

aursec - Master a blockchain approach to securing software packages/

Lukas Krismer & Bennett Piater

October 20, 2016

Universität Innsbruck - QE - Christian Sillaber

2016-10-20

aursec - Master a blockchain approach to securing software packages/

aursec - Master a blockchain approach to securing software packages/

Lukas Krismer & Bennett Piater
October 20, 2016
Universität Innsbruck - QE - Christian Sillaber

2016-10-20

aursec - Master a blockchain approach to securing software packages/

└─Outline

Outline

AUR

Our Project

AUR

Our Project

2016-10-20

aursec - Master a blockchain approach to securing
software packages/
└─ AUR

AUR

AUR

2016-10-20

aursec - Master a blockchain approach to securing
software packages/
└─AUR

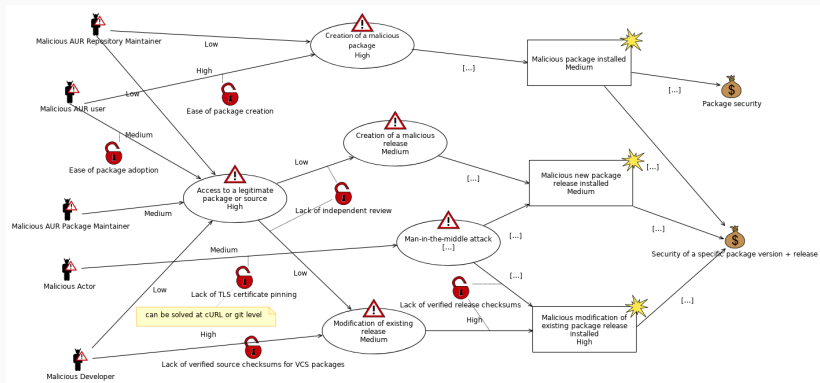
└─AUR

- AUR=Arch Linux Repository
- Contains package descriptions (PKGBUILDs)
- everybody can upload PKBUILDs
- 3 different Requests
- voting system

- AUR=Arch Linux Repository
- Contains package descriptions (PKGBUILDs)
- everybody can upload PKBUILDs
- 3 different Requests
- voting system

Orphan,Deletion,Merge

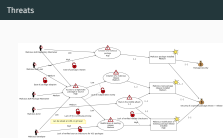
Threats



2016-10-20

aursec - Master a blockchain approach to securing software packages/
└ AUR

└ Threats



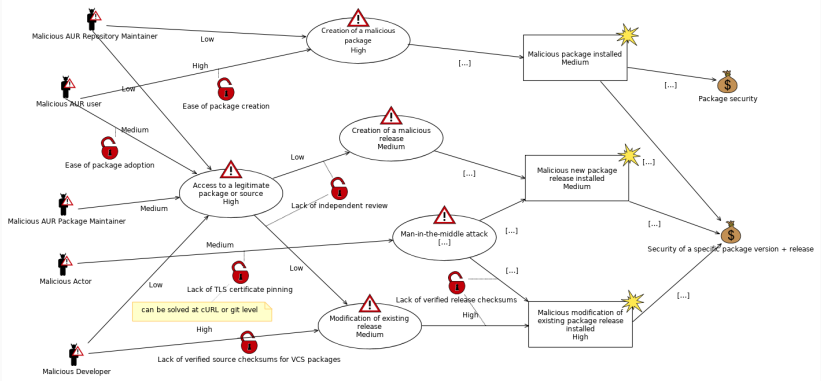
2016-10-20

aursec - Master a blockchain approach to securing
software packages/
└─ Our Project

Our Project

Our Project

Covered Threats



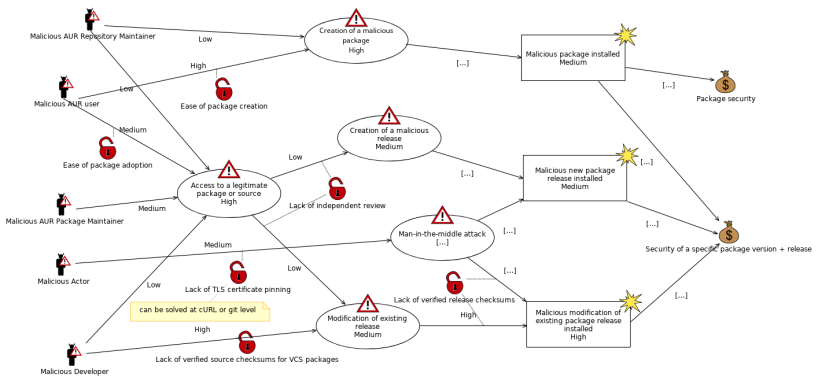
2016-10-20

aursec - Master a blockchain approach to securing software packages/
└ Our Project

└ Covered Threats



Covered Threats



2016-10-20

aursec - Master a blockchain approach to securing software packages/
└ Our Project

└ Covered Threats



2016-10-20

aursec - Master a blockchain approach to securing software packages/

└─ Our Project

└─ Basic Workflow

- Ethereum program
- library
- arch-package
- web- and/or CLI-Interface
- integration

2016-10-20

aursec - Master a blockchain approach to securing
software packages/
└─ Our Project

└─ Components

- Ethereum program
- library
- arch-package
- web- and/or CLI-Interface
- integration

- 25.10 Prototype hashing B
- 08.11 Initial-Presentation L
- 15.11 Library-prototyp without blockchain-backend B/L
- 15.11 Bash-API for the blockchain L
- 30.11 Solidity-program finished B
- 08.12 unified local library for development L
- 08.12 runnable server with ethereum-node B/L
- 15.12 library-backend L
- 20.12 contrib: rudimentary pre-build-hooks in aurutils B

2016-10-20

aursec - Master a blockchain approach to securing software packages/
└ Our Project

└ Schedule

Schedule		
- 25.10	Prototype hashing	B
- 08.11	Initial-Presentation	L
- 15.11	Library-prototyp without blockchain-backend	B/L
- 15.11	Bash-API for the blockchain	L
- 30.11	Solidity-program finished	B
- 08.12	unified local library for development	L
- 08.12	runnable server with ethereum-node	B/L
- 15.12	library-backend	
- 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 testing: integration in aurutils B
- 15.02 arch-package inc. 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 End-Presentation L

2016-10-20

aursec - Master a blockchain approach to securing software packages/
└ Our Project

└ Schedule

Schedule	
• 10.01 contrib: TLS-public-key-pinning in aurutils	B
• 10.01 configuration and trust-cutoff	L
• 15.01 testing: integration in aurutils	B
• 15.02 arch-package inc. 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 End-Presentation	L