ISCAS 中国科学院软件研究所学术年会’2022
暨计算机科学国家重点实验室开放周

工具系统

面向npm的第三方开源软件风险分析工具

丁昊[†]，向雨新，朱家鑫[*]，窦文生，魏峻
{ † dinghao19， * zhujiaxin }@otcaix.iscas.ac.cn

应用需求

复用第三方软件是一种普遍的软件开发实践，在开源JavaScript生态中尤其如此，平均每个npm包会复用超过80个其他npm包

近年来，复用（或使用）第三方开源软件引发的问题屡见不鲜：

left-pad等独立开发者npm包被广泛使用

2016 年 3月，left-pad的所有者Azer Koçulu停止提供该包，令包括Node、Babel在内的数千项目无法构建

开源软件许可证规定了相关的权利和义务

2016年，一家韩国企业在其出售的软件产品中使用了AGPL授权的软件构件，被开发该构件的公司起诉

OpenSSL是互联网软件安全通信的根基

2014年，OpenSSL被爆出严重安全漏洞HeartBleed，波及了购物、网银、社交、门户等众多知名网站

软件项目（用户）需要准确知晓其使用的开源npm包带来的风险

工具特性

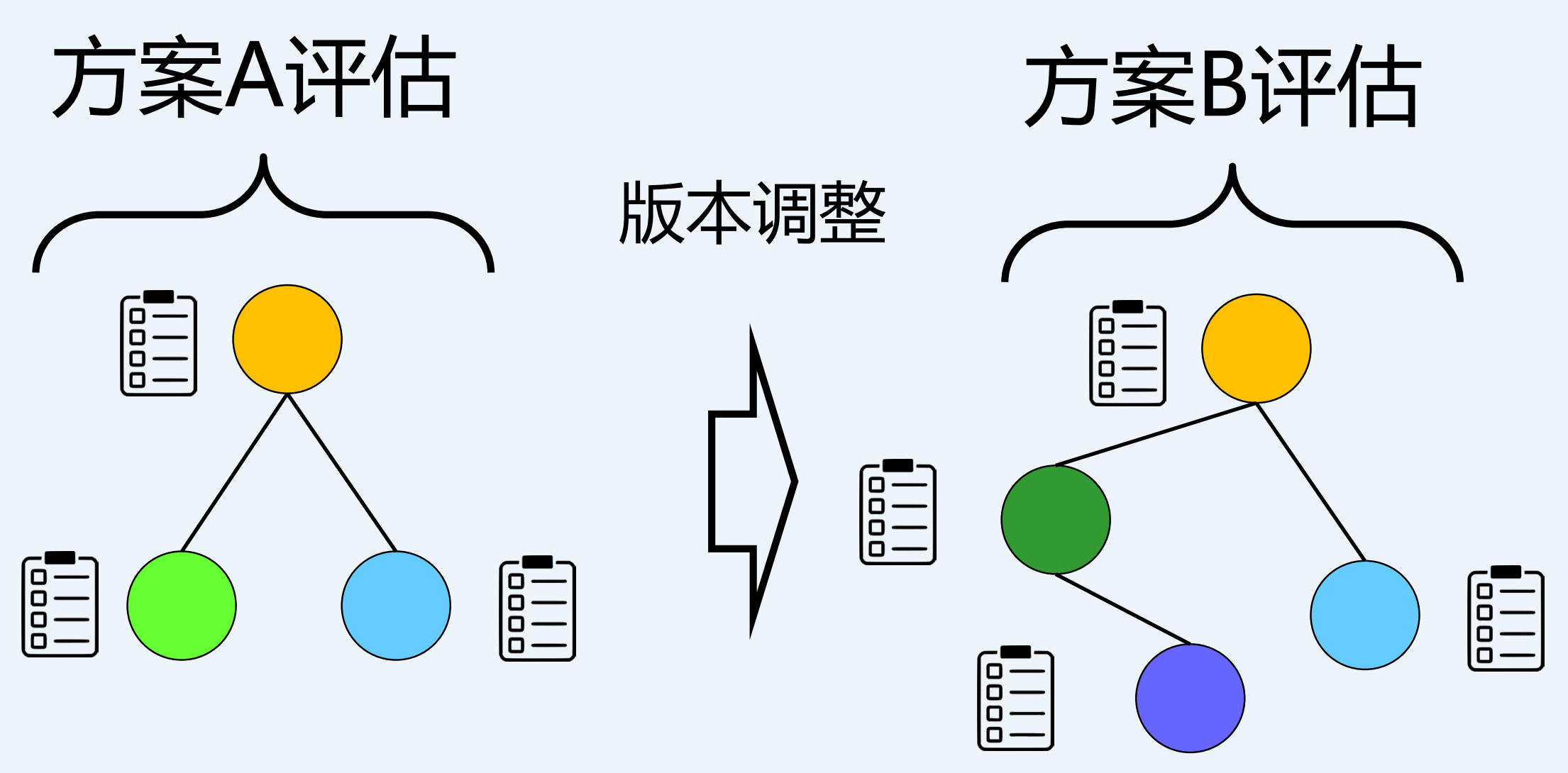
面向核心关切点的软件属性量化体系

技术支持可持续性

知识产权合规性

安全等传统属性

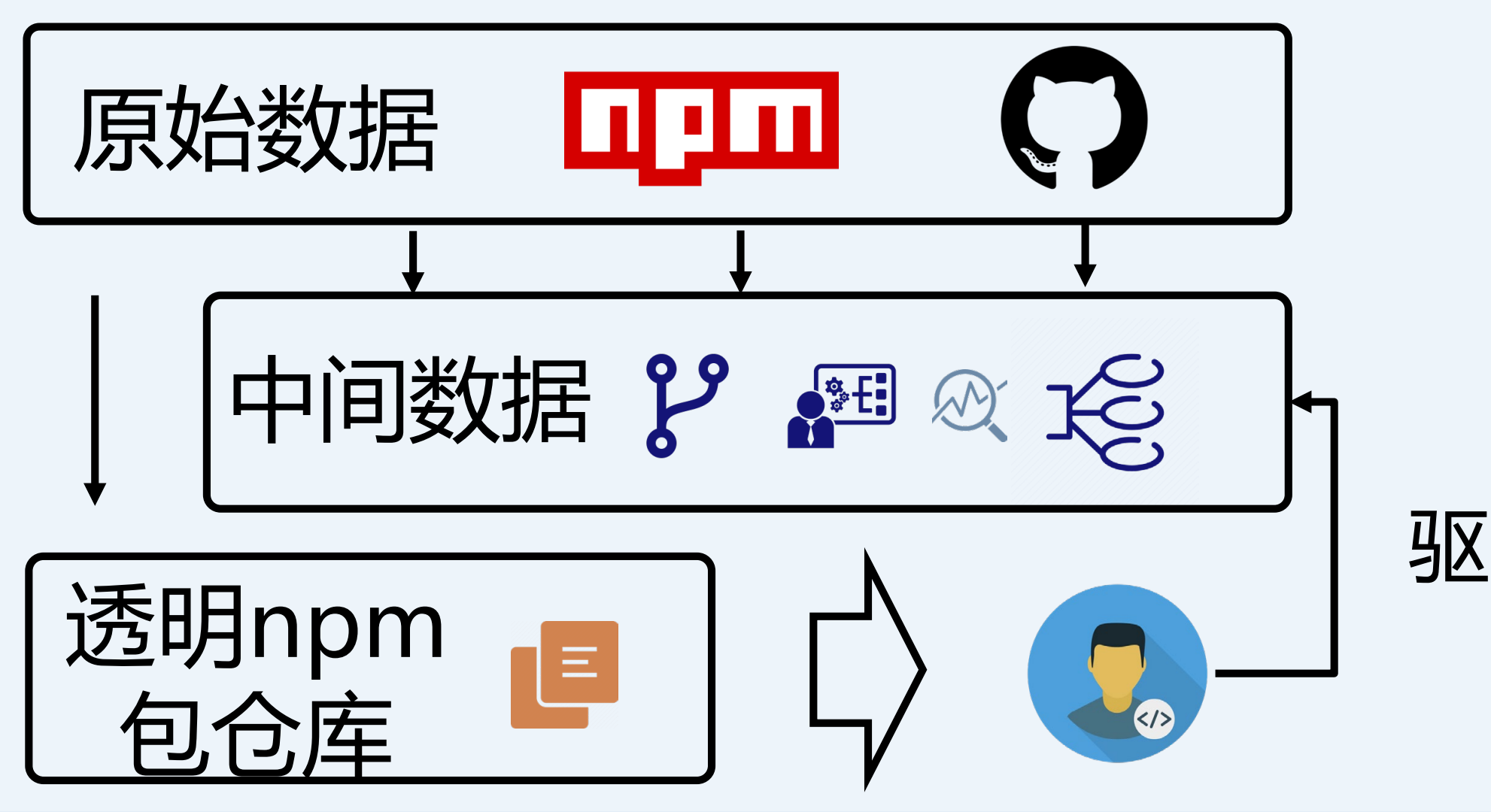
基于完整依赖视图的精准分析



有效的风险评估技术

- 软件维护行为预测
- 许可证兼容性问题检查
- 关键属性数据收集与分级

大规模依赖数据的高效管理



应用效果

工具展示目标npm包及其所有依赖包的相关量化属性，提示风险点位，给出优化建议

技术支持可持续性评级示例

array-flatten	3
execa	2
cross-spawn	4

知识产权合规性问题示例

@0xgabi/evmcrispr@0.0.1	MIT&LGPL
@jsmlt/jsmlt@0.1.18	ISC&AGPL

高危安全问题数量示例

plist@3.0.0	1
express@4.13.1	3
hapi@18.1.0	5