セキュアOS関連の研究

岡山大学大学院自然科学研究科　山内研究室

1.はじめに

ソフトウェアのぜい弱性を利用した様々な攻撃により，個人情報の漏えいなどの被害が発生している

➡ Security Enhanced Linux（SELinux）を代表とするセキュアOSの登場

＜セキュアOSの特徴＞

(1) 強制アクセス制御(Mandatory Access Control:MAC)
システム管理者が定めたセキュリティポリシ (ポリシ)により，全てのファイルやプログラムのアクセス権限を制御

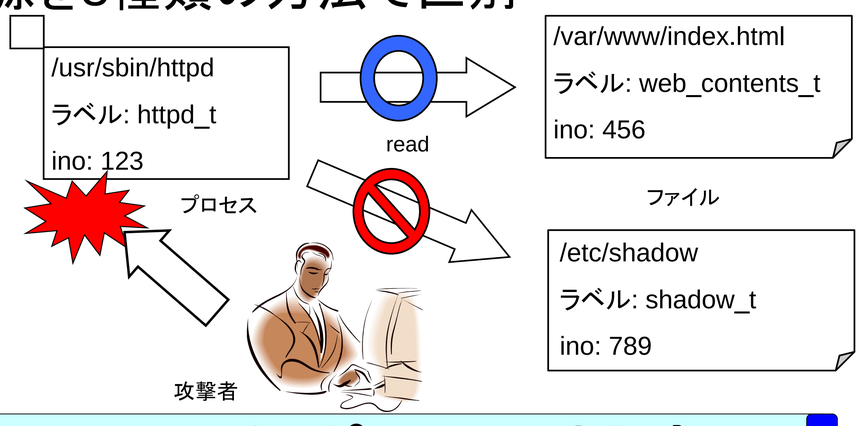
(2) 最小特権
サブジェクトに必要最小限のアクセス権を与えることができる機能

➡ 被害を最小限に抑えることが可能

＜セキュアOSのアクセス制御の仕組み＞

セキュアOSは資源を3種類の方法で区別

(1) フルパス
(2) ラベル
(3) inode番号



2.SELinuxの不要なポリシの削減

SELinuxはMLS，RBAC，およびTEにより高いセキュリティを実現可能なセキュアOS

(1) ホワイトリスト方式のポリシに従い，アクセス制御を実施
(2) ラベルでリソースを識別

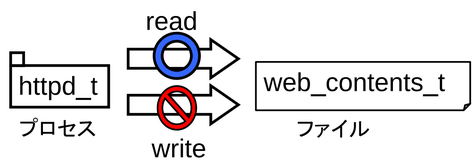
SELinuxのポリシとして広く利用されているrefpolicyはマクロ (1000種類以上)を利用してアクセス権限を付与

➡ ポリシの設定や読解が難しいため，最小特権の実現が困難

```
read_files_pattern(httpd_t web_contents_t, web_contents_t)
```

マクロを全て展開

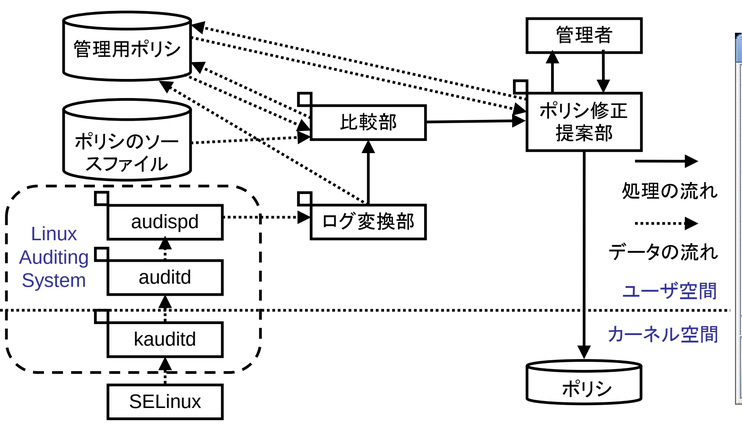
```
allow httpd_t web_contents_t:dir { getattr search open };
allow httpd_t web_contents_t:file { open getattr read ioctl lock };
```

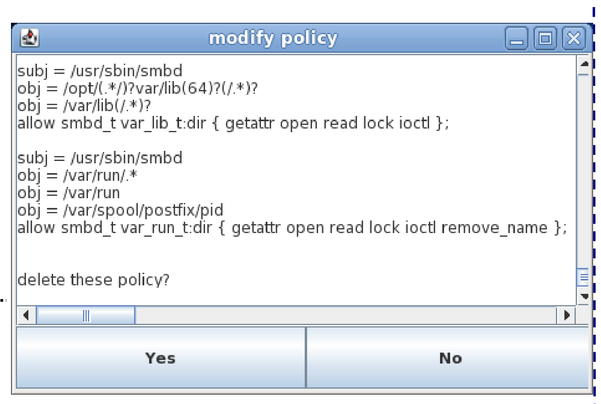


利用しているシステムに存在する不要なポリシを自動で発見し，削減する方法を提案

(1) SELinuxが出力するログを利用して，不要なポリシを自動的に検出
(2) 管理者にポリシの修正を提案し，自動的に修正

➡ SELinuxのポリシの問題点を解決





3.SEEditのパーミッションの設計

＜SELinux Policy Editor (SEEdit)＞

(1) SELinuxのポリシの設定を簡易化するツール
(2) 独自の中間言語SPDLでポリシを記述

➡ ポリシ開発者の負担を削減

```
domain httpd_t
program /usr/sbin/httpd;
allow /var/www/ r;
```

コンパイラで変換

```
allow httpd_t var_www_t:
{ fifo_file file lnk_file sock_file } { ioctl lock read } ;
```

/var/www：オブジェクト
r：統合パーミッション

ファイルに関するアクセスベクタパーミッション（18種類）を8種類のパーミッションに統合

安全性の低下を最小限にし，ポリシの設定を簡易化

統合パーミッション	オブジェクトクラス	許可するAVPs
追記（APPEND_PRM:a）	common_file	append
生成（CREATE_PRM:c）	dir	append, create, link, write
	common_file	create, link
消去（ERACE_PRM:e）	dir	rename, reparent, rmdir, unlink, write
	common_file	rename, unlink
実行（EXECUTE_PRM:x）	dir, fifo_file, lnk_file, sock_file	execute
	file	execute_no_trans
書き込み（OVERWRITE_PRM:o）	common_file	write
読み込み（READ_PRM:r）	common_file	ioctl, lock, read
探索（STAT_PRM:s）	dir	read, search
属性変更（SETATTR_PRM:t）	common_file, dir	setattr

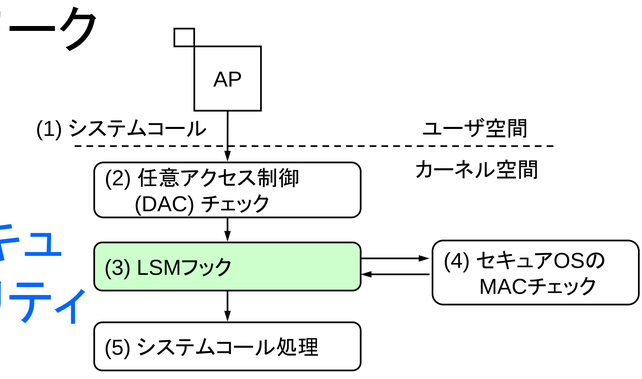
common_file：file, fifo_file, lnk_file, sock_file

4.LSMPMON

＜Linux Security Modules (LSM)＞

カーネルにセキュリティ機能を拡張するためのフレームワーク

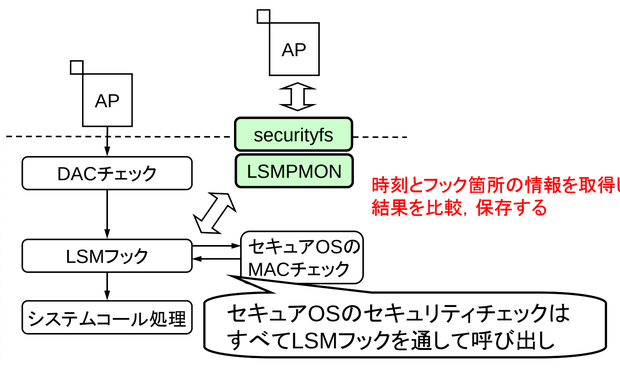
LSMを利用することで，セキュアOSなどの様々なセキュリティ機能を実現可能



＜LSMPMON (LSM Performance Monitor)＞

LSMのオーバヘッドを測定する機能であり，各LSM のフック箇所の処理時間と呼び出し回数を記録

➡ セキュアOSの各フックでどの程度処理時間がかかるかの正確な把握が可能




```
  LSMPMON 有効化
% echo 1 > /sys/kernel/security/lsmpmon/control
  LSMPMON 無効化
% echo 0 > /sys/kernel/security/lsmpmon/control
  結果を表示
% cat /sys/kernel/security/lsmpmon/result
hook                min       max       ave     count
-----------------------------------------------------
inode_create        97        1818075   105     3035605
inode_link
inode_unlink        97        80903     114     3035600
```

LSMPMONはセキュアOSのオーバヘッドを測定可能

➡ セキュアOS導入の1つの指標