

2016-10-27

aursec - A blockchain approach to securing software packages

aursec - A blockchain approach to securing software packages

Lukas Krismer & Bennett Piater

October 27, 2016

Universität Innsbruck - QE - Christian Sillaber

aursec - A blockchain approach to securing software packages

Lukas Krismer & Bennett Piater
October 27, 2016
Universität Innsbruck - QE - Christian Sillaber

aursec - A blockchain approach to securing software packages

2016-10-27

└─ Outline

Outline

AUR

Our Project

AUR

Our Project

1 min L

2016-10-27

aursec - A blockchain approach to securing
software packages
└─ AUR

AUR

AUR

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

2016-10-27

aursec - A blockchain approach to securing software packages

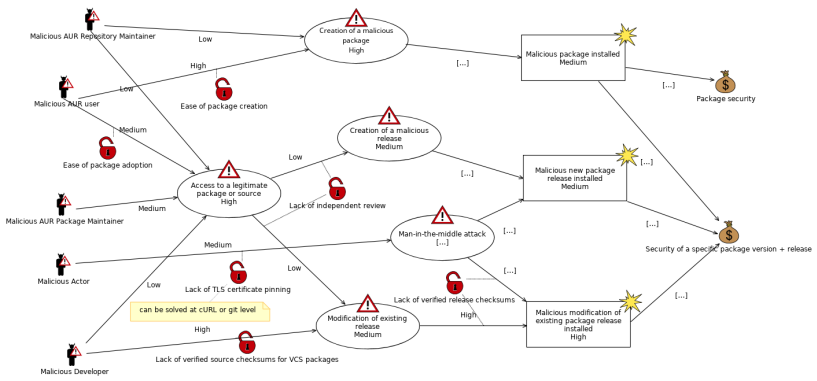
└─AUR

└─AUR

2min L

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

Threat Assessment



2016-10-27

aursec - A blockchain approach to securing software packages
└ AUR

└ Threat Assessment

2 min B



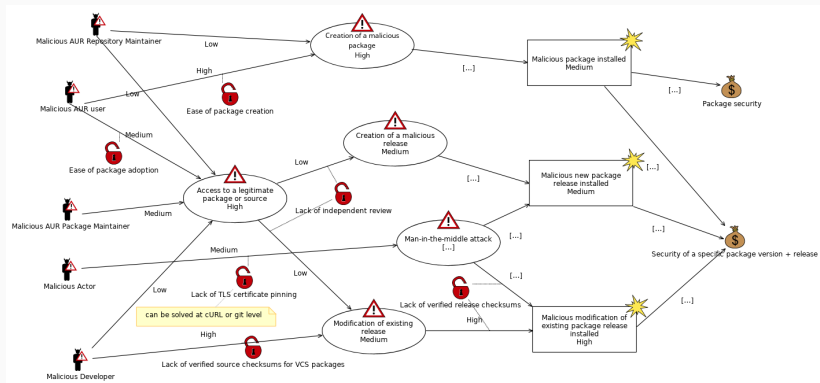
2016-10-27

aursec - A blockchain approach to securing
software packages
└─ Our Project

Our Project

Our Project

Covered Threats



2016-10-27

aursec - A blockchain approach to securing software packages
└ Our Project

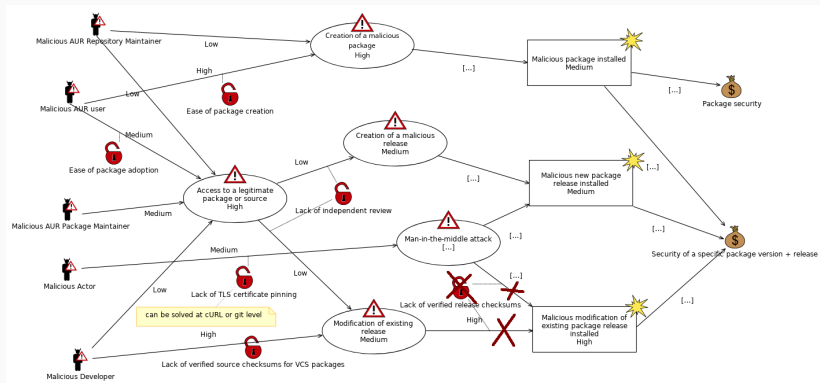
└ Covered Threats

1 min L

Covered Threats



Covered Threats



2016-10-27

aursec - A blockchain approach to securing software packages
└ Our Project

└ Covered Threats

1 min L

Covered Threats



2016-10-27

aursec - A blockchain approach to securing software packages

└─ Our Project

└─ Basic Workflow of the Core Library

3 min L

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

2016-10-27

aursec - A blockchain approach to securing
software packages
└─ Our Project

└─ Components

2 min B

- Program on a private Ethereum blockchain
- Library and program using it
- AUR package
- Integration in aurutils
- Threat analysis of the AUR and our software
- 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

2016-10-27

aursec - A blockchain approach to securing
software packages
└─ Our Project

└─ Schedule

2 min 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
- 20.12 *contrib*: rudimentary pre-build-hooks in aurutils B

- 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: library and aurutils-Hook B
- 01.04 finish: Web- and/or CLI-Interface L
- 15.04 Draft paper
- ??05 finish: Paper
- ??05 Final presentation L

2016-10-27

aursec - A blockchain approach to securing software packages
└ Our Project

└ Schedule

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: library and aurutils-Hook	B
• 01.04 finish: Web- and/or CLI-Interface	L
• 15.04 Draft paper	
• ??05 finish: Paper	
• ??05 Final presentation	L