Reproducing Vote Verification Application Builds for Estonian I-Voting System

Report in Research Seminar in Cryptography (MTAT.07.022)

Annika Tammik

December 5, 2017

Introduction

Internet voting and Vote Verification Apps

- Internet voting in Estonia (from 2005)
- In 2011 several potential attacks were published
- From 2013 possibility to verify cast vote with a mobile device
  - Android and iOS supported
  - Distributed in Google Play Store and iOS App Store
  - Source code available in Estonian National Electoral Committees GitHub repository

Objective of the work

Verify if binary distributed during I-voting held in October 2017 matches the source code published in GitHub

Tasks

- Monitoring the Apps in the App Stores
- Building the Android Vote Verification App from Source Code
- Reproducing the Android Vote Verification App
- Recommendations for VVA Developers

Monitoring the Apps in the App Stores

- Downloading Android apps
  - Unofficial web-sites
  - Downloading tools
  - Google Play Unofficial Python API
    - No monitoring functionality
    - Google Play Store App Monitor
- Downloading iOS apps
  - Web-sites with a promise
  - No downloading tools
  - Removed functionality from iTunes
  - No relevant documentation

Downloaded Android Binaries

I-voting period from 5th until the 11th of October 2017

1. ee.ivxv.ivotingverification 21.apk[1] (downloaded on October 2, 2017)
2. ee.ivxv.ivotingverification 22.apk[2] (downloaded on October 10, 2017)
   - recentChangesHtml: "Parandused seoses uuendamata ID-kaartidega"

---

[1] SHA256: 35dac3859ffbe4d85acd20e51c117f17425b26e2db4520ce9aea7533e7583c94

[2] SHA256: cbb1f86cebfcd2c02715e6ca2999b5d609ab6aecb092115d25b205ddc00f221b

Building the Android App

- Lack of documentation / required versions information
- Assumptions based on the technology stack
  - Android SDK
  - Java JDK
  - Gradle
- Assumptions based on the runtime errors
  - Dependencies in the lib folder

Reproducing the Android Vote Verification App

- Expected differences
  - Signed vs un-signed
  - Only one commit in GitHub (from the 3rd of September)
  - Version differences in ivotingverification/app/build.gradle (vc. 16 and vs. 3.1.3 versus vc. 21 and vs. 3.1.7)
  - Versions of dependencies
- Comparing the binaries
  - Different tools available (diffoscope and apkdiff)
  - Challanges in related to the reproduction

diffoscope

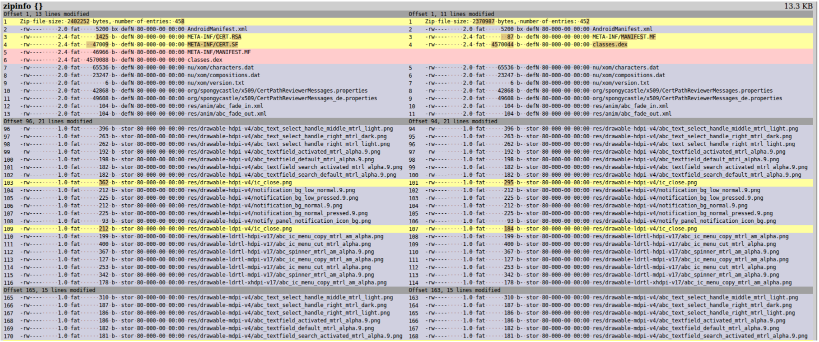

Figure: Output from diffoscope

Recommendations for VVA Developers

- Detailed build instructions
- Commit tags for build versions
- Updated source code

Thank you!

Questions?