.NET企业应用可信开发实战

主讲：邹溪源 /深圳敢为软件&长沙.NET技术社区组织者

背景概述

随着云原生时代的到来，企业开发者面临着相较于以往更加严峻的挑战。这些挑战既包括软件功能方面，也可能来自基础设施运维能力方面，而来自安全上的威胁，更是从方方面面影响着我们。

首先是隐私安全保护方面，各种层出不穷的数据泄密事件，让我们真正实现了在黑客面前的隐私数据共享。

2022年7月，某地爆出大规模隐私数据泄密事件，黑客在某论坛上猖狂放话，称“出售上海政府国家警察数据库，包含数十亿中国公民的信息，包括姓名、身分证及所有犯罪详情，以20万美元出售。”案件迄今仍未被证实，如果被证实，将可能成为有史以来最大的隐私数据泄漏事件。

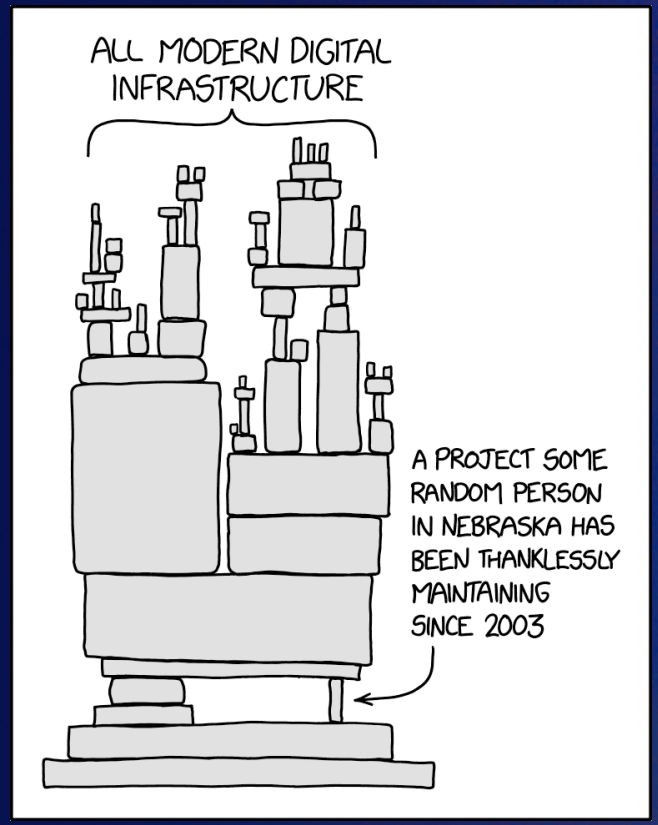
2020年，某著名互联网公司向警方报案，称其公司遭受黑客攻击，造成了一定程度的数据泄漏，经司法鉴定，当事人逯某任职于长沙浏阳某公司，在为2019年11月-2020年7月的8个月时间里，其通过该电商平台公开链接，批量爬取用户的数字ID、淘宝昵称、手机号码等加密信息爬取淘宝用户信息共计11.8亿条，堪称人均一条。

背景概述

在第三方开源软件安全方面，不断涌现的新漏洞一次又一次的挑战着我们的认知。

2021年12月11日，著名日志框架log4j爆出核弹级漏洞，攻击者只需向目标机器传送一段特殊代码，就能触发漏洞，实现在远程执行代码控制目标机器。众所周知，log4j已经被广泛运用于大量基础设施如kafka、redis、jenkins等组件中，一旦出现问题，无异于大厦基础设施崩塌，时至今日，log4j的遗毒依然令人闻之色变。

据媒体10月25日报道，研究人员披露了SQLite数据库库中整数溢出漏洞（CVE-2022-35737）。该漏洞是2000年10月的代码更改时引入的，这个已存在22年的漏洞影响了SQLite版本1.0.12到3.39.1。如果在C API的字符串参数中使用数十亿字节可能导致数组边界溢出，攻击者成功利用该漏洞可在目标系统上执行任意代码。



背景概述

除了安全方面的威胁，软件稳定性问题也逐渐从互联网故事走入了我们的日常生活。

9月1日至4日，成都在全市范围内开展全员核酸检测。9月2日晚，核酸检测系统出现异常，导致采样排队时间过长，核酸检测进度缓慢，给市民群众带来困扰和不便。做核酸的队伍至少排3个小时，还有工作人员齐齐举起手机找信号的场面也令人唏嘘，网友调侃原来抬头并不一定是看星星，而有可能只是在找信号。这也是继西安健康码崩溃后的又一大核酸系统故障事件。

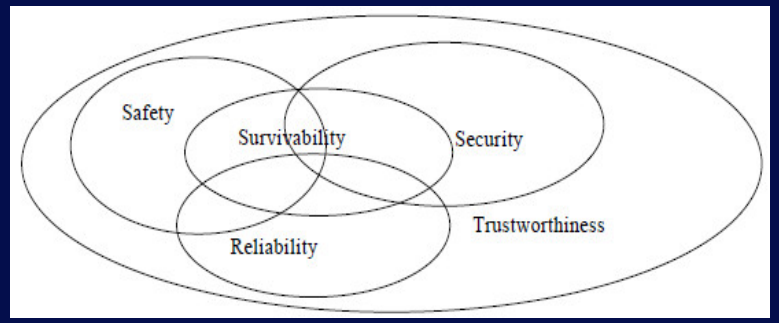
而三个月后的11月24日7时左右，“四川天府健康通”又出现了页面一直无法登录问题。部分市民排队做核酸检测时，也无法打开四川天府健康通扫码录入。

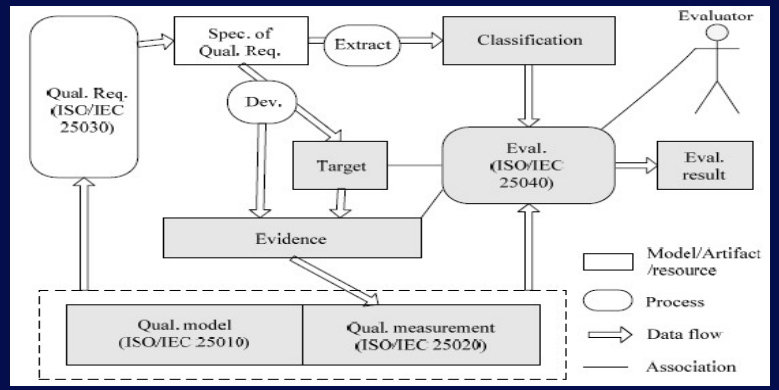
背景概述

各种问题层出不穷，是否有一种更高效的解决方案?

何为可信开发

2007年底，国家自然科学基金委员会启动了“可信软件基础研究”重大研究计划，投入经费1.9亿元，至2016年底结题。2013年出版的《可信软件设计》对该概念进行了进一步说明，可信大概包含了安全性(safety)、保密性(security)、可靠性(reliability)、可生存性(survivability)、完整性(integrity)等，总体上可信性覆盖以上这些术语的内涵。





中国信息通信研究院推出了《可信云》的云计算服务评估品牌，从上述5个大方面，建立了软件研发效能度量成熟度评估标准。而安全能力被设计为基石。

可信开发实战

可信开发实战

需求规划	应用设计	应用开发	应用测试	应用发布	运维运营
• 安全红线设计 • 可信需求分析	• 隐私影响分析 • 威胁建模分析 • 可信设计与评审	• 可信编码规范、代码审查 • 开源及第三方软件管理 • 代码漏洞检查，静态代码扫描 • 密钥保护	• 白盒测试 • 黑盒测试 • 渗透测试	• 哈希校验 • 网站检查 • 证书检查 • 环境配置检查 • 日志存储	• 主机安全扫描 • 补丁管理 • 持续监控、动态风险管理

可信开发流程中的常见问题

开发工具

- 来自开发工具、开发环境的威胁。如破解软件、后门软件等。
- 来自jenkins等持续集成工具等漏洞。

开发团队

- 内部无意识的安全隐患。如配置文件明文密钥，密码过于简单，隐私数据未加密等。
- 密码明文分享。
- 外部有意识的攻击行为。

开发生命周期

- 硬编码密钥。
- 第三方软件威胁
- 代码腐化
- 加密算法
- 用户隐私保护

软件产品发布

- 恶意获取软件。
- 篡改签名。

产品部署

- 环境攻击
- 生产环境隐私数据泄漏

如何应对常见的威胁

通信矩阵

如各种高危漏洞，务必要保持端口最小化

防范病毒和后门

定期进行漏洞扫描，补丁管理。

应用安全

用户身份验证，谨慎设计匿名接口，防范窃听，标识欺骗，越权攻击。
使用TLS1.2以上。

加密算法

采用可信的加密算法，杜绝使用低安全等级低加密算法，如DES，3DES，AES-cbc填充模式。
Md5或base64。
采用AES- ECB256 以上或pdkdf2 100w次迭代，rsa2048以上。

隐私保护

严格按照最小化获取隐私数据的政策，隐私数据采用多重加密保护，如AES+盐加密。

密码管理

密码杜绝明文存储，应使用多重加密，使用一组可替换的根密钥和工作密钥进行保护。

操作失误

多做备份，加强培训，谨防删库跑路。

开源及第三方软件安全

开源风险较高 开源风险较低

行业	2021年开源漏洞代码库占比（%）	2020年开源漏洞代码库占比（%）	变化趋势
物联网	64	40	↑
航空航天、汽车、运输和物流	60	59	↑
互联网和移动APP	56	28	↑
教育科技	54	53	↑
能源与清洁科技	53	79	↓
营销科技	53	95	↓
金融服务和金融科技	53	62	↓
零售与电子商务	51	71	↓
制造业、工业和机器人	51	21	↑
企业软件/SaaS	50	62	↓
虚拟现实、游戏娱乐和媒体	46	55	↓
医疗保健、健康科技和生命科学	45	68	↓
计算机硬件及半导体	43	42	↑
大数据、AI、BI和机器学习	42	58	↓
互联网和软件基础架构	41	35	↑
电信和无线	41	57	↓
网络安全	38	57	↓

来源：新思科技，中国信息通信研究院

图 21 全球重点行业开源代码库安全风险热力图

Table 2: Vulnerability Severity Levels Based on the NVD and CVSS

Table 2 describes how an ASV scan solution categorizes vulnerabilities and risks that are considered High or Medium severity.

CVSS Score	Severity Level	ASV Scan Result	Guidance
7.0 through 10.0	High Severity	**Fail**	To achieve a passing ASV scan, these vulnerabilities must be corrected and the affected systems must be re-scanned after the corrections (with a report(s) that shows a passing ASV scan).
4.0 through 6.9	Medium Severity	**Fail**	Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical, until all vulnerabilities rated 4.0 through 10.0 are corrected.
0.0 through 3.9	Low Severity	**Pass**	While passing ASV scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

解决方案：制定第三方开源软件管理制度，严选软件，严格遵循开源协议，定期了解漏洞情况，及时更新版本。

安全测试的套件

- OWASP Zap
- NMap
- Burpsuit
- 安全扫描工具

结语

互联网时代不断涌现的新的技术固然能够给我们的生活带来改变，但切不可追求技术的先进性，而忽略了软件工程的自身修炼。可信开发涵盖了安全、运维、稳定性、第三方软件、代码质量等多方面的内容，有望为企业应用开发者构筑起一道道防线，构建出真正可信赖的高质量软件，为客户不断的赋能，不断的创造出更加丰富的业务价值。


.NET Conf China
2022
开源 · 安全 · 赋能
THANK!
感谢聆听