4Z-1

SEAndroidにおけるアクセス制御の可視化

鈴木舞音† 天野桂輔‡ 齋藤孝道†

†明治大学 ‡明治大学大学院

1. はじめに

近年，携帯電話向け開発プラットフォームの共通化，オープン化の動きが加速する中で，米 Google 社が提供する Android 搭載端末が国内外で大きな注目を集めている．プラットフォームの普及に伴い，そのセキュリティ上の問題も増加してきた．

現在，Android でセキュリティ上の問題が発生するほぼ全ての場面は，アプリのインストールが起点である．アプリのインストールを通して利用者が攻撃を受けるシナリオは大きく二つある．

第一は，Android セキュリティ機構である「パーミッション」を正規に得たアプリが，（利用者の想定とは違えて）不正な目的で個人情報を取得したり，不正な動作をしたりするというものである．

第二の攻撃シナリオは，アプリに Android システム・プログラムの脆弱性を攻撃するコードを埋め込み，管理者権限(root 権限)を奪ってシステムを乗っ取るというものである．

これらの二つの攻撃に対して，NSA の SEAndroid が権限昇格されにくい構造になっているため有効である．しかし，SEAndroid では，端末にインストールされている全てのアプリに対して一括でアクセス制御を行うため，個々のアプリに対して制御を行えない．

そこで，本論文では，SEAndroid のアクセス制御に柔軟性をもたせる前段階として，アクセス制御の可視化を行い，セキュリティ向上を図った．

Visualization of the Access Control in SEAndroid

† Maine Suzuki, Takamichi Saito ‡ Keisuke Amano

Meiji University (†), Graduate School of Meiji University (‡)

1 -1-1 Higashimita, Tama-ku, Kawasaki-shi, Kanagawa, 214-83571, Japan (†) (‡)

{ee97084, ce16002}@meiji.ac.jp, saito@cs.meiji.ac.jp

2. Android

Android 用の公式アプリ・マーケットである「Google Play」では，アプリ審査を行わないため，誰でも簡単に不正なアプリを配信することができてしまう．そこで，マルウェアを検知する「Bouncer」システムが導入された．それによって，マルウェアをダウンロードしてしまうケースが 40%も削減された．しかし，一度端末内にインストールしてしまったアプリに対しては，攻撃を防ぐことができないため，安全性は不十分である．

3. SEAndroid

Android の安全性向上に有効なのが，Android のセキュア OS 化である．セキュア OS では，管理者を含むすべてのユーザの行動や参照可能な資源を大幅に制限ができる．また，ポリシーを適切に設定することによって，管理者権限を奪われた場合でも安全性を確保できる．上記のようなセキュア OS を採用した SEAndroid が 2012 年 1 月に米 NSA より発表された．

SEAndroid は，NSA が開発した SELinux を Android に合わせて改変したものである．SELinux では，プロセスごとに許可される動作を定義しておくことで，それを逸脱した動作を禁止する．

また，各プロセスの動作を限定することでマルウェアがシステムを改ざんするのを防げる．SEAndroid では，root 権限で動作する各種プロセスから，システム領域の書き換えや再マウントができないように設定しておくおことで，権限昇格攻撃を回避できる．

3.1. SEAdmin

SEAndroid では，強制アクセス制御(MAC 制御)という管理者を含めた全ユーザのアクセス制御を行うセキュリティモデルを採用しており，SEAdmin というアプリで設定できる．リソースに対するアクセスを

「リファレンスモニタ」と呼ばれるソフトウェアが一律にチェックし，セキュリティポリシーに反するアクセスについては，それが管理者からの要求であっても拒否できる様になっている．また，強制アクセス制御(MAC 制御)を活用すると，「最少権限」ポリシーも実現できる．システムで稼働するプロセスなどに，稼働に最低限必要な権限を与える方式である．

これによって，マルウェアによってプロセスが乗っ取られた場合でも，マルウェアに与えられた権限の範囲の動作しか許可されないので安全性が高まる．

しかし，この様なアクセス制御は SEAndroid の端末内の全てのアプリに対して，一括でアクセス制御を行っている．よって，アプリごとの柔軟なアクセス制御が出来ない．

3.2. SEManager

SEManager の設定項目を図 1 に示す．
ここでは，4 つの項目がある．

まず，Enforcing Mode では強制アクセス制御(MAC 制御)や SELinux のモードの切り替えが行える．

次に，Booleans ではユーザ規定で用意されているポリシーの設定を行うことができる．しかし，それらの設定の説明はなく，どの様なアクセス制御が掛かるのかをアイテム名で判断するのは困難である．

最後に，Logs では既定ポリシーでアクセス禁止にしている資源にアクセスをした場合に出力される監査ログを確認することができる．

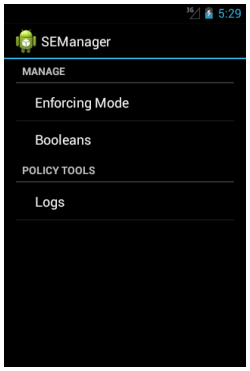

図 1　SEManager 設定画面

4. アクセス制御の可視化

SEAndroid におけるアクセス制御に関して，ユーザにとって視覚的に理解しやすい設定画面にするため，以下の 2 つの機能を SEManager に追加した．

4.1. 出力ログの画面

Logs では，どの資源がどの様なアクセス制御を拒否しているかを判断するのが困難である．そこで，ログを解説する画面を作成した．

4.2. Booleans でのダイアログ表示

ユーザが SEManager でポリシー設定をする際には，Booleans という項目から行う必要がある．ここで，SEAndroid で制御出来るポリシーを設定できる．しかし，アイテムが羅列されているだけなので，どの様な制御が掛けられるか判断が難しい．そこで，このアイテムをユーザが選択する際に，どの様な制御が掛けられるかをダイアログで表示した．ダイアログの表示画面を図 2 に示す．

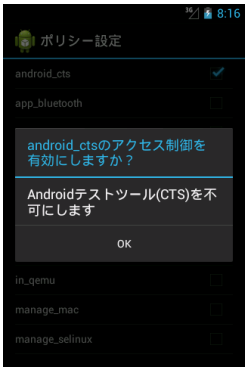

図 2　Booleans でのダイアログ表示画面

5. まとめ

本論文では，SEAndroid におけるアクセス制御の可視化を行った．ログ解説の機能及びダイアログの表示機能を追加することで，設定画面が容易に確認できるようになった．また，ユーザにアクセス制御に関する注意喚起を行うことで，セキュリティに対する意識を高める効果があると考えられる．

SEAndroid は安全性が高いが，ポリシーの設定がユーザの意図する設定を新たに追加しづらいものとなっている．今後の課題としては，アプリごとにポリシーの設定を柔軟に行えるアプリの開発が挙げられる．

謝辞　本研究の成果の一部は，科学研究費補助金（課題番号 22700086）の助成を受けたものである．

参考文献

[1] http://selinuxproject.org/page/SEAndroid
[2] 田口　裕也，根津　研介，林　秀幸，Bill McCarty　SELinux システム管理　セキュア OS の基礎と運用