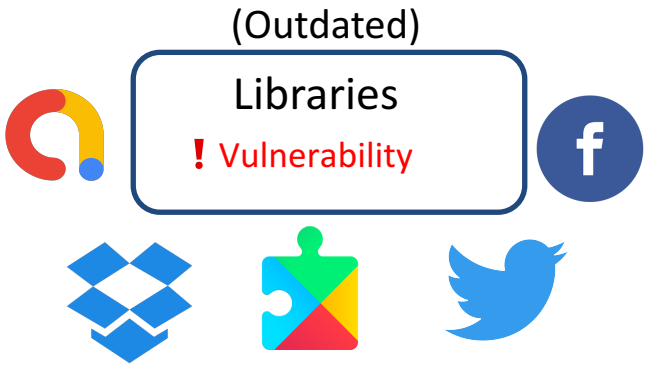
Up2Dep: Android Tool Support to Fix Insecure Code Dependencies

Duc Cuong Nguyen, Erik Derr, Michael Backes, Sven Bugiel

Motivation

- (Outdated) third-party library increases apps' attack-surface



- App developers tend to keep using outdated libraries
  - e.g., even when security fixes are available

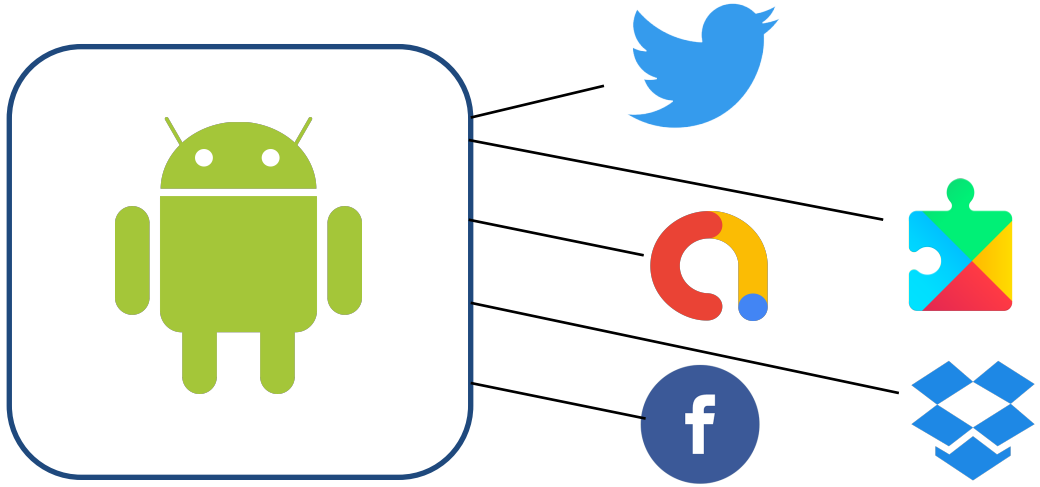
Motivation

- Possible directions to fix app's outdated dependencies

1. Automatic patching on compiled apps

Library's code and app's code are merged
→Automatic patching fails

2. Fix during development phase



Not an easy task for developers:

- Incompatibility problems
- No security related information is available
- Lack of practical tool support

Up2Dep

1. Tool support integrated in development environment
   - App code and library code are separated
   - Versions information is available
2. Provides developers with security related information
   - Avoiding libraries (versions) with security & privacy problems
3. Provides developers with updatability information
   - Easily navigate and update project's dependency if API incompatibility occurs

Methodology

Guarantee developers (API level) compatibility when suggesting updates

→ Pre-analyze libraries to find changes across versions (LibScout - *Backes et al.*)

Avoid re-using insecure libraries (versions)

→ Scan libraries for cryptographic API misuse (CogniCrypt - *Krüger et al.*)

→ Manually check for publicly disclosed vulnerabilities of libraries

Provide developers with security & updatability information

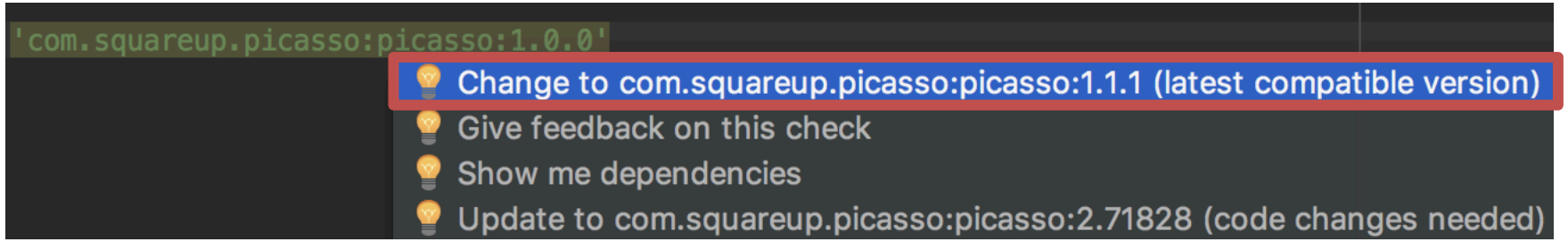
→ Statically analyze developer's code as they write it

Methodology - Library Database

- 1,878 libraries (37,402 versions)
  - 10 libraries (spanning across 97 versions) contain publicly disclosed vulnerabilities
  - 20 libraries (spanning across 93 versions) still use insecure connection (http connection)
  - 13.80% contain at least 1 cryptographic API misuse, nearly 1/3 of them have fixes in their latest versions

Methodology - Examples

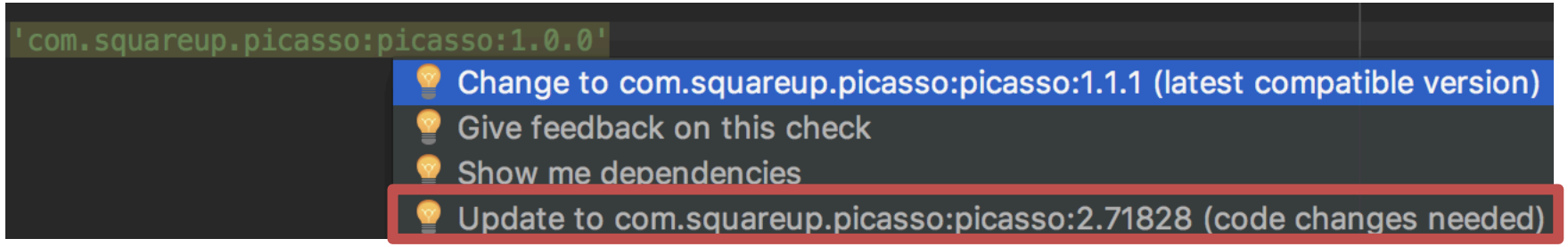
Up2Dep warns developers about an outdated library



Up2Dep shows different options to update an outdated dependencies

Methodology - Examples

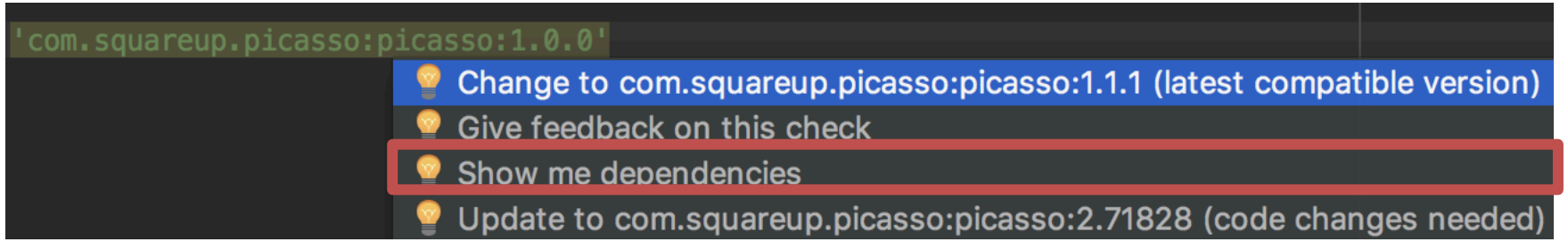
Up2Dep warns developers about an outdated library



Up2Dep shows different options to update an outdated dependencies

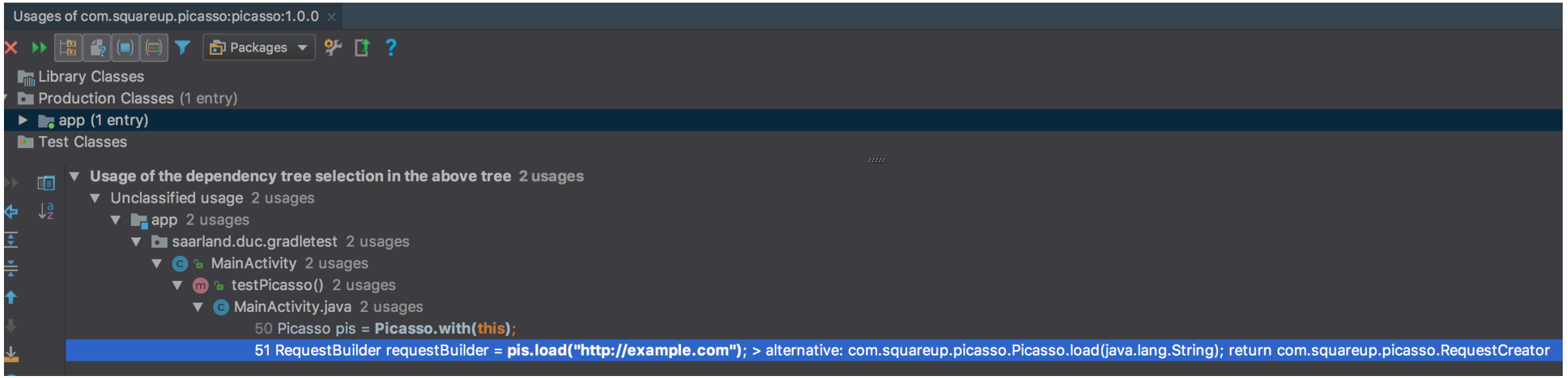
Methodology - Examples

Up2Dep warns developers about an outdated library



Up2Dep shows different options to update an outdated dependencies

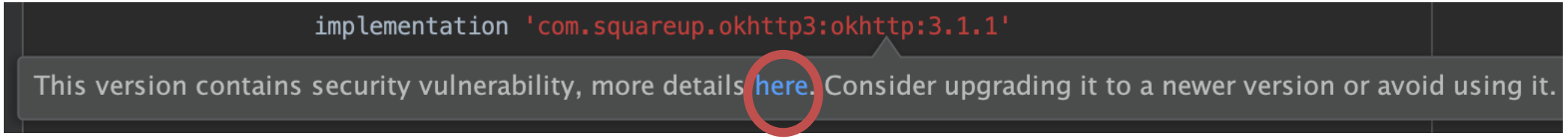
Methodology – Examples



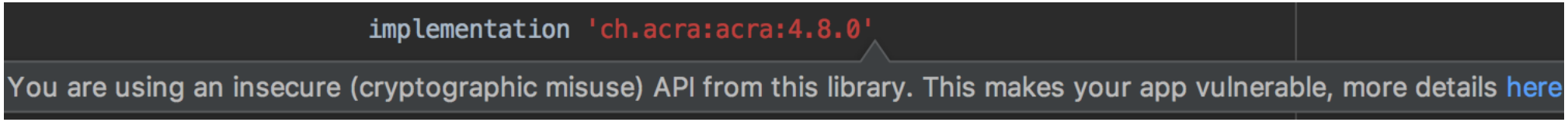
Return type of method **load** has changed from **RequestBuilder** to **RequestCreater**

Up2Dep shows API usages of an outdated dependency

Methodology – Examples



Up2Dep provides security warning about an insecure library



Up2Dep provides security warning about re-using cryptographic API misuse

Evaluation

- Release
  - Publicly released Up2Dep on Android Studio plugin repository
  - Presented Up2Dep at DroidCon 2018 (International Android Developer Conference)
  - Used Twitter, Facebook, Reddit, Ycombinator to further advertise

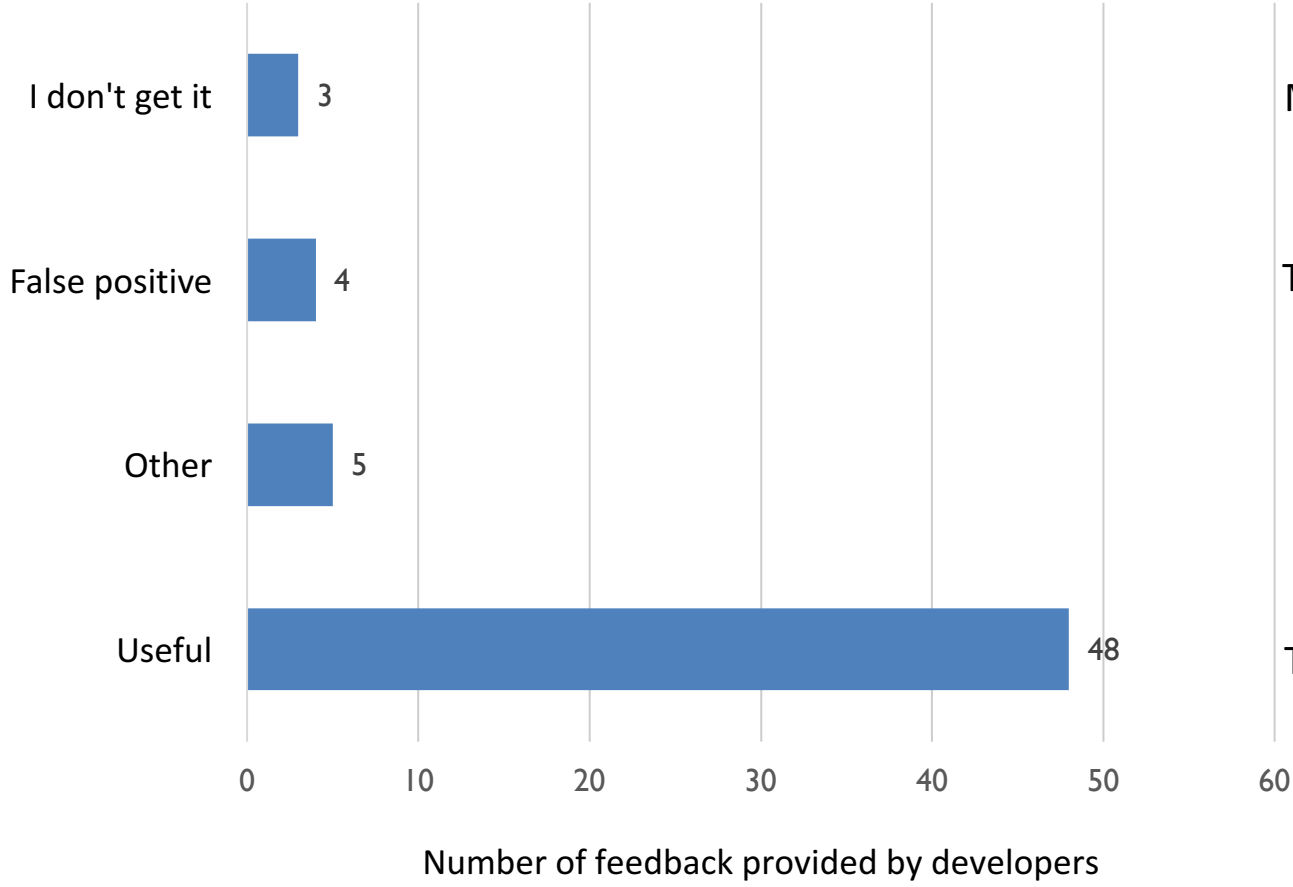
- Measure
  - Built-in telemetric features to gather anonymized information
  - Built-in in-context feedback feature to allow developers to provide feedback
  - Survey to ask developers for more information

Results

- 56 developers tried Up2Dep within their daily programming tasks
- 116 outdated dependencies (34 projects) have been updated
  - 8 dependencies with security problems have been avoided
- SUS score of 76.20 (“good” in terms of usability)

Results

In-context feedback received: 60 feedbacks from 22 developers



More information needed on the warning message (5%)

The check is incorrect (6.67%)

(8.33%)

The check is correct, and I find it useful (80%)

Limitations & future work

- Up2Dep only guarantees API-level compatibility while semantic changes might cause undesired behaviors
- Automatically retrieve publicly disclosed vulnerabilities and notify developers accordingly
- Study on long-term impact of tool-support to examine developers' behavior
- Third-party library analysis to cover different aspects of their security & privacy implications e.g., permission usages

Conclusion

- First presented tool support to ease the task of keeping project's dependencies up-to-date
- Tool support during development phase does reduce security & privacy related problems introduced by third-party libraries
- There is an urgent need for designated tool support for developers to detect and update insecure third-party libraries
- Up2Dep is publicly available https://github.com/ngcuongst/up2dep

Thank you!

duc.nguyen@cispa.saarland
ducnst