CCF-华为胡杨林基金 系统软件专项-2022年系统软件安全技术课题指南介绍

华为技术有限公司 安全技术专家 顾嘉辉

2022年5月15日

系统软件专业委员会
Technical Committee of Systems Software

HUAWEI

系统软件安全的目标

安全可信的系统软件是产品安全可信的基础

系统面临的安全挑战增大，用户对系统可信提出更高要求

系统安全挑战

- 软件规模增大导致漏洞同步上升
- 对于未知漏洞及攻击手段，系统无法提前构建防御能力，导致攻防长期不对等
- 架构演进导致原有防护机制弱化或失效

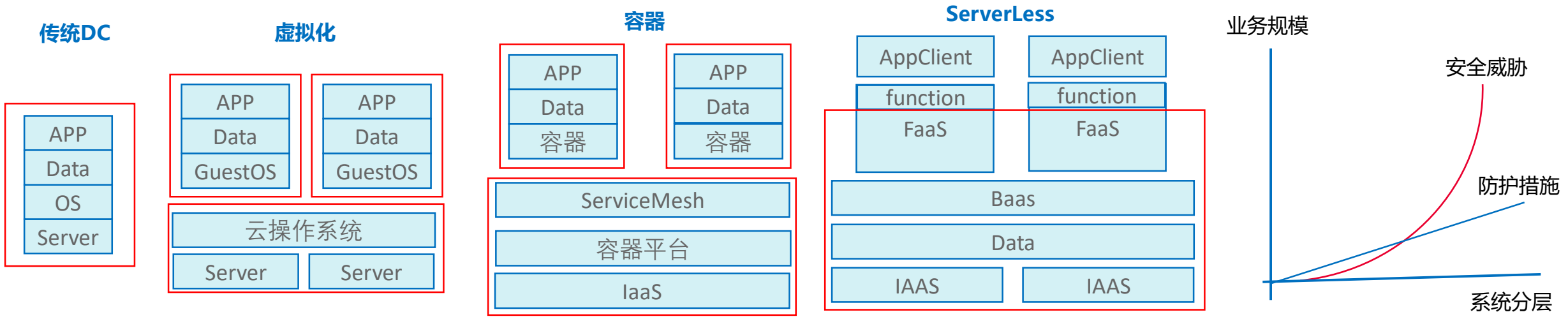
数据资产安全挑战

- 数据价值上升，分布环节广泛，攻击价值上升、攻击面扩大
- 法律法规对数据资产合规有更高要求，一旦泄露影响扩大
- 数据泄露存在不可撤销性

软件开发安全挑战

- 产品大规模集成开源及第三方组件，供应链成为新的攻击面
- 大规模采用开源社区开发模式，社区开发环节成为供应链攻击重要途径

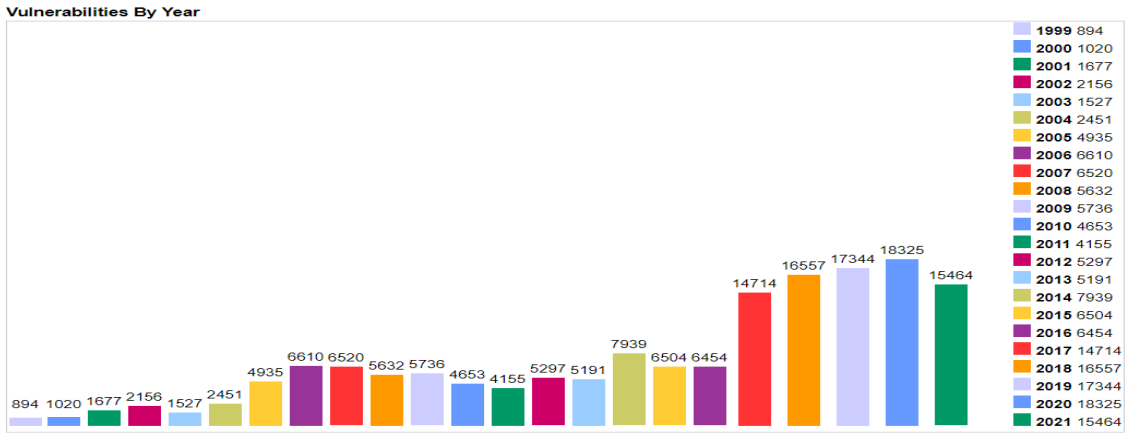
软件分层深化，安全边界逐渐模糊；威胁面及攻击手段累加，线性发展的安全技术无法应对指数上升的安全威胁



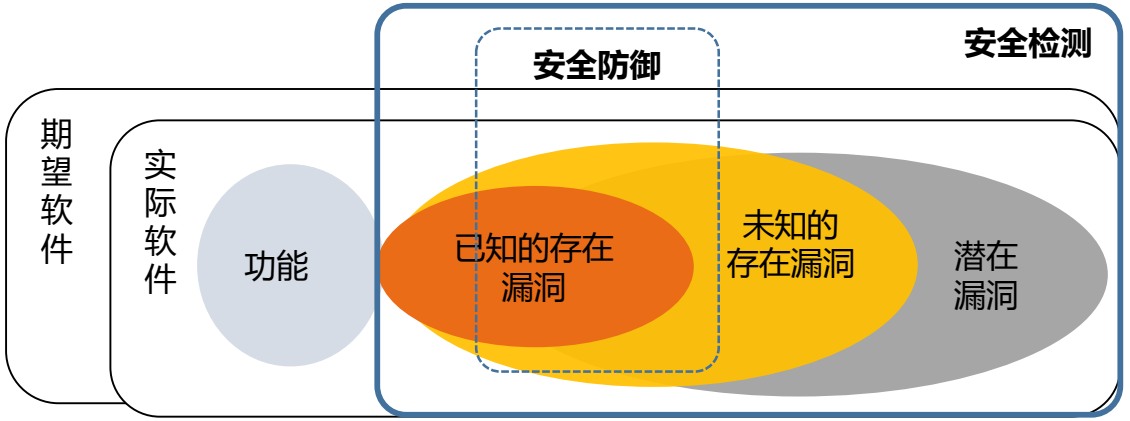
安全挑战		物理机	虚拟化/IaaS	容器/PaaS	ServerLess
系统	安全边界	物理边界	虚拟机-Hypervisor	容器-OS	Function-FaaS
	主要威胁	近端攻击、软件病毒、软件漏洞利用等	虚拟机逃逸	容器逃逸	恶意函数植入
网络	安全边界	数据中心边界网络	租户边界	微服务边界	BaaS服务边界；多云间
	主要威胁	ddos，扫描嗅探，畸形报文攻击，web攻击	利用虚拟机发起攻击；绕过边缘安全设备	绕过主机外安全防护；利用servicemesh网络发起攻击	针对API网关或IOT网关攻击；利用function触发攻击

构建系统内生的纵深和主动防御能力，提升系统韧性

漏洞不可避免且持续增加：随着软件复杂度提升漏洞逐年增加，漏洞的修补和部署成本高，漏洞修补的及时性和有效性难以保证，



被动防护体系难以应对复杂挑战：对于频发的未知威胁、侧信道攻击等检测和防御能力不足。



系统安全挑战

- 安全边界模糊，传统边缘安全机制失效
- 软件规模剧增，漏洞无法杜绝且修复成本高
- 攻击手段多样，系统无法提前应对未知威胁
- 系统运行平台多样化，硬件防护能力参差不齐

潜在技术方向

- 防护增强：基于不同硬件能力构建安全防护能力，异构TEE支持多种TCB
- 系统韧性：多级隔离和访问控制能力（容器-进程-函数），构建纵深防御能力，降低单点缺陷影响
- 主动防御：基于系统行为的入侵检测和主动防护技术，增强对未知攻击的感知

以数据为中心业务趋势下，为数据提供安全提供安全运行环境是系统安全关键价值

数据规模增大，促进存内计算等新计算架构发展

挑战一：对数据的攻击行为增多，缺少针对数据全生命周期的保护措施

挑战二：以数据为中心架构下，传统系统防护技术易被绕过

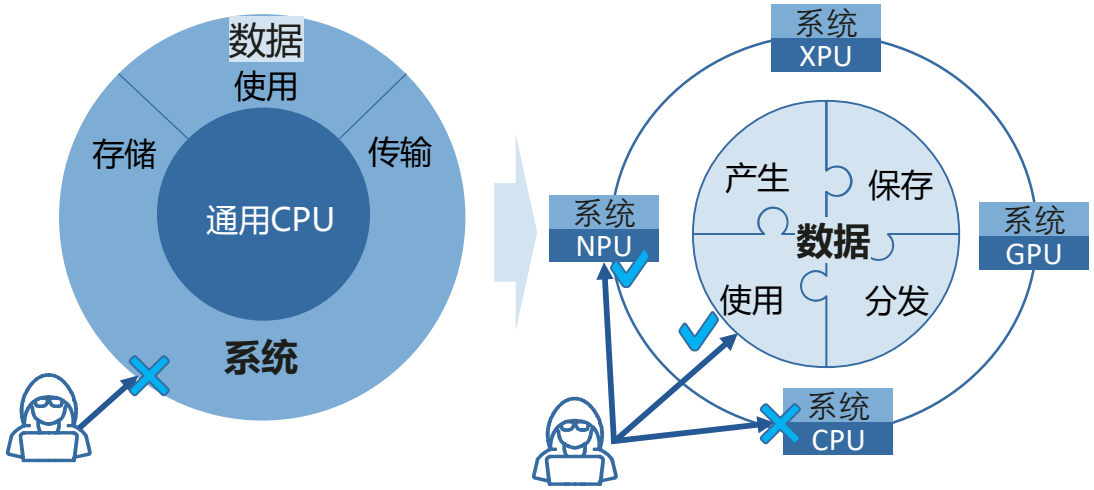
数据在运行态缺少保护

存储态
保护措施：磁盘加密、文件加密、文件权限等
主要挑战：密钥泄露，算法漏洞，权限配置错误

运行态
保护措施：权限隔离、进程隔离等
主要挑战：软件漏洞无法杜绝、数据在内存中明文

传输态数据保护
保护措施：传输通道加密、网络隔离等
主要挑战：密钥泄露，算法漏洞，网络入侵

计算架构演进，传统系统防护技术易被绕过



潜在技术方向：新计算架构下的系统安全技术，包括异构算力单元对数据的访问控制，安全DMA等技术

HUAWEI

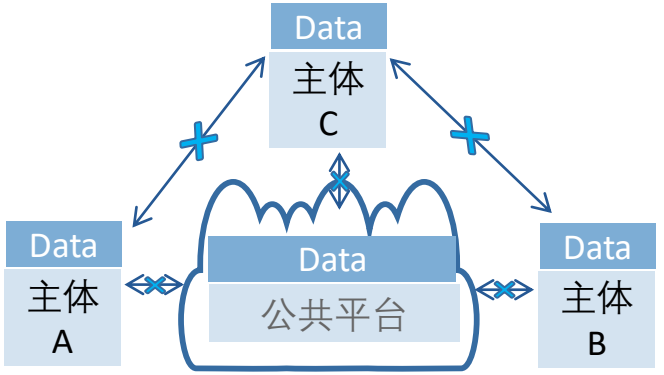
数据驱动业务场景下，数据资产安全合规使用成为实现数据价值变现的关键

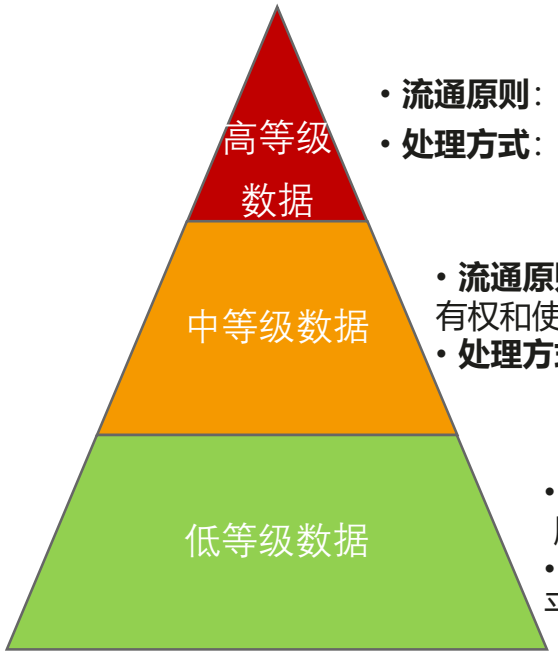
云计算深入发展：信息资产分离部署，端边云协同发展

挑战一： 基础设施分离部署导致可信链被打破，阻碍关键业务上云

挑战二：数据多方共享与隐私保护的矛盾，阻碍云上数据价值创造

挑战三：政策法规对数据等级和使用规范有明确要求，对数据合规使用提出更高要求





4/5级数据

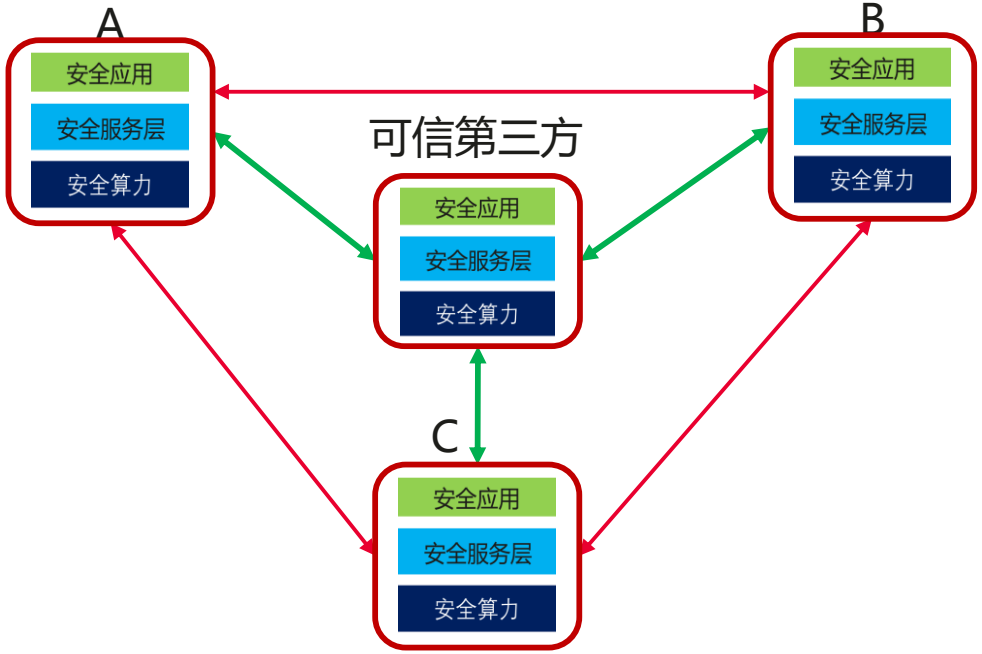
- **流通原则**：不允许流通，其所有权和使用权不能让渡
- **处理方式**：在数据所有者领地内进行

2/3级数据

- **流通原则**：通过**隐私计算**手段进行流通，其所有权和使用权可适当让渡
- **处理方式**：在数据所有者领地内或**可信方**进行

1级数据

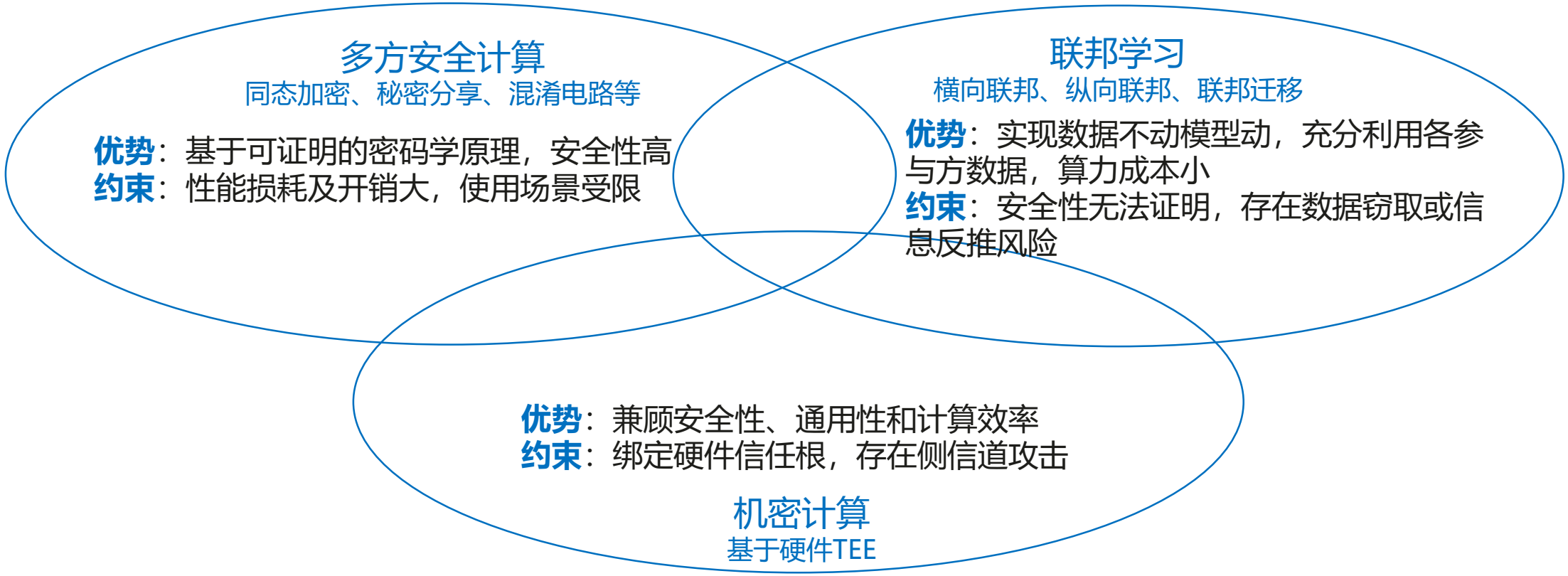
- **流通原则**：通过各种公开途径获得使用，所有权和使用权可让渡
- **处理方式**：本地、第三方、各数据开放平台



HUAWEI

数据驱动业务场景下，数据资产安全合规使用成为实现数据价值变现的关键

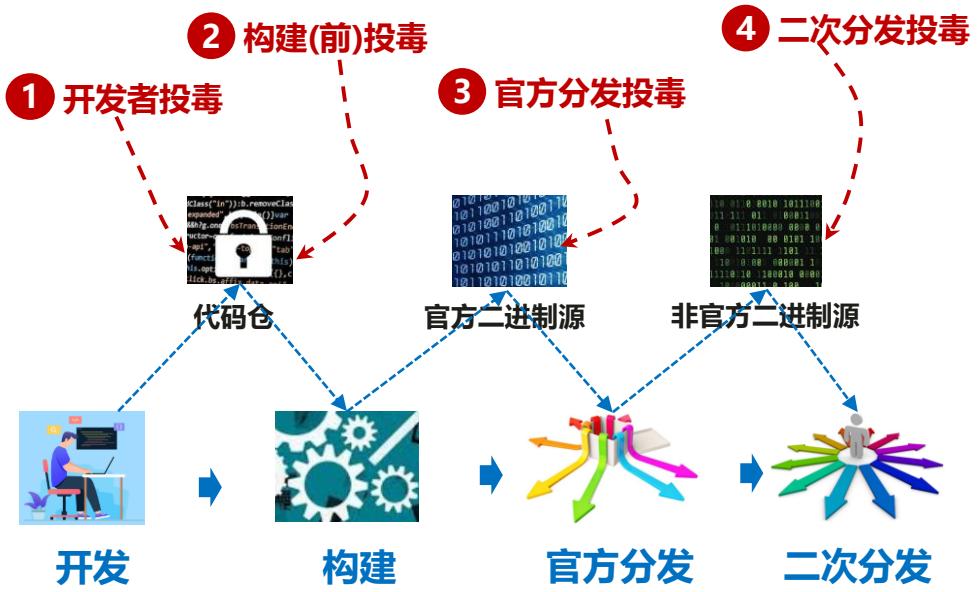
政务领域	金融领域	医疗领域	……
跨部门协同、政企共享	联合风控、反洗钱	联合建模、数据聚合	



潜在技术方向：提供普惠安全算力，系统原生隐私计算框架支持大数据、AI等安全应用

软件开发模式变化：软件生产过程成为攻击面，供应链投毒攻击日益增多

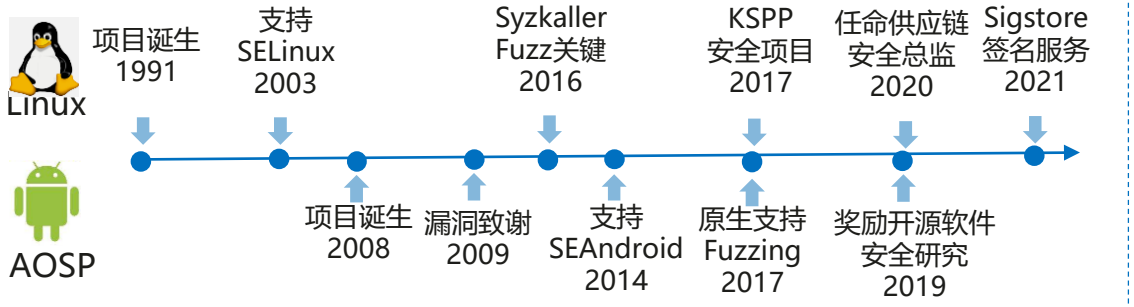
产品阶段	组件引入	软件开发	软件构建	软件发布	软件部署	系统运行
攻击手段	➢ 开源社区恶意代码植入 ➢ 恶意组件	➢ 代码非法合入 ➢ 开发工具	➢ 编译构建环境入侵 ➢ 构建工具篡改	➢ 非法软件源 ➢ 传输过程篡改	➢ 恶意修改系统组件、配置	➢ 漏洞利用
防护措施	• 代码检视	• 代码检视 • 编码规范	• 网络隔离	• 软件包签名	• 安全扫描 • 系统加固	• 漏洞防利用



投毒环节	可能投毒者	典型案例
开发	恶意开发人员	明尼苏达大学向Linux内核社区提交存在漏洞的patch。
构建	黑客	APT组织UNC2452，入侵SolarWinds公司，篡改源码植入恶意代码，构建后通过该公司的官方网站正式发布。
官方分发	黑客	攻击者在开源仓库（PyPI/RubyGems/NPM）发布恶意包，用户从官方渠道下载安装后中招，当前已发现170多起投毒案例。
非官方二次分发	黑客	黑客对Xcode植入恶意代码，通过非苹果官方渠道分发，开发这下载后编译出的APP被自动植入恶意代码。

建设安全基础设施、保障供应链安全，构建软件安全系统化防护体系

开源社区从单点安全特性逐步向整体安全架构、供应链安全和安全基础设施等系统化建设方向发展



分类		社区安全能力发展趋势
安全架构		**单点安全技术→ 整体安全架构** • Linux社区创立KSPP安全项目 • AOSP建立SEAndroid项目
供应链安全		**自身安全 → 上下游供应链安全** • Linux基金会任命供应链安全总监 • Linux建立Sigstore签名服务
安全基础设施	漏洞挖掘	**单个漏洞奖励 → 漏洞挖掘等基础设施** • Linux社区产生Syzkaller fuzz • AOSP原生支持Fuzzing
	安全开发	**单一构建工具支持→安全开发基础设施支持** • Github支持Yarn Audit（漏洞审计）、LGTM(持续安全分析)等

围绕开源件健康度和依赖度评估、漏洞感知与修复等系统化建设，是供应链安全发展的重点

开源软件使用存在的薄弱点

缺少安全Metadata
（缺乏文档、LICENSE、反馈渠道、维护状况等）

未做到默认安全
（使用不安全的加密算法、协议、设计等）

软件依赖链不明确
（较难获知依赖链的安全状况）

开源软件漏洞风险

漏洞库信息缺乏
（具体版本漏洞信息不准确）

代码质量参差，存在漏洞风险
（潜在漏洞数量多）

标准+基础设施促进上游社区改进

业界安全实践

2020年布局OpenSSF社区，构建开源社区安全能力量化评估体系

2021年发布OSI（Open Source Insights），建立开源软件依赖链信息库

2021年发布OSV（Open Source Vulnerabilities），建立开源软件漏洞信息库，支持开源版本漏洞查询

发布OSS-Fuzz平台及Patch奖励项目，提供Fuzz算力和修复资源，增强开源软件漏洞挖掘力量

潜在研究方向：软件要素分析和溯源技术、漏洞自动化挖掘技术、面向软件供应链的投毒检测和拦截技术

系统软件安全技术方向课题指南

端边云协同场景下用户对于系统和数据的安全可信有了更多关切，计算架构演进对传统安全模型带来了新的挑战，基于开源社区进行大规模软件开发带来了新的威胁，针对以上变化趋势，需要探索和构建相关安全技术，保障系统和数据安全。

包括但不限于

- 构建系统内生安全能力，实现数据安全共享，面向隐私计算等研究方向，探索包括异构TEE、系统原生安全多方计算\联邦学习框架等；
- 面向以数据（内存）为中心架构演进，研究非冯架构下的系统安全技术，包括多算力单元对数据的访问控制，安全DMA等技术；
- 针对大规模软件系统自身缺陷以及供应链攻击带来的威胁，探索软件要素分析和溯源技术，漏洞自动化挖掘技术、面向软件供应链的防投毒技术。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI