WWW2014　勉強会 Session 6 (Security 2) 3本目

Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?

Bin Liu, Jialiu Lin. Norman Sadeh

担当　：　吉國（お茶大）

概要

- スマートフォンにおけるアプリケーションのパーミッション設定は利用者にとって負荷になっている
  - 設定しなくてはいけないパーミッションの数が多い
- この論文ではパーミッション設定のデータの分析結果をレポートしている
  - ユーザの負担が少なくて，かつ希望に近いパーミッションの設定ができることを目指す

Data Collection

- LBE Privacy Guard
  - Android用のセキュリティアプリケーション
  - Root化状態のAndroid上で利用可能
  - 各アプリケーションのパーミッション設定を管理する
- LBEのデータセットを用いて分析を行う
  - LBEを利用している4.8Mユーザのデータを利用
  - そのうち，パーミッションを自分で設定し，かつ最低20個以上のAppを持つユーザ
  - またデータセット内の10人以上がインストールしているApp

- 239,402 representative users
- 12,119 representative apps
- 28,630,179 records

Data analysis

- ユーザの各パーミッションに対する設定についてモデル化する
- $f:(user, app, permission) \rightarrow decision$
- $decision$："Allow" or "Deny“
- 線形カーネルSVMを使って分類
  - ユーザをランダムに10個のグループに分割
  - 9個をトレーニングセット，残りをテストセットとする
  - テストセットのユーザがインストールしているアプリケーションの20%を選択
  - このアプリケーションのdecisionを推定する

Data analysis

- Preferences P における行列を生成
- Model 1 :
  - $\#User \times \#Permissions$
  - $Permissions$：LBEが管理しているパーミッション12個
- Model 2 :
  - $\#User \times \#app\_permissions$
  - $app\_permissions$: Appが要求しているパーミッション
  - スパースであるため特異値分解を用いてサイズを小さくしている

Data analysis

Table 1: Feature Compositions

Feature Set	Features	Description
FS-1	Permission IDs	Preference statistics of all users on apps & permissions
FS-2	App IDs	
FS-3	App ids & Permission IDs	
FS-4	User IDs	+ Users' overall preferences
FS-5	User ids & Permission IDs	
FS-6	User ids & App IDs	
FS-7	User ids, App IDs & Permission IDs	
FS-8	FS-7 appended with aggregated P[u][m] for corresponding user and permission	+ Numerical estimation of users' preferences from aggregation of permission or SVD on user and app-permission pairs.
FS-9	FS-7 appended with estimated P[u][m] for corresponding user and app-permission pairs from top-200 apps	
FS-10	FS-7 appended with estimated P[u][m] for corresponding user and app-permission pairs from top-1000 apps	

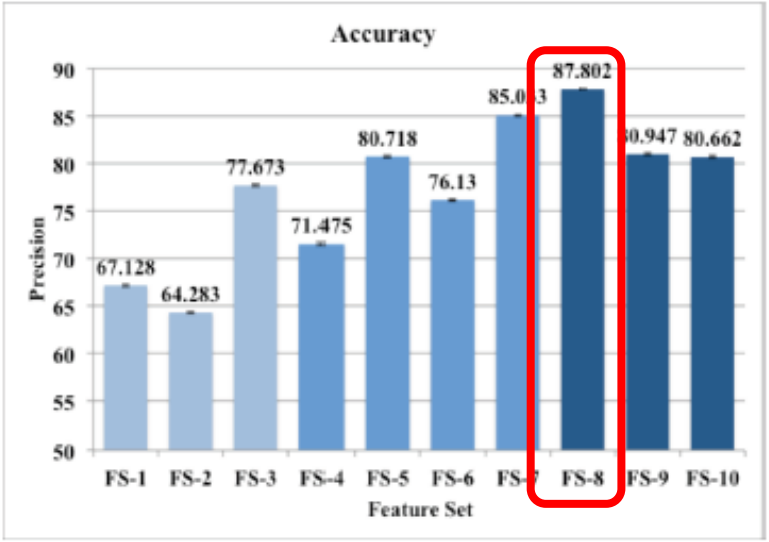

Figure 2. Accuracy of Predictions

Model 1を素性として使った時が一番結果が良かった

Data analysis

- ユーザのプライバシプロファイルを使ってクラスタリングすることでパーミッション設定の予測ができるのではないか
  - （プライバシプロファイルはいくつかユーザに質問し回答してもらうことで得られるといっている）
- Model 1 を$k-means$法でクラスタリングし分析する

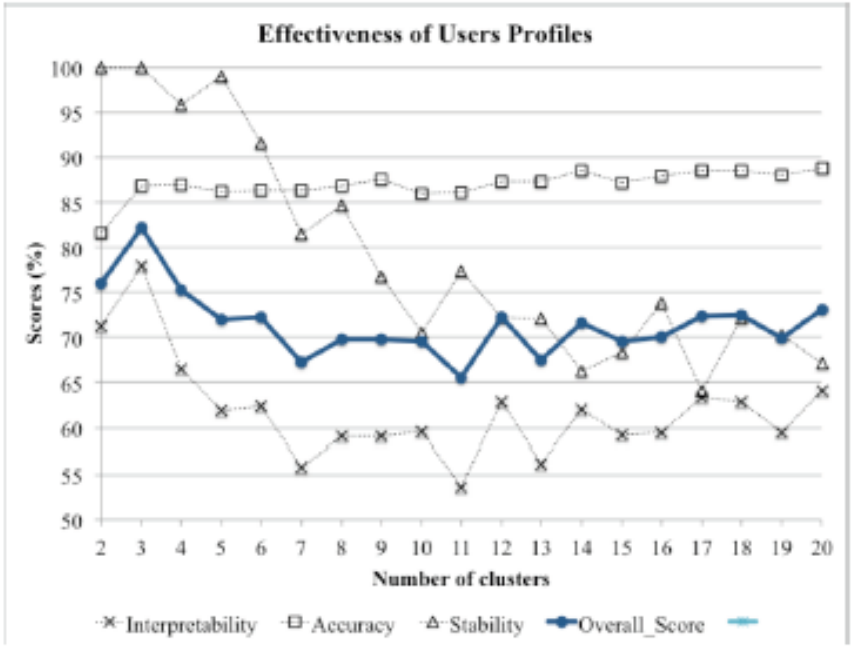

Figure 4. Effectiveness of Privacy Profiles

- クラスタ数3が良いように見える

Data analysis

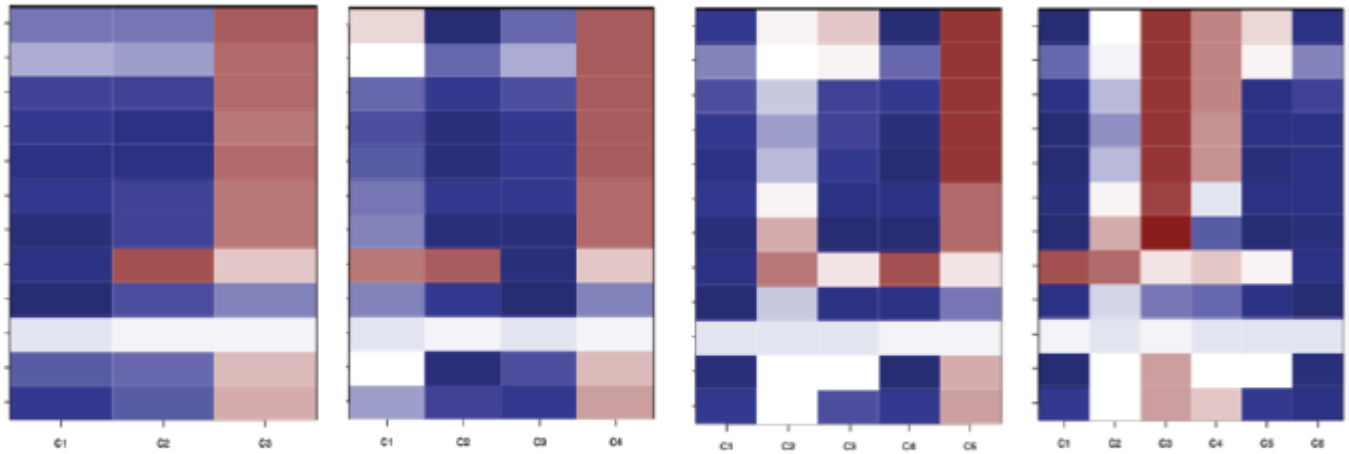

Figure 7. Colored Matrix Map of Average Preferences in Each Privacy Profile

- クラスタ数3ではプライバシレベルが高いクラスタが顕著に出ているがのこり2つは同じようになっている
- クラスタ数6ぐらいになるとプライバシレベルが最も高いクラスタのほかに，異なるプライバシレベルを持つクラスタをみることができる