Permission Model

Nitin Satpal

M.Tech. CSE,

Indian Institute of Technology Bombay

Outline

- Introduction
- Literature survey
- Conclusion

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

Introduction

- Smartphone popularity
- Role of Android

Introduction

- App development in Android
- Over 25 billion downloads

Introduction

- Risk involved
- Malicious apps can be uploaded

Introduction

- Private data can be stolen
- Current permission model is not sufficient

Permission Model of Android

- Coarse-Grained Model
- User is bound to accept all the permissions for successful installation

Drawback

- Random permission can be requested at the time of installation

- It can then be misused once user grants the access

Solution

- Fine-Grained Permission model

Outline

- Introduction
- Literature survey
- Conclusion

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

TISSA [1]

- Permission Category: Trusted

  'Trusted' works same as the current permission model of Android

TISSA

- Permission Category: Anonymized

  ‘Anonymized’ gives anonymized version of original data

TISSA

- Permission Category: Bogus

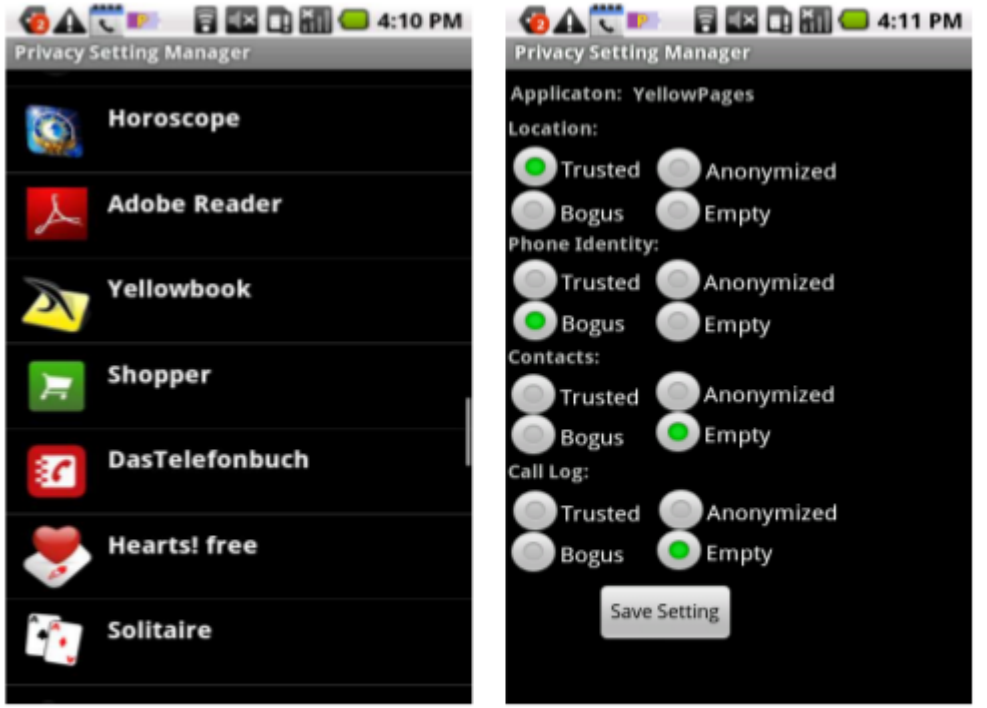
  'Bogus' provides fake result to the requested app

TISSA

- Permission Category: Empty

  ‘Empty’ gives empty results to the requested app

TISSA



(a) A list of installed apps

(b) The privacy settings for the *YellowPages* app

Figure: Paper Toss

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

TISSA

- Behavior of the app will change accordingly
- No runtime control

Mockdroid [2]

- Mockdroid provides user a real runtime control
- It works very similar to TISSA in mocking the permissions
- E.g.: Empty data, random device id, etc.

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

Paper Toss

- ‘Paper Toss’ should not require internet Permission
- User can mock the internet permission
- User can give legitimate internet permission at runtime

Paper Toss

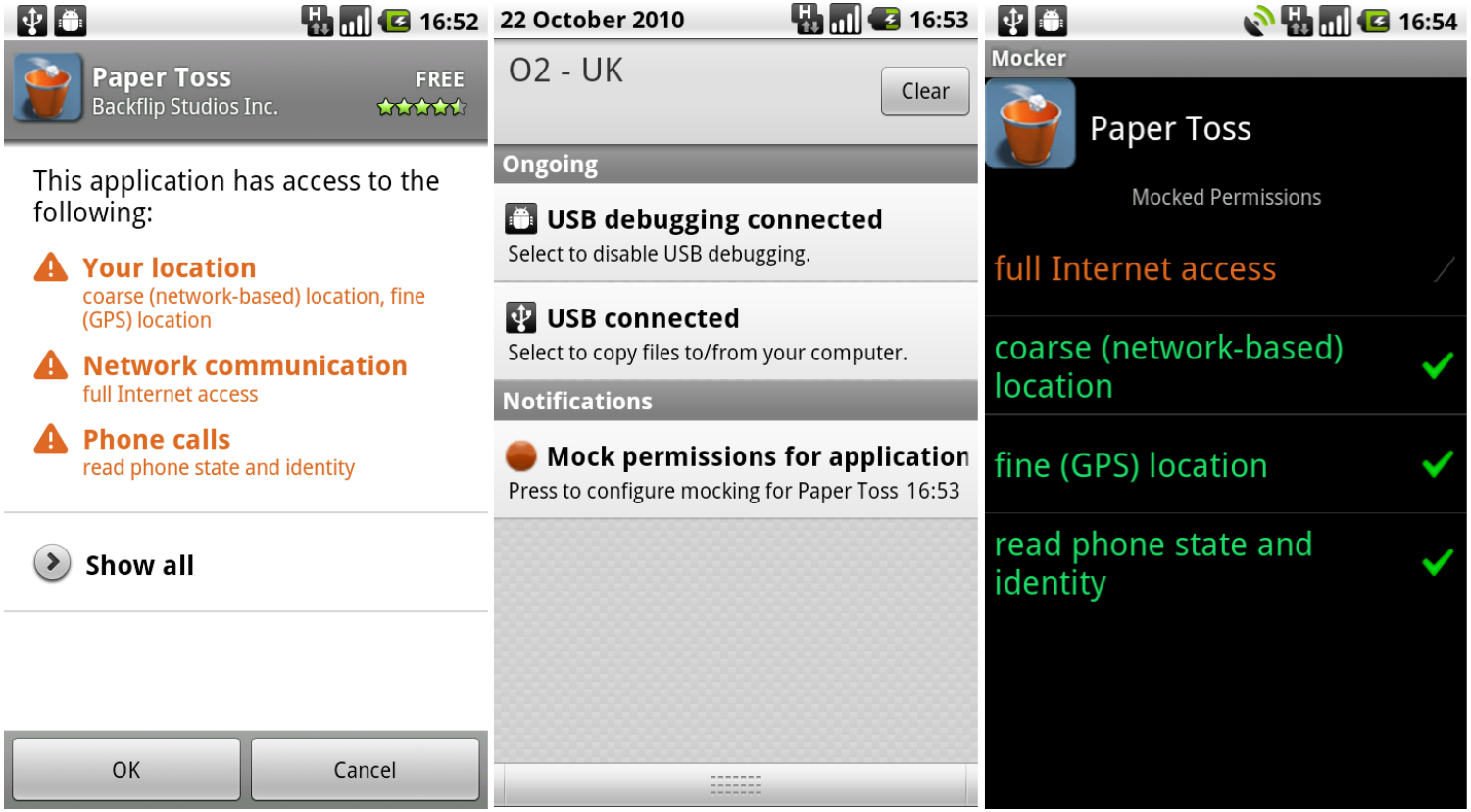


Figure: Paper Toss

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

Outline

- Introduction
- Literature survey
- Conclusion

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

Conclusion

- We compare the existing ideas of permission model
- We will implement and integrate TISSA and Mockdroid

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

References

1. Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and Vincent W. Freeh. Taming information-stealing smartphone applications (on android). In Proceedings of the 4th international conference on Trust and trustworthy computing, TRUST'11, pages 93–107, Berlin, Heidelberg, 2011. Springer-Verlag.

2. Alastair R. Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. Mockdroid: trading privacy for application functionality on smartphones. In Proceedings of the 12th Workshop on Mobile Computing Systems and Applications, HotMobile '11, pages 49–54, New York, NY, USA, 2011. ACM.