

A detailed technical diagram of a telescope mechanism, likely from a historical document. The diagram shows a large circular structure with various components labeled in all caps. Labels include: LOUVER, UPPER CURTAIN, UPPER POSITION OF MOUNT, SNITTERS, TRACK, CABLES, LOWER CURTAIN, ROCKY PLATFORM, SPECTROGRAPH BODY, ELEVATING PLATFORMS, OBSERVING FLOOR, STAIRS, TURNING CABLE GUARD, 30 FT. 3 IN. RADIUS OF BAIL, 62" TELESCOPE, and BALANCE. The diagram is rendered in a light gray, semi-transparent style, serving as a background for the text.

Computer System Security CS3312

计算机系统安全

2024年 春季学期

主讲教师：张媛媛 副教授

上海交通大学 计算机科学与技术系



The background features a faint, technical diagram of a celestial globe. It includes concentric circles representing lines of celestial longitude and latitude. A vertical axis on the left is labeled 'zenith distance °' with a scale from 20 to 90. The top of the globe is marked 'N' (North) and the bottom 'S' (South). Several curved lines are labeled with declination values: $\delta = 60$, $\delta = 30$, $\delta = 0$, $\delta = -30$, and $\delta = -50$. Two specific annotations with arrows point to parts of the diagram: one points to the lower-left quadrant with the text 'bottom shutter vignettes below this elevation (18°)', and another points to the lower-right quadrant with the text 'clearance for Nasmyth level deck (elevation 33.3°)'.

第二章

计算机安全基本概念

Basic Concepts in Computer Security

目录/CONTENTS

01. 定义安全

Defining Security

02. 术语表

Terminology

03. 安全设计准则

Security Design Principles

04. 安全工程

Engineering Security



01

定义“安全”

Defining Security

安全：感性认识

一个计算机系统被称为“安全的”，应满足：

- 完成**规定工作**
- 且，不做任何其他工作

策略 (Policy)

用于指明计算机系统的“规定工作”通常根据安全的三个方面 (aspects)来制定...

安全的三个方面

ISO/IEC 15408
COMMON
CRITERIA

Julio Gómez Torres



机密性
Confidentiality

保护资产免受未经
授权的披露



完整性
Integrity

保护资产免受未经
授权的修改



可用性
Availability

保护资产不丢失

*资产(assets): 包括“数据”、“代码”、“硬件设备”、“通信带宽”、“频段”等等

机密性 Confidentiality

保护资产免受未经授权的披露
即，规定哪些主体被允许“知道”什么

例：

- 文件内容不可读 (通过访问控制，或者通过数据加密得以实现)

CONFIDENTIAL

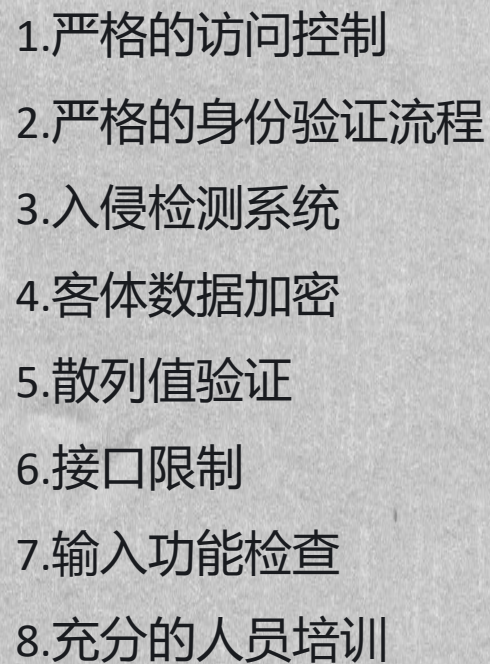
术语辨析

- 保密性 (secrecy) 是机密性的近义词
- 隐私 (privacy) 指个体的信息的机密性 (“个体”包括“个人”、“组织”等)，通常被解释为合法权利。
注意：隐私，不是“机密性”或“保密性”的同义词

完整性 Integrity

保护资产免受未经授权的修改

即，系统及其环境允许发生什么变化，包括输入和输出

- 
- 1.严格的访问控制
 - 2.严格的身份验证流程
 - 3.入侵检测系统
 - 4.客体数据加密
 - 5.散列值验证
 - 6.接口限制
 - 7.输入功能检查
 - 8.充分的人员培训

可用性 Availability

保护资产不丢失

即，明确“何时/何处 会发生何事”

例如，可用性包括对客体的有效的持续访问，及抵御拒绝服务(DoS)攻击，操作系统安全可用性期待的效果包括：

- 操作系统必须定期接受输入
- 程序必须在指定的时间产生输出
- 请求必须被公平处理(顺序，优先级等)

策略 Policy



情景分析1：老刘偷看了小王的业绩报告。

- Q1. 老刘的行为违背了什么策略？
- Q2. 该策略涉及到“CIA”哪一个？



情景分析2：小王偷偷登录HR的电脑，把老刘的年度考核成绩由 A 改成了 C。

- Q1. 小王的行为违背了什么策略？
- Q2. 该策略涉及到“CIA”哪一个？

“制定策略”的一些建议：

- 策略是一种“期望达到的状态”，不总是具体的技术手段
- 安全策略要具体：
 - 围绕“资产”和“主体”
 - 提供“CIA”保护

安全的三个方面



机密性
Confidentiality

保护资产免受未经
授权的披露



完整性
Integrity

保护资产免受未经
授权的修改



可用性
Availability

保护资产不丢失

IS308主要解决 C 和 I 上的问题

Usable Security是
另一个有趣的安全话题

02

若干安全术语

T e r m i n o l o g y



攻击 Attack



Attacks are perpetrated by **threats** that inflict **harm** by exploiting(利用) **vulnerabilities** which are controlled by **countermeasures**.



威胁 Threats

有可能对资产造成损害的主体：

- 对手或攻击者：
 - 有动机，且有能力的人类威胁
- 有时候，人类没有主观恶意：
 - 但意外发生了
- 有时候，非人为因素会造成伤害：
 - 洪水、地震、停电、硬件故障



漏洞 Vulnerability



系统(设计、实现或配置)的一个非主观意愿导致的问题，它可能引发系统不按照设定进行工作

- 生活中的漏洞：健康码非实时更新，快递投递无需亲自签收
- 常见漏洞：缓冲区溢出，代码注入，跨站脚本，身份验证或访问控制缺失，配置错误
- 忽视漏洞是有风险的
 - 常见的逃避态度：“没人会/可以利用它。”
 - Weakest Link现象

漏洞 Vulnerability

漏洞数据库: **CVE** (Common Vulnerabilities and Exposures @ MITRE)

NVD (National Vulnerability Database @ NIST, US)

漏洞知识库: **CWE** (Common Weakness Enumeration @ MITRE)



中国国家级漏洞库:

- **CNNVD** (China National Vulnerability Database of Information Security, 中国国家信息安全漏洞库)
 - 隶属 中国信息安全测评中心 (简称“国测”, 主管单位是公安部)
- **CNVD** (China National Vulnerability Database, 国家信息安全漏洞共享平台)
 - 隶属 国家计算机网络应急技术处理协调中心 (CNCERT, 主管单位是工信部)



漏洞 Vulnerability

知道创宇

<https://www.seebug.org>

漏洞银行

<https://skills.bugbank.cn>



Seebug



漏洞银行



EXPLOIT
DATABASE

<https://www.exploit-db.com/>

攻击 Attack

利用漏洞实施以破坏为目的的行为，不一定取得有效结果

- 例如，漏洞“健康码非实时更新”，
攻击者利用该漏洞实施攻击“截屏他人健康码出行”
- 例如，漏洞“快递投递无需亲自签收”，
实施攻击“偷窃他人物品”
- 例如，向带有解析漏洞的服务器发送一个精心设计的HTTP
请求，它可能会非法地启动一个shell响应

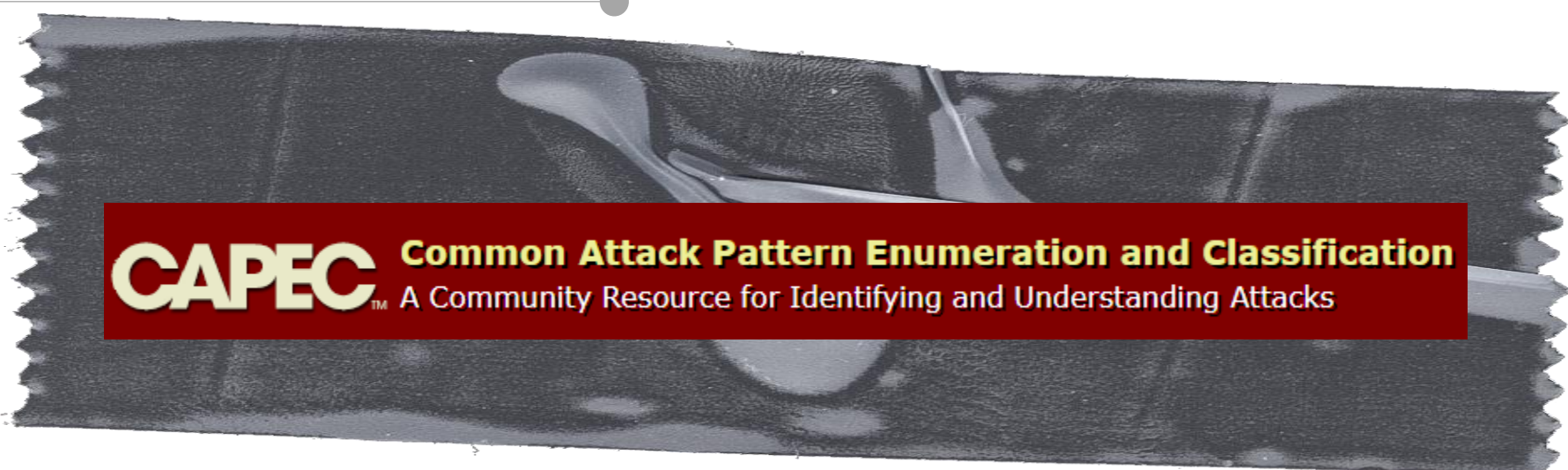


危害 Harm/Damage

对资产产生了损害结果

- 对“机密性”的损害 (如, 窃听、截取)
- 对“完整性”的损害 (如, 修改、伪造)
- 对“可用性”的损害 (如, 中止)





CAPEC **Common Attack Pattern Enumeration and Classification**
A Community Resource for Identifying and Understanding Attacks

缓解措施 Countermeasure

通过消除威胁或漏洞来防止攻击的防御策略

- 预防：阻断攻击或关闭漏洞
- 转移：使其他目标更具吸引力
- 减轻：降低伤害程度严重性
- 检测：当它发生时或之后
- 威慑：让攻击变得更困难，但不是不可能
- 恢复：消除伤害

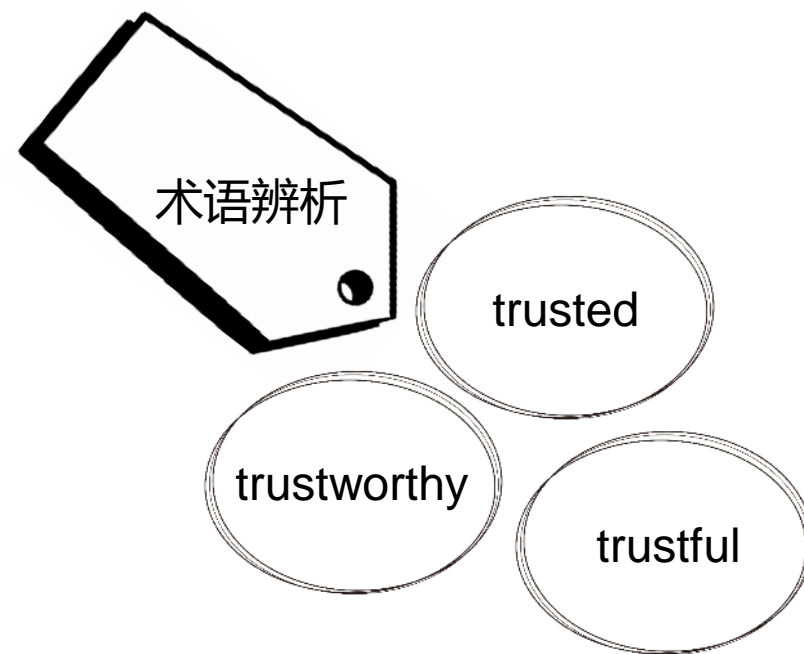
六类实现方法：

- 物理(physical)：有形的东西(墙，锁，守卫)
- 程序(procedural)：人们如何行动的规程(法律、法规、政策、合同)
- 技术(technical)：硬件和软件(密码学、访问控制、密码、入侵检测系统.....)
- 隔离(isolation)：限制组件之间的通信(虚拟机、沙箱、进程、防火墙)
- 监控(monitors)：一个程序分析执行和阻止坏的事情发生(参考监控，入侵检测系统)
- 恢复(recovery)：检测和逆转损害的影响(事务、备份、关键更改)

信任 Trust

信任(trust)是一个理想化的安全假设

- 可信(trusted)的组件是满足安全策略的
- 值得信赖(trustworthy)的组件，需要通过证据来证明它是满足安全策略的，
 - 我们的研究方法试图将信任转化为可信赖性(trustworthiness)，把理想化的不可度量的概念转换为“可被证明的”
 - 这种做法也成为 relocating trust



03

安全设计准则

Security Design Principles



The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND
MICHAEL D. SCHROEDER, MEMBER, IEEE

[About this paper](#)

Manuscript received October 11, 1974; revised April 17, 1975.
Copyright © 1975 by J. H. Saltzer.

Fourth ACM Symposium on Operating System Principles (October 1973).
Revised version in *Communications of the ACM* 17, 7 (July 1974).

[Original web version](#) created by Norman Hardy.

Accountability
Complete Mediation
Least Privilege
Failsafe Defaults
Separation of Privilege
Defense in Depth
Economy of Mechanism
Open Design
Psychological Acceptability

问责制
完备的中间审查
最少特权
故障保险机制
权限分离
深度防御
经济适用
开放设计
心理接受度

问责制 Accountability

为自己的行为负责

- 授权 (Authorization): 规定哪些行为是被允许的
- 认证 (Authentication): 规定哪些主体是可以实施操作的
- 审计 (Audit): 记录和检查上述行为



“The Gold Standard”
From *Computer Security in the Real World*
Butler Lampson (Turing Award Winner 1992),
Microsoft, August 2005



<http://t.cn/A6iEQSAh>

最少特权 Least Privilege

主体应被给予完成其任务所需的最低权限

限制可能由意外或恶意造成的损害



- 1) 清洁工的门禁卡可以打开电院一号楼三楼所有的办公室。
- 2) 计算机guest用户只能访问guest目录下的文件

权限分离 Separation of Privilege

- **不同的操作需要不同的权限**
 - 它是对“最少权限”原则的延续
 - 当参与系统的主体、对象、操作过多时，需要进行特权的分离，避免重叠决策、权限踩踏
- **权限应被分散到多个主体 (职责分离)**
 - 不一定每个主体都必须享有特权
 - 特权根据级别高低发生作用，平级间应无重叠
 - 无更高级别的命令/规定时，权限不可发生移交或覆盖

开放设计 Open Design

安全不应依赖于对系统设计和实现过程的保密

例如，密码学研究中备受推崇的“Kerckhoffs's principle”

支持开放设计的论据:

- 秘密最终会浮出水面
 - 代码逆向工程
 - 员工跳槽可能泄露信息
- 公开细节将帮助识别、修复漏洞以改善设计

反对开放设计的论据:

- 保密支持深度防御，使其更难发现漏洞
- 莱纳斯定律Linus' Law成立: “Given enough eyeballs, all bugs are shallow”, 如果解决不了bugs, 就解决眼球。。。
- 识别后，一些漏洞不能快速或容易地修复

本章要点

- 定义 “安全” (Security)
- 安全策略目标：
 - 为特定资产和主体，提供 CIA 防护
 - 安全策略是一种 “期望”，不是 “手段” 更不是 “结果”
- 十大安全设计准则：
 - 1975年论文提出，至今仍然具有指导意义

开发与安全共识13条

第一条：安全是企业各部门、各层级共同的责任。

第二条：打破职责边界，共建安全保障。

第三条：共同构建和执行完整、有效、可行的安全开发生命周期方案。

第四条：安全是产品的基本属性之一。

第五条：安全不止于成本中心，还将是核心竞争力。

第六条：安全文化，意识先行。

第七条：安全有效左移，风险有效降低。

第八条：工具平台化、经验制度化、流程系统化。

第九条：高度重视软件供应链安全。

第十条：安全服务于业务发展，安全必须持续运营。

第十一条：建立有效的安全风险管理体系。

第十二条：法律是红线，合规是刚需。

第十三条：以用户为中心，致力于保护用户隐私和数据安全。



OWASP中国北京区域负责人

张坤



数世咨询创始人

常杰



金融科技公司信息化工总

白晖



金融机构开发安全管理团队成员

常青



互联网公司基础安全负责人

陈雪



云平台安全运营总监

韩



快帆网安CTO

高



新浪网络安全经理

王



央企技术总

王



小红书安全技术负责人

周



金融科技企业安全团队负责人

谢

Explore the world of cyber security

Driven by volunteers, OWASP resources are accessible for everyone.



Quick access to our highlighted
flagship resources

See all [flagship resources](#) (15)

code

documentation

SAMM

Software assurance maturity model to improve security posture



OWTF

Web testing framework for pentesters



standards

CycloneDX

BOM standard for advanced supply chain cybersecurity risk mitigation



Have an [idea](#) for a project?

Take advantage of our resources and let it grow with OWASP.

Start a project

Our Vision

No more insecure software.

Our Mission

To be the global open community that powers secure software through education, tools, and collaboration.

The Open Worldwide Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.