# 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<sup>1</sup> (downloaded on October 2, 2017)
- 2. ee.ivxv.ivotingverification 22.apk<sup>2</sup> (downloaded on October 10, 2017)
  - recentChangesHtml: "Parandused seoses uuendamata ID-kaartidega"

<sup>&</sup>lt;sup>1</sup>SHA256:

## 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

```
zipinfo {}
Offset 1, 13 lines modified
                                                                                                                                                                                                                                                   13.3 KB
      Zip file size: 2482252 bytes, number of entries: 458
                                                                                                                                   Zip file size: 2370987 bytes, number of entries: 452
    -rw-----2.0 fat ---5200 bx defN-80-000-00-00:00 AndroidManifest.xml
                                                                                                                                  -rw-----2.0-fat----5200-bx-defN-80-000-00-00:00-AndroidManifest.xml
                            TADE h. Hafty co. occ. oc. oc. oc. META, THE /FEST BEA
                                                                                                                                                          WIRE No. Harfty no. non-no. no-no. MCTA. THE MANTEE'ST ME
                2.4 fat 47609 b- defn 80-000-00 00:00 META-INF/CERT.SF
                                                                                                                                               2.4 fat 4570044 b. defN 88-800-80 00:00 classes.dex
     - Dat - - - - - 2 . 4 - fat - - - 46966 - b - - doffn - 60 - 000 - 00 - 00 - META - TNE / MANTEEST - MI
                -2.4 fat - 4570000 b- defN 80-000-00-00:00 classes.dex
     -ne---- 2.0 fat 65536 b- defN 80-000-00 00:00 nu/xom/characters.dat
                                                                                                                                 -rv----- 2.0 fat 65536 b- defN 80-600-00 00:00 ru/xen/characters.dat
     -rw-----2.0 fat --23247 b- defN 80-000-00-00:00 nu/xom/compositions.dat
                                                                                                                                  -rw-----2.0-fat---23247-b--defN-80-600-00-00-00-nu/xon/compositions.dat
                             --- 6-b--defN-80-000-00-00:00-nu/xom/version.txt
                                                                                                                                                           --- 6-b--defN-80-000-00-00:00-nu/xom/version.txt
      -rw----- 2.0 fat
                           42868 b- defN 80-000-00 00:00 org/spongycastle/x509/CertPathNeviewerMessages.properties
                                                                                                                                                         42868 b - defN 80-800-80 00:00 org/spongycastle/x509/CertPathReviewerMessages.properties
               -- 2.8 fat
                           -49668 b--defW 88-888-88 08:88 org/spongycastle/x589/CertPathReviewerMessages_de.properties
                                                                                                                                  -rw------2.8-fat-
                                                                                                                                                         49688 b. defN 88-888-88 88:88 org/spongycastle/xS89/CertPathReviewerMessages_6e.properties
    -Dr------2.8-fat-
                           --- 184 b -- defN-88-888-888-88-88-res/anim/abc fade in.xml
                                                                                                                              18 - Dr ---- 2.9 fat
                                                                                                                                                           -104-b--defN-80-800-00-00:00-res/anin/abc fade in.xnl
                             104 b- defN 80-000-00 00:00 res/anim/abc fade out.xm
                                                                                                                                                           104 b. defN 00-000-00 00:00 res/anim/abc fade out.xm
Offset 96, 21 lines modified
                                                                                                                              Offset 94, 21 lines modified
                             296 b- stor 80-000-00 00:00 res/dravable-hdpi-v4/abc text select handle middle mtrl light.prg
                                                                                                                                                           396 b- stor 80-800-80 00:00 res/dramable-hdpi-v4/abc text select handle middle mtrl light.png
    263 b- stor 88-888-88 88:88 res/drawable-hdpi-v4/abc_text_select_handle_right_mtrl_dark.pmg
                                                                                                                                                           263-b--stor-88-600-88-60:88-res/drawable-hdpi-v4/abc_text_select_handle_right_mtrl_dark.png
                             -262-b--stor 80-000-00-00:00-res/drawable-hdpi-v4/abc_text_select_handle_right_mtrl_light.png
                                                                                                                                                            262 b--stor-80-000-00-00-00-res/drawable-hdpi-v4/abc_text_select_handle_right_mtrl_light.png
99 - DE-----
                             192 b- stor 80-900-00 00:00 res/drawable-bdoi-v4/abc textfield activated mtrl alpha.9.pmg
                                                                                                                                                           192 b. stor 80-000-00 00:00 res/dramable-hdoi-v4/abc textfield activated mtrl alpha 9.000
                             198 b. stor 88-888-88 88:80 res/drawable-hdpi-v4/abc textfield default mtrl alpha.9.pmp
                                                                                                                                                           198 b. stor 88-888-88 88:88 res/drawable-hdoi-v4/abc textfield default mtrl aloha,9.ong
100 -Di-----
                             -182-b -- stor 80-000-00-00:00-res/drawable-hdpi-v4/abc textfield search activated mtrl alpha.9.png
                                                                                                                                                           182-b--stor-80-600-00-00:00-res/drawable-hdpi-v4/abc textfield search activated mtrl alpha.9.png
192 -m-----
                -- 1.0 fat-
                             -182 b- stor 80-000-00-00-00-res/drawable-hdpi-v4/abc textfield search default mtrl alpha.9.pmg
                                                                                                                                   - PM------
                                                                                                                                                           -182 b. stor 88-800-90 00:00 res/dramable-hdpi-v4/abc textfield search default mtrl alpha.9.psg
                              362 b- stor 88-888-88 00:00 res/dravable-hdpi-v4/ic
                                                                                                                                                            285 h. stor an.een.ee en en reszéravable.hén
               -- 1.8 fat
                             212 b - stor 88-898-88-88:68 res/drawable-hdpi-w4/notification_bg_low_normal.9.png
                                                                                                                                                           212 b stor 88-88-88 88 88: res/drawable-hdgi-v4/notification_bg_low_normal.9.png
                             -225 b- stor 80-000-00-00-00-res/drawable-hdpi-v4/notification bg low pressed.9.png
185 - De-----
                                                                                                                              183 - pe----- 1.0-fat
                                                                                                                                                           -225 b- stor-80-800-00-00:00 res/draumble-hdoi-v4/notification bo low pressed.9.ong
                             212 b- stor 80-000-00 00:00 res/drayable-hdpi-v4/notification bg normal.9.png
106 - De-----
                                                                                                                              184 -ry----- 1.0 fat-
                                                                                                                                                           212 b- stor 80-800-00 00:00 res/drawable-hdoi-v4/notification bo normal,9.pmg
107 - De-----
                             225 b. stor 80-000-00-00-00 res/drayable-hdpi-v4/notification bg normal pressed.9.pmg
                                                                                                                                                           225 b. stor 88-888-88 98:88 res/drawable-hdpi-v4/netification_bg_normal_pressed.9.png
188 - rw-----
                             - 93 b--stor-80-000-00-00:00-res/drawable-hdpi-w4/notify panel notification icon bg.png
                                                                                                                              186 - rw------ 1.0-fat-
                                                                                                                                                           - 93-b--stor-80-000-00-00:00-res/drawable-hdpi-v4/notify panel notification icon bg.png
                                    stor 80-000-00 00:00 res/drawable-ldpi-v4/i
                                                                                                                                                            184 b. stor 00-000-00 00:00 res/dramable-l
110 -rw----- 1.0 fat
                             199 b. stor 88-888-88 88:88 res/dravable-ldrtl-hdpi-v17/abc_ic_menu_copy_mtrl_am_alpha.png
                                                                                                                              108 - Ov----- 1.8 - fat
                                                                                                                                                           199 b. stor 88-888-88 88:88 res/drawable-ldrtl-hdp1-v17/abc_ic_menu_copy_mtrl_am_alpha.png
111 - pe---- 1.8-fat
                             -490 b - stor 80-000-00-00:00 res/dravable-ldrtl-hdpi-v17/abc ic menu cut mtrl alpha.ong
                                                                                                                              169 - Dr .... 1.0 fat
                                                                                                                                                           -400 b - stor-80-000-00-00:00 res/dravable-ldrtl-bdoi-v17/abc ic menu cut mtrl alpha.ong
112 - pr----- 1.0 fat
                             367 b. stor 80-000-00 00:00 res/drayable-ldrtl-hdpi-v17/abc spinner mtrl am alpha.9.peg
                                                                                                                              118 - pe---- 1.0 fat-
                                                                                                                                                           367 b. stor 80-800-00 00:00 res/drausble-ldrtl-hdoi-v17/abc spinner mtrl am alpha.9.pnp
                                                                                                                                                           127 b. stor 88-888-88 88:88 res/drawable-ldrtl-mdpi-v17/abc_ic_menu_copy_mtrl_am_alpha.png
111 -ne---- 1.0 fat
                             127 b. stor 88-888-88 88:88 res/dravable-ldrtl-mdoi-v17/abc ic menu copy mtrl am alpha.ong
                                                                                                                              111 -rw----- 1.0 fat-
114 - m-----
                             -253 b - stor 80-000-00-00:00 res/dravable-ldrtl-mdpi-v17/abc ic menu cut mtrl alpha.ong
                                                                                                                                   -rw------1.0-fat-
                                                                                                                                                           -253 b--stor-80-000-00-00:00-res/drawable-ldrtl-mdgi-v17/abc ic menu cut mtrl alpha.png
                              342 b stor 80-000-00 00:00 res/drawable-ldrtl-mdpi-v17/abc spinner mtrl am alpha.9.pmg
                                                                                                                                                           342 b. stor 80-800-00 00:00 res/draumble-ldrtl-mdpi-v17/abc spinner mtrl am alpha.9.png
115 -rw------ 1.0 fat
                                                                                                                              113 -rw----- 1.0-fat-
                              178 b- stor 80-000-00 00:00 res/dravable-ldrtl-xhdpi-v17/abc ic menu copy mtrl am alpha.pmg
                                                                                                                                                           178 b. stor 80-000-00 00:00 res/drawable-ldrtl-xhdpi-v17/abc ic menu copy mtrl am alpha.png
Offset 165, 15 lines modified
                                                                                                                              Offset 163, 15 lines modified
165 -rw----- 1.8 fat
                                                                                                                                                           310 b. stor 80-800-00 00:00 res/drawable-mdoi-v4/abc text select handle middle mtrl light.onc
                                                                                                                                                            187-b--stor-88-888-88-88-88-res/drawable-mdpi-v4/abc_text_select_handle_right_mtrl_dark.png
                             -187 b- stor 88-898-89 98:80 res/drawable-mdpi-v4/abc text select handle right mtrl dark.png
167 -rw------ 1.0-fat-
                             -185 b- stor ED-000-00 00:00 res/drawable-mdpi-v4/abc text select handle right mtrl light.pmg
                                                                                                                              -186 b- stor 80-000-00 00:00 res/drawable-mdpi-v4/abc text select handle right mtrl light.pmg
168 -rw---- 1.0 fat
                             186 b- stor 88-888-88 08:80 res/dravable-mdpi-v4/abc textfield activated mtrl alpha.9.png
                                                                                                                              166 -rw----- 1.0 fat
                                                                                                                                                            186 b. stor 80-000-00 00:00 res/dramable-mdpi-v4/abc textfield activated mtrl alpha.9.pmg
169 - Pe------- 1.8-fat
                             -182 b- stor 88-888-88 88:80 res/drawable-mdpi-v4/abc_textfield_default_mtrl_alpha.9.png
                                                                                                                              167 - De------- 1.0 - fat
                                                                                                                                                            182 b. stor 88-888-88 88:88 res/drawable-mdpi-v4/abc_textfield_default_mtrl_alpha.9.pmg
128 - De----- 1.9 fat
                             - 181 b - stor 80-000-00-00-00 res/drayable-mdpi-wi/abc textfield search activated mtrl alpha 9 pps 168 - pv ... 1.0 fat
                                                                                                                                                           -181 b -- stor-80-000-00-00:00 res/drawable-mdpi-v4/abc_textfield_search_activated_mtrl_alpha.9.png
```

Figure: Output from diffoscope

## Recommendations for VVA Developers

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

## Thank you!

Questions?