Practical Course
ANDROID Security

Alei Salem
Chair for Software and Systems Engineering (I4)
Prof. Dr. Alexander Pretschner

Android Facts

- 80% market share
- 550,000 activations per day
- Attracts a lot of (unnecessary) attention
- Targeted by 97% of mobile malware
- 2000 samples discovered per day

Android Security Issues

- Vulnerable apps
- Repackaging/Piggybacking

Android Security Issues

- Vulnerable apps enable:
  - Leak private data e.g. contacts
  - Steal license keys
  - Hijack accounts
  - Pirate/piggyback software

Android Security Issues

- Repackaging is a common practice.

1. Download legitimate app,
2. decompile APK,
3. insert (malicious) payload in code,
4. recompile, sign, upload to marketplace.

Repackaging

- Trendmicro in 2015*:
  - 77% of the top 50 free apps on Play Store have fake versions
  - As of April 2015: 890,482 fake apps were discovered
  - 51% of which are malicious.
- Total apps on Play Store → approx. 2,200,000

* https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fake-apps.pdf

Repackaging: Examples

- Durak
  - 5-10 million downloads.
  - Dormant for 30 days.
  - Ads with phone unlocking.

- Fake BBM Messenger

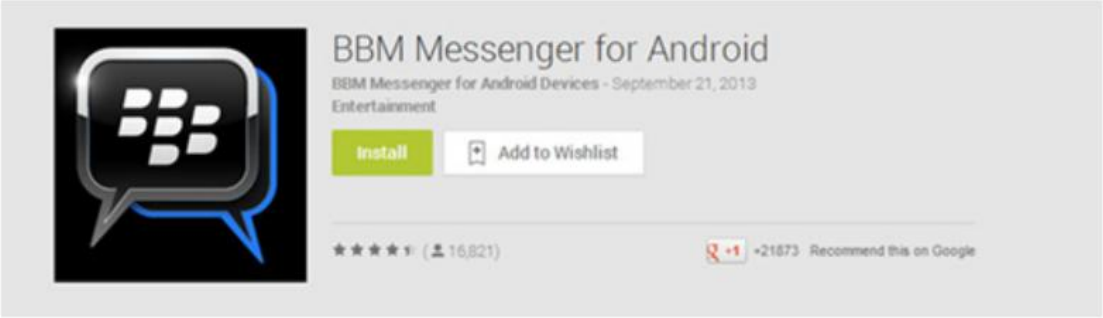


Figure 10: Google App download page for fake BBM for Android

Repackaging: Examples

- Other payloads?
  - Delete contacts, spy using camera, SMS to premium numbers, steal WiFi credentials, location tracking, encrypt data for ransoms, etc.
  - Logic bombs.

Topics Covered

- Basics
  - Android app components and permissions
  - Android security architecture
  - Environment Setup
- Common Vulnerabilities
  - Logging Vulnerabilities
  - Leaking Content Providers
  - Input Validation Issues
  - Tapjacking
  - Access Control Vulnerabilities
  - Hardcoding Vulnerabilities

Topics Covered

- Reverse Engineering
  - Reverse engineering APKs
  - Patching and hooking APKs
  - Repackaging benign apps with malicious content
  - Integrity protection

- Malware Analysis and Detection
  - Manual analysis of malware
  - Automated analysis and feature extraction
  - Detection (with machine learning)

Course Plan

- Work in teams 2-3
- Phase I: Weekly exercises/submissions (50%)
- Phase II: A research project + presentations (50%)

Course Plan: Phase I

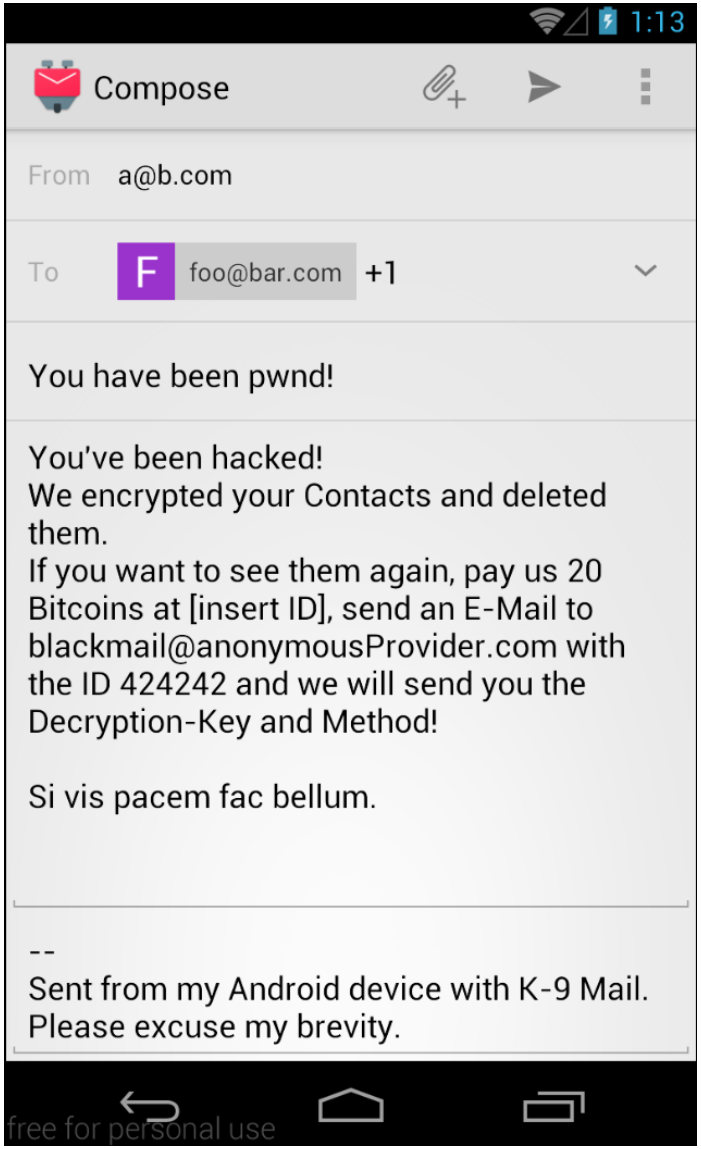
- More like CTF challenges
  - Exploit vulnerable apps
  - RE and algorithm extraction
  - Retrieving a secret/key from an app
  - Repackage apps

- Submit a short report containing:
  - The secrets/keys/functionalities you elicited
  - What tools/techniques you used?
  - Break down of “who did what”

Course Plan: Phase II

- Pick a related topic to research:
  - An attack you wish to investigate/develop
  - A tool to defend against some attack(s)
  - A malware analysis/detection tool/approach
- I will help you choose a topic:
  - Proposing some topics
  - Brainstorming
- Present the project + submit code + submit a report

Course Plan: Phase II



Course Plan: Phase II

```
Enter "exit" any time to abort.
Choose between the following options and input the respective number:
READ_CONTACTS = 1, DELETE_CONTACTS = 2, READ_SMS = 3;, SEND_SMS = 4, EXEC_CMD = 5, DISCONNECT=99
1
Command sent.
Contacts:

Clinton Wheatley
MOBILE: 512-625-2531
EMAIL: ClintonWWheatley@gustr.com

Steve Hopkins
MOBILE: 641-251-9199
EMAIL: SteveAHopkins@fleckens.hu

Alisa Priest
MOBILE: 918-318-8435
EMAIL: AlisaMPriest@jourrapide.com

Robert Lovell
MOBILE: 219-809-3025
EMAIL: RobertDLovell@gustr.com

John Davis
MOBILE: 919-440-8664
EMAIL: JohnMDavis@gustr.com

Francisco Miller
MOBILE: 810-891-8482
EMAIL: FranciscoTMiller@armyspy.com

Steven Thornton
MOBILE: 215-621-6671
EMAIL: StevenMThornton@teleworm.us

Robert Lopez
MOBILE: 773-843-6802
EMAIL: RobertCLopez@teleworm.us

Elizabeth Keene
MOBILE: 573-453-3275
EMAIL: ElizabethJKeene@fleckens.hu

Floyd Copeland
MOBILE: 417-354-2499
EMAIL: FloydCCopeland@gustr.com

Julio Anderson
MOBILE: 507-922-3091
EMAIL: JulioIAnderson@fleckens.hu

Elliott Gonzalez
MOBILE: 229-518-7981
EMAIL: ElliottDGonzalez@teleworm.us

Gordon Lord
MOBILE: 301-767-0608
```

Miscellaneous

- Registration: Using the matching system
  - http://matching.in.tum.de
  - Advantage: fill up this questionnaire

- Administrative:
  - Language: English
  - B.Sc. + M.Sc.
  - Max. members: 15
  - Day/time/location: TBD

Thank you

Questions?