Reproducing Vote Verification Application Builds for Estonian I-Voting System

Research Seminar in Cryptography

September 5, 2017
I-Voting Protocol
I-Voting Protocol

1. Authentication

2. Candidate list $L$

3. $\text{Sig}_v(\text{Enc}_{spub}(c_v, r))$

4. Vote reference $vr$
1. Authentication

2. Candidate list $L$

3. $\text{Sig}_v(\text{Enc}_{s_{pub}}(c_v, r))$

4. Vote reference $vr$

5. $r, vr$

6. $vr, L$

7. $\text{Enc}_{s_{pub}}(c_v, r), L$

8. $c_v$
Source Code

ios-ivotingverification
iOS based vote verification application for Estonian i-voting system

ivotingverification
Android based vote verification application for Estonian i-voting system
Application: Android

https://github.com/vvk-ehk/ivotingverification
Application: iOS

https://github.com/vvk-ehk/ios-ivotingverification
R reproducible builds allow for independent verifications that a binary matches what the source intended to produce.
Reproducible Builds

How to know that binaries distributed are compiled using the source code published?
Reproducible Builds

How to know that binaries distributed are compiled using the source code published?

“Reproducible builds allow for independent verifications that a binary matches what the source intended to produce.”
Tasks

I-voting period: October 5–11, 2017
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period

Reproducible builds everywhere and beyond: https://www.youtube.com/watch?v=65eDYwNqW-I

Build reproduction for Android VVA is a priority.
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores

Reproducible builds everywhere and beyond: https://www.youtube.com/watch?v=65eDYwNqW-I
Tasks

i-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
  - Build application package from the source code

Reproducible builds everywhere and beyond: https://www.youtube.com/watch?v=65eDYwNqW-I
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
- Build application package from the source code
  - Study differences in the binaries

Reproducible builds everywhere and beyond: https://www.youtube.com/watch?v=65eDYwNqW-I
Tasks

I-voting period: October 5–11, 2017

• Monitor binary packages distributed in the i-voting period
  • Figure out how to monitor binaries distributed by the stores
• Build application package from the source code
  • Study differences in the binaries
  • Adjust the build process to eliminate differences
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
- Build application package from the source code
  - Study differences in the binaries
  - Adjust the build process to eliminate differences
  - Repeat until binary package build is reproduced fully

- Provide build script for reproducing binaries
- Provide recommendations for making the build process more reproducible-friendly
- Describe the process in the report

Reproducible builds everywhere and beyond: https://www.youtube.com/watch?v=65eDYwNqW-I
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
- Build application package from the source code
  - Study differences in the binaries
  - Adjust the build process to eliminate differences
  - Repeat until binary package build is reproduced fully
- Provide build script for reproducing binaries
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
- Build application package from the source code
  - Study differences in the binaries
  - Adjust the build process to eliminate differences
  - Repeat until binary package build is reproduced fully
- Provide build script for reproducing binaries
- Provide recommendations for making the build process more reproducible-friendly

Reproducible builds everywhere and beyond: https://www.youtube.com/watch?v=65eDYwNqW-I
Tasks
I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
- Build application package from the source code
  - Study differences in the binaries
  - Adjust the build process to eliminate differences
  - Repeat until binary package build is reproduced fully
- Provide build script for reproducing binaries
- Provide recommendations for making the build process more reproducible-friendly
- Describe the process in the report
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
- Build application package from the source code
  - Study differences in the binaries
  - Adjust the build process to eliminate differences
  - Repeat until binary package build is reproduced fully
- Provide build script for reproducing binaries
- Provide recommendations for making the build process more reproducible-friendly
- Describe the process in the report
- Build reproduction for Android VVA is a priority
Tasks

I-voting period: October 5–11, 2017

- Monitor binary packages distributed in the i-voting period
  - Figure out how to monitor binaries distributed by the stores
- Build application package from the source code
  - Study differences in the binaries
  - Adjust the build process to eliminate differences
  - Repeat until binary package build is reproduced fully
- Provide build script for reproducing binaries
- Provide recommendations for making the build process more reproducible-friendly
- Describe the process in the report
- Build reproduction for Android VVA is a priority

Reproducible builds everywhere and beyond:
https://www.youtube.com/watch?v=65eDYwNqW-I