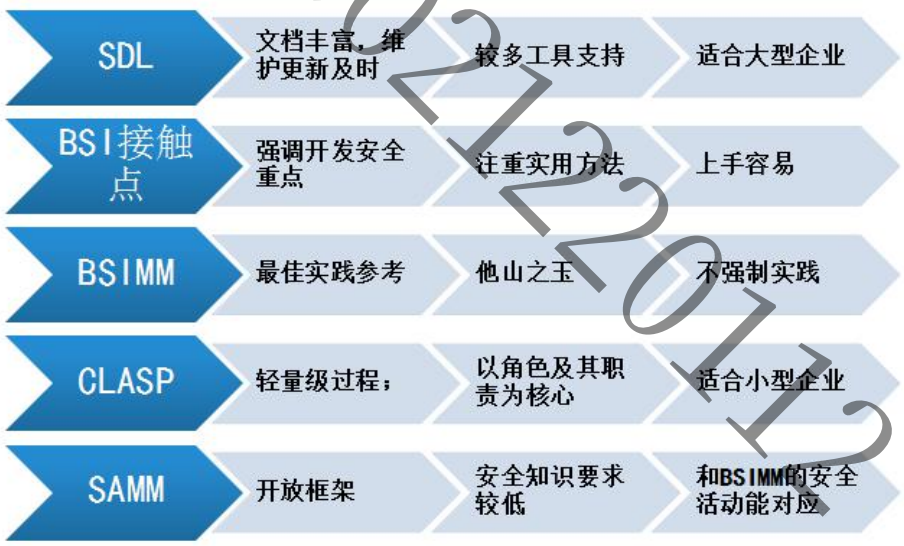
《软件安全开发》知识点串讲

第一节 软件安全开发基础

1.软件工程三要素：方法、过程、工具。
2.软件开发模型：瀑布模型、迭代模型、增量模型、螺旋模型、原型模型、净室模型。
3.千行代码缺陷率：KLOC。
4.软件安全原因：内因、外因。
5.软件安全目标：
（1）可信赖性：无论是恶意而为还是无意疏忽，软件都没有可利用的漏洞存在。
（2）可预见性：对软件执行时其功能符合开发者的意图的信心。
（3）遵循性：软件开发跨学科的活动计划并系统化，以确保软件过程和软件产。
6.软件安全思想
（1）需要贯彻风险管理的思想。
（2）软件安全开发覆盖软件整个生命周期。
（3）软件安全保障—思想之提前介入思想。

第二节 软件安全开发模型



1、**SDL**：七个阶段、16 项活动（了解）。
2、**BSI** 的三个部分：风险管理、接触点、安全知识。
3、**SAMM** 的四个部分：监管（治理）、构造、验证、部署。
4、**CLASP**：轻量级、应用，基于不同角色（活动）而实现的。
5、**CMMI**：能力集成成熟度模型 1-5 级。

第三节 安全需求、设计、编码、测试、交付

1、需求来源：
- 政策、法律、标准、业务、应用场景、安全威胁。
- 标准化需求建议采用 **PP** 的方法。

2、设计原则：
- 标准化的设计建议采用 **ST** 的方法。

- **原则**：不信任、**纵深防御**、**最小特权**、权限分离、**完全中立**、**经济性**、**公开设计**、攻击面最小化、心理可接受、隐私保护、保护薄弱环节、默认故障处理、最小共享等。

3、受攻击面：针对一个对象受到**攻击方法和路径**的集合。

4、降低受攻击面的方法：

（1）分析产品的**功能及特征**。

（2）分析从哪些路径可以访问该**产品**。

（3）降低**访问的特权**和增强防护措施。

5、威胁建模

（1）流程：确定对象、识别威胁、评估威胁、消减威胁。

（2）方法：基于 **STRIDE** 的威胁建模方法。

（3）**S**-欺骗；**T**-篡改；**R**-抵赖；**I**-信息泄露；**D**-拒绝服务；**E**-权限提升。

6、安全编码工作

（1）语法规范

（2）逻辑开放性

（3）不存在冗余代码

（4）代码要精简清晰

（5）不存在复杂代码

（6）完全符合设计及详细设计

（7）源代码编写要进行体系化的规划和分解

（8）进行安全的标识

（9）进行安全输入的验证（内部之间、外部输入）

（10）进行安全的输出，最小化

（11）安全的协议、组件、命令使用调用

（12）统一的返回值设计

（13）写软件的代码注释

（14）源代码的安全审计（前提是对安全需求和安全设计的审计）

7、测试工作

（1）**模糊**测试：提供**非预期的输入**监视异常的结果。

（2）**渗透**测试：测试结果真实严重，但是测试的结果有限。

8、**灵活组合**：根据软件开发实际情况，设计软件开发的安全措施。

9、验收交付：1）供应链的安全；2）安全部署运行维护。

（END）

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请根据你的理解程度和需要，结合教材和其他可信文献进行理解和掌握全面，以免产生以偏概全的问题。