My Project Ideas

Joseph Bisch

University of New Haven

September 1, 2015

Senior Design Project Ideas

- Cross-distro Reproducible Builds
- Android Reproducible Builds
- Cryptographically Secured Voting System

Table of Contents

What are reproducible builds?

- Byte-for-byte identical binaries from source code

What are reproducible builds?

- Byte-for-byte identical binaries from source code
- Then users can verify that no flaws have been introduced during the build process

Brief History of Reproducible Builds

- Gitian (2011) was first system, developed for Bitcoin Core and adopted by Tor Browser Bundle (TBB)

Brief History of Reproducible Builds

- Gitian (2011) was first system, developed for Bitcoin Core and adopted by Tor Browser Bundle (TBB)
- Debian toolchain came later (2013) after it saw the success of TBB adopting Gitian. Very large scale project (an entire OS).

Cross-distro Reproducible Builds Idea

- Currently there is no reproducible build system that allows the builder to choose from among multiple distros

Cross-distro Reproducible Builds Idea

- Currently there is no reproducible build system that allows the builder to choose from among multiple distros
- Multiple distro choices will allow greater security

Cross-distro Reproducible Builds Idea

- Currently there is no reproducible build system that allows the builder to choose from among multiple distros
- Multiple distro choices will allow greater security
  - vulerabilities in one distro can be detected

Cross-distro Reproducible Builds Idea

- Currently there is no reproducible build system that allows the builder to choose from among multiple distros
- Multiple distro choices will allow greater security
  - vulerabilities in one distro can be detected
- So my idea is to implement at least one other distro into Gitian

Table of Contents

Backstory

- Checked with the Gitian maintainer about my first idea to get feedback on the feasibility of it...

Backstory

- Checked with the Gitian maintainer about my first idea to get feedback on the feasibility of it...
- ...he replied with a related idea (Android Reproducible Builds)

Android Reproducible Builds Idea

- Android apps are written in Java and typically some sort of build system is used

Android Reproducible Builds Idea

- Android apps are written in Java and typically some sort of build system is used
- To make Android apps reproducible:

Android Reproducible Builds Idea

- Android apps are written in Java and typically some sort of build system is used
- To make Android apps reproducible:
  - Need to make sure that all sources of variability are removed

Android Reproducible Builds Idea

- Android apps are written in Java and typically some sort of build system is used
- To make Android apps reproducible:
  - Need to make sure that all sources of variability are removed
  - Also need to make sure the dependencies are built reproducibly

Android Reproducible Builds Idea

- Android apps are written in Java and typically some sort of build system is used
- To make Android apps reproducible:
  - Need to make sure that all sources of variability are removed
  - Also need to make sure the dependencies are built reproducibly
- Idea is to make a plugin for the build system to automate reproducibility

Table of Contents

Crypto Voting System Idea

- Existing systems typically use usernames and passwords or insecure data distribution methods

Crypto Voting System Idea

- Existing systems typically use usernames and passwords or insecure data distribution methods
- Idea is to use digital signatures for authentication

Crypto Voting System Idea

- Existing systems typically use usernames and passwords or insecure data distribution methods
- Idea is to use digital signatures for authentication
  - voting (USGA elections)

Crypto Voting System Idea

- Existing systems typically use usernames and passwords or insecure data distribution methods
- Idea is to use digital signatures for authentication
  - voting (USGA elections)
  - award acceptance (financial aid)

Crypto Voting System Idea

- Existing systems typically use usernames and passwords or insecure data distribution methods
- Idea is to use digital signatures for authentication
  - voting (USGA elections)
  - award acceptance (financial aid)
- Estonia already has voting over the Internet using digital signatures since 2005, therefore, need an enhancement to make this a possible senior design project