aursec - A blockchain approach to securing software packages

Lukas Krismer & Bennett Piater

October 25, 2016

Universität Innsbruck - QE - Christian Sillaber

2016-10-25

aursec - A blockchain approach to securing software packages

aursec - A blockchain approach to securing software packages

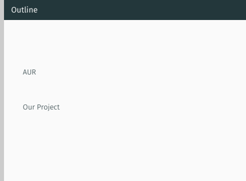
Lukas Krismer & Bennett Piater
October 25, 2016

Universität Innsbruck - QE - Christian Sillaber

Outline

AUR

Our Project



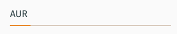
Outline

AUR

Our Project

1 min L

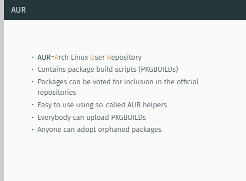
AUR



AUR

AUR

- AUR=Arch Linux User Repository
- 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



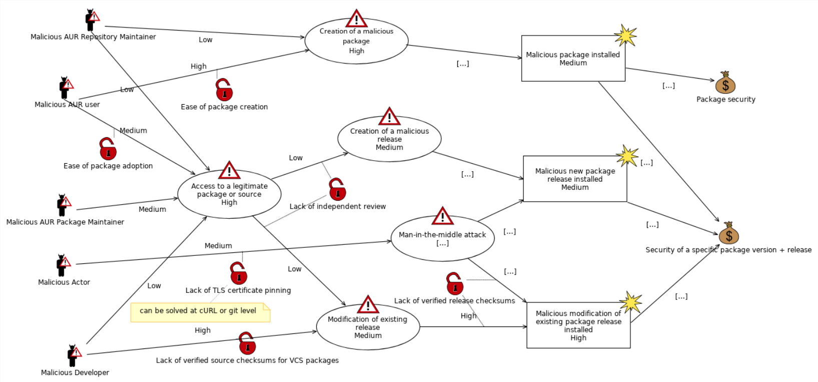
AUR

- AUR=Arch Linux User Repository
- 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

└─AUR

2min L

Threat Assessment

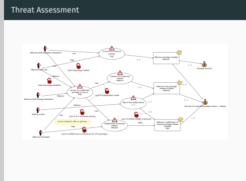

Malicious AUR Repository Maintainer
Low
Creation of a malicious package
High
Malicious package installed
Medium
[...]
Package security
High
Low
Malicious AUR user
Ease of package creation
Medium
Ease of package adoption
Creation of a malicious release
Medium
Low
[...]
Malicious new package release installed
Medium
[...]
Access to a legitimate package or source
High
Lack of independent review
Malicious AUR Package Maintainer
Medium
[...]
Man-in-the-middle attack
[...]
[...]
Security of a specific package version + release
Medium
Malicious Actor
Low
Lack of TLS certificate pinning
Low
[...]
Lack of verified release checksums
can be solved at cURL or git level
High
Modification of existing release
Medium
Malicious modification of existing package release installed
High
[...]
High
Malicious Developer
Lack of verified source checksums for VCS packages

2016-10-25

aursec - A blockchain approach to securing software packages

└AUR

└Threat Assessment



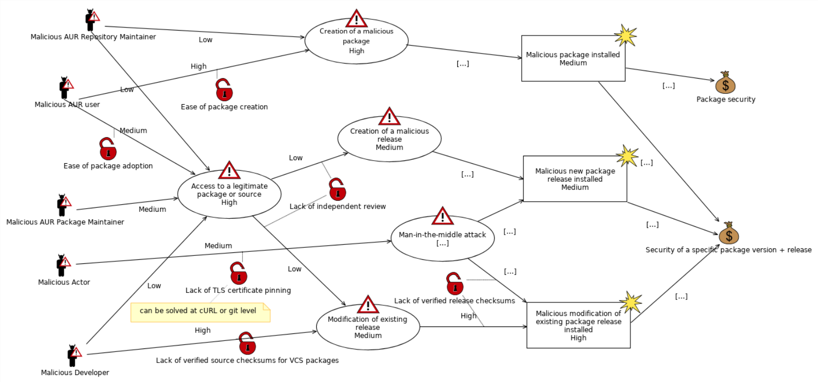
Threat Assessment

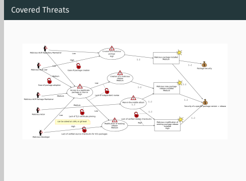
2 min B

Our Project

Our Project

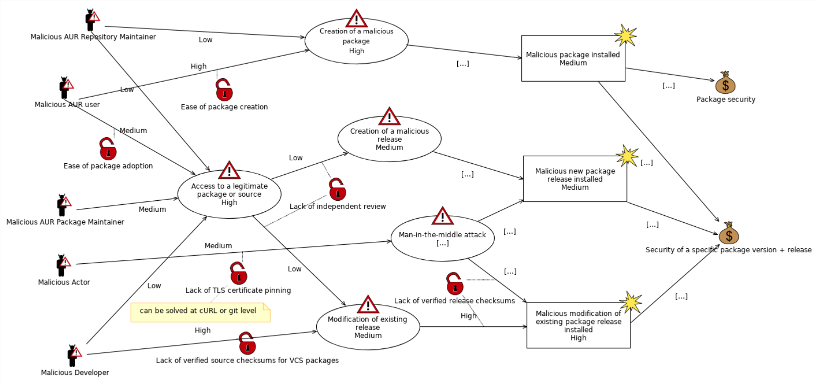
Covered Threats


Malicious AUR Repository Maintainer
Low
Creation of a malicious package
High
Malicious package installed
Medium
[...]
High
Low
Malicious AUR user
Ease of package creation
[...]
Package security
Medium
Creation of a malicious release
Medium
Ease of package adoption
Low
[...]
Malicious new package release installed
Medium
[...]
Access to a legitimate package or source
High
Lack of independent review
Malicious AUR Package Maintainer
Medium
[...]
Man-in-the-middle attack
[...]
[...]
Security of a specific package version + release
Medium
Malicious Actor
Low
Low
Lack of TLS certificate pinning
[...]
[...]
can be solved at cURL or git level
Lack of verified release checksums
High
Modification of existing release
Medium
Malicious modification of existing package release installed
High
High
Lack of verified source checksums for VCS packages
Malicious Developer



1 min L

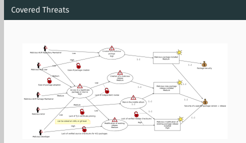
Covered Threats


Malicious AUR Repository Maintainer
Low
Creation of a malicious package
High
Malicious package installed
Medium
[...]
High
Low
Malicious AUR user
Ease of package creation
[...]
Package security
Medium
Creation of a malicious release
Medium
Ease of package adoption
Low
[...]
Malicious new package release installed
Medium
[...]
Access to a legitimate package or source
High
Lack of independent review
Malicious AUR Package Maintainer
Medium
[...]
Man-in-the-middle attack
[...]
[...]
Security of a specific package version + release
Medium
Malicious Actor
Low
Low
[...]
Lack of TLS certificate pinning
Lack of verified release checksums
[...]
can be solved at cURL or git level
High
Modification of existing release
Medium
Malicious modification of existing package release installed
High
High
Lack of verified source checksums for VCS packages
Malicious Developer

2016-10-25

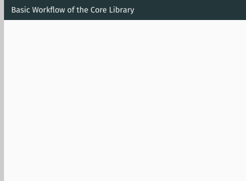
aursec - A blockchain approach to securing software packages
└Our Project

└Covered Threats



1 min L

Basic Workflow of the Core Library



Basic Workflow of the Core Library

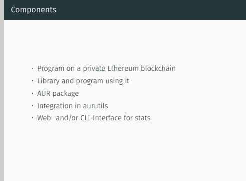
3 min L

Components

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

2016-10-25

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


Components

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

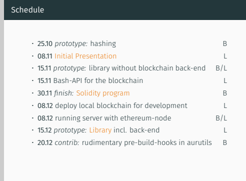
2 min B

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

2016-10-25

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



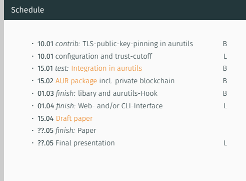
Schedule

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



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