Monthly Research

SELinux 再入門
-Android編-

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.02

SE for Androidの概要

- Android向けのSELinux応用プロジェクト
  - NSAが開発

- Android Open Source Project(AOSP)に一部がマージされ、4.4(KitKat)では一部のデーモンが**enforcing**で動作
  - vold, installd, netd, zygoteがenforcing
  - 今後、他のsystem daemonもenfocingがデフォルトになっていく予定

SE for Androidの脅威モデル

- root権限を持ったサービスに対する攻撃
  - 例1：CVE-2012-0056（Mempodipper）
    - /proc/pid/memに書き込めてしまい、攻撃者が権限昇格できてしまう
    - SELinuxが有効であれば、権限昇格してもSELinuxポリシーで許可されたことしかできなくなる

- アプリのアクセス権設定の不備を突いた情報漏洩
  - 例2：Lockout Mobile
    - 不適切なumaskでファイルを作成できてしまうため、他のアプリから読み取られ、情報漏洩してしまう可能性がある
    - SELinuxが有効であれば、新規作成したファイルに適切なラベルが割り当てられるため、他のアプリから読めない

SE for Androidの歴史

- 2012.01 SE for Androidリリース
- 2012.03 NSAとSamsungのKNOX開発にNSAが協力を開始
- 2013.04 SELinuxが組み込まれたGalaxy S4が販売
- 2013.07 Android 4.3にSELinuxが標準機能として組み込まれる（ただしpermissiveモード）
- 2013.10 Android 4.4のSELinuxにおいて、一部のアプリが標準でenforcingモードで動作するように

用語の整理（Terminology）

- SE Android
  - NSAが開発している、Android向けのSELinux拡張機能及びリソース
- AOSP
  - SEAndroidの機能及びリソースのうち、Androidのmainlineにマージされたもののこと
- Security Enhancements(SE) for Android
  - 上記をひとまとめにした、Android向けのSELinuxという意味
- KNOX
  - 2012年3月からNSAの協力の元、Samsungが開発している、Androidのセキュリティ強化版

Security Enhancements for Android

- カーネル空間への追加コンポーネント
  - xattrを使えるようにyaffs2を拡張
  - Binder（AndroidのIPC機構）へのフックを追加

- Androidミドルウェアへの追加機能 (Middleware MAC)
  - Install-time MAC
  - Enterprise Ops
  - Intent Firewall

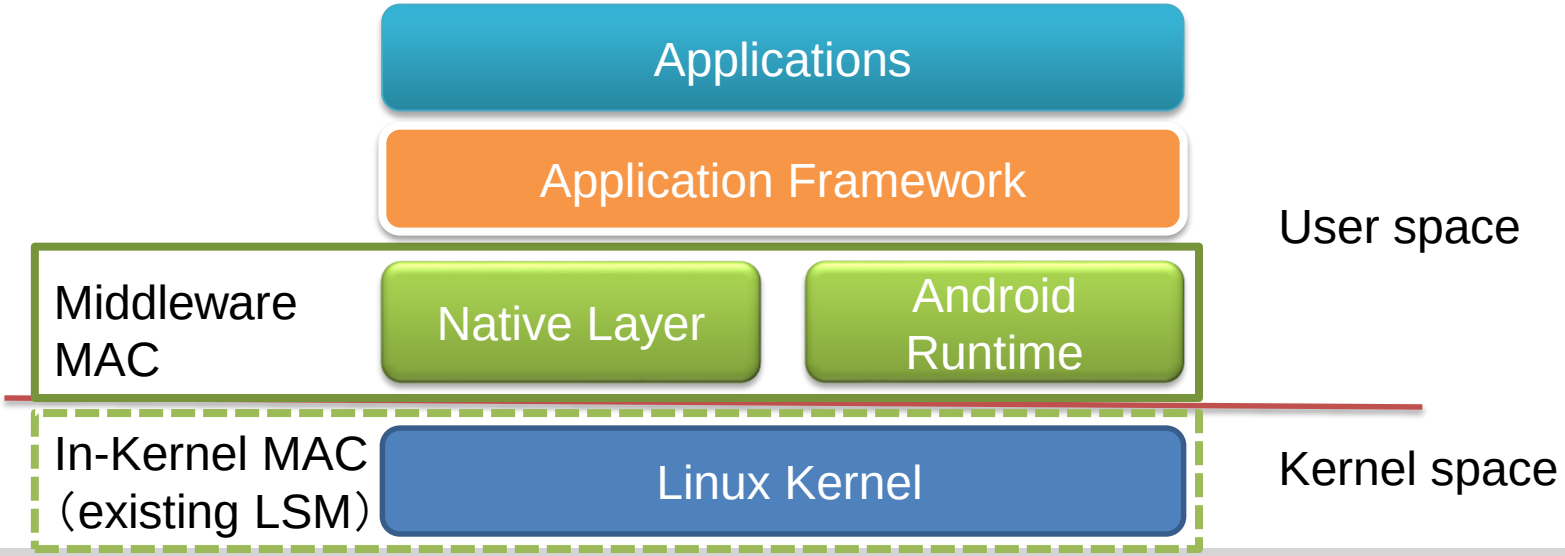
- ユーザーランドの整備
  - Bionic Libcの拡張
  - SELinuxライブラリやツールの移植

MAC : Mandatory access control（強制アクセス制御）

Middleware MACの必要性

- SELinuxは本来カーネルを経由するイベント、データしかチェックすることができない
  - Zygoteのようなユーザーランドの実行単位管理とは合わない

- SE for Androidでは、Zygote, Runtime(Dalvikなど）, installdなど native layerにアクセス制御機構を追加



Install-time MAC

- PackageManagerServiceが強制アクセス制御をおこなう
  - アプリ証明書とseinfoという識別子をマッピングする
    - external/sepolicy/mac_permissions.xml
  - ホワイトリスト/ブラックリストを用いてアプリの実行管理が可能

- installdがPackageManagerServiceのマッピング結果を用い、seapp_contextポリシーを使ってプロセスをラベル付けする

- アプリの起動時、zygoteはこのラベルを使ってドメイン遷移する

seapp_contexts

sepolicy/seapp_contexts:

isSystemServer=true domain=system_server
user=system domain=system_app type=system_app_data_file
user=bluetooth domain=bluetooth type=bluetooth_data_file
user=nfc domain=nfc type=nfc_data_file
user=radio domain=radio type=radio_
user=shared_relro domain=shared_r
user=shell domain=shell type=shell_
user=_isolated domain=isolated_app
user=_app seinfo=platform domain=platform_app type=app_data_file
user=_app domain=untrusted_app type=app_data_file

プリインストールされたアプリなどをseinfoの値で識別、3rd-partyとは違うドメインとする

3rd-partyアプリは基本untrusted_app

Enterprise Ops & Intent Firewall（開発中）

- Enterprise Ops(eops)
  - 端末開発ベンダーが、特定のアプリに特定のパーミッションを与えないような設定が可能
  - 4.3以前のpermission revocation mechanismを置き換える
- Intent Firewall
  - Intentを要求元アプリや要求先アプリに基づいて制限する仕組み
  - 4.3以前のIntent MACを置き換える

```
<?xml version="1.0"?>
<app-ops>
    <debug/>
    <seinfo name="system">
        <op name="CAMERA"/>
    </seinfo>
</app-ops>
```

例1：systemラベルが割り当てられているアプリのカメラ起動を禁止するeopsポリシー

```
<?xml version="1.0"?>
<rules>
    <service log="true" block="true">
        <not><sender type="system"/></not>
        <intent-filter />
            <component-filter
name="com.se4android.isolatedservice/.DemoIsolatedService"/>
    </service>
</rules>
```

例2：DemoIsolatedServiceからシステムアプリ以外を呼び出せなくするintent firewallポリシー

まとめ

- SE for Androidは、アプリ、プラットフォームのセキュリティを向上させ、同時に、特別なセキュリティ要求があるカスタマーの需要を満たすセキュリティ拡張が実現できる

- Android端末開発者は、AOSPに取り込まれた機能、取り込まれる予定のSE for Android機能を把握しておく必要がある
  - 例えば特別なデバイスを使うプリインストールアプリに対し、適切にポリシーを設定しておかないと、動作しなくなる可能性がある

- 今後は3rd-partyアプリに対してもenforcingモードが適用されるため、アプリ開発者も意識する必要がある

参考文献

- Security Enhancements (SE) for Android™
  http://seandroid.bitbucket.org/
- Security Enhanced (SE) Android: Bringing Flexible MAC to Android, 20th Annual Network and Distributed System Security Symposium (NDSS '13), Feb 2013.
  http://www.internetsociety.org/sites/default/files/Presentation02_4.pdf
- Security Enhancements (SE) for Android, Android Builders Summit 2014, Apr 2014.
  http://events.linuxfoundation.org/sites/events/files/slides/abs2014_seforandroid_smalley.pdf
- The Flask Security Architecture: System Support for Diverse Security Policieshttp://www.nsa.gov/research/_files/publications/flask.pdf
- NB SEforAndroid 1
  http://selinuxproject.org/page/NB_SEforAndroid_1
- NB SEforAndroid 2
  http://selinuxproject.org/page/NB_SEforAndroid_2
- Iintent firewall(unofficial documentation)
  http://www.cis.syr.edu/~wedu/android/IntentFirewall/

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research