Androidにおける情報伝搬の追跡と漏洩防止手法の提案

岡山大学大学院自然科学研究科
工学部情報系学科　　山内研究室

1.はじめに

(1)Androidにおいて，情報漏洩を狙ったマルウェアが増加

⇒ Androidは多くの個人情報を保存
　APIの利用により個人情報の取得が容易

(2)利用者はマルウェアによる情報漏洩を検知困難

⇒ 他のAPとの連携や個人情報の取得のタイミングを検知困難

＜提案手法＞

(1)APIとインテントの使用のフックによる情報伝搬の追跡と利用者のAPI使用可否入力による情報漏洩の防止

⇒ マルウェアによる情報漏洩の検知と防止

(2)情報伝搬経路の可視化

⇒ 利用者のAPIの使用可否入力時に判断を支援

2.Androidのセキュリティ機構

＜Androidのパーミッション＞

必要最低限のアクセス許可をAPに与えることで資源の安全を保つ機能

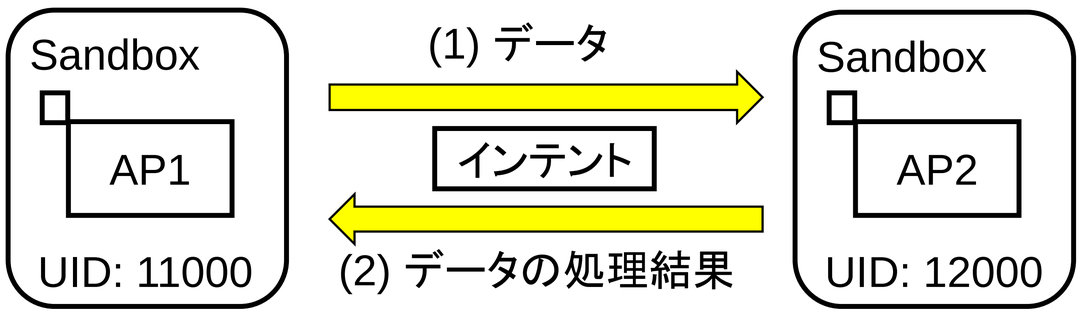
APは，標準では個人情報を取得するAPIと外部と通信をするAPIの使用不可

⇒ APは利用者にAPIの使用の許可を要求

- インターネットに接続する許可（INTERNET）
- 端末の情報を読み込む許可（READ_PHONE_STATE）

＜Androidのインテント＞

Androidにおいて異なるUser ID(UID)をもつAP間での連携を実現



- AndroidのAPはサンドボックス内で動作
- APごとに異なるUIDが指定

⇒ 通常，異なるUIDをもつAP間での連携不可

3.情報漏洩防止手法の基本方式

＜Androidフレームワークの変更点＞

(1)個人情報取得APIと，情報伝搬APIをフックし，利用者に，APIを使用したAPと使用されたAPI名を提示

⇒ APがいつ，どのような個人情報を取得し，外部と通信しているか検知可

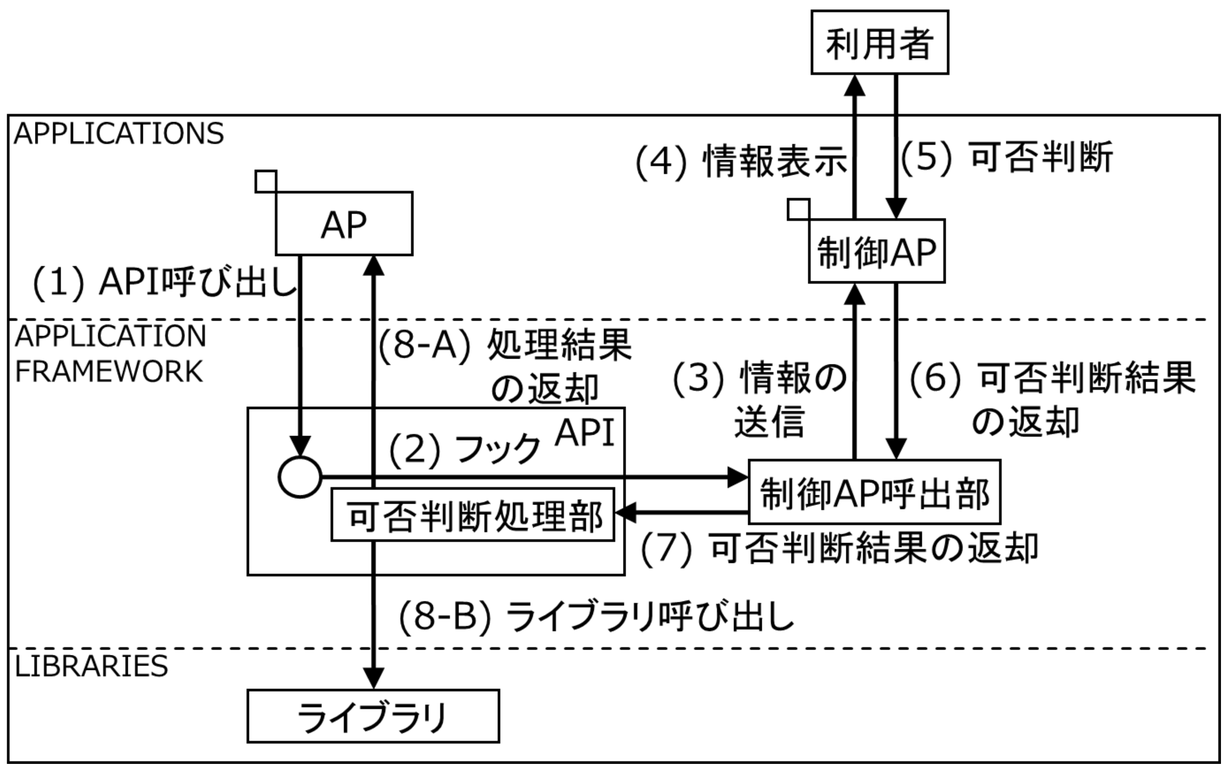
(2)インテントの使用をフックし，利用者インテントを使用したAP名と，インテントにより呼ばれたAP名を提示

⇒ インテントの使用による個人情報の伝搬を検知可

(3)利用者は，APIまたはインテントの使用可否を入力し，フレームワークは入力結果に応じた処理を実行

利用者が拒否を入力することで情報漏洩を防止

4.APIの制御の流れ



5.動作例

評価APを作成し実行

＜評価AP＞

(1)　電話番号を取得するgetLine1Numberを使用
(2) sendTextMessageを使用して取得した個人情報を外部へ書き出し

警告表示時
APIの使用を
(1)許可するなら「はい」
(2)拒否するなら「いいえ」
を押下

⇒

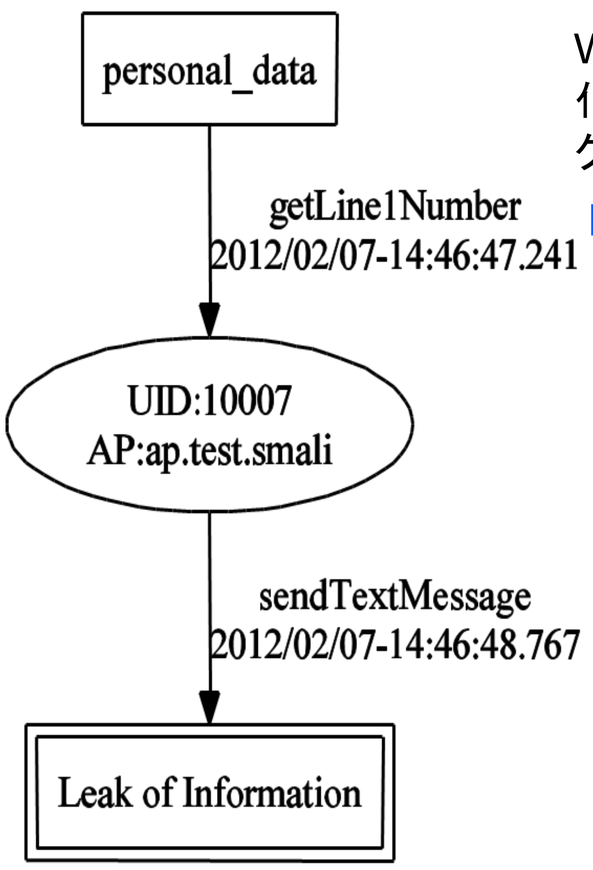
APIの使用を拒否することで情報漏洩を防止

6. Windows上での可視化の実現

＜Android上のログの取得＞

Windows上で情報伝搬経路を可視化するため，制御APの保持するログファイルを取得

⇒ 現段階ではAndroid上での可視化は未実装



(1) 個人情報を「personal_data」と表記
(2) 外部への情報漏洩を「Leak of Information」と表記
(3) APのUIDとAP名を楕円で表記
(4) 情報の伝搬を矢印で表記し，API名とAPIの使用時刻を表記