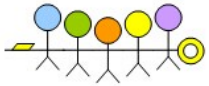
安全软件开发生命周期(S-SDLC)与业务安全

OWASP 中国

The Open Web Application Security Project



火龙果•整理
uml.org.cn

自我介绍&培训

- CWASP高级讲师:包悦忠

- 专场培训

1）北京市朝阳区北四环中路8号 五洲皇冠国际酒店 会议室8

2）高级会员免费参与

火龙果•整理
uml.org.cn

软件安全保障

OWASP 中国
The Open Web Application Security Project

- **Software Security Assurance (软件安全保障)** is the **process (流程)** of ensuring that software is **designed (设计)** to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the **data and resources (数据和资源)** that it uses, controls, and protects.

-摘自英文Wikipedia网站

火龙果•整理
uml.org.cn

OWASP 中国
The Open Web Application Security Project

软件安全保障
流程

火龙果•整理
uml.org.cn

安全软件开发生命周期 (S-SDLC)
——关键要素

需求	设计	开发	测试	部署和运维
- 风险评估	- 威胁建模 - 设计审核 - 攻击面分析	- 安全开发 - 代码审核	- 安全测试 - 渗透测试	- 安全加固 - 补丁管理 - 漏洞管理 - 安全事件响应
- 风险评估模板	- 威胁库 - 设计审核模板	- 公共安全组件 - 静态分析工具	- 动态分析工具 - 第三方渗透测试	- 安全基线 - 扫描、监控、管理工具

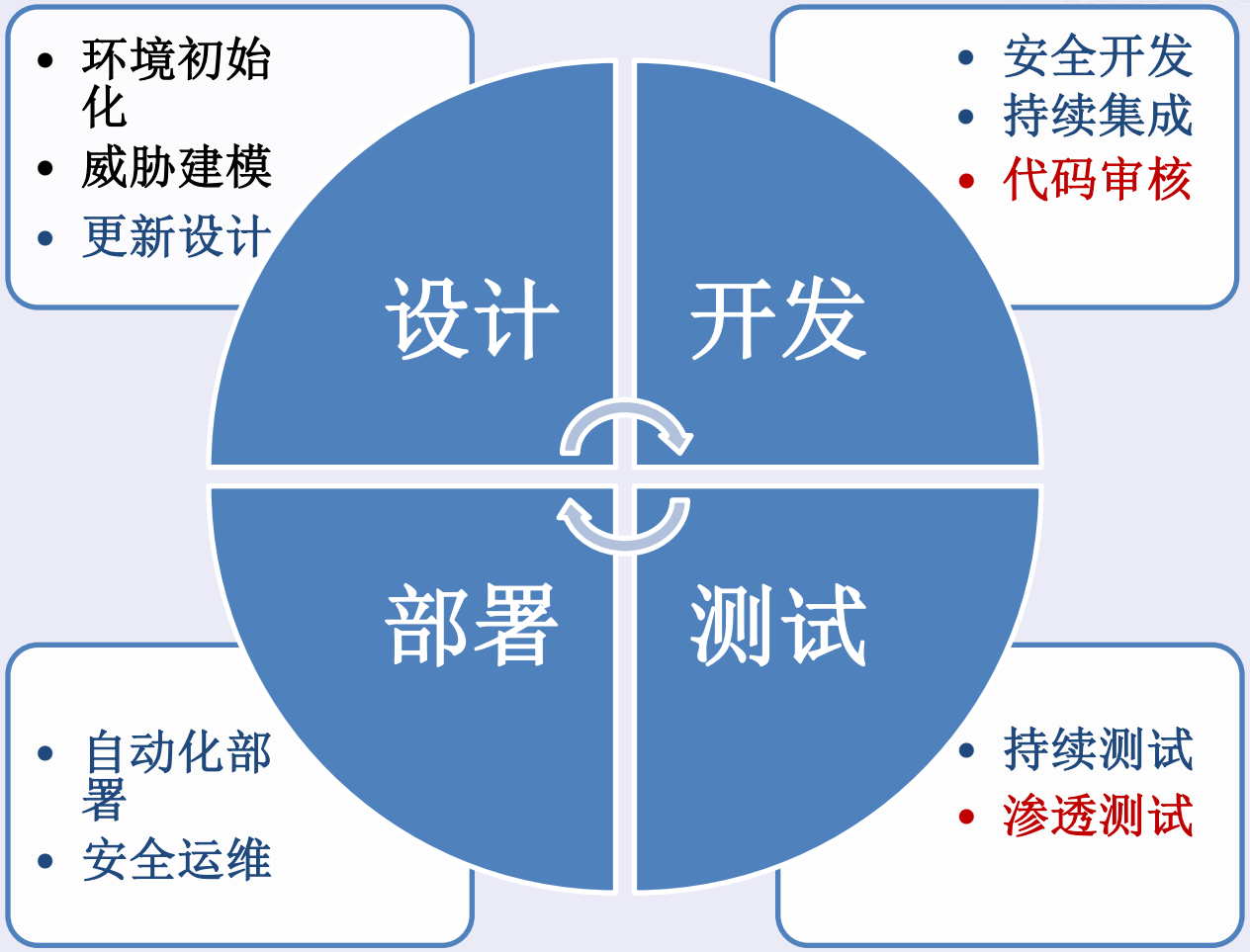
培训、政策、组织能力

火龙果•整理
uml.org.cn

安全软件开发生命周期 (S-SDLC)

——流程与敏捷开发

OWASP 中国
The Open Web Application Security Project



火龙果•整理
uml.org.cn

软件安全保障
——业界最佳实践

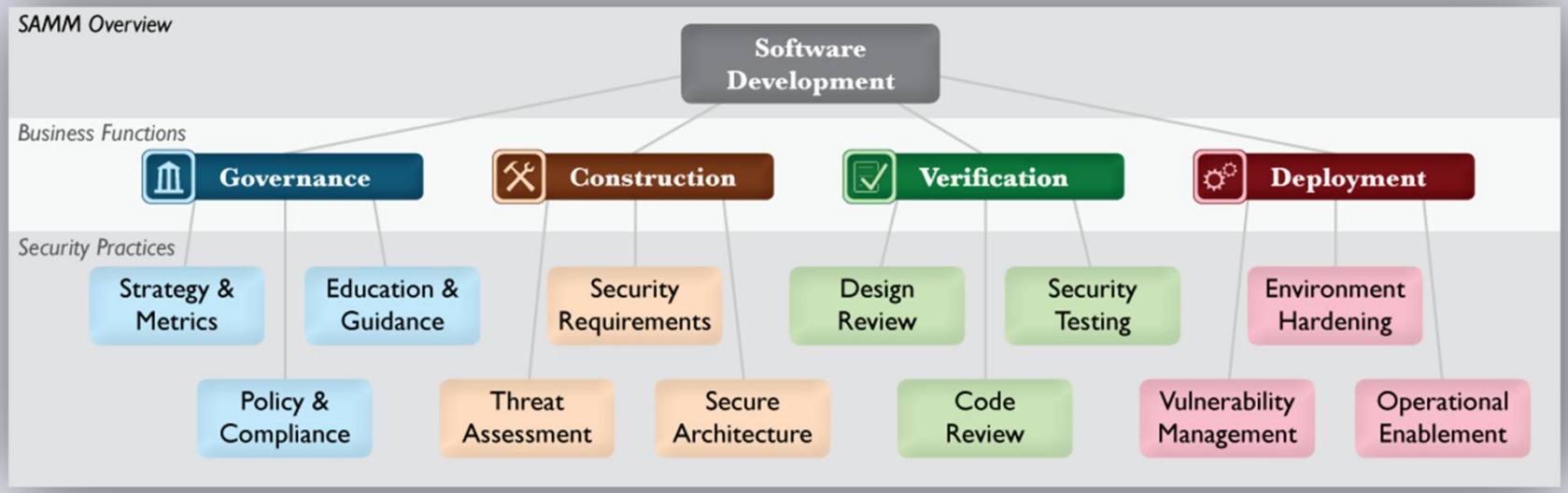
- 流程体系、持续改进
  - 固化→实施→评估→改进→再固化
- 设计安全
- 培训、意识和能力
- 管理层实际的、可见的支持

火龙果•整理
uml.org.cn

软件安全保障
——流程成熟度模型

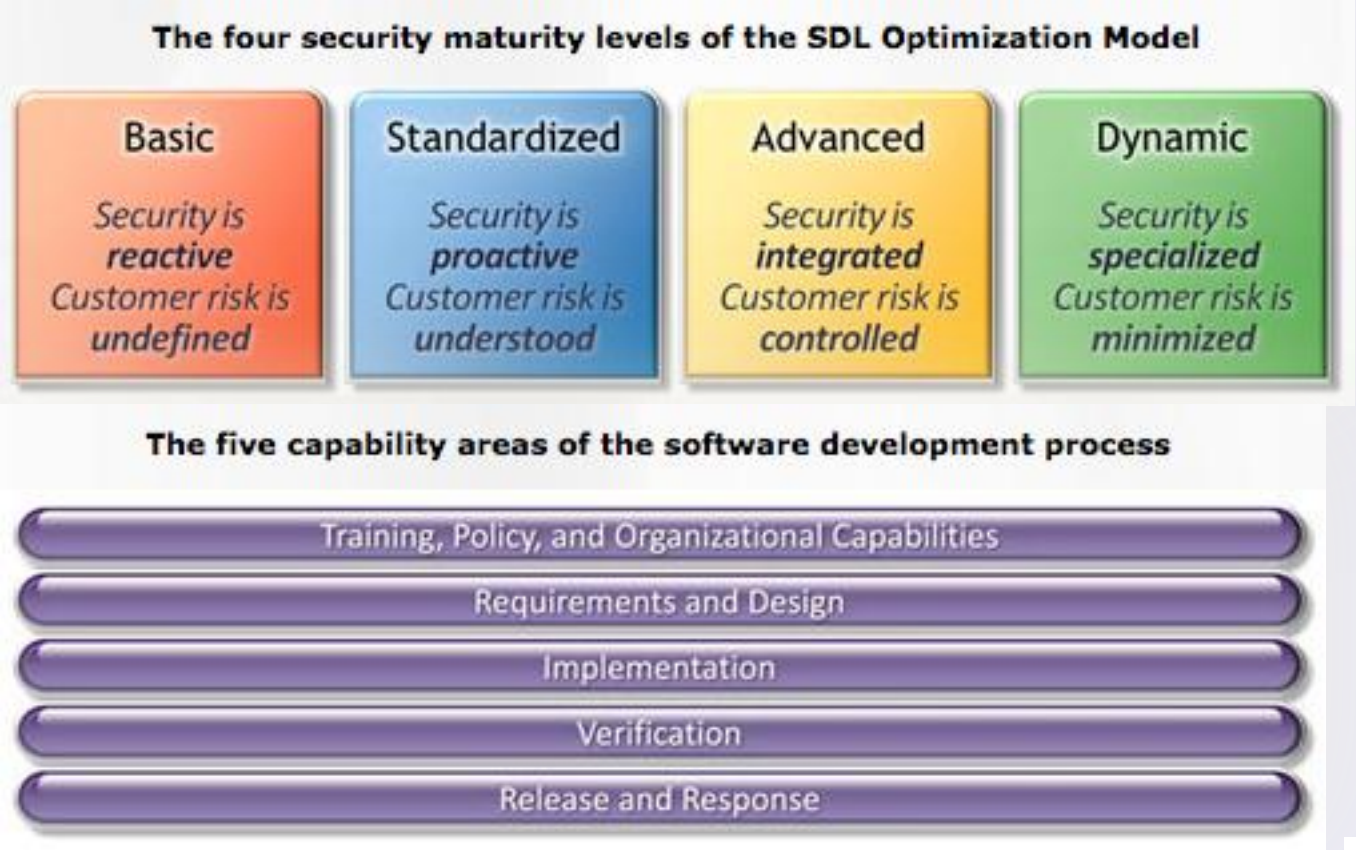
OWASP 中国
The Open Web Application Security Project

- Software Assurance Maturity Model (SAMM)



火龙果•整理
uml.org.cn

- Microsoft SDL Optimization Model



火龙果•整理
uml.org.cn

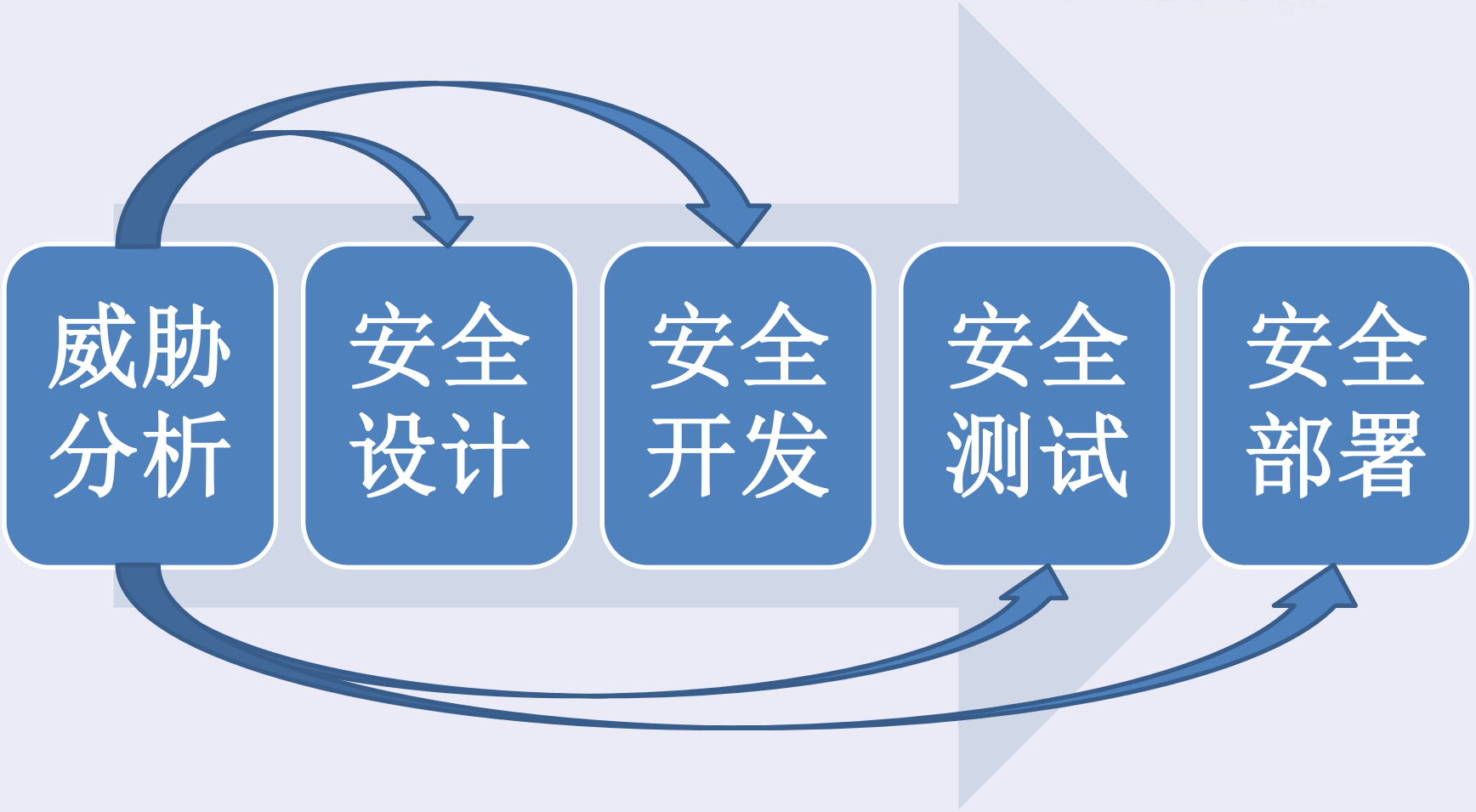
OWASP 中国
The Open Web Application Security Project

软件安全保障
设计暨业务安全

火龙果•整理
uml.org.cn

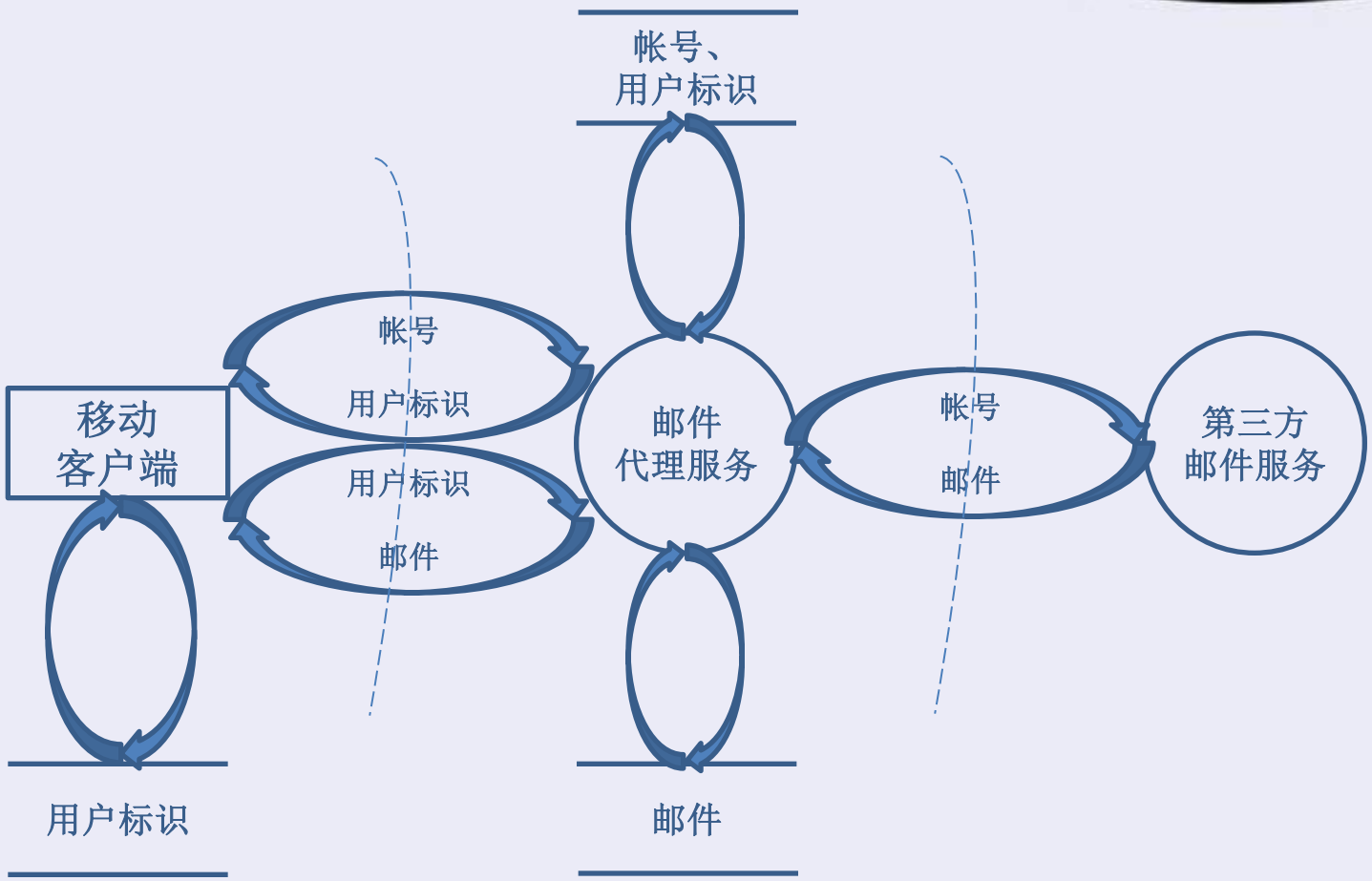
威胁分析目的

OWASP 中国
The Open Web Application Security Project



火龙果•整理
uml.org.cn

数据流图



火龙果•整理
uml.org.cn

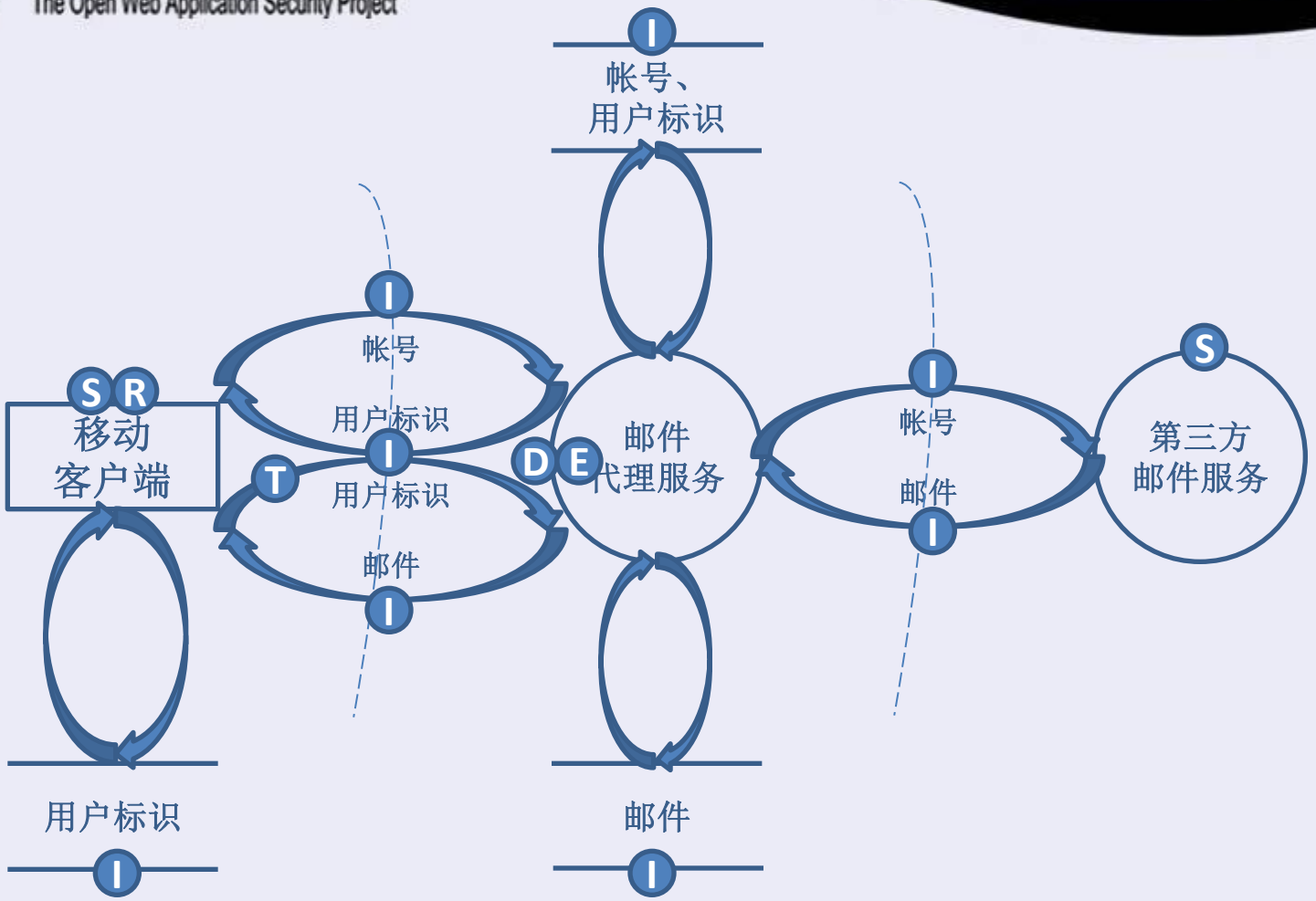
威胁模型 S.T.R.I.D.E.

OWASP 中国
The Open Web Application Security Project

数据流图元素	仿冒 (Spoofing)	篡改 (Tampering)	抵赖 (Repudiation)	信息泄露 (Information Disclosure)	拒绝服务 (Denial of Service)	权限提升 (Elevation of Privilege)
外部交互方	√		√			
处理过程	√	√	√	√	√	√
数据存储		√	√	√	√	
数据流		√		√	√	

火龙果•整理
uml.org.cn

威胁分析



火龙果•整理
uml.org.cn

消减措施

——方法、技术手段

OWASP 中国
The Open Web Application Security Project

S.T.R.I.D.E.	消减措施	方法、技术手段
仿冒(Spoofing)	身份验证(Authentication)	用户名/密码、Cookie、数字签名、挑战-应答、自定义
篡改(Tampering)	完整性(Integrity)	访问控制、数字签名
抵赖(Repudiation)	防抵赖(Non Repudiation)	日志审计、数字签名
信息泄露(Information Disclosure)	保密性(Confidentiality)	加密、访问控制
拒绝服务(Denial of Service)	可用性(Availability)	访问控制、过滤、配额
权限提升(Elevation of Privilege)	授权(Authorization)	访问控制、输入验证

火龙果•整理
uml.org.cn

威胁库示例

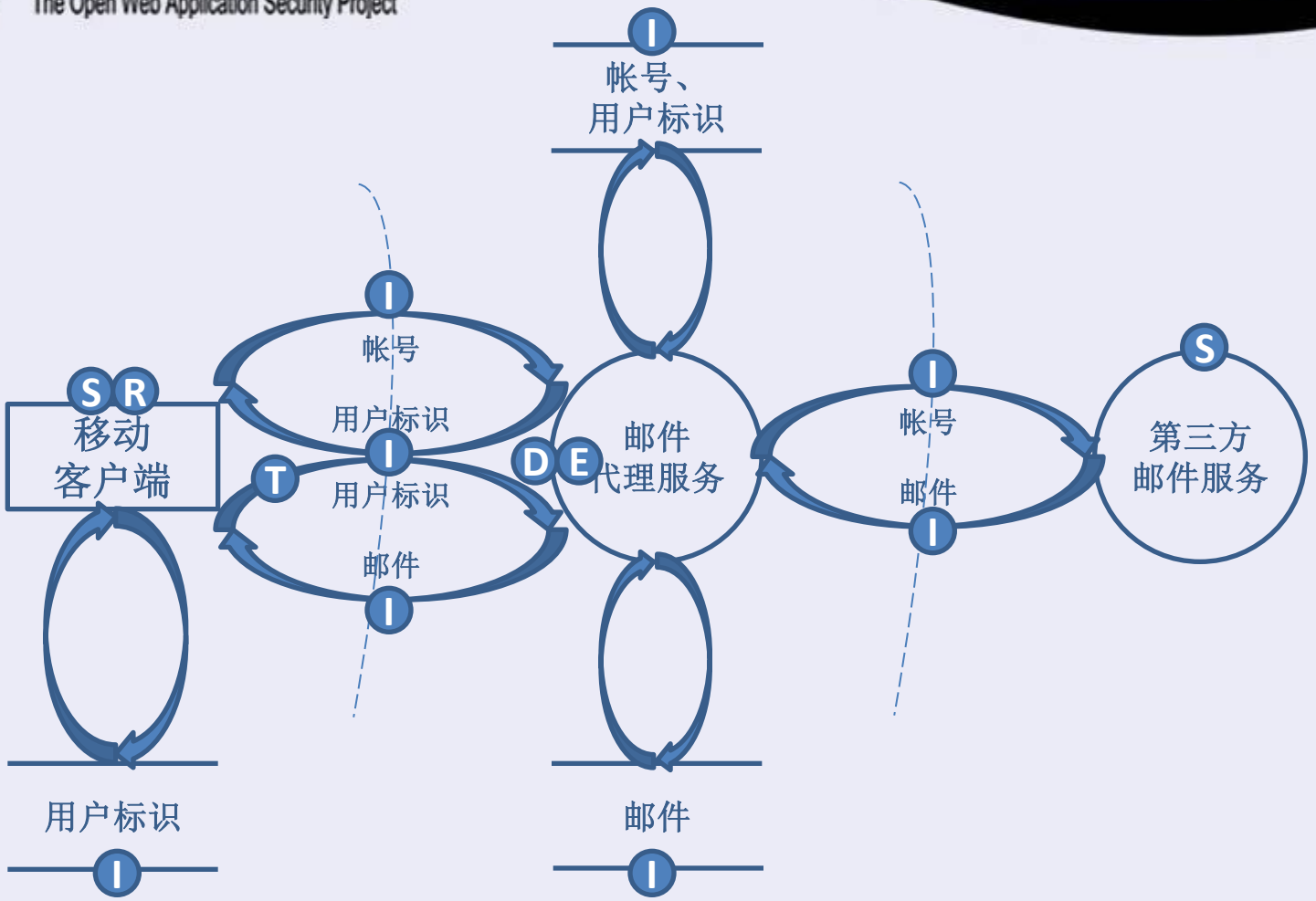
——仿冒外部交互方或处理过程

OWASP 中国
The Open Web Application Security Project

缺乏身份验证		
绕过身份验证		客户端、服务器端 参数操纵攻击
身份验证漏洞	用户名/密码	没有实施密码策略 密码重置安全绕过漏洞
	Cookie	Cookie值具有可预料性 Cookie重放攻击 用户退出登录后Cookie不失效 Padding Oracle攻击
	数字签名、证书	证书验证相关问题
	挑战-应答	反射攻击
	自定义	**服务生成的用户标识具有可预料性**
…	…	…

火龙果•整理
uml.org.cn

风险分析



火龙果•整理
uml.org.cn

威胁分析输出

OWASP 中国
The Open Web Application Security Project

设计

(H) 客户端和代理服务间讯息加密
(H) 客户端应用对代理服务的认证
(H) 用户帐户信息删除
(M) 用户标识客户端存储加密
(M) 代理服务和第三方服务间讯息加密
(M) 代理服务对第三方服务的认证
…

开发

(H) 生成用户标识的随机性
(H) 用户标识客户端存储安全性
(H) 防止SQL注入
…

部署

服务器安全加固
数据库安全加固
…

测试

客户端和代理服务间讯息加密
客户端应用对代理服务的认证
生成用户标识的随机性检查
用户标识存储在应用隔离储存区
SQL注入攻击测试
目录遍历和强制浏览攻击测试
…

火龙果•整理
uml.org.cn

总结

1. 软件安全是软件质量的一个重要维度
2. 安全活动是软件开发活动的一部分，而不是被随后添加或“bolted on”
3. 软件安全漏洞==缺陷(bug)
4. 尽可能早的执行安全活动，尽早发现安全缺陷，降低安全漏洞的修复成本
5. 软件安全保障的方法既适用于内部软件开发，也同样适用于第三方软件开发、集成

火龙果•整理
uml.org.cn