JCrypTool

The cryptography e-learning platform.

Thorben Groos, Simon Leischnig, Dominik Schadow

Agenda

JCrypTool Basics

JCrypTool 1.0

Outlook

Agenda

JCrypTool Basics

JCrypTool 1.0

Outlook

JCrypTool Basics

Based on Eclipse Rich Client Platform (RCP) and Java

- Available for all major platforms in 64bit - Linux, macOS, Windows
- Transparent for the developer (in theory)
- Common limitations of the Eclipse IDE, look & feel is challenging for non-developers

Platform independent plug-ins

- Completely extensible with plug-ins (everything is a plug-in)
- Learn and develop cryptography - everyone can develop an own plug-in
- High barriers to entry for developers - Eclipse RCP is not that common any more

Complete Extensibility with Plug-ins

Core

- More than **20** core plug-ins
- Providing common functionality like editors (text and hex), views (log, keystore, file and algorithm navigators, …), keystore services (BouncyCastle and FlexiProvider)
- Fall-through hierarchy of crypto providers
- Multi-language support (currently German and English)

Crypto

- More than **60** crypto plug-ins
- Analysis, classic and modern algorithms, games and visualizations
- From relatively simple algorithms to complex visualizations

Facts and Figures

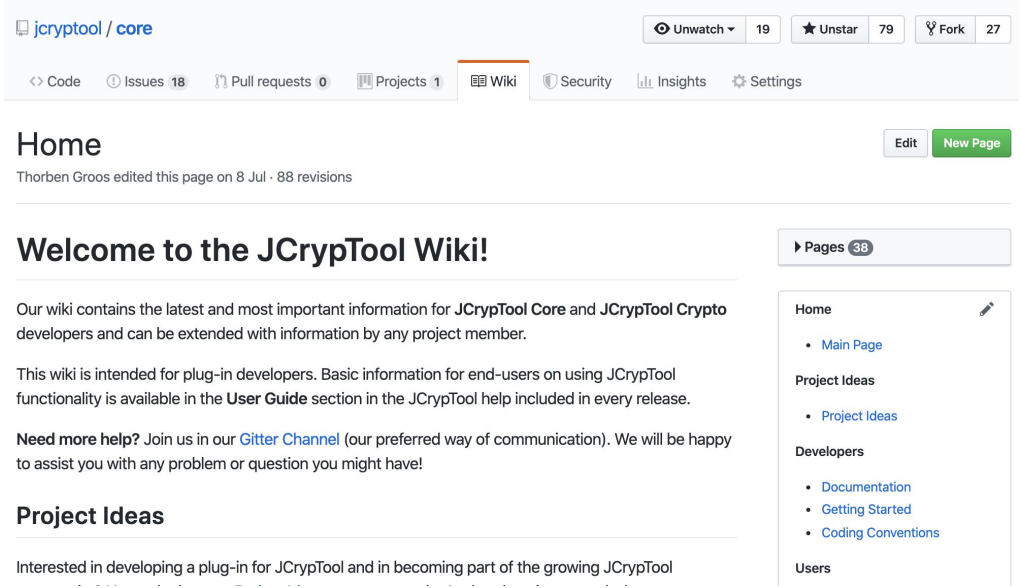
Keeping everything up-to-date (technologies and tools)

- Started on SourceForge (SVN), moved to GitHub (Git)
- Release builds on TravisCI - fully automated weekly builds
- Updating:
  - Eclipse RCP is relatively easy - we switch to every new version
  - Java is (now) more challenging - moving away from Java 8 now

More than 50 contributors

- From one-time contributors, students and student teams to regulars
- Divided into core and crypto teams - with read only or write access

Attracting Developers



More than 25 source **code forks**

Public **wiki** with getting started guides, technology information, some common requirements, style guides, and release planning

Gitter channel

Public **issue tracker** for core and crypto

Approaching release 1.0.0 -- more on that by Thorben Groos

Agenda

JCrypTool Basics

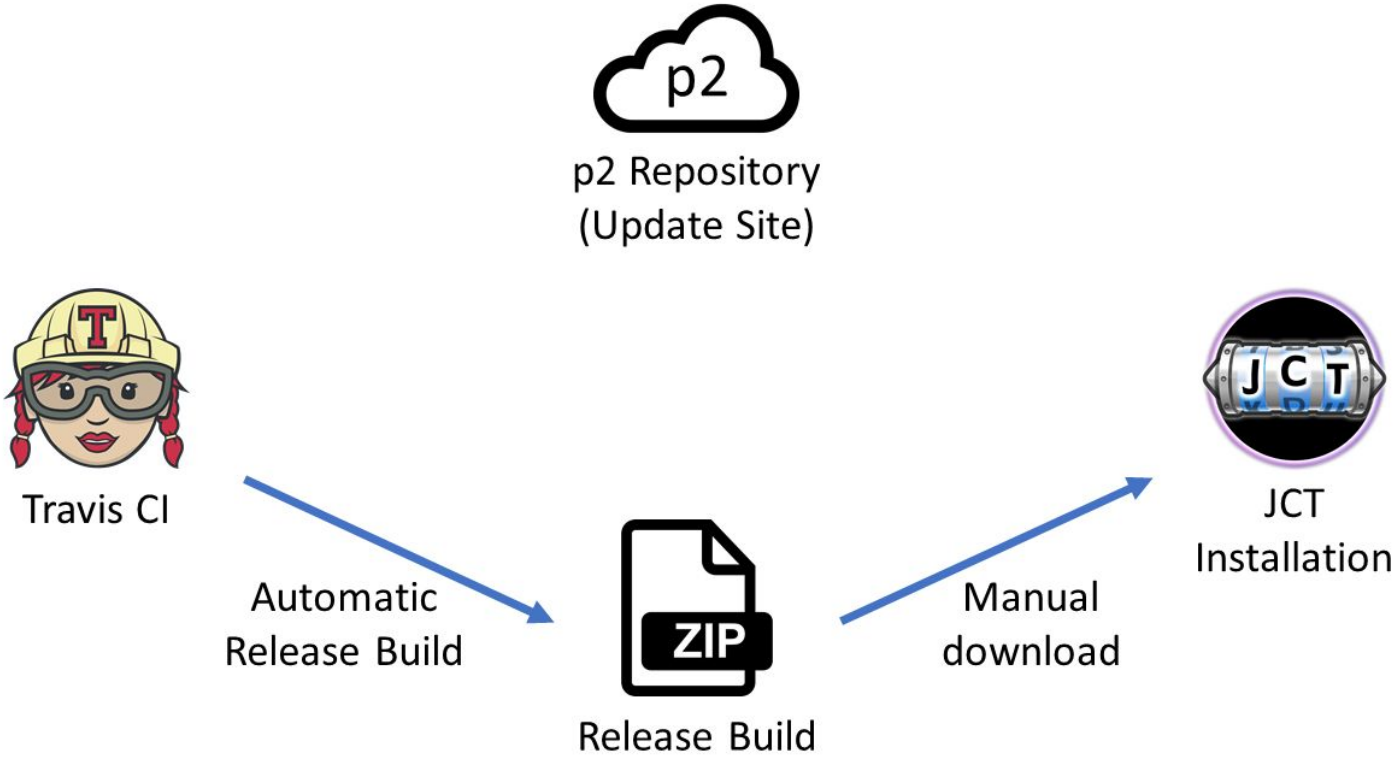
JCrypTool 1.0

Outlook

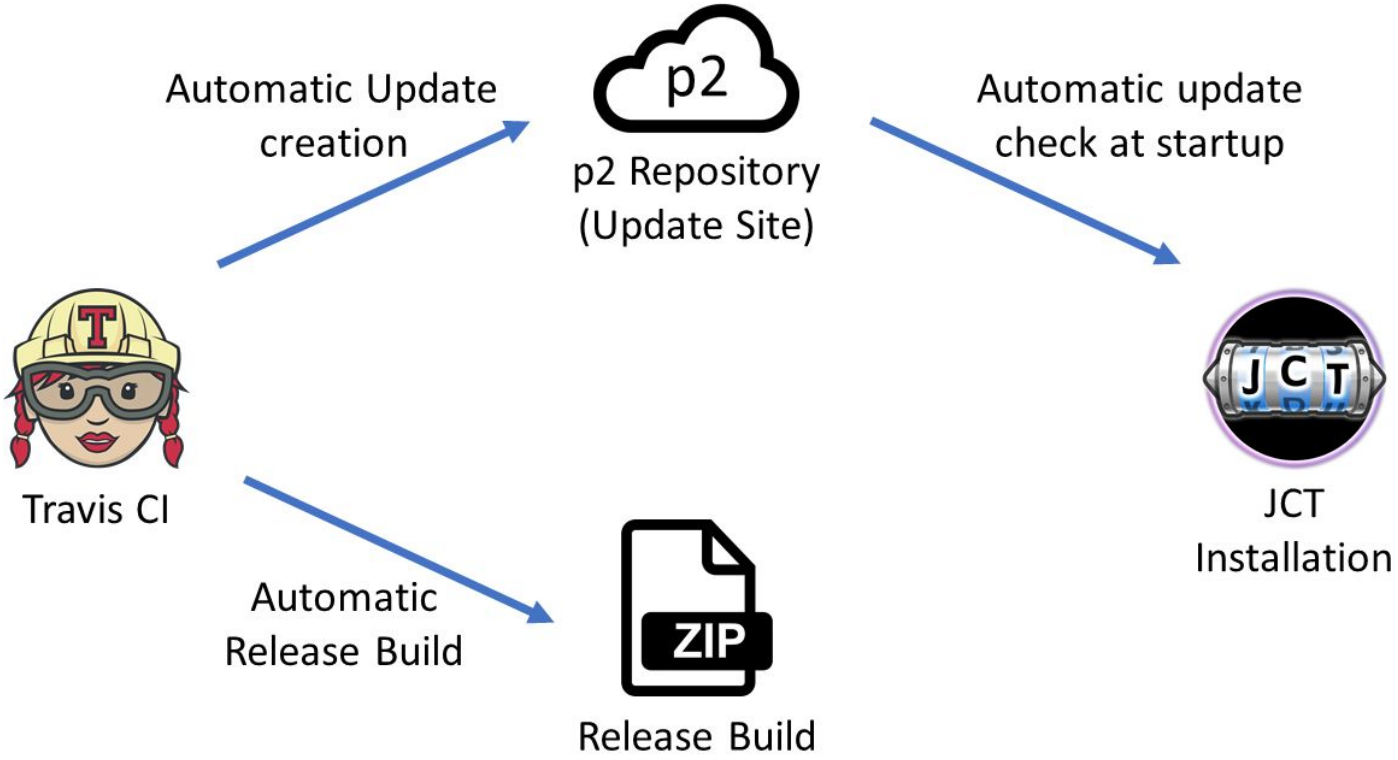
What’s new in JCrypTool 1.0

- Completely available in German and English
- 2 new plug-ins: SPHINCS+ Signature visualization and Grille analysis
- New update process
- JCrypTool - JRE - Bundle
- GUI improvements and bug fixes

Update Process - conventional



Update Process - via a provisioning platform (p2)



JCrypTool-JRE-Bundle

- Migrating from Java 8 to Java 11
- We ship a Java 11 JRE with JCrypTool 1.0

Advantage: No installed JRE is needed anymore to run JCrypTool

Agenda

JCrypTool Basics

JCrypTool 1.0

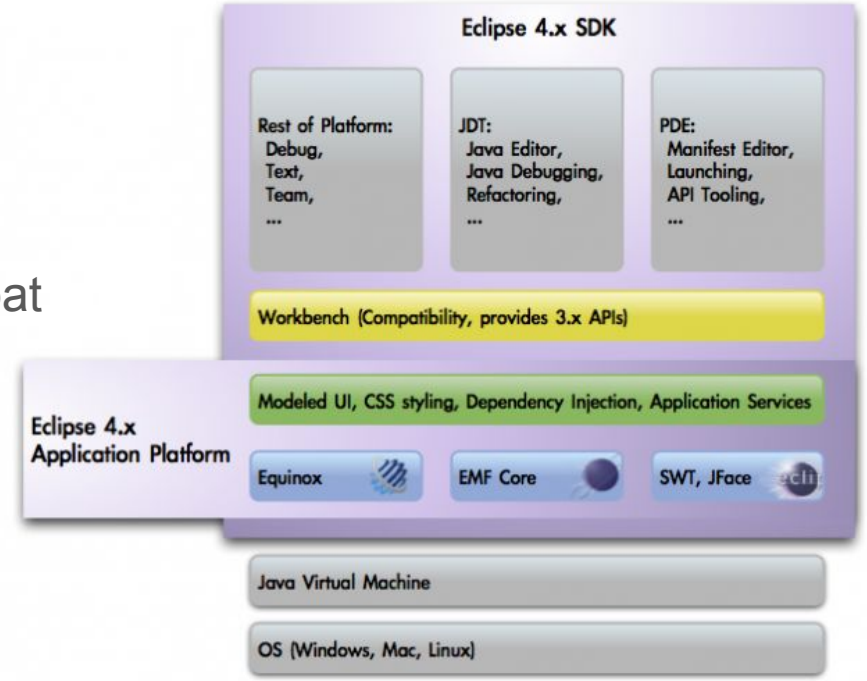
Outlook

Outlook

1. Eclipse E4 Migration
2. BouncyCastle und JCrypTool
3. Build process improvements

Eclipse 4 (e4) Migration

- Future-proof JCrypTool
- Currently: compatibility layer
- Multi-stage migration:
  - core
  - common prototypes & own compat
  - batch



BouncyCastle and JCT

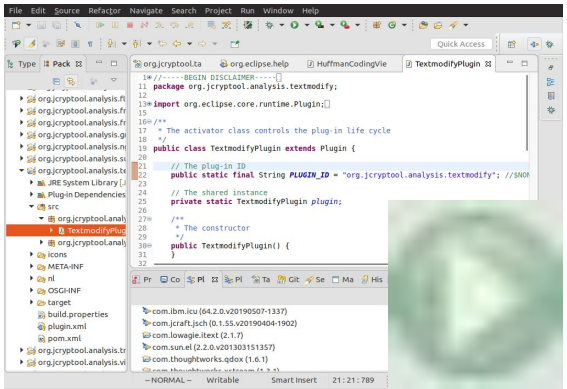
- BouncyCastle: APIs for cryptography
  https://www.bouncycastle.org
- Many modern algorithms included
- Challenge: Generic UI model
- Goal: JCT as GUI for BouncyCastle

Build Process

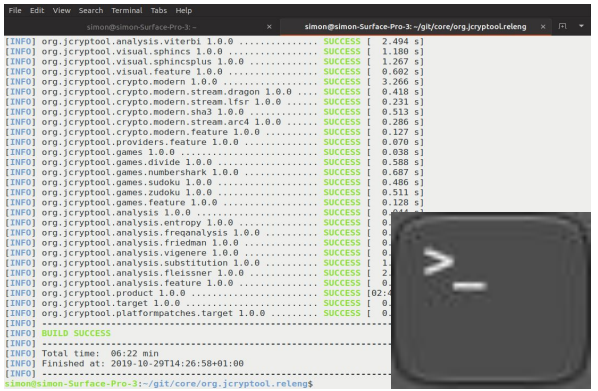
“Developer Build” is not “Release Build” !

Target Platform

Developer Build (Eclipse PDE)



Release Build (Maven/Tycho)



Build Process - New Possibilities

Through a new experimental project...
https://github.com/simlei/org.jcryptool.thirdparty

- Depend on libraries from Maven Central
  - <dependency>{group:id:version}</dependency>
- Load off heavy features (e.g. JRE)
- Patch the eclipse platform!

Outlook

- **Big future projects**: E4 migration, BouncyCastle UI
- **Stable infrastructure** through further improving our build process

Thank you

https://github.com/jcryptool