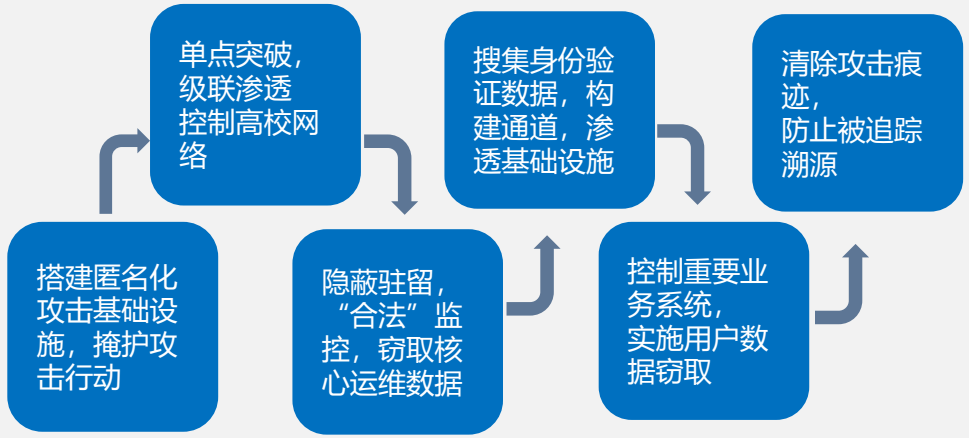
CCF-华为胡杨林基金 系统软件专项2023年指南发布
系统软件安全技术课题指南

2023年4月7日

HUAWEI

热点事件启示



攻击事件	事件影响
2022年某高校攻击事件	攻击时间跨度长达数年，140G敏感数据泄露，运营商网络被渗透控制
2021年全美最大油气输送管道运营商Colonial Pipeline遭勒索	启动应急响应后停止所有管道运行，美国宣布进入国家紧急状态
2015年乌克兰电网攻击事件	停电长达6小时，直接影响超过20万居民
2010年伊朗核设施遭攻击事件	近1/5的离心机，感染了20多万台计算机，导致1000台机器物理退化

APT具有长期渗透，隐蔽高，攻击手段先进，关键信息基础设施面临威胁压力增大。

生产端面临新挑战

安全挑战1：
数据包含敏感、有害、偏见内容

安全挑战2：
算法不鲁棒易受对抗攻击影响，缺乏可解释性

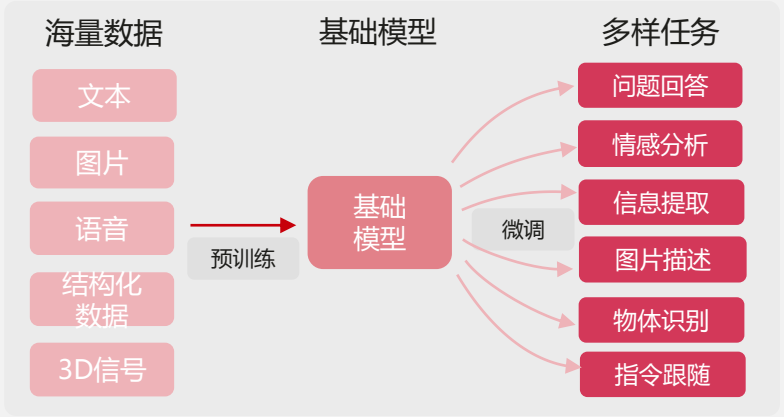
安全挑战3：
分布式训练投毒

数据处理 → **算法开发** → **预训练** → **微调** → **压缩** → **部署**

安全挑战4：
微调数据上云泄露大模型记忆微调数据

安全挑战5：
压缩可能降低模型对抗鲁棒性

安全挑战6：
大模型资产被盗取推理数据上云泄露



消费端产生新应用

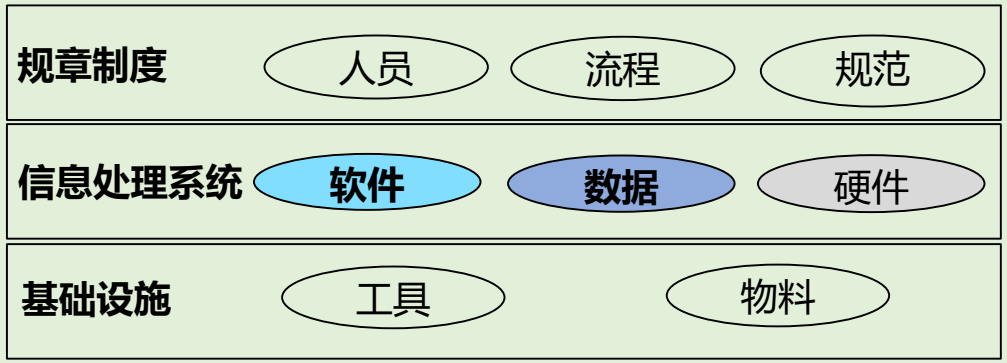
IDE辅助编程	基于AI的安全漏洞过滤，提高代码质量
辅助安全测试	基于AI的fuzz测试用例生成，提高覆盖率表现
辅助软件分析	基于AI修复反编译代码和生成注释描述，提高代码分析效率

以ChatGPT为代表的利用云上大算力，实现海量数据驱动大模型在各领域应用，带来新安全挑战和机遇

安全可信的系统软件是信息系统安全的基础

信息系统是一组互相交互元素的组合，用于实现特定意图和功能，系统元素包括：硬件、软件、数据、工具、物料，人员、流程规范等。

--来源：ISO/*IEC 27000:2014*，*NIST 800-160*



NIST CSF	关键信息基础设施安全保护要求
风险识别（I）	识别认定
防御（P）	**安全防护：** 安全计算环境、数据安全防护
检测（D）	检测评估
	监测预警
	主动防御 收敛暴露面、攻击发现和阻断
响应（R）	事件处置
恢复（R）	

基础软件主要关注信息处理系统中的**软件**和**数据**

安全威胁：利用系统缺陷实现攻击

目标有价值 & 系统有缺陷 & 缺陷可利用

- 缺陷：系统存在某种影响正常运行能力的问题、错误
- 漏洞：在设计、实现、配置及使用过程中出现的缺陷，可被利用于非法访问或破坏系统
- 威胁：使用特定手段利用系统缺陷实现攻击，影响产品的机密性、完整性和可用性

实现安全目标途径

- 消除缺陷：系统中不存在缺陷
- 阻断攻击路径：系统中缺陷无法被利用
- 提高攻击成本：通过减少缺陷、提高缺陷利用难度等措施，使攻击者在时间，技术上的投入高于攻击成功收益

开发阶段
减少或消除缺陷

运行阶段
阻断缺陷利用或提高攻击成本

系统安全构建：开发阶段消除缺陷引入，使用阶段阻断缺陷利用

开发阶段：减少或消除缺陷

缺陷引入因素	• 三方件漏洞 • 供应链投毒	• 机制性缺陷 • 技术选型缺陷	• 编码缺陷 • 恶意代码合入	• 构建工具篡改 • 研发环境破坏	• 伪造下载源 • 软件包篡改	• 安全配置缺陷 • 补丁遗漏
缺陷引入环节	组件引入	系统设计	编码开发	软件构建	软件发布	系统部署
缺陷削减措施	• 选型评估 • 社区防投毒	• 威胁建模	• 安全编程语言 • 形式化验证 • Fuzz测试	• 构建一致性 • 研发信息安全	• 软件包签名 • 证书认证	• 安全扫描 • 漏洞扫描

运行阶段：阻断缺陷利用

攻击步骤	攻击前准备：确定目标、情报收集	攻击实施：渗透接触	漏洞利用	提权	植入恶意软件	实现攻击目的：长期控制、窃取或破坏信息
威胁削减措施	• 人员管控 • 信息隐藏	• 网络隔离 • 物理隔离	• 系统加固 • 漏洞修复	• 身份管理 • 访问控制	• 病毒查杀 • 安全审计	• 数据加密 • 入侵检测

业务场景发展和攻击技术演进，带来新的安全挑战

业务场景

攻击技术

旧场景&新威胁：防护技术失效

- **挑战**：新攻击技术和手段，使传统安全防护技术失效

举例

- 侧信道使传统的软件隔离机制失效
- 勒索攻击以数据可用性为攻击目标

新场景&新威胁：产生新安全需求

- **挑战**：新场景下，关键资产以及安全目标产生新形态

举例

- AI应用打破了数据安全、系统安全边界
- 数据流动共享与数据泄露不可撤销性的矛盾

旧场景&旧威胁：防护技术有效

- **挑战**：防护技术可有效应对已知威胁，但攻防不对等依旧存在

举例

- 漏洞修复不及时，N-day漏洞被低成本利用
- 弱密码等管理类问题无法杜绝

新场景&旧威胁：防护技术缺失

- **挑战**：传统业务信息化后，安全防护技术未同步提升，产生新的攻击面

举例

- 网联化，智能化使车辆内部原有封闭系统开放
- IOT等硬件能力受限场景，无法部署基础防护能力

目标有价值

目标价值上升

- 承载国计民生关键业务
- 信息资产价值上升

系统有缺陷

系统缺陷增多

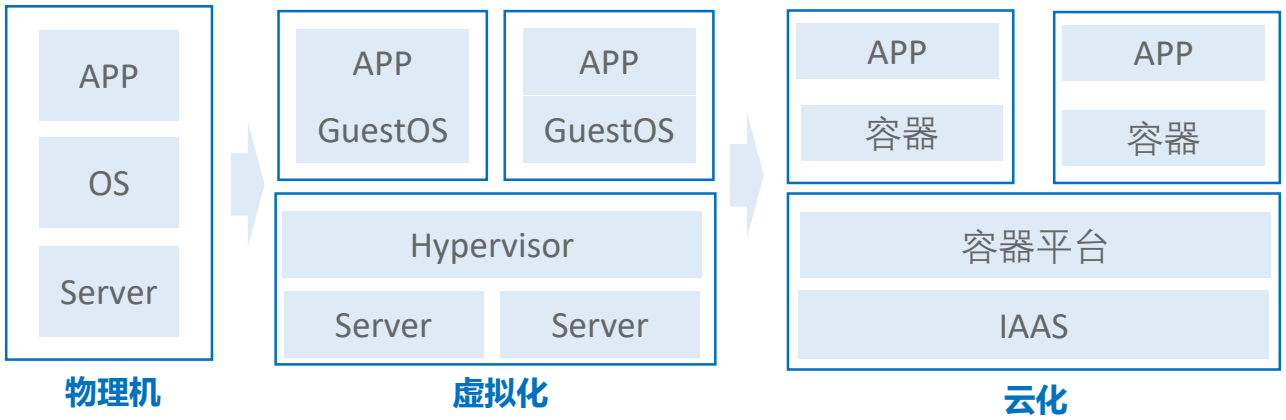
- 软件规模增大
- 老旧系统缺少维护

缺陷可利用

攻击手段增强

- 攻击技术发展
- 攻击者资源丰富

系统自身安全：纵深防御提升系统韧性



产业挑战

系统复杂度与开放性提升，增大了系统脆弱性

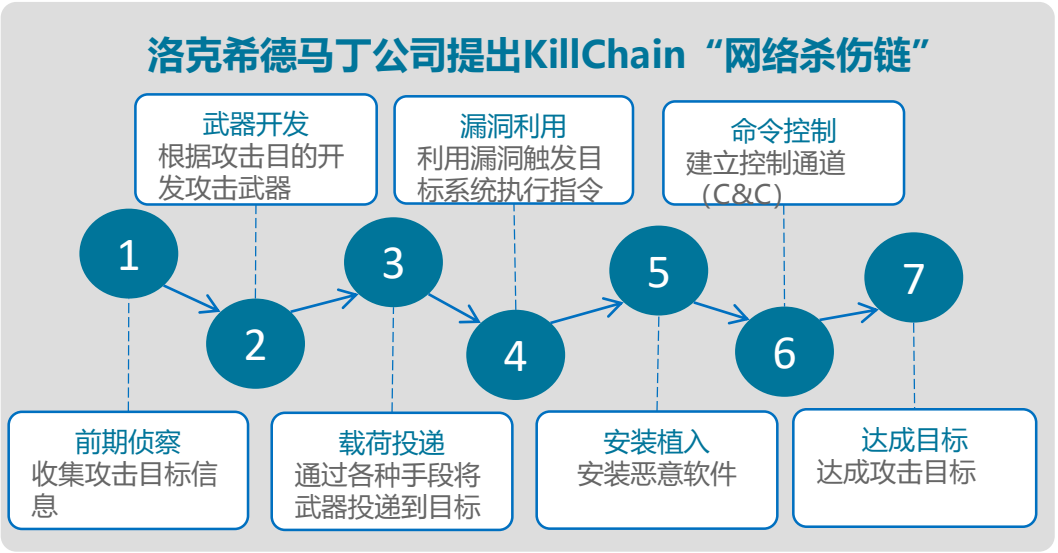
- 软件分层、业务下移边缘，增加了开放性，也导致安全边界模糊，增加了攻击面
- 系统规模变大，业务长期在网，扩大了攻击窗口
- 多设备互联，分布式系统中的单点薄弱环节成为系统安全短板

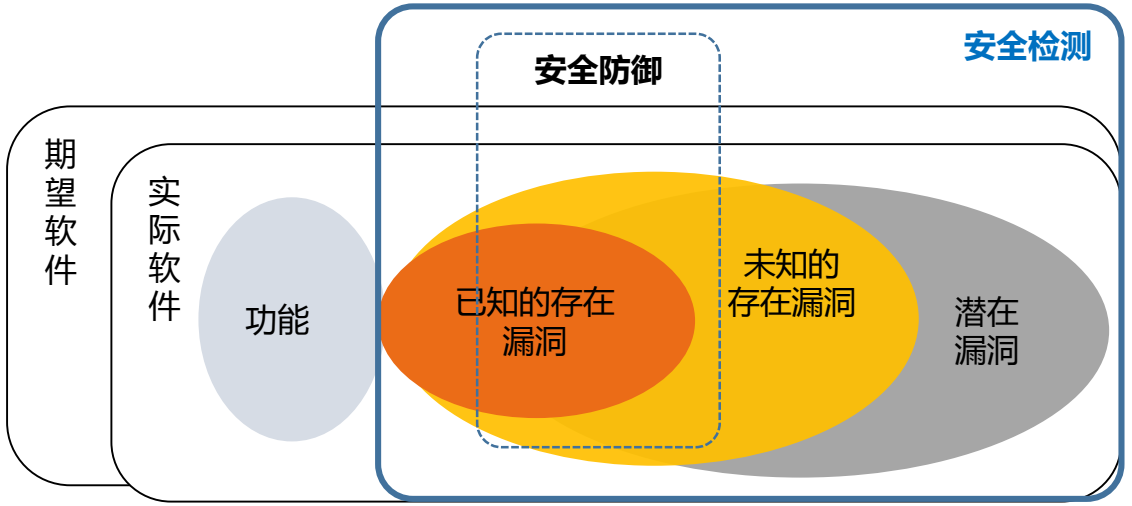
潜在技术方向

纵深防御提升系统韧性

- 多种粒度的隔离技术，实现多级隔离，提升系统韧性
  - ➢ 技术难点：安全性，兼容性，性能多维度指标最大化
- 基于状态的细粒度访问控制规则
  - ➢ 技术难点：访问控制规则的准确性和自动化

系统自身安全：应对系统化攻击，构建主动防御能力





产业挑战

攻防不对等导致系统长期暴露于未知风险

- 面对战术化，武器化攻击威胁，传统防御手段无法有效应对
- 系统软件本身成为高价值攻击目标
- 基于已知攻击手段构建的防护技术，落后于攻击技术发展，长期处于亡羊补牢状态

潜在技术方向

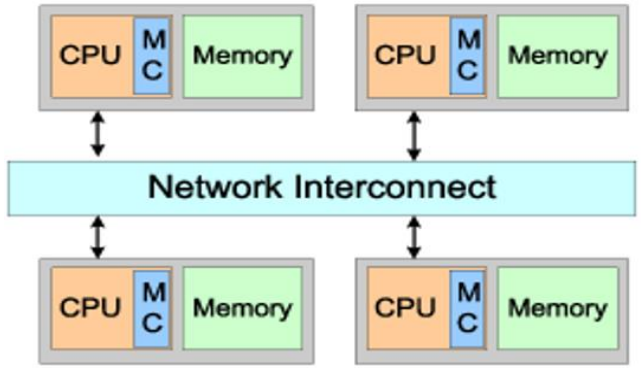
系统内构主动防御能力

- 基于系统状态的入侵检测框架
  - ➢ 技术难点：检测有效性评估方法，检测机制与判断策略分离
- 攻击本地阻断
  - ➢ 技术难点：性能开销及后向兼容

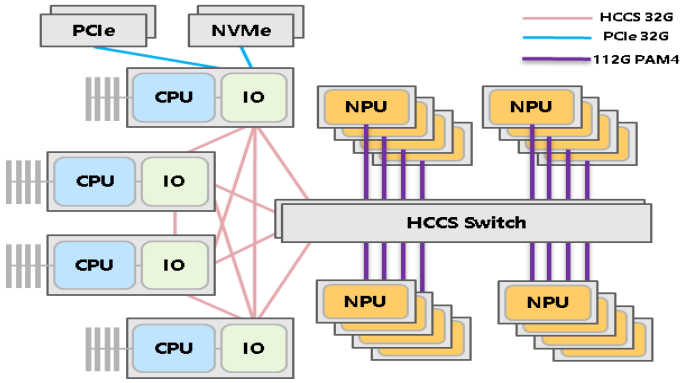
HUAWEI

数据资产安全：构建以数据为中心安全架构

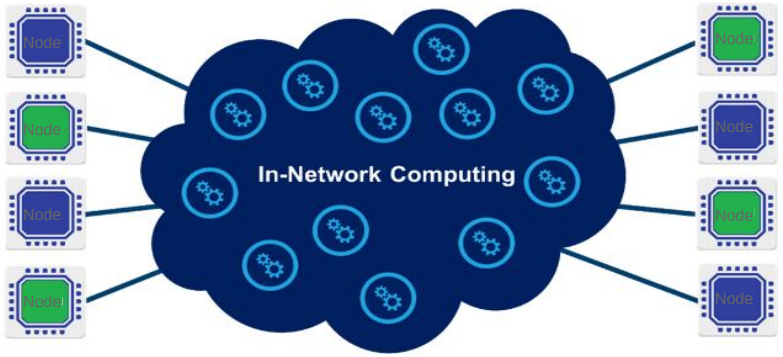
过去：以CPU为中心的计算架构



现在：CPU + NPU/GPU



未来：以数据为中心的异构计算架构



产业挑战

计算架构演进带来新的挑战

- 以数据为中心构建多算力单元系统，导致冯.诺伊曼架构下了以CPU为中心的安全机制失效
- 多种异构算力单元的安全能力存在差异，如何有效协同

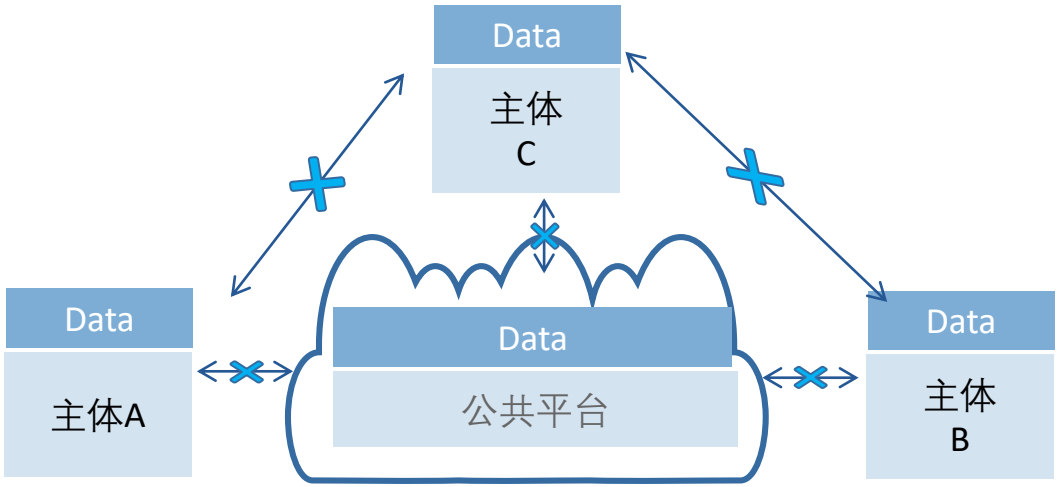
潜在技术方向

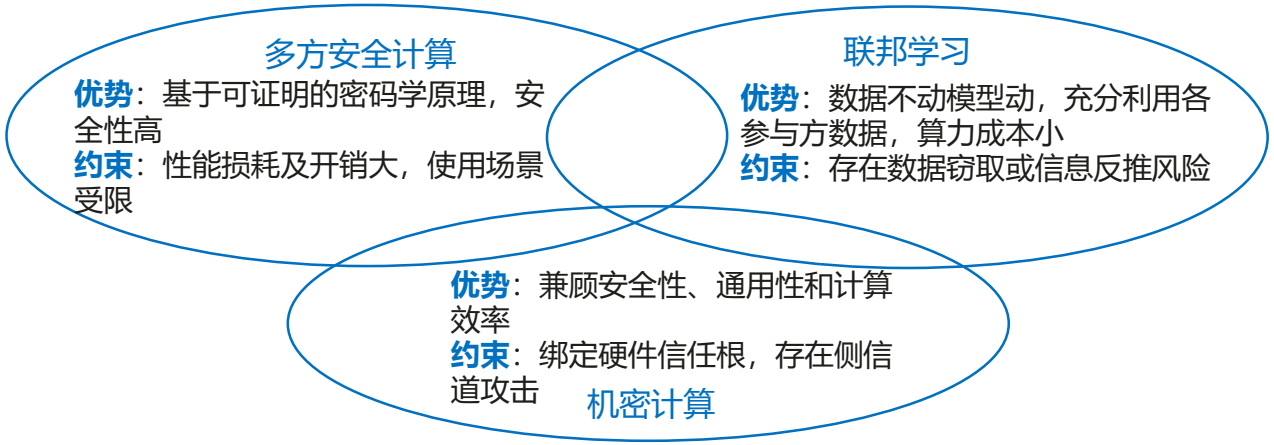
以数据为中心的安全架构

- 异构算力单元对数据的访问控制，安全DMA等技术
  - ➢ 技术难点：软硬协适配多种数据访问方式
- 面向异构算力单元的安全调度与算力卸载
  - ➢ 技术难点：算子拆分与自动化调度

HUAWEI

数据资产安全：支持数据安全使用，实现可用不可见，所有权与使用权分离





产业挑战

数据安全要求制约数据价值发挥

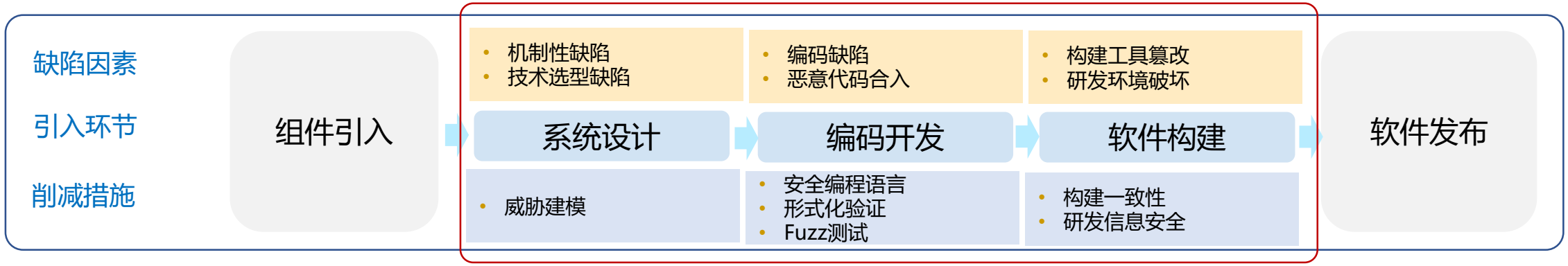
- 基础设施分离部署导致可信链被打破，阻碍关键业务上云
- 数据传播的不可撤销性，造成数据共享与数据安全之间矛盾，影响数据作为关键生产要素价值发挥

潜在技术方向

数据安全分享和流转

- 可信安全外包计算，实现用云不信云
  - ➢ 技术难点：可验证的多方半诚实模型
- 数据流转可控可度量

减少系统缺陷：提升开发阶段编码质量和问题发现效率



产业挑战

软件开发阶段安全编码和缺陷拦截

- 编码质量依赖开发人员，无法有效保障
- 安全编程语言开发组件，受存量非安全语言污染
- FUZZ测试执行效率、复杂场景下的问题发现能力覆盖率，以及业务逻辑缺陷发现能力

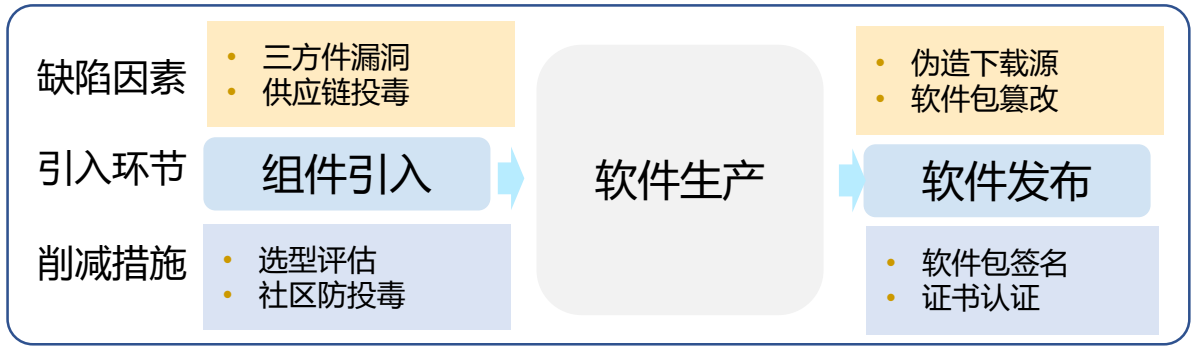
潜在技术方向

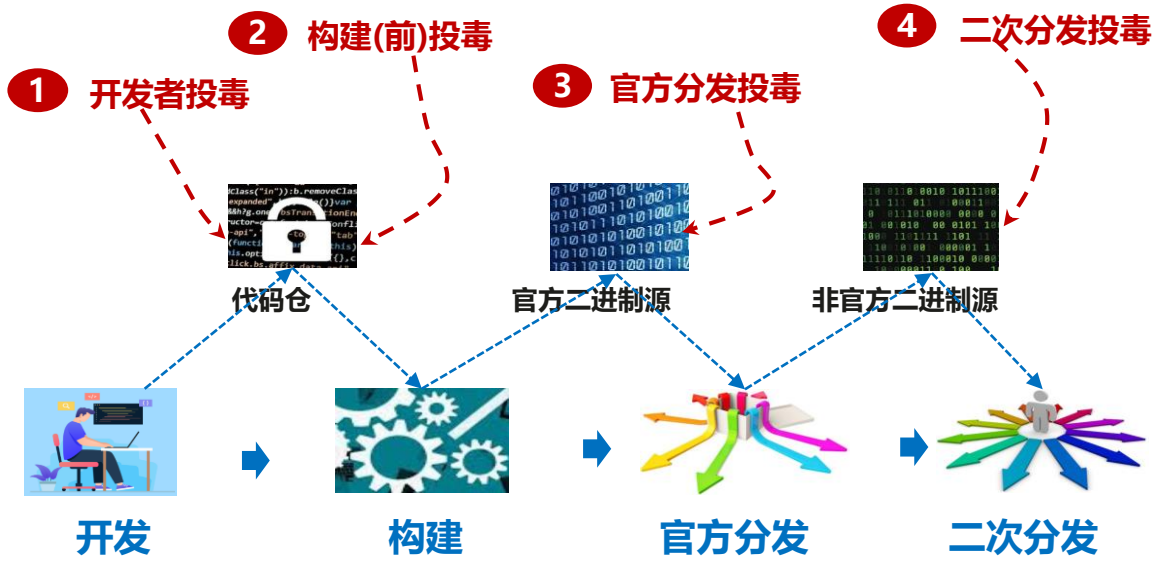
辅助编程及智能FUZZ

- 开发编译阶段安全辅助
- 编程语言内存安全增强及多语言安全隔离

- 智能FUZZ提升问题发现效率和覆盖度
  - ➢ 技术难点：数据流分析，条件竞争类问题发现；AI辅助发现逻辑类缺陷；

减少系统缺陷：面向软件供应链构建防护体系





产业挑战

供应链成为新供给面

- 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

潜在技术方向

面向软件供应链的防护体系

- 软件要素分析和溯源技术
- 软件供应链投毒检测和拦截技术
- 面向开源社区开发模式的FUZZ平台

系统软件安全技术方向课题指南

系统可信和数据安全是业务正常运行的基础，频发的APT攻击事件使信息系统面临的威胁日益显性化，计算架构的演进也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模式使软件系统面临的攻击面，针对以上挑战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

- o 构建系统内生安全能力，应对APT攻击威胁，构建系统纵深防护能力，探索包括异构可信执行环境，函数级隔离、系统入侵检测等技术；
- o 面向以数据为中心场景，探索包括可信外包计算，多算力单元访问控制，安全DMA等技术；
- o 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，探索安全编程语言，软件要素分析和溯源技术，智能化漏洞挖掘技术、软件供应链防投毒技术。

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