of Agriculture and Technology

3 設計方針

保護ドメインを用いた安全なアプリケーションの設計方針を示す．

(1) 保護対象の重みつけ

保護の対象となるもの(ファイル等)をリストアップして，その価値・重みを評価する．この情報はセキュリティレビューにおいて，重要となる．

(2) モジュール構造図の作成

アプリケーションに必要なコンポーネントを列挙し，モジュール設計をする．モジュールとデータの流れの関係を図示する．

(3)ドメイン作成

モジュールを保護ドメインとする．各ドメインの機能・アクセス権限を定義する．ドメインが機能する範囲での最低限の権限しか与えない．

(4)ドメイン分割

(3)の定義において，権限のレベルが違う処理は別ドメインに分割する．また(1)で定めた，重要情報に関する操作も別ドメインに分割する．

(5)API の設計

ドメイン間のアクセス権限を定義し，API の設計を行う．ドメインに対して，明示的に許可されている API のみ呼び出し可能とする．

(6)セキュリティレビュー

想定される攻撃を列挙し，各ドメイン毎に安全性の検証を行う．脆弱性が発見された場合は，(3)に戻り再びドメインの定義を再考する．また権限のレベルが同等で，統合しても脆弱性が見つからないドメインは統合する．(3)～(6)の過程を繰り返し行うことで，安全性が向上する．

4 設計

図 1 にディレクトリ構造を示す．点線で囲んだ部分が重要情報として定義されたメール本文，アカウント設定ファイル，アドレス帳ファイルである．

図 2 にメール受信側の保護ドメインの構成図を示す．また，図の矢印の横に API の名前も示す．次に各ドメインの機能を説明する．

(1)COMMANDER ドメイン

UserInterface から入力された指示を受けて，各ドメインへ指令を送る．

(2)POP ドメイン

POP サーバからメールを受信して，一時フォルダに書き込む．

(3)MBOX ドメイン

メールボックスを管理する．一時フォルダのメールをメールボックスに保存し，メールボックスのメッセージを読み書きする．

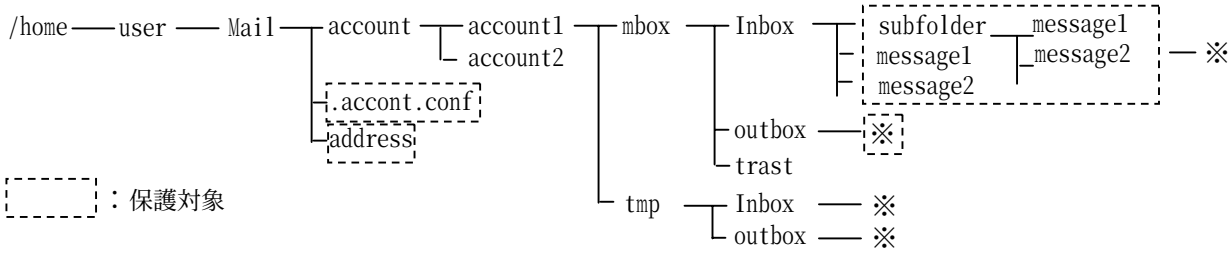

図 1 ディレクトリ構造

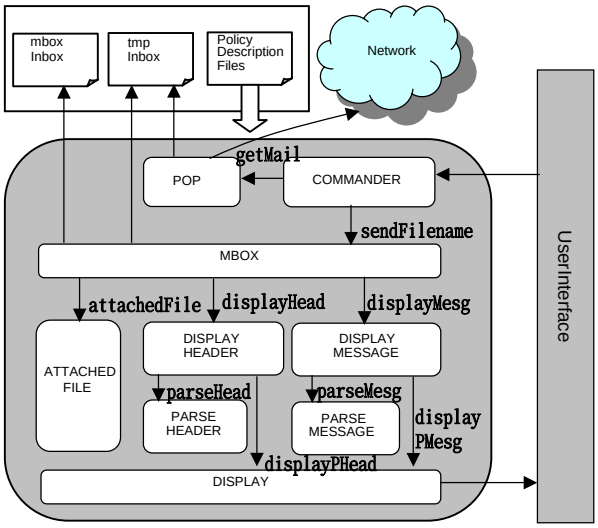

図 2 メール受信側システム構成

(4)DISPLAY HEADER ドメイン
ヘッダ一覧を表示するために，PARSE HEADER ドメインにヘッダの解析を依頼し，解析済みヘッダ一覧を作成する．

(5)PARSE HEADER ドメイン
ヘッダを解析する．例には，許可されていないヘッダの発見・通知などがある．

(6)DISPLAY MESSAGE ドメイン
メッセージ本文を表示するために，PARSE MESSAGE ドメインに本文の解析を依頼する．

(7)PARSE MESSAGE ドメイン
メッセージ本文を解析する．例には SCRIPT タグの無効化などがある．

(8)DISPLAY ドメイン
解析済みヘッダ一覧とメッセージ本文を表示する．

(9)ATTACHED FILE ドメイン
添付ファイルをサンドボックス内で実行する．

また，表 1 に各ドメイン・ファイル間のアクセス権限の一覧を示す．表の rwx は read,write,execute を表す

表 1 ドメインインタラクションテーブル

アクセスされるドメインとファイル

アクセスするドメイン	1	2	3	4	5	6	7	8	9	Tmp	mbox
1		x	x								
2	x									rw	
3				x		x			x	r	rw
4					x			x			
5				x							
6							x	x			
7						x					
8									x		
9											

5 検証

安全性の検証のために以下の例を示す．

POP ドメインの安全性

POP ドメインに関する危険性の中に，POP プロトコルの実装のバグをついて，POP サーバがメーラの制御を乗っ取るものがある[1]．本研究が提案するメーラでは，POP ドメインは POP サーバからメールを受信する権限と一時フォルダにファイルを作る権限しか持っていないため，受信済みメールを破壊したり，ネットワークにウィルスをばら撒いたりすることはできない．

MBOX ドメインの安全性

保護対象となるメールボックスを管理するのが MBOX ドメインである．MBOX ドメインは，バグが起こりやすい，外部のホストと通信をするドメインやメール本文を解釈するドメインから直接にアクセスできないようになっているため，メールボックスが破壊・改竄される可能性は極めて低い．

6 まとめ

本稿では保護ドメインを用いた安全なメーラを設計した．またその過程において，保護ドメインを用いた安全なアプリケーションの設計の手順についても述べた．今後は細粒度保護ドメイン[6]等の保護ドメイン技術を用いて，実際にメーラを実装し，実用的なレベルまで引き上げたい．

参考文献

[1]Bugzilla Bug 157644:Malicious pop3 server can write to arbitrary memory,Oct 21 2002, http://bugzilla.mozilla.org/.

[2]Sylpheed. http://sylpheed.good-day.net/.

[3]Security Focus:複数のメールソフトに不適切なセキュリティゾーンが適用される欠陥,Jun 30 2003, http://www.securityfocus.com/.

[4]Ian Goldberg,David Wagner,Randi Thomas and Eric Brewer. A Secure Environment for Untrusted Helper Applications: Confining the Wily Hacker,In *Proc. of the 6th USENIX Security Symposium*,page 1-13,July 1996.

[5]J.Team,J.Gosling,B.Joy and G.Steele.*The Java Language Specification*.Addison Wesley Longman,1996.

[6]品川高廣,河野健二,高橋雅彦,益田隆司:拡張コンポーネントのためのカーネルによる細粒度保護ドメインの実現,情報処理学会論文誌,Vol.40,No.6,6 月 1999.