

FASTEN: Fine-grained Analyses of Software Ecosystems as Networks

Sebastian Proksch, Delft University of Technology

The leftpad incident

- A developer removed an NPM library, consisting of just 11 lines of code, over a naming dispute.
- The web broke in response.

The Register

{* SOFTWARE *}

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

Chris Williams, Editor in Chief Wed 23 Mar 2016 // 01:24 UTC

UPDATED Programmers were left staring at broken builds and failed installations on Tuesday after someone toppled the Jenga tower of JavaScript.

A couple of hours ago, Azer Koçulu unpublished more than 250 of his modules from **NPM**, which is a popular package manager used by JavaScript projects to install dependencies.

Koçulu yanked his source code because, we're told, one of the modules was called Kik and that apparently **attracted the attention of lawyers** representing the instant-messaging **app** of the same name.

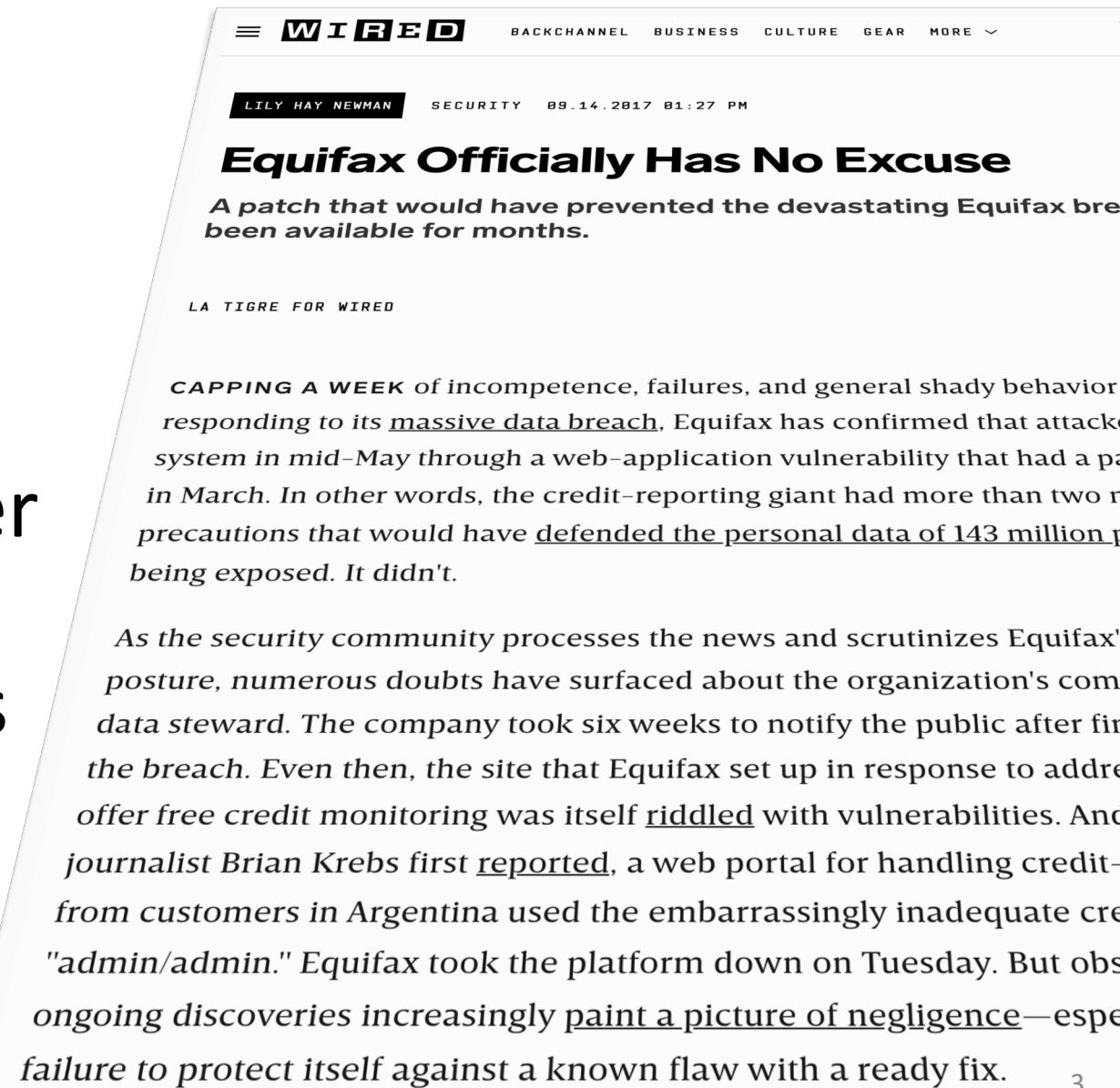
According to Koçulu, Kik's briefs told him to rename the module, he refused, so the lawyers went to NPM's admins claiming brand infringement. When NPM took Kik away from the developer, he was *furious and unpublished all of his NPM-managed modules*. "This situation made me realize that NPM is someone's private land where corporations are more powerful than the people, and I do open source because *Power to The People*," Koçulu blogged.

Unfortunately, one of those dependencies was **left-pad**. The code is shown below. It pads out the lefthand-side of strings with zeroes or spaces. Thousands of projects including Node and Babel relied on it.

With left-pad removed from NPM, these applications and widely used parts of open-source infrastructure were unable to obtain the dependencies they needed, thus fell over during development and deployment. Thousands, in fact, worldwide. Left-pad was fetched 2,486,696 times in just the last 24 hours, according to NPM. It was that popular.

The equifax disaster

- Security breach through vulnerability in Apache Struts dependency
- Details stolen for 143M user accounts
- Estimates of >\$4B damages
- Patch was available for more than two month



Untamed Use of Dependencies

```
package.json x
1  {
2    "name": "csv-parser",
3    "version": "1.9.3",
4    "description": "Streaming CSV parser that aims for maximum speed",
5    "repository": {
6      "type": "git",
7      "url": "git+https://github.com/mafintosh/csv-parser.git"
8    },
9    "dependencies": {
10     "generate-function": "^1.0.1",
11     "generate-object-property": "^1.0.0",
12     "inherits": "^2.0.1",
13     "minimist": "^1.2.0",
14     "ndjson": "^1.4.0"
15   },

```

Dependencies

Library

«depends»

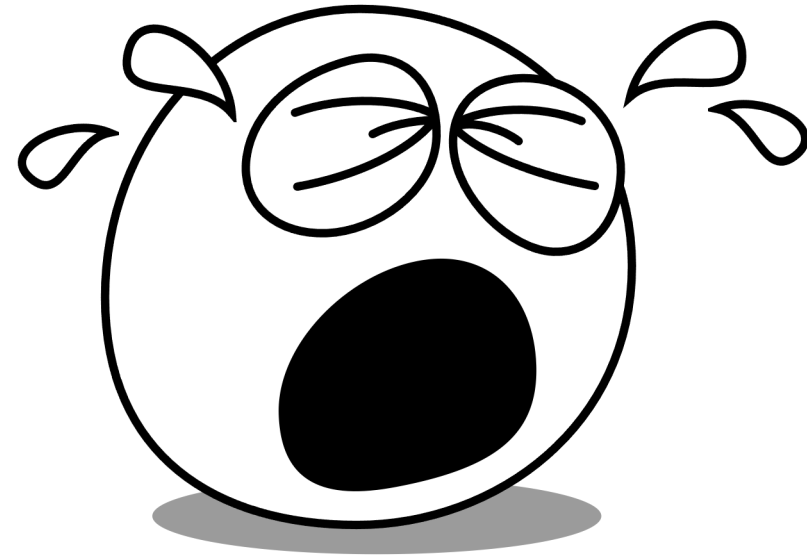
Transitive Dependencies

```
package.json x
1  {
2    "name": "ndjson",
3    "version": "1.5.0",
4    "description": "streaming newline delimited json parser + serializ",
5    "main": "index.js",
6    "scripts": {
7      "test": "tape test.js"
8    },
9    "bin": {
10     "ndjson": "cli.js"
11   },
12   "author": "max ogden",
13   "license": "BSD-3-Clause",
14   "dependencies": {
15     "json-stringify-safe": "^5.0.1",
16     "minimist": "^1.2.0",
17     "split2": "^2.1.0",
18     "through2": "^2.0.3"
19   },

```


The Sorry State of the Art

- Not much beyond simple **package version** matches
- No support for **assessing updates**
- No support for making decisions on which **libraries to use**
- No support for **maintainers**



We need to do better than that!

H2020 EU Project: FASTEN



Delft University of Technology



Software Improvement Group



**Athens University of
Economics and Business**



XWiki



Endocode



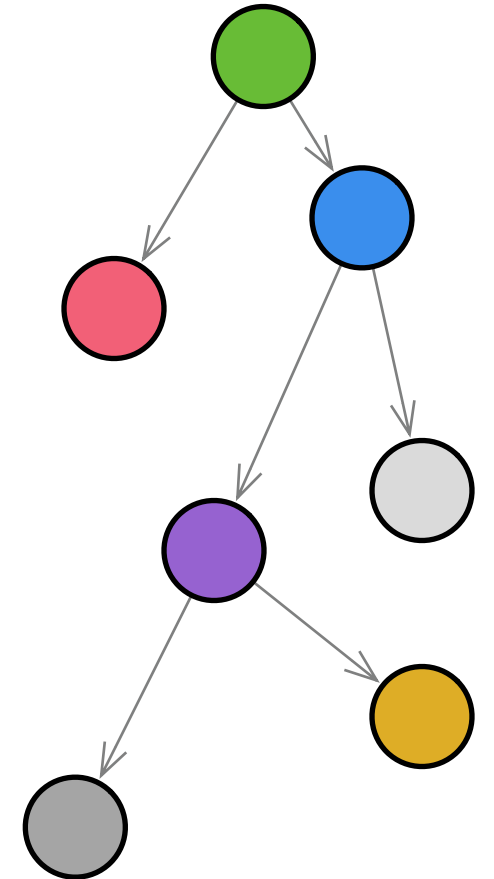
University of Milano



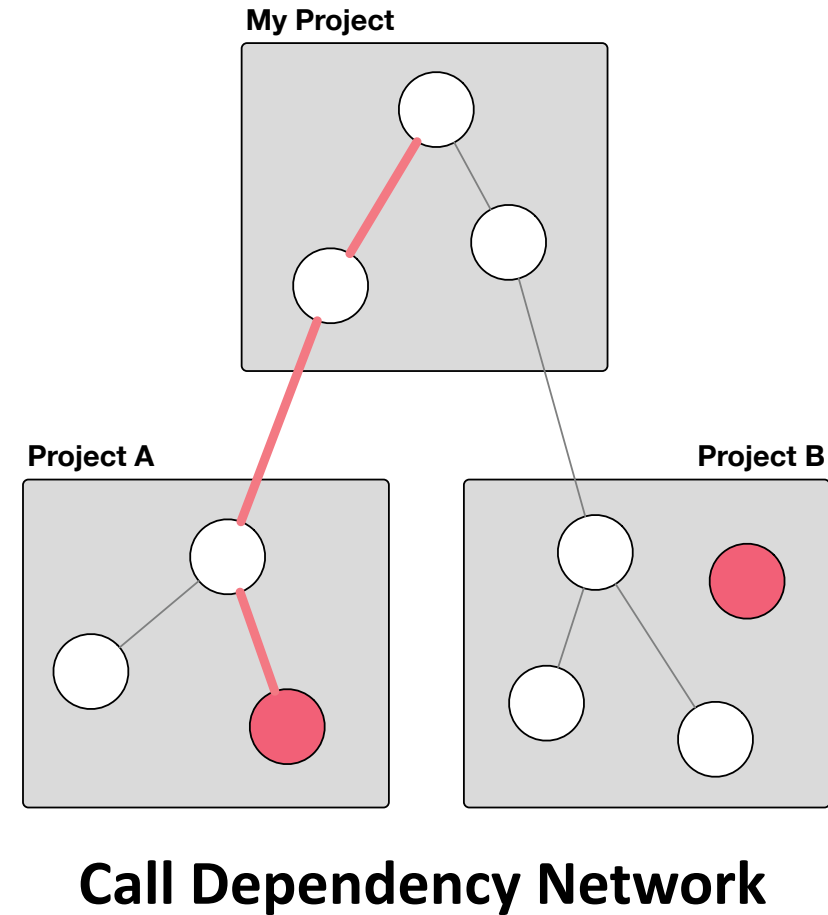
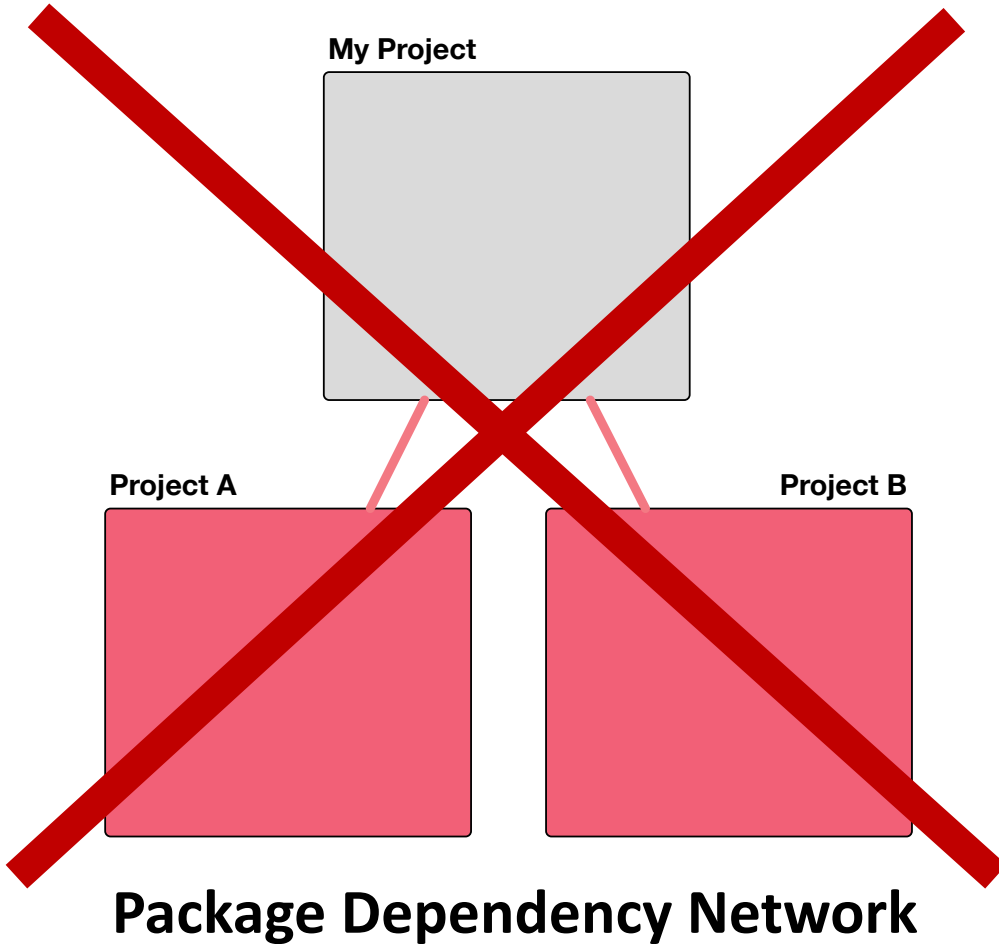
OW2

FASTEN: Revolutionize Dep. Management

- Improve **Vulnerability Detection**
- Reliable **Impact Analysis**
- Better **License Management**

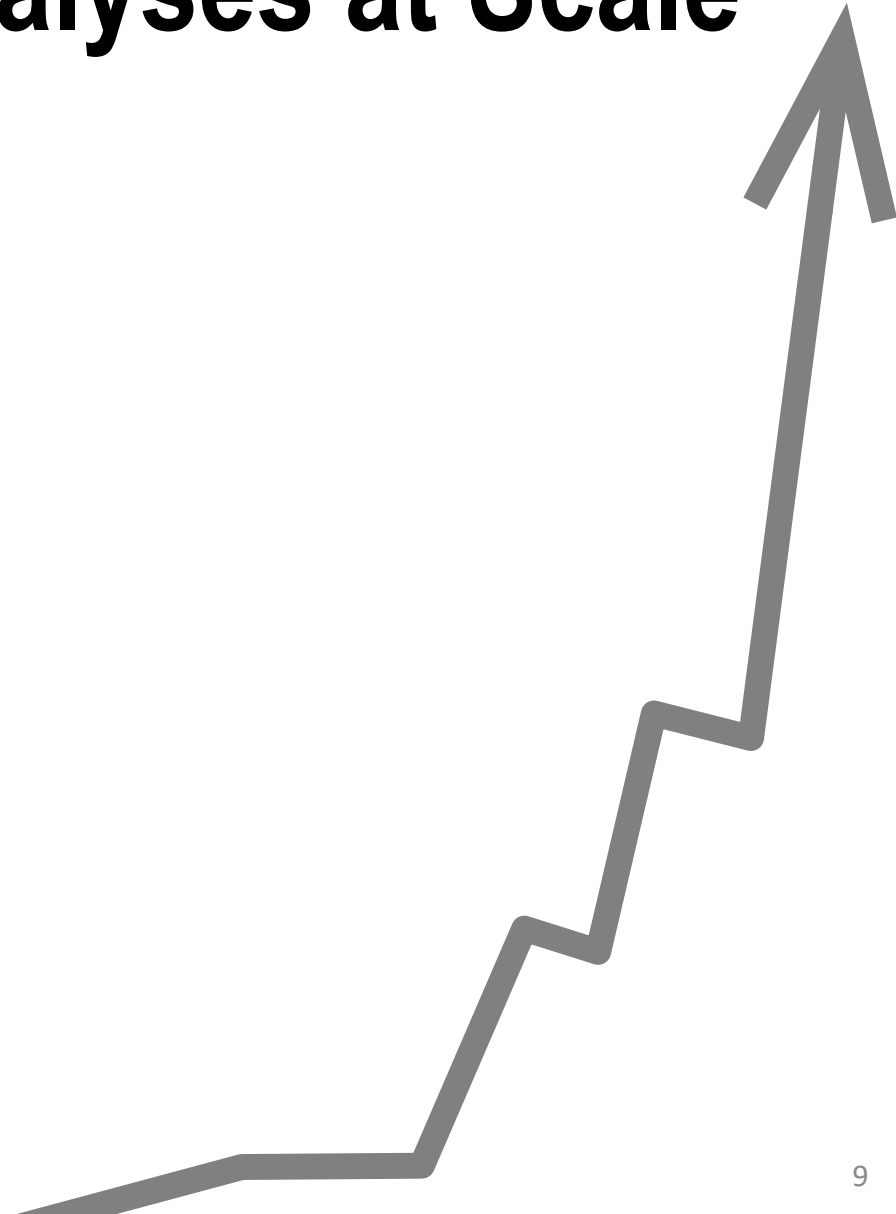


Dependency Networks



Our Research Goal: Static Analyses at Scale

- Scale Call-Graph Generation
- Use Cases
 - Licensing
 - Impact analysis
 - Vulnerability Detection
- Infrastructure



Incremental Call-Graph Generation

1. Resolve

2. Compute (and cache) results

3. Merge Into Complete CG

Comparative Accuracy to State of the Art Approaches

Dependency Set

HTTPClient-0.3-3.jar
abbot-0.13.0.jar
Abbot-0.12.3.jar
costello-1.4.0.jar

abbot:abbot:jar:0.13.0

abbot:abbot:jar:0.12.3

abbot:costello:jar:1.4.0

...

Type Hierarchy

Call Sites

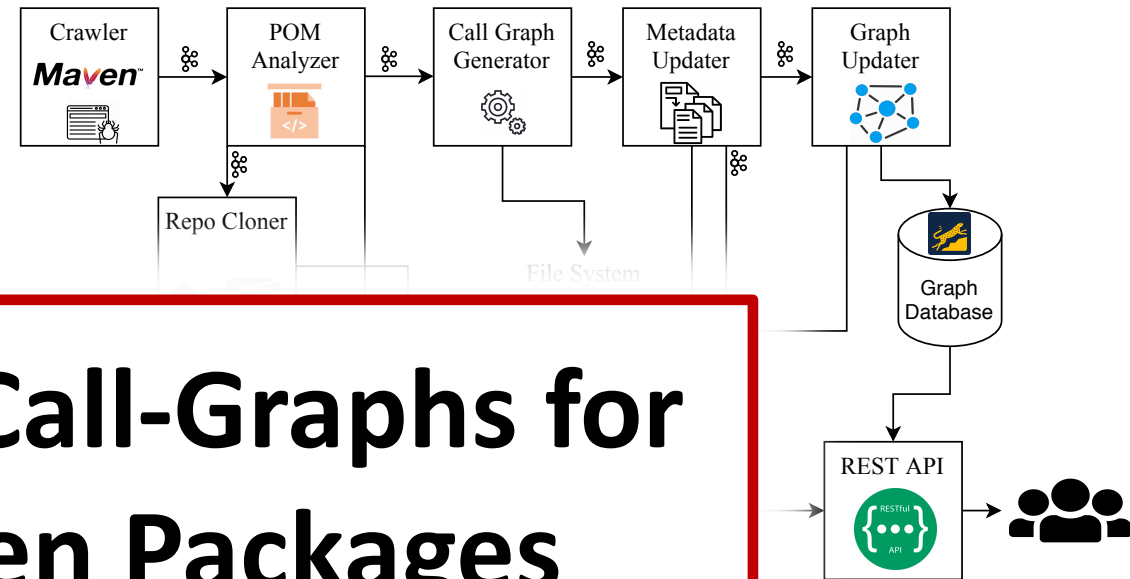
61% Speed-up on Cached Call-Graph Generation

Data Processing Pipeline

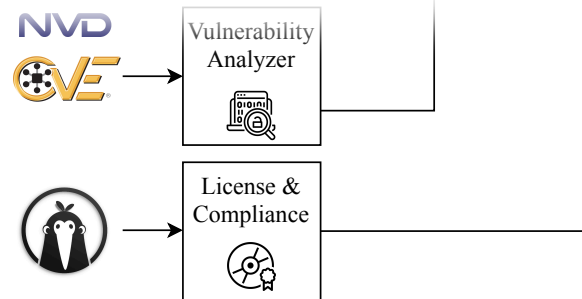
Kubernetes Cluster

- 4 Machines
- 120 Cores
- 1.25 TB
- 233 TB

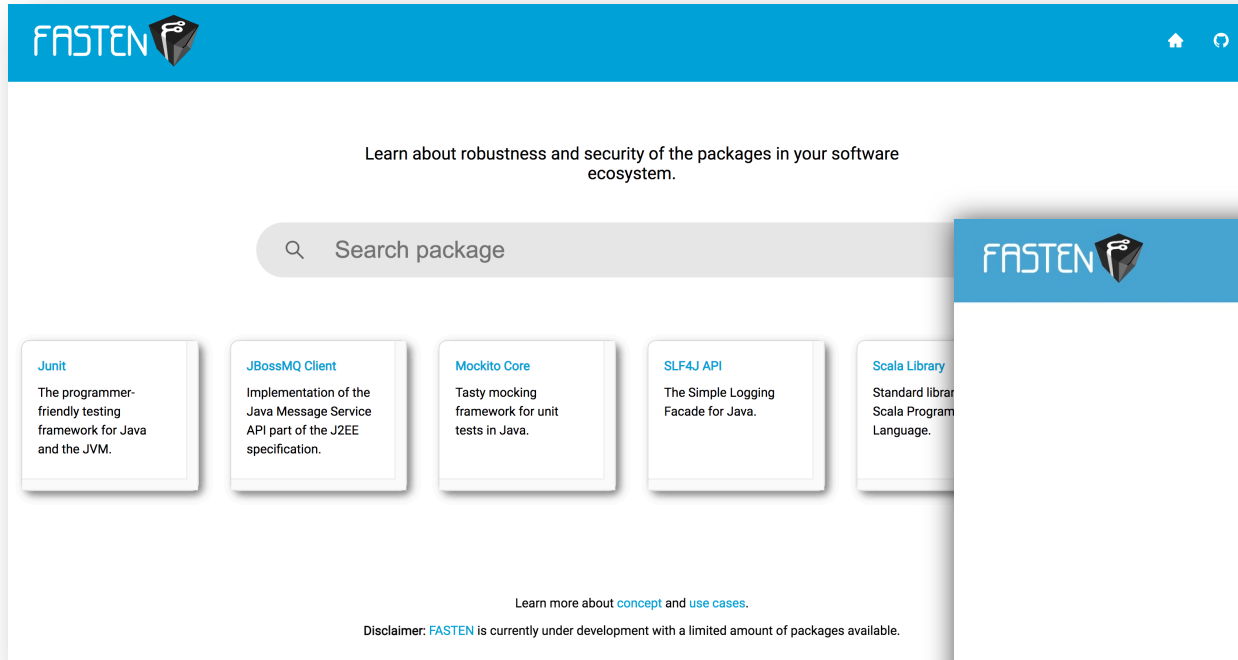
**We have Call-Graphs for
3M+ Maven Packages**




Apache Kafka



Browsable Dependency Information



FASTEN 

Learn about robustness and security of the packages in your software ecosystem.

Search package

- JUnit**
The programmer-friendly testing framework for Java and the JVM.
- JBossMQ Client**
Implementation of the Java Message Service API part of the J2EE specification.
- Mockito Core**
Tasty mocking framework for unit tests in Java.
- SLF4J API**
The Simple Logging Facade for Java.
- Scala Library**
Standard library for Scala Program Language.

Learn more about [concept](#) and [use cases](#).

Disclaimer: FASTEN is currently under development with a limited amount of packages available.

proof-of-concept



FASTEN 

JUnit 4.12

Modules Vulnerabilities Versions

Vulnerabilities

- AknowledgmentRequest.init()
 - `JavaLang.Parse()`
 - `ParserJackson.ParseJson()`
- Connection.newThread()
 - `EasyThreading.threadRequest()`
- DurableSubscriptionID.getClientId()
 - `UserRequest.getUser()`
 - `NumberGenerator.generateID()`

Build-System Integration



Stay Tuned & Get Ready for Public Testing



@FastenProject



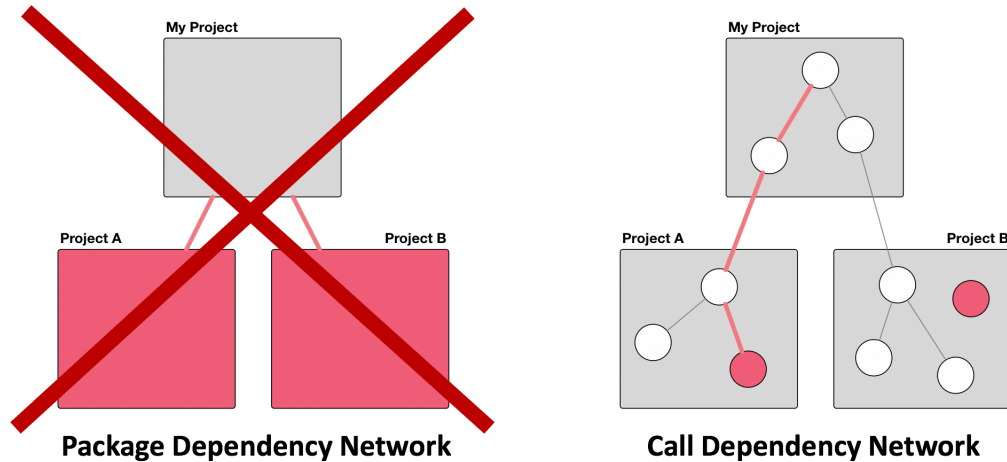
<https://github.com/fasten-project>



<https://www.fasten-project.eu/>

Summary

Dependency Networks



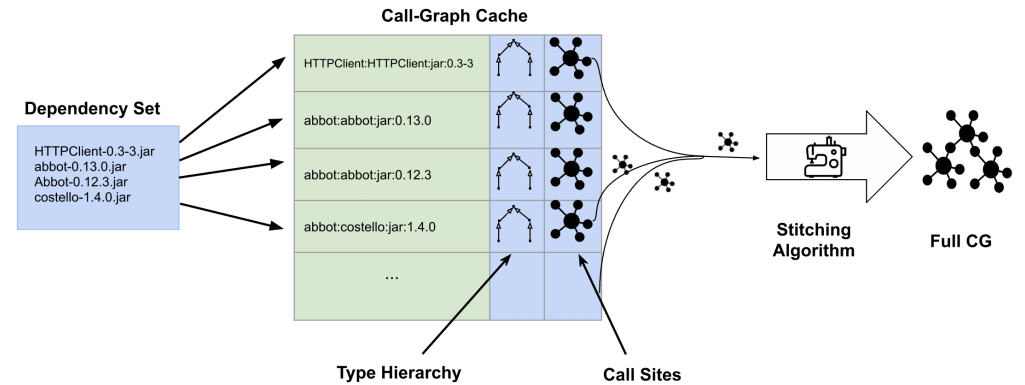
8

Incremental Call-Graph Generation

1. Resolve Dependencies

2. Compute (and cache) partial results

3. Merge Into Complete CG



Sebastian Proksch

S.Proksch@tudelft.nl

Delft University of Technology

www.fasten-project.eu



Build-System Integration

