細粒度の情報追跡による機密情報送信の動的制御手法

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

(2)機密情報の漏洩防止に関する様々な手法が研究

誤検知，AP の動作の妨害，および一般の利用者では理解や操作が難しいなどの問題がある

＜提案手法＞

(1)細粒度の情報追跡による機密情報送信の動的制御
(2)AP の通常の動作を妨害しない機密情報の漏洩防止
(3)利用者の負担の軽減と判断の支援

2.機密情報を漏洩させるアプリ

(1)全国電話帳

- Google Playで実際に配布され，76万人の個人情報を流出させ問題
- 後に「全国共有電話帳」という名前で再配布

(2)the Movie系

- Google Playで実際に配布され，数万人～数百万件の個人情報を流出させ問題
- 「〇〇the Movie」という名前で配布

この他にも，「電池改善アプリ」や「電池長持ち」など様々な種類のアプリで個人情報の漏洩が問題となっている

機密情報の漏洩防止に関する様々な手法が研究

3.既存手法とその問題点

(1)APIに着目した手法

- APIに着目しているため，追跡粒度が粗く誤検知が多い
- 利用者に提示される情報が分かり難い

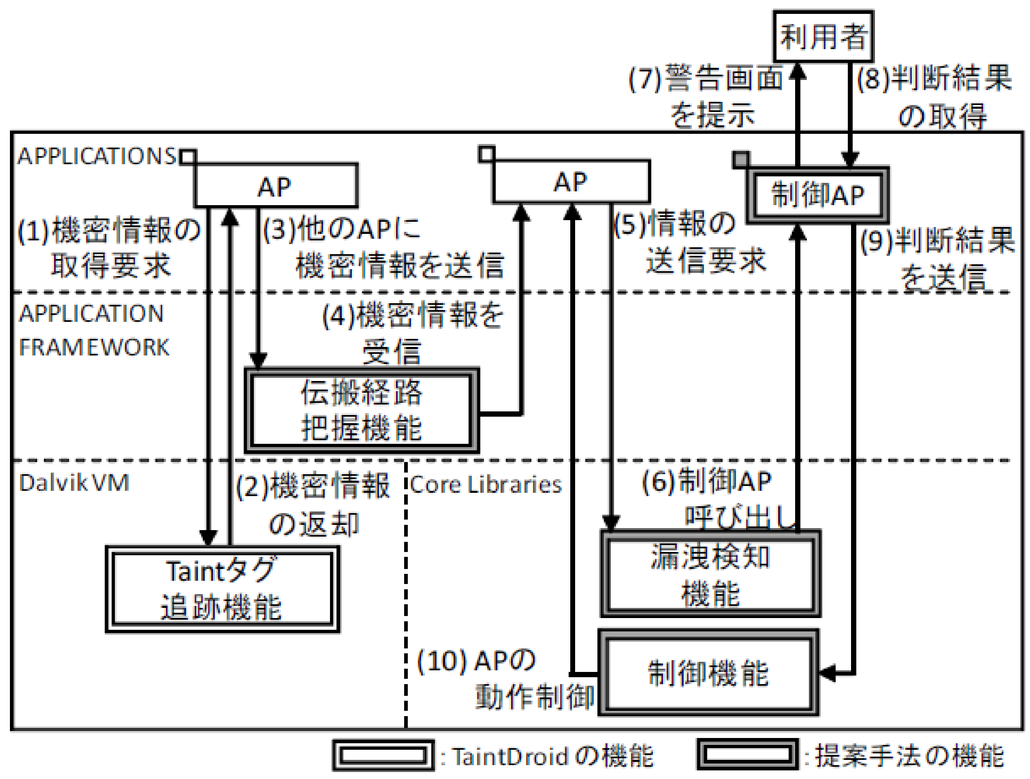
(2)ダミーデータを用いた手法

- アプリが取得する機密情報をダミーデータに置換するため，アプリの動作を妨害

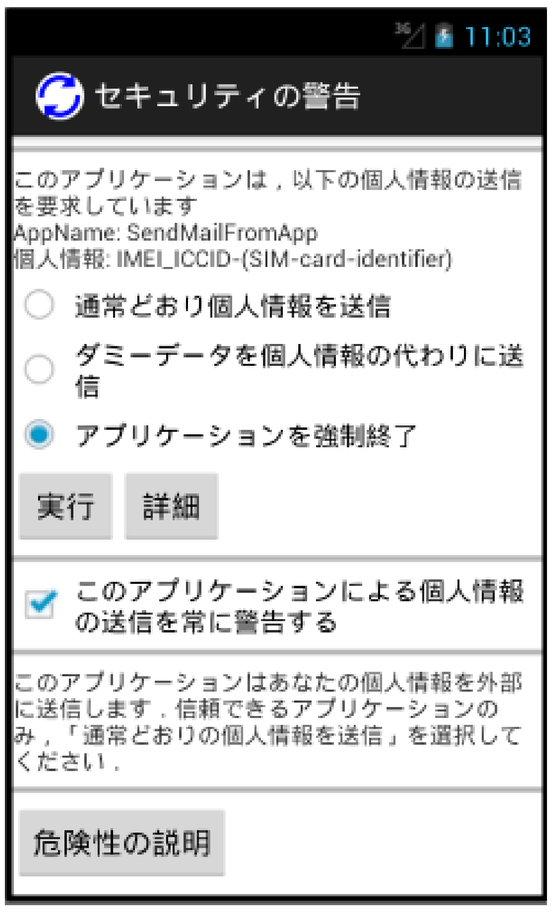
このように，既存手法にも問題点がある

既存手法の問題点を解決した機密情報の漏洩防止手法

4.全体像



5.動作例



＜評価目的＞

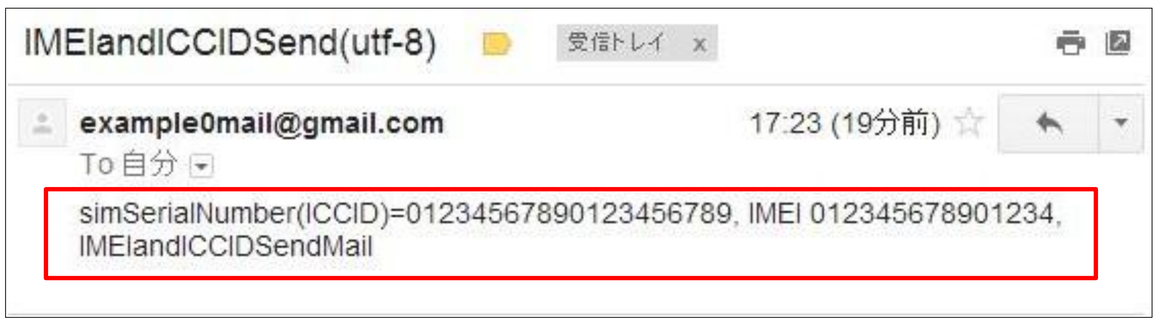
(1) 機密情報の漏洩防止の確認
(2) 外部に漏洩する機密情報の置換結果の確認

＜評価AP＞

(1) 機密情報を取得
　(A) IMEI（International Mobile Equipment Identifier）
　(B) ICCID（Integrated CircuitCard ID）
(2) Gmail を用いて端末外部に取得した情報を送信

利用者の判断に従って，APの動作を動的に制御

(1) 通常動作
　(A)「通常どおり個人情報を送信」を選択し，「実行」ボタンを押下
　(B) 端末外部に機密情報が送信される



(2) ダミーデータの送信
　(A)「ダミーデータを個人情報の代わりに送信」を選択し，「実行」ボタンを押下
　(B) 機密情報をダミーデータに置換した内容を送信