aursec - A blockchain approach to securing software packages

Lukas Krismer & Bennett Piater

October 22, 2016

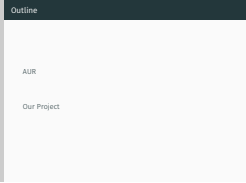
Universität Innsbruck - QE - Christian Sillaber

2016-10-22

aursec - A blockchain approach to securing software packages

Outline

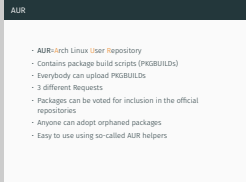
1 min L



AUR

AUR

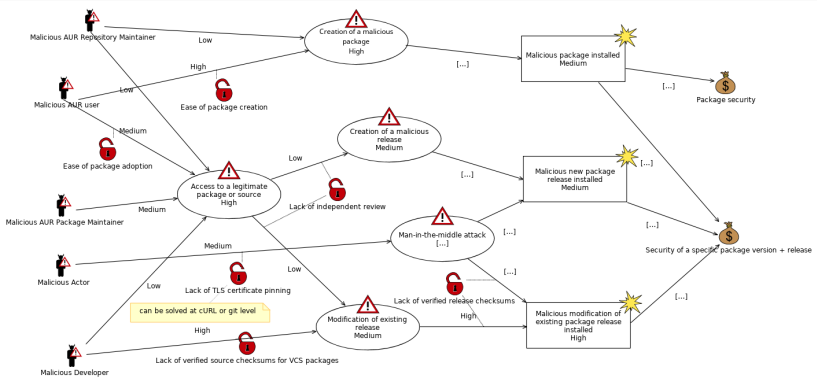
- **AUR**=Arch Linux User Repository
- Contains package build scripts (PKGBUILDs)
- Everybody can upload PKGBUILDs
- 3 different Requests
- Packages can be voted for inclusion in the official repositories
- Anyone can adopt orphaned packages
- Easy to use using so-called AUR helpers



2min L

Orphan,Deletion,Merge

Threat Assessment

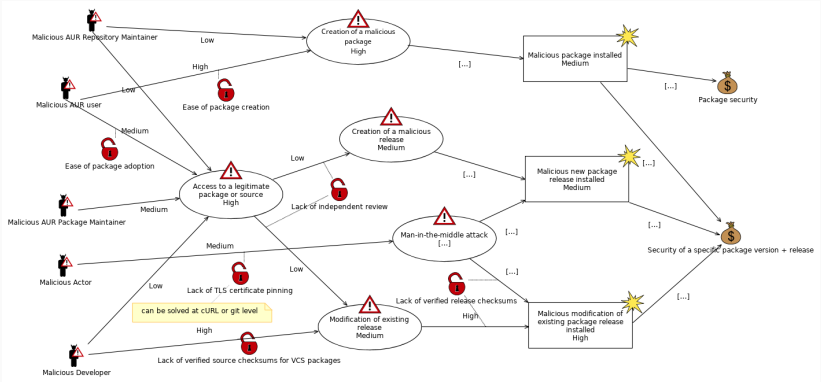


Threat Assessment

2 min B

Our Project

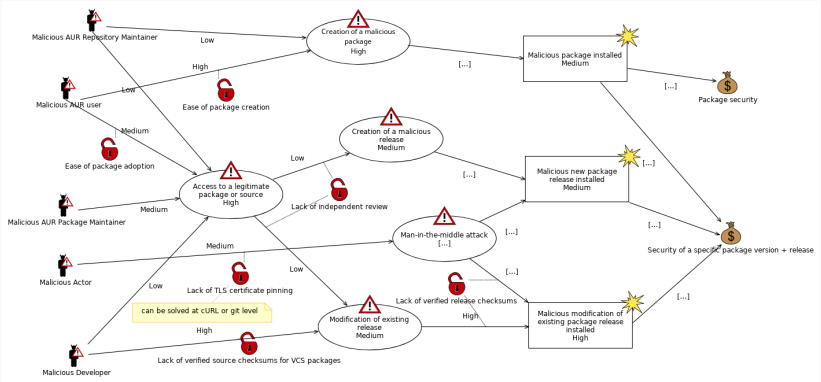
Covered Threats



Covered Threats

1 min L

Covered Threats



Covered Threats

1 min L

Basic Workflow

Basic Workflow

3 min

Components

- Program on a private Ethereum blockchain
- Library and program using it
- AUR package
- Integration in aurutils
- Web- and/or CLI-Interface for stats

2 min B

Components
- Program on a private Ethereum blockchain
- Library and program using it
- AUR package
- Integration in aurutils
- Web- and/or CLI-Interface for stats

Schedule

- **25.10** *prototype:* hashing B
- **08.11** Initial Presentation L
- **15.11** *prototype:* library without blockchain back-end B/L
- **15.11** Bash-API for the blockchain L
- **30.11** *finish:* Solidity program B
- **08.12** deploy local blockchain for development L
- **08.12** running server with ethereum-node B/L
- **15.12** *prototype:*Library incl. back-end L
- **20.12** *contrib:* rudimentary pre-build-hooks in aurutils B

Schedule
- **25.10** *prototype:* hashing B
- **08.11** Initial Presentation L
- **15.11** *prototype:* library without blockchain back-end B/L
- **15.11** Bash-API for the blockchain L
- **30.11** *finish:* Solidity program B
- **08.12** deploy local blockchain for development L
- **08.12** running server with ethereum-node B/L
- **15.12** *prototype:*Library incl. back-end L
- **20.12** *contrib:* rudimentary pre-build-hooks in aurutils B

2 min B

Schedule

- 10.01 *contrib:* TLS-public-key-pinning in aurutils B
- 10.01 configuration and trust-cutoff L
- 15.01 *test:* Integration in aurutils B
- 15.02 AUR package incl. private blockchain B
- 01.03 *finish:* libary and aurutils-Hook B
- 01.04 *finish:* Web- and/or CLI-Interface L
- 15.04 Draft paper
- ??.05 *finish:* Paper
- ??.05 Final presentation L

2 min B

Schedule
- 10.01 contrib: TLS-public-key-pinning in aurutils B
- 10.01 configuration and trust-cutoff L
- 15.01 test: Integration in aurutils B
- 15.02 AUR package incl. private blockchain B
- 01.03 finish: libary and aurutils-Hook B
- 01.04 finish: Web- and/or CLI-Interface L
- 15.04 Draft paper
- ??.05 finish: Paper
- ??.05 Final presentation L