ISCAS 中国科学院软件研究所学术年会'2024
暨重点实验室科技活动周

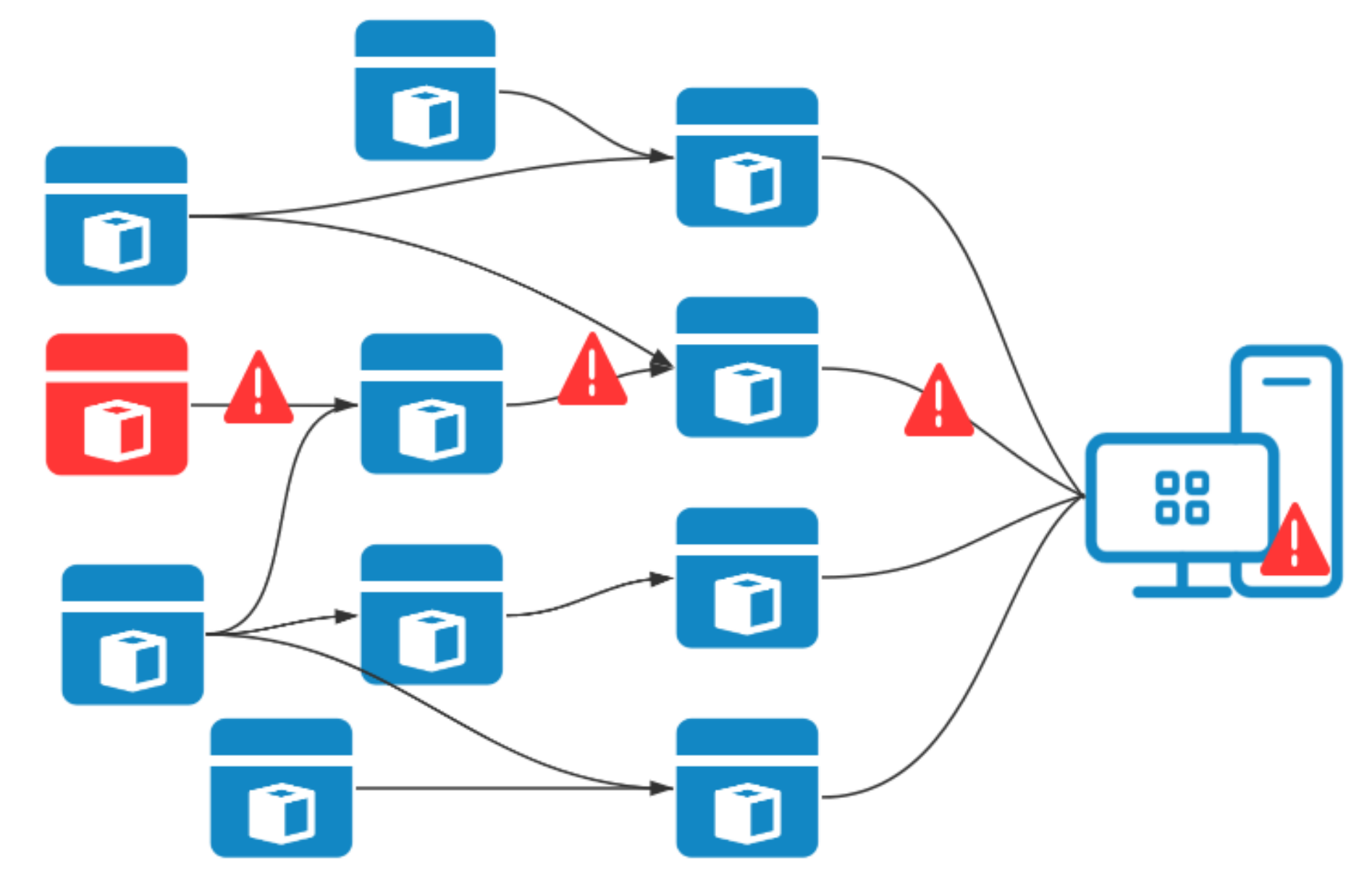
工具系统

Linux发行版SBOM模型与SBOM生成工具

邱童，朱家鑫*，陈伟，魏峻
* zhujiaxin@otcaix.iscas.ac.cn

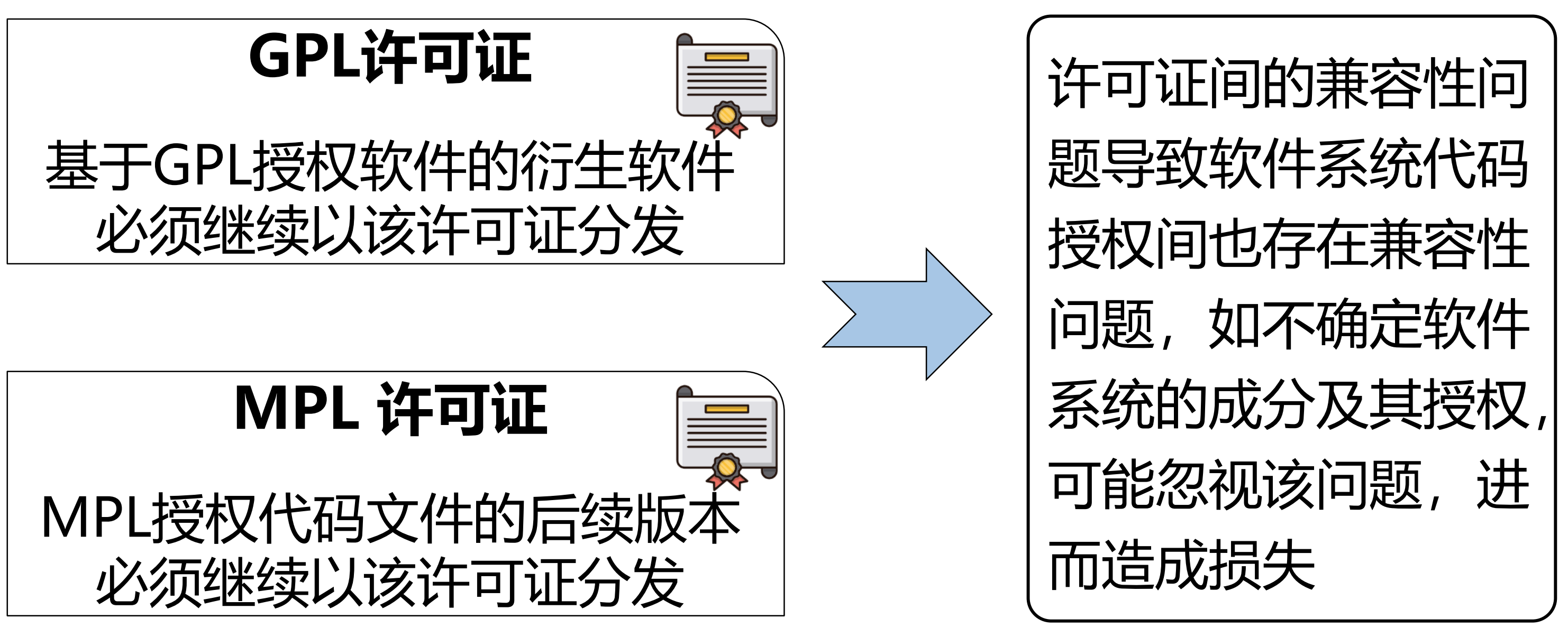
研制背景

现代软件系统常复用大量第三方开源软件（代码），形成复杂的开源软件供应链，软件成分的不透明性隐藏了诸如安全性、合规性、兼容性、可维护性等多种风险。Linux发行版是一类被广泛使用的关键基础软件，其成分尤为复杂，准确识别成分及其问题和风险，成为openEuler等国内外发行版的日益迫切的需求。



Apache Log4j远程代码执行漏洞

漏洞传播



GPL许可证

基于GPL授权软件的衍生软件必须继续以该许可证分发

MPL 许可证

MPL授权代码文件的后续版本必须继续以该许可证分发

许可证间的兼容性问题导致软件系统代码授权间也存在兼容性问题，如不确定软件系统的成分及其授权，可能忽视该问题，进而造成损失

TikTok Live Studio APP因违反GPL条款遭下架

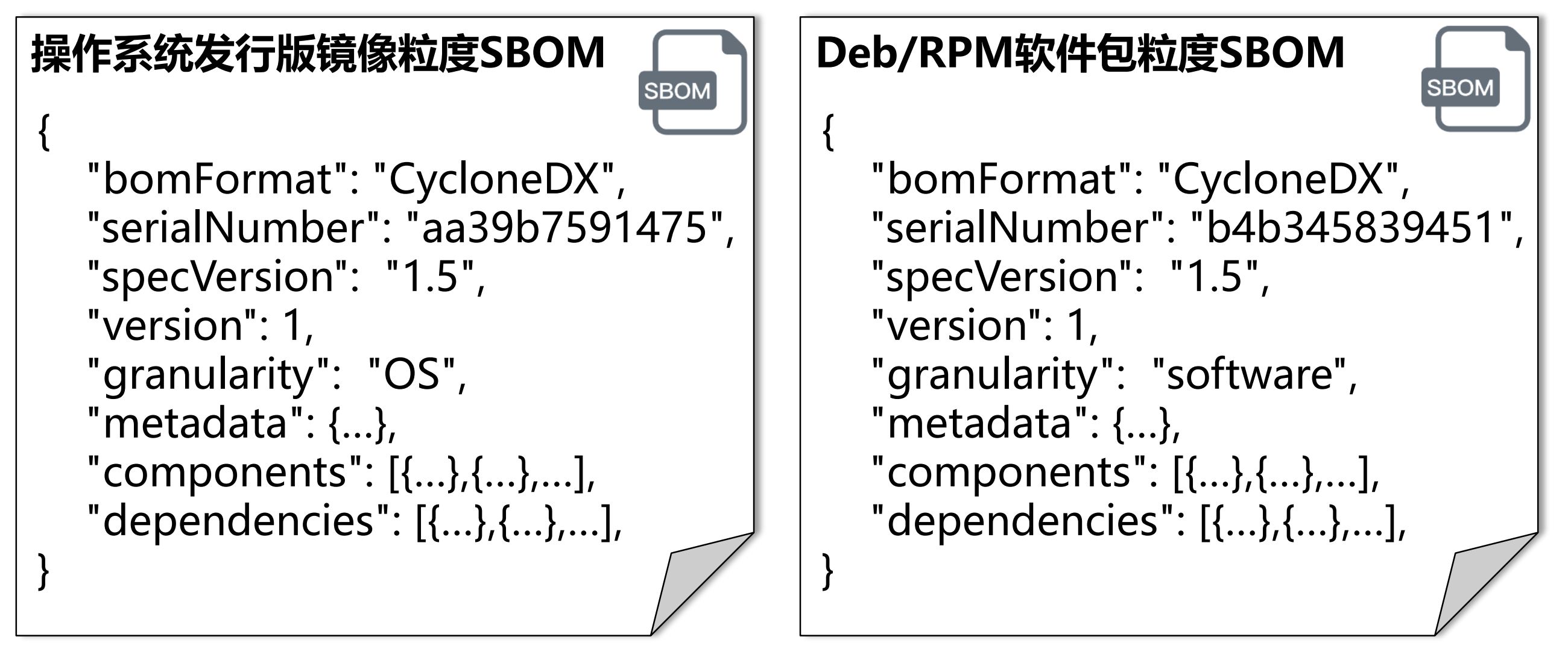
License冲突

Linux发行版SBOM模型

现有通用SBOM模型无法准确反映Linux发行版在不同阶段的成分，难以支持精准的风险识别，我们基于对Linux发行版开发和发布过程的分析结果，提出了多粒度多阶段的Linux发行版SBOM模型。

□ **Linux发行版镜像粒度、Deb/RPM软件包粒度**

□ **不同用户关注的信息各有侧重**



操作系统发行版镜像粒度SBOM

```
{
    "bomFormat": "CycloneDX",
    "serialNumber": "aa39b7591475",
    "specVersion":  "1.5",
    "version": 1,
    "granularity":  "OS",
    "metadata": {...},
    "components": [{...},{...},...],
    "dependencies": [{...},{...},...],
}
```

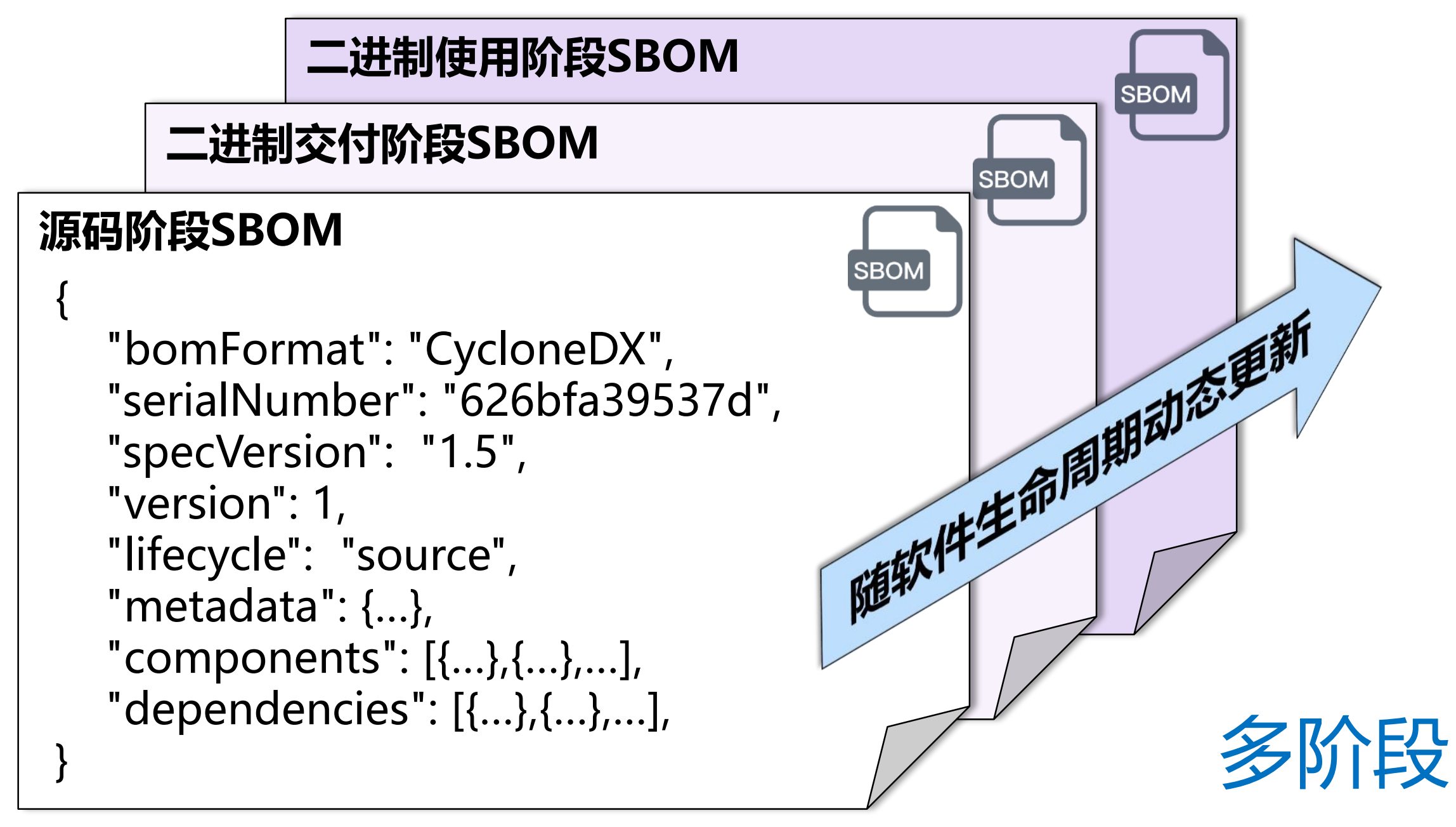
Deb/RPM软件包粒度SBOM

```
{
    "bomFormat": "CycloneDX",
    "serialNumber": "b4b345839451",
    "specVersion":  "1.5",
    "version": 1,
    "granularity":  "software",
    "metadata": {...},
    "components": [{...},{...},...],
    "dependencies": [{...},{...},...],
}
```

多粒度

□ **SBOM按软件包生命周期分阶段**

□ **SBOM在软件开发的早期阶段产生，并持续演进**



二进制使用阶段SBOM

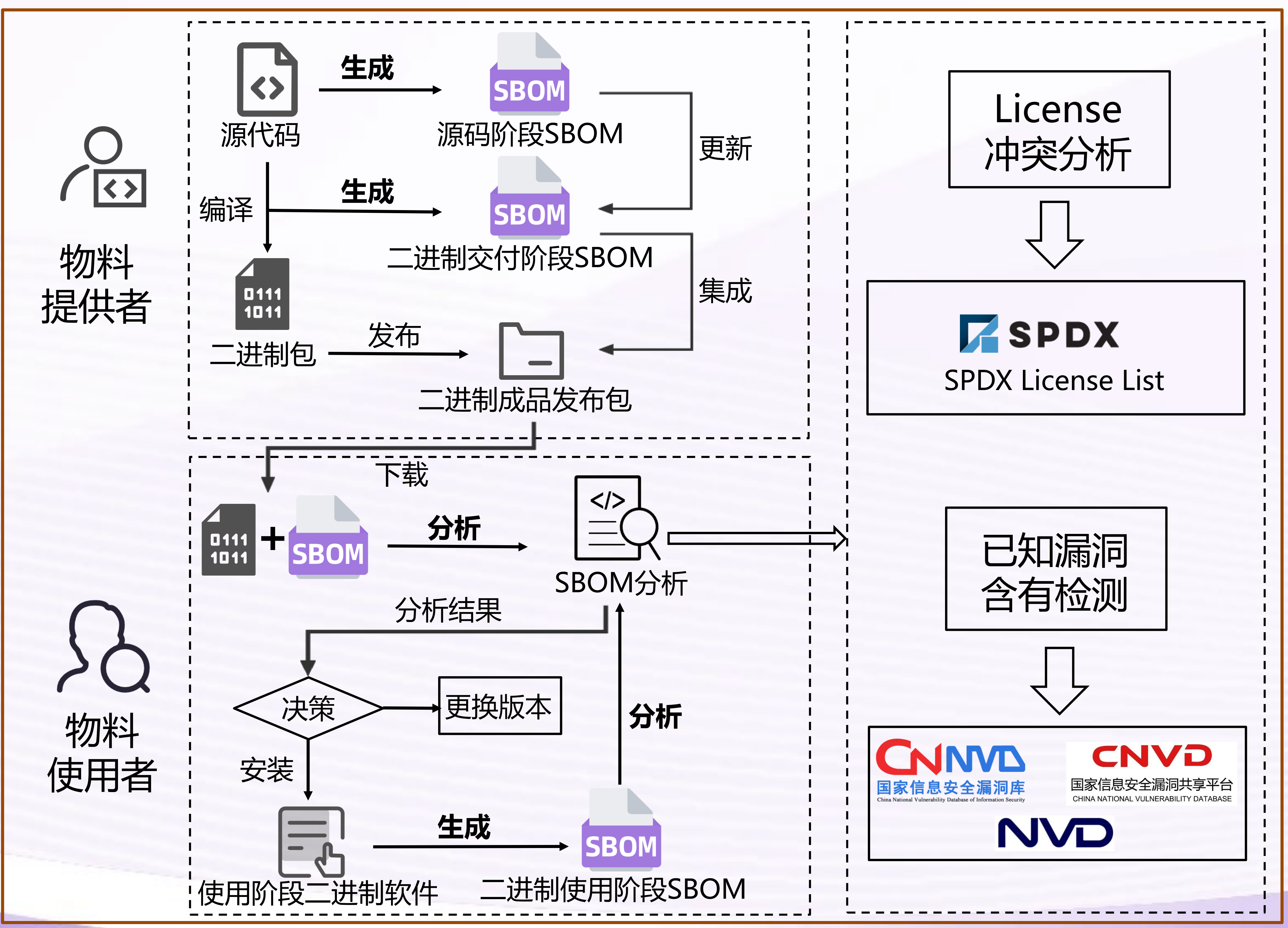
二进制交付阶段SBOM

源码阶段SBOM

```
{
    "bomFormat": "CycloneDX",
    "serialNumber": "626bfa39537d",
    "specVersion":  "1.5",
    "version": 1,
    "lifecycle":  "source",
    "metadata": {...},
    "components": [{...},{...},...],
    "dependencies": [{...},{...},...],
}
```

多阶段

SBOM生成工具



使用本工具可及早发现诸如xz后门（CVE-2024-3094）等已知漏洞对当前软件包或镜像的影响：生成Debian testing，unstable等版本镜像的SBOM可直接发现有后门的xz-utils 5.6.0 和 5.6.1。