046258 信息安全概论（本）

课程简介

讲课老师：王艺
1478128896@qq.com
网络空间安全学院

本课程的基本信息

- 选课人数：18人
- 班级：2016级软件1-3/卓越1班
- 学时：36 讲授28+实验8
- 时间：[1-12周]—9-11节
- 地点：讲授6F-302；实验8B407
- 答疑：
  - 课前、课间与课后一对一问答
  - 课后采用QQ、电子邮件答疑
  - 课堂上针对共性问题进行统一答疑
- 实验报告上传至 ftp://wangyis@172.28.89.9

课程主要目的

- 课程简介
  - 信息安全概论课程全面介绍了信息安全的基本概念、原理和知识体系。主要内容包括密码学技术、用户身份验证 、访问控制、操作系统安全、多媒体安全、网络通信协议安全等。
- 课程目标
  - 信息安全概论课程以**导论**的形式对信息安全学科中的主要领域进行了全面而适度的介绍，有助于计算机专业的学生在较短时间内获得对信息安全基础理论和基本技术的概貌认识。
  - 侧重于对主流信息安全技术的全面介绍，扩大学生的知识面，为将来进一步查阅或学习信息安全相关知识奠定基础。

教材与参考资料

- 教材：
  - 石文昌，《信息系统安全概论》第二版，电子工业出版社，2014
  - 信息与网络安全概论（第3版），清华大学出版社，2010
- 主要参考资料：
  - 张焕国，王张宜，《密码学引论（第二版）》[M]，武汉大学出版社，2009
  - 斯托林斯[美]（译者：白国强），《网络安全基础应用与标准(第5版)》，清华大学出版社，2014

成绩评定

- 随堂小测：10% [2次，每次5%]
- 实验报告：20% [4次，每次5%]
  - **评价标准**：实验态度，实验报告的规范性、数据分析的准确性和回答实验思考题的正确性。
  - **要求**：准确记录实验数据，按照实验报告要求对实验数据进行合理分析，回答实验思考题。
- 期末考试：70%

（一）信息系统安全绪论

1、信息安全的威胁

巴纳比•杰克：破解ATM机

杰克原来是黑客，后任职于世界资深电脑安全公司IOActive公司，做着最核心的工作：专门探寻各类新出现的网络威胁，并且不断推动和为公司寻找新的研究方向。

“黑帽子”大会上，一位名叫巴纳比•杰克的网络安全专家用了两种方法令ATM机吐钞票。一种是做出一台任何人可以解锁的ATM机，插入特制的U盘，然后控制网络并命令机器吐钱；另一种方法是通过查询信用卡使用者的历史记录和PIN号码，然后把他们送发给黑客。他的表演让所有在场的同行无不惊诧地表示：“智能真的不可靠。”

点击视频链接：

ATM狂吐钱　　医疗设备隐患

信息安全的重要性

- 截至2013年底，中国网民规模突破6亿，其中通过手机上网的网民占80%；手机用户超过12亿，全球十大互联网企业中我国有3家。
- 2013年网络购物用户达到3亿，全国信息消费整体规模达到2.2万亿元人民币,同比增长超过28%,电子商务交易规模突破10万亿元人民币。
- 互联网已经嵌入到了国家经济政治文化的各个方面，关乎社会的稳定和国家的安全，没有网络安全，国家安全也就无从谈起。

“互联网黑洞”

- 互联网时代，黑客们利用网络交易平台上软件的漏洞或网民投资或购物时的大意而埋设的窃取、吞噬顾客钱财的“黑洞”或“陷阱”
- 据国家计算机网络应急技术处理协调中心2007年的评估数据显示：
  - 全球620万台僵尸电脑zombies，约有360万台在中国，占58%以上。同时，感染了特洛伊木马病毒的电脑数量仍在稳步上升。中国在成为世界上网民最多的国家的同时，也成为了僵尸电脑最多的国家，还有可能成为网络安全的重灾区。

（一）信息系统安全绪论

1.1 攻击案例

攻击者

- 足够诱惑的动机（Motive）
  - 吸引攻击者冒险和花费时间 、精力成本
- 相应的技术和方法（Method）
  - 包括知识、技能、工具等以实施攻击
- 充分的机会（Opportunity）
  - 时间、运算能力、漏洞等以完成攻击

安全攻击案例

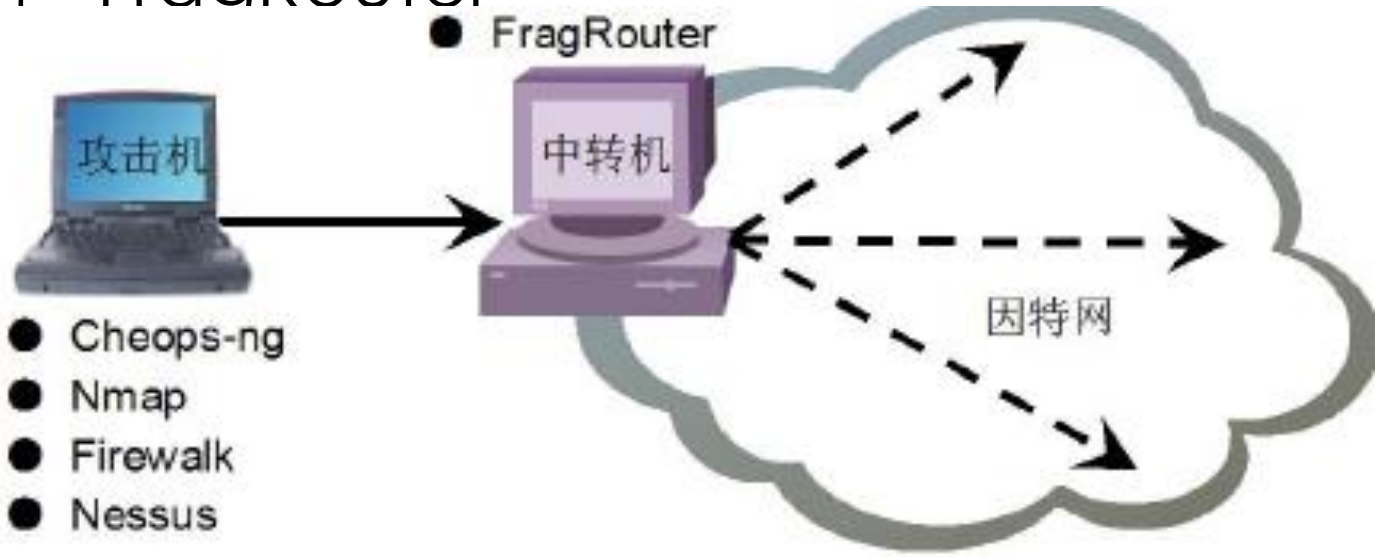
- 攻击者的目的
  - 炫耀自己的技术能力
  - 获取经济利益
  - 报复
- 案例背景介绍——某黑客“卡尔”
  - 深谙信息安全攻击之术（Method）
  - 实施信息安全攻击以获取经济利益（Motive）

诱惑与行动

- 寻找攻击对象
  - “好运”公司
  - 发展迅速，一年时间网点遍布全国
  - 在安全方面可能存在漏洞
- 寻找有关该公司的IT系统资料
  - 访问互联网信息中心InterNIC：提供DNS信息，从而根据域名可以找到主机的IP地址
  - 获知该公司网络IP信息：a.b.c.0~255

对网络系统进行扫描前的准备

- 利用该公司的IP地址信息可以对该公司的网络信息系统进行扫描
- 为了防止可能存在的入侵检测系统的检测或入侵防御系统的阻拦，寻找替罪机器，为它安装工作软件--FraaRouter



卡尔通过第三方扫描方案

网络入侵检测逃避工具

- Fragrouter 是一款单向分段路由器，发送/接收IP数据包都是从攻击者到Fragrouter，将数据包转换成分段数据流发给受害者。很多入侵检测系统都不能重建一段被视为一个整体的网络数据（通过IP分段和TCP流重组）。
- Fragrouter可以帮助黑客在逃避入侵检测后发起基于IP的攻击，避免黑客自己的系统直接暴露在扫描信息通信的前方

打探：扫描工具

- 网段扫描（网络映射）：Cheops-ng
- 端口扫描：Nmap
- 防火墙扫描：Firewalk
- 无线接入扫描：Wellenreiter
- 拨号扫描：THC-Scan
- 漏洞扫描：Nessus

用Cheops-ng扫描

- Cheops-ng是一个网络系统管理工具，可以映射和监视你的网络。它可以进行主机/网络查找、系统监测，而且还能扫描每台计算机的端口并了解哪些服务正在运行，以便你使用和管理它们。
- 软件主页http://cheops-ng.sourceforge.net/
- 利用cheops-ng提供的路径跟踪功能，**卡尔发现**好运公司网络系统布局
  - 有三个系统在运行，一个前端，两个在后

用Nmap作SYN和UDP扫描

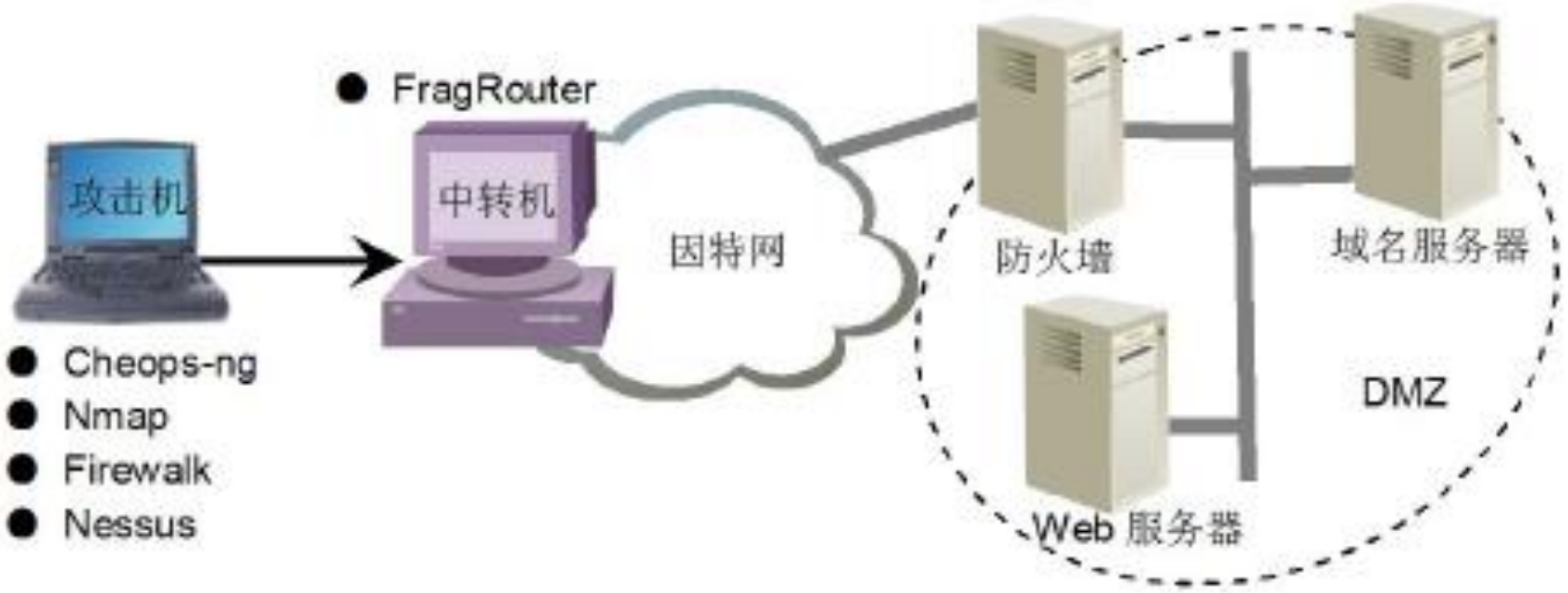
- Nmap是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端，以确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统。可作漏洞探测器或安全扫描器:
  - 检测活在网络上的主机（主机发现）
  - 检测主机上开放的端口（端口发现或枚举）
  - 检测到相应的端口（服务发现）的软件和版本
  - 检测操作系统，硬件地址，以及软件版本
  - 检测脆弱性的漏洞（Nmap的脚本）
  - 软件主页 https://nmap.org/
- **卡尔发现**:
  - 一个TCP 80端口打开 =› Web服务器
  - 一个UDP 53端口打开--› DNS服务器
  - 另外一个系统没有任何端口打开

用Firewalk软件扫描

- Firewalk采用的traceroute技术来分析IP包的响应，以确定网关ACL过滤和映射网络。firewalk确定一个数据包转发设备中发生的过滤规则。
  - 能够用于探测网关上打开或允许通过的端口。更进一步地，它能够测定带有各种控制信息的数据包是否能通过给定网关。
- 卡尔发现未知系统是一个包过滤防火墙且
  - 允许通过TCP 80和UDP 53 端口对好运公司网络的非军事区（简称DMZ）进行访问

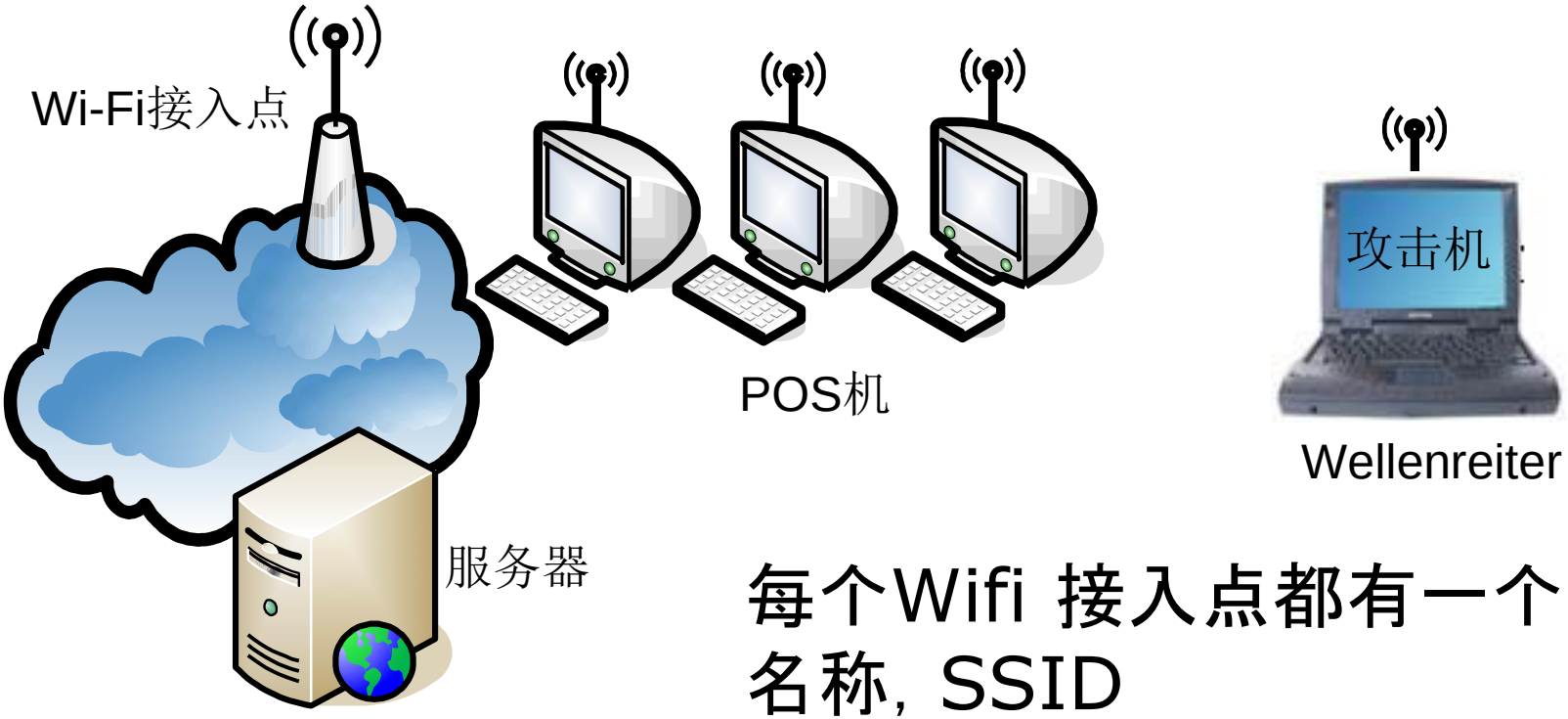
初探-摸清公司网络的基本布局

- 卡尔基本摸清了好运公司网络的因特网DMZ和防火墙的一般结构
- 用Nessus软件作系统漏洞扫描与分析，**卡尔发现**
  - DMZ区没有可利用的漏洞



寻找突破口：无线网络接入点

- 寻找好运公司销售点A的无线网络接入点



每个Wifi 接入点都有一个名称，SSID

用Wellenreiter探测无线接入点

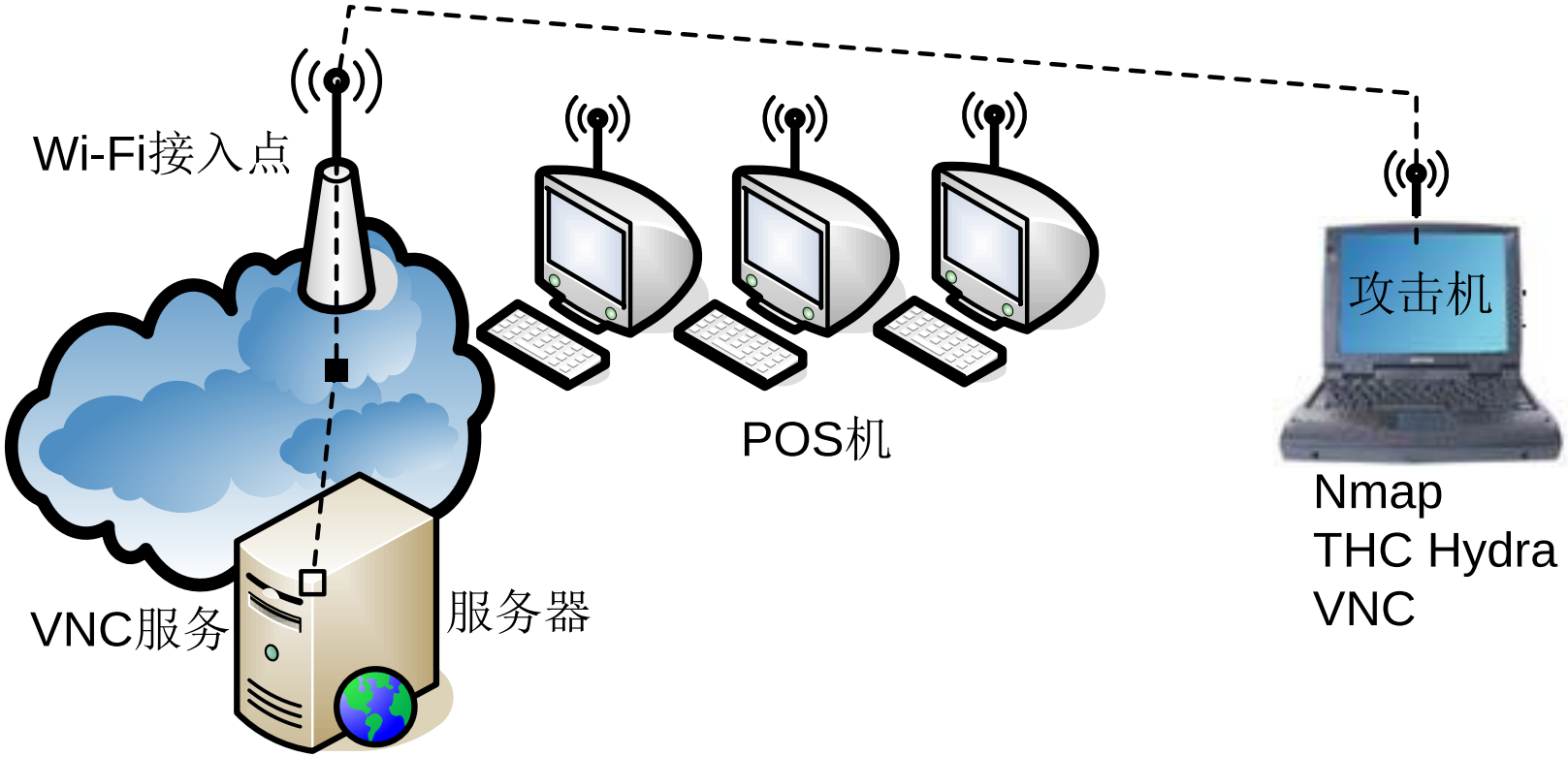
- Wellenreiter软件是一个无线网络查找和审核工具。它的扫描器窗口可以用来发现wifi接入点AP、网络和ad-hoc 的网卡
- 通过Wellenreiter显示的通信信息，**卡尔发现**
  - 一个SSID信息（网络名）：golucorp041
    - 提示：公司名为Good Luck Corporation
- 用该SSID配置无线客户端尝试接入：无响应
- 用ifconfig假冒选定的MAC地址再尝试：
  - 成功接入
  - 被分配了DHCP式的IP

突破口–尝试进入系统

- 用Nmap作ping扫描，**卡尔发现**
  - 无线POS机和销售点服务期的IP
- 用dig命令和服务器IP作逆向DNS查询，**卡尔发现**
  - 服务器域名： store041.internal_goodluck.com
- 用Nmap作SYN扫描，**卡尔发现**
  - TCP 5900端口打开=〉**VNC服务（虚拟网络控制）**
- 用THC Hydra猜测VNC服务器口令，**卡尔发现**
  - 帐户：operator，口令：rotarepo
  - hydra是著名黑客组织thc的一款开源的暴力密码破解工具，可以在线破解多种密码
  - 软件主页 https://www.thc.org/thc-hydra/

通过VNC进入销售点A的服务器

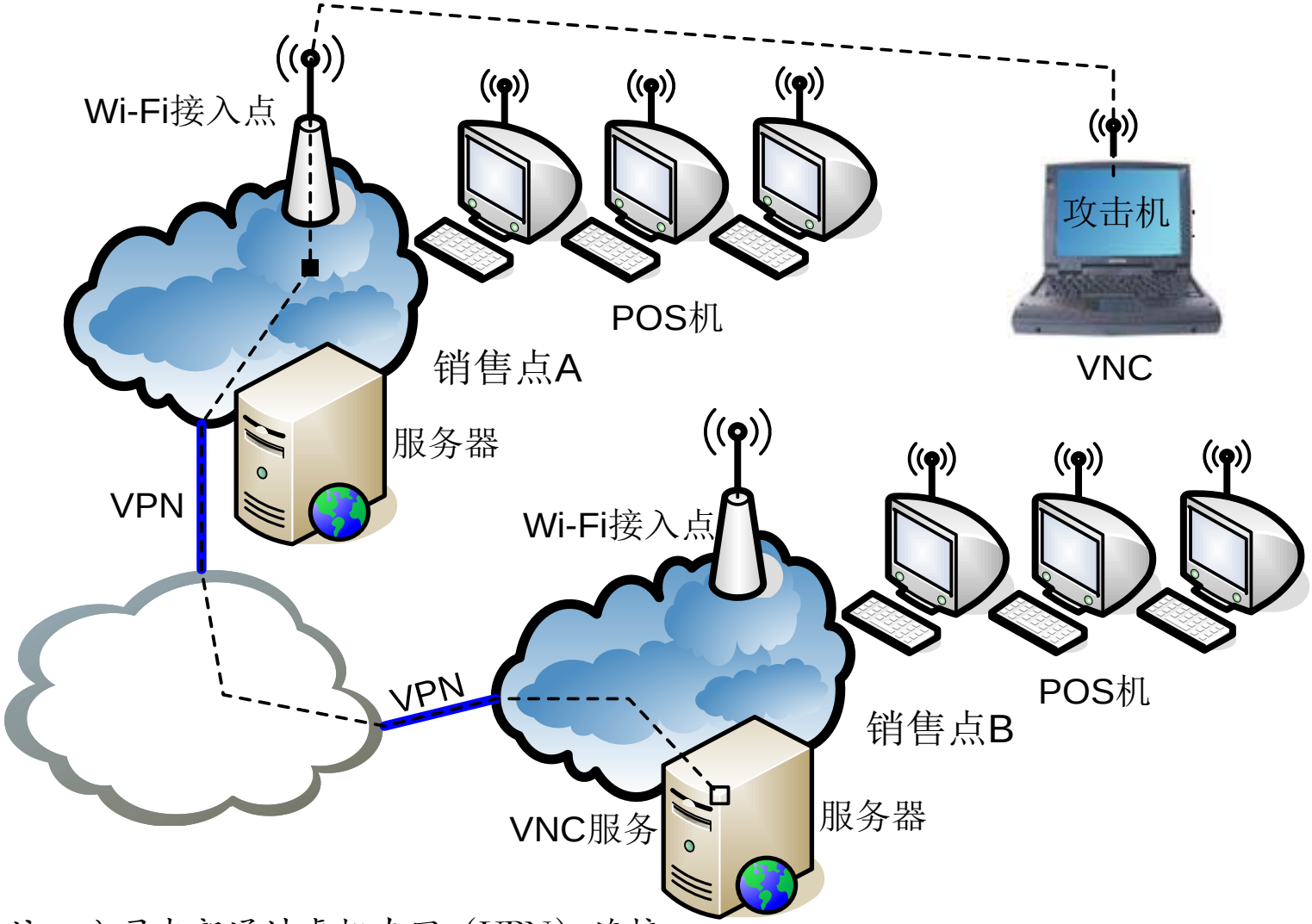
- 登录系统后，**卡尔发现**
  - 某目录下某文件中的交易记录显示出10万张信用卡资料！！！



扩大战果-尝试进入另一个VNC

- 提示：上一台VNC服务器的IP是w.x.y.z
- 尝试w.x.y.z+1：
  - 成功！！
  - 帐户名与口令与上一台相同
  - 获得由一批信用卡资料

通过VNC进入销售点B的服务器



注：公司内部通过虚拟专网（VPN）连接。

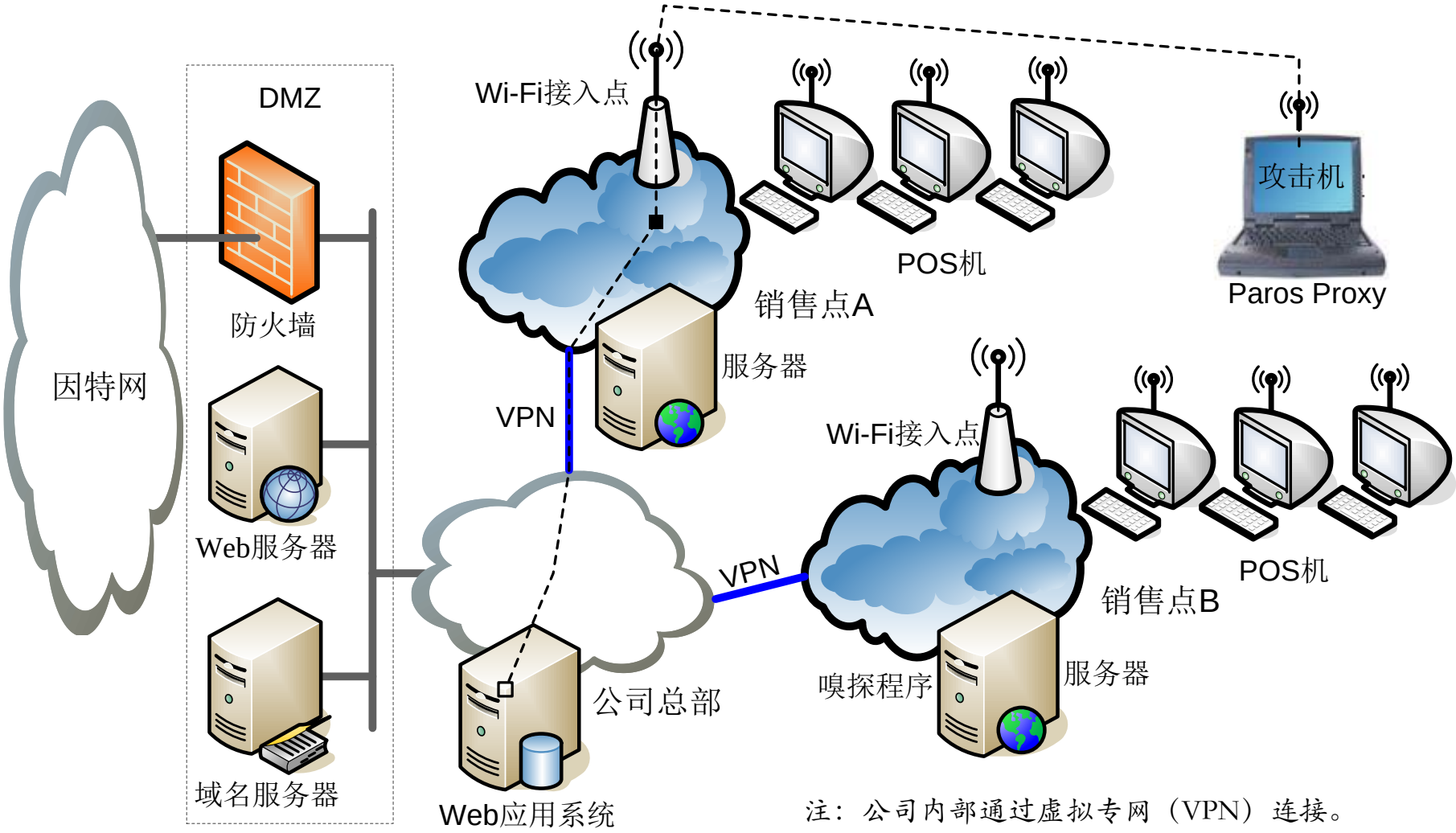
制胜之巅-攻击公司总部系统

- 用Nmap对服务器C（总部）扫描发现：
  - TCP 443端口打开-->HTTPS服务
    - 公司Web业务信息系统
- 尝试登录Web业务信息系统：
  - VNC口令失败，THC Hydra口令猜测失败。
- 用Paros Proxy自动扫描Web应用：
  - 寻找跨站脚本和SQL注入缺陷：
    - 在cookie中发现SQL注入缺陷
- 发起SQL注入攻击：
  - 成功，在Web应用后端数据库中获得100万张信用卡资料！！！

Paros Proxy ：Web应用掌控代理

- paros proxy，这是一个对Web 应用程序的漏洞进行评估的代理程序，即一个基于Java的web代理程序，可以评估Web应用程序的漏洞。它支持动态地编辑/查看HTTP/HTTPS,从而改变cookies和表单字段等项目。它包括一个Web 通信记录程序，Web 圈套程序(spider)，hash 计算器，还有一个可以测试常见的Web 应用程序攻击(如SQL注入式攻击和跨站脚本攻击)的扫描器。该工具检查漏洞形式包括：SQL 注入、跨站点脚本攻击、目录遍历

通过SQL注入进入内部Web应用系统



信息安全攻击的主要环节

- 侦察
- 扫描
- 获取访问
- 维持访问
- 掩盖踪迹

安全攻击的侦察环节

- 社会工程学
  - 通过普通谈话诱导受害者透露敏感信息
- 淘垃圾
  - 从遗弃的办公用品中搜寻敏感信息
- 受害者的Web网站
- 公共信息服务网站:
  - Whois数据库、InterNIC、Uwhois
- DNS服务器
- 侦察工具：Sam Spade等

安全攻击的扫描环节

- 网段扫描（网络映射）：Cheops-ng
- 端口扫描：Nmap
- 防火墙扫描：Firewalk
- 无线接入扫描：Wellenreiter
- 拨号扫描：THC-Scan
- 漏洞扫描：Nessus

安全攻击的获取访问环节

- 攻击操作系统
  - 缓冲区溢出攻击、口令攻击
- 攻击Web应用系统
  - 账户捕获、会话捕获、SQL注入、浏览器漏洞
- 攻击网络系统
  - 嗅探、IP欺骗、会话劫持
- 拒绝服务攻击

安全攻击的维持访问环节

- 木马
  - 表面上非常有用/吸引人，暗地隐藏恶意功能
- 后门
  - 能够让攻击者躲开正常的安全控制
- 木马后门：
  - 应用层木马后门：远程控制程序、BOT和间谍软件
  - 用户态rootkit：替换login 和sshd等操作程序系统
  - 内核态rootkit：对执行请求进行重定向
    - 文件/目录隐藏
    - TCP/UDP端口隐藏
    - 进程隐藏

安全攻击的掩盖踪迹环节

- 攻击者设法隐藏他们的攻击行为，以期不被发现
- 修改反映攻击行为的日志信息：
  - 失败的登录尝试
  - 特殊账户的使用
  - 安全敏感命令的运行
- 为防范日志记录信息被篡改
  - 采用独立的日志服务器
  - 对日志文件进行加密
  - 定期转存日志信息到DVD备份

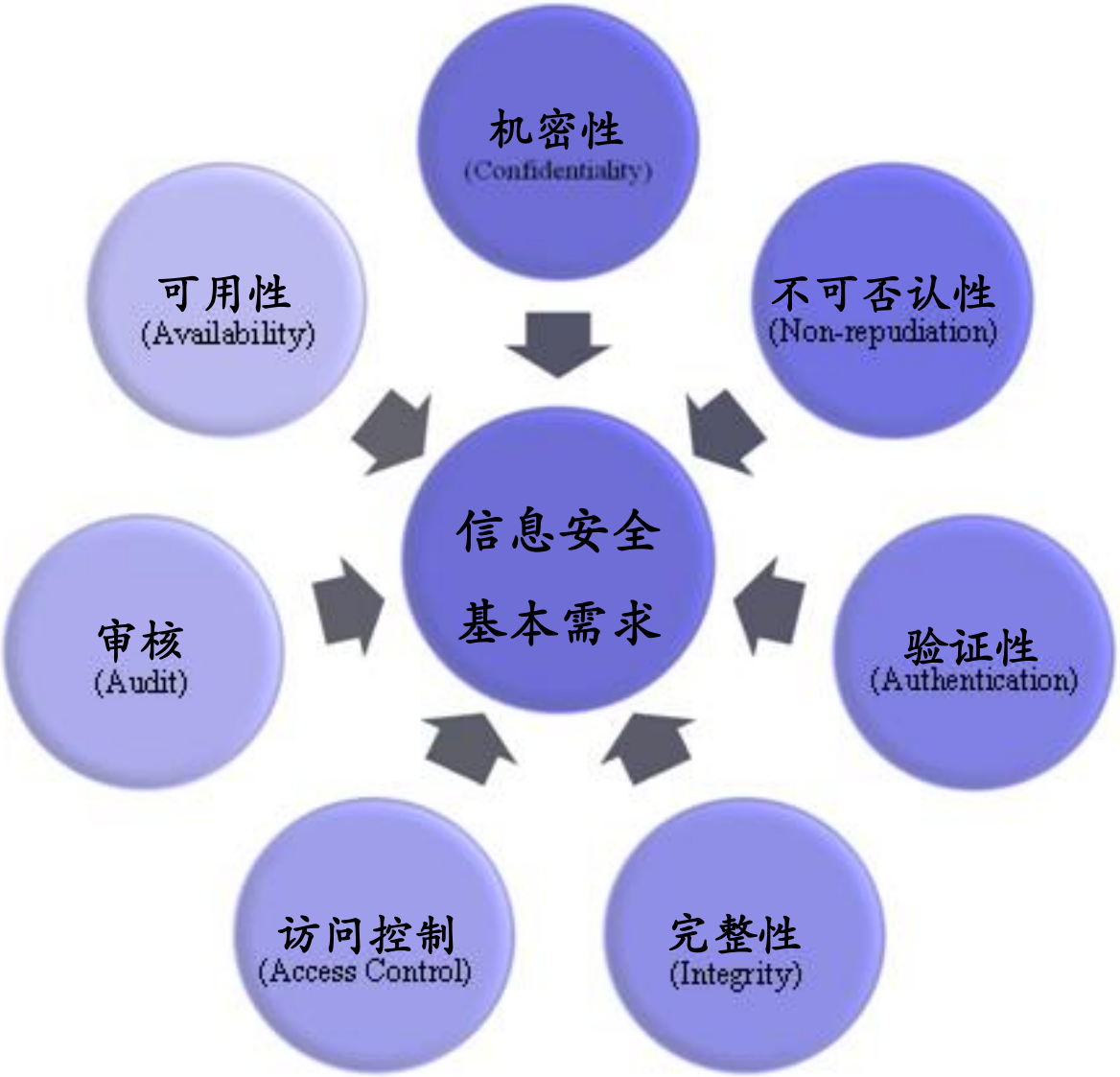
尾声

- 安全响应
  - 信用卡公司发现出现大量的信用卡欺骗行为
  - 进行数据分析可以关联到“好运”公司
  - “好运”公司展开内部调查，发现安全事故
  - “好运”公司将安全事故告知持卡人
  - “好运”公司履行赔偿，造成重大声誉损失
  - 有关机构进行电子取证，查找犯罪嫌疑人

（一）信息系统安全绪论

2、信息安全的基本需求

信息安全的基本需求


机密性
(Confidentiality)
不可否认性
(Non-repudiation)
验证性
(Authentication)
完整性
(Integrity)
访问控制
(Access Control)
审核
(Audit)
可用性
(Availability)
信息安全
基本需求

保密性或机密性

- 确保信息的机密，防止机密信息泄露給未经授权的用户。机密性数据内容不能被而仅能被授权者所访问 。未经授权者所窃取，
- 存取包括读出、浏览及列印。另外「数据是否存在于系统」也是一项很重要信息。
- 可通过资料加密程序来达到数据的保密性或机密性。

完整性

- 数据内容仅能被合法授权者所更改，不能被未经授权者所篡改或伪造。
- 数据完整性必须确保数据传输时不会遭受篡改，以保证数据传输内容的完整性。
- “数字签名”可用来确保数据在传输过程中不会被黑客篡改及伪造，从而保证数据的完整性 。

验证性

验证性包括身份验证(Entity Authentication)及数据或消息来源验证(Data or Message Authentication)。

- 信息来源的验证
  - 是要能确认数据信息的传输来源，以避免有恶意的传送者假冒原始传送者传送不安全的信息内容。
  - 一般均利用数字签名或数据加密等方式来解决信息的来源验证问题 。
- 身份验证
  - 对于用户身份的识别而言，系统必须快速且正确地验证身份。
  - 为了预防暴力攻击者的恶意侵犯，对于用户身份验证的时效性比信息验证要严谨。

可用性

- 确保信息系统运行过程的正确性，以防止恶意行为导致信息系统毁坏(Destroy)或延迟(Prolong)

不可否认性

- 在信息安全需求中，对于传送方或接收方，都不能否认曾进行数据传输、接收和交易等行为，即传送方不得否认曾传送过某份数据，而接收方也无法否认未曾接收到某信息数据。
- 数字签名及公开密钥基础设施(Public Key Infrastructure，PKI)对用户身份及信息来源做身份验证(User Authentication)及数据来源验证(Message Authentication)，并可再与用户在系统上的活动进行连接，从而实现权责分明及不可否认性。

访问控制

- 信息系统内每位用户依其服务等级而有不同的使用权限。服务等级越高者其权限越大，相反的，服务等级越小者其权限越小 。
- 访问控制主要是根据系统的授权策略，对用户做授权验证，以确认其是否为合法授权者，防止未经授权者访问计算机系统及网络资源。

审核

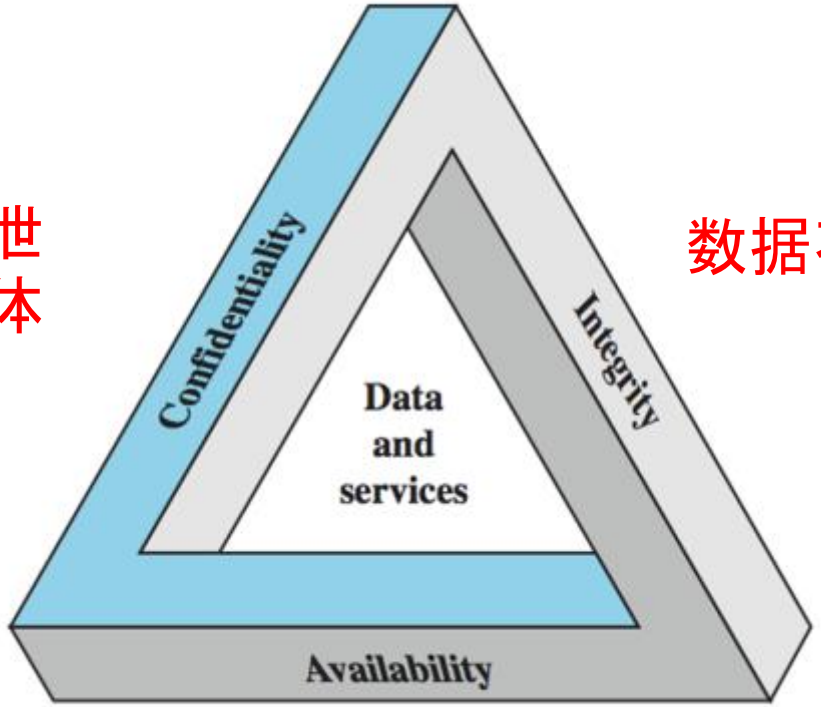
- 信息系统不可能达到绝对安全，也就是百分之百的安全。
- 因此，必须通过审核记录(Audit Log)来追踪非法用户，一旦发生入侵攻击事件，就可以尽快找到发生事件的原因，以作为恢复系统(Recovery)并预防此类入侵的手法，从而防止系统再一次被入侵。

信息安全三大要素

信息安全最经典的三个要素是：机密性、完整性、可用性

Confidentiality, Integrity, Availability

防止私密信息泄露给非授权实体

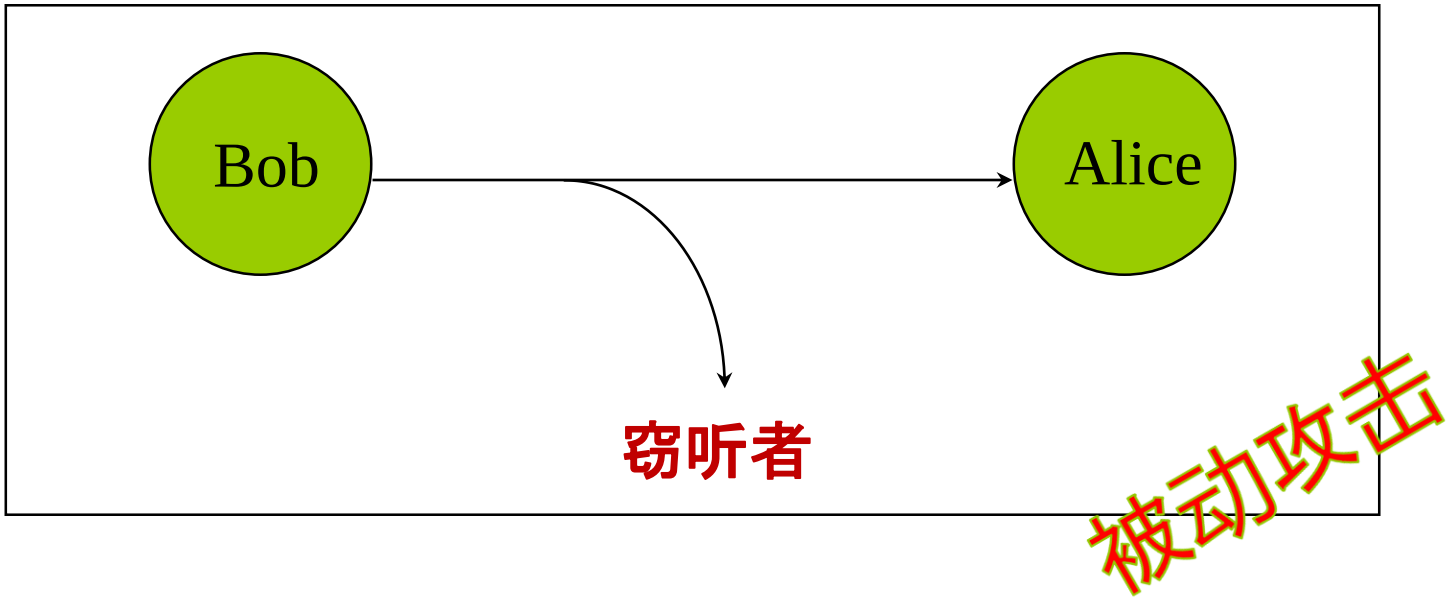


数据不被非法修改

确保系统及时工作并向授权用户提供所需服务

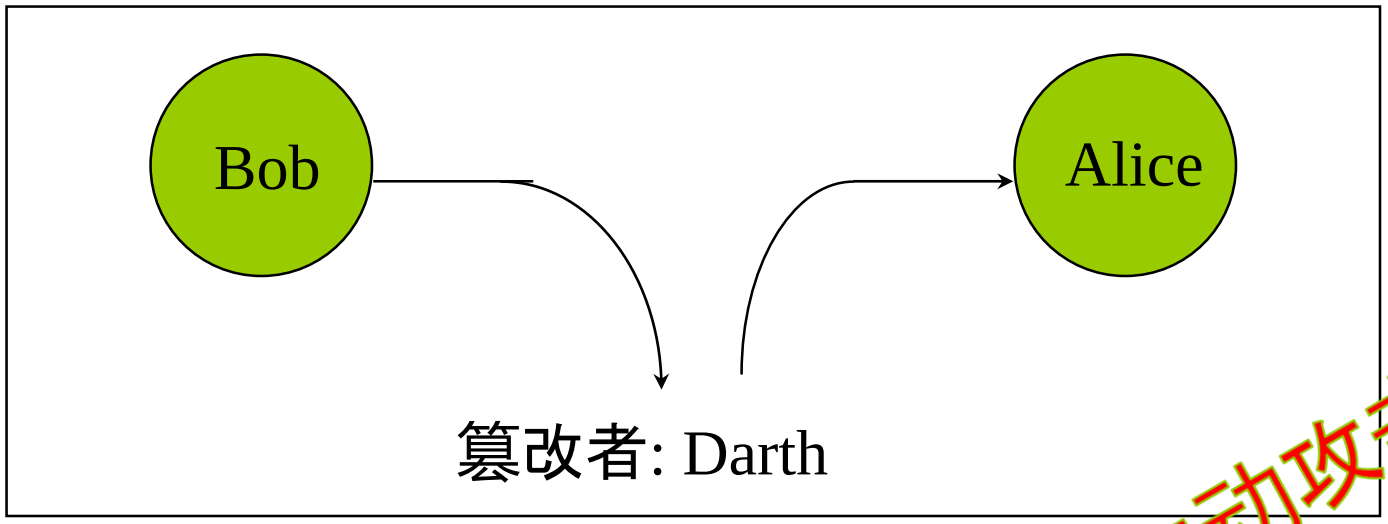
对机密性的攻击

- 消息截获
  - 非授权访问私密（privacy)或机密（secrecy）信息
  - 典型攻击：数据包嗅探器和窃听器
  - 非法复制文件和程序



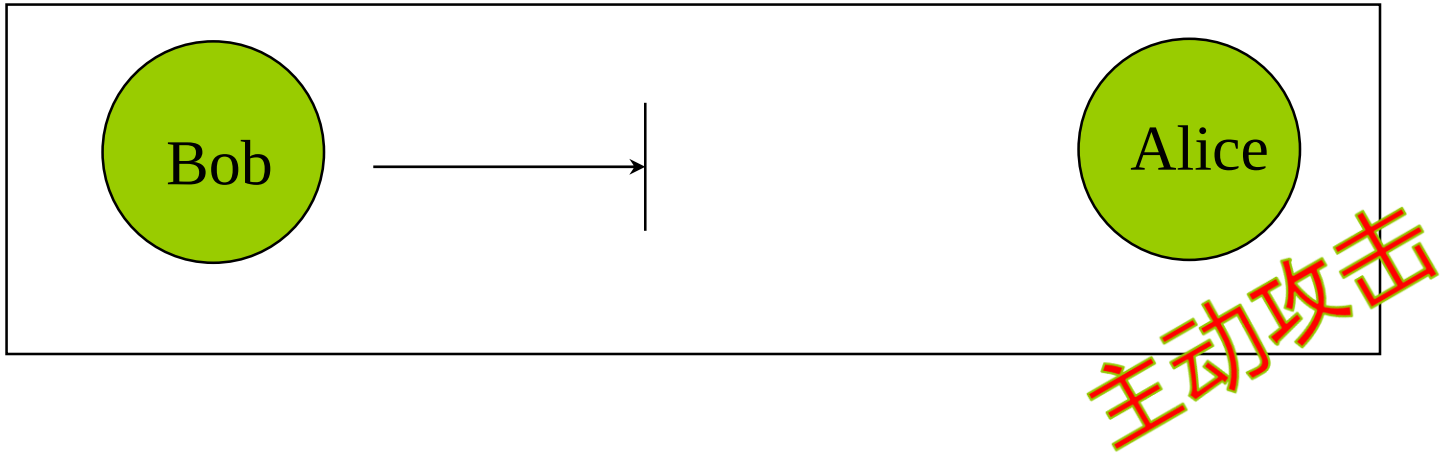
对完整性的攻击

- 消息篡改
  - 消息流会出现中断、延迟等现象
  - 消息可能经过改变后，再次释放



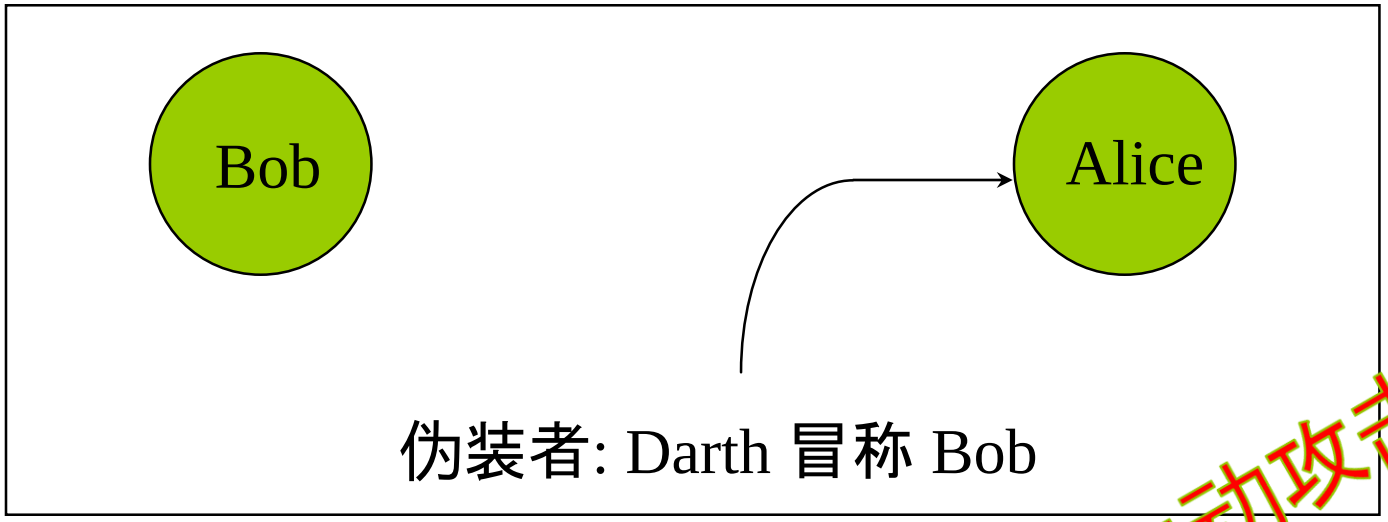
对可用性的攻击

- 阻断服务或者通信
  - 破坏硬件或者软件设备
  - 修改软件使其丧失功能
  - 损坏传输中的数据包
- DoS拒绝服务网络攻击
  - 使服务器崩溃
  - 用尽服务器资源



对真实性的攻击

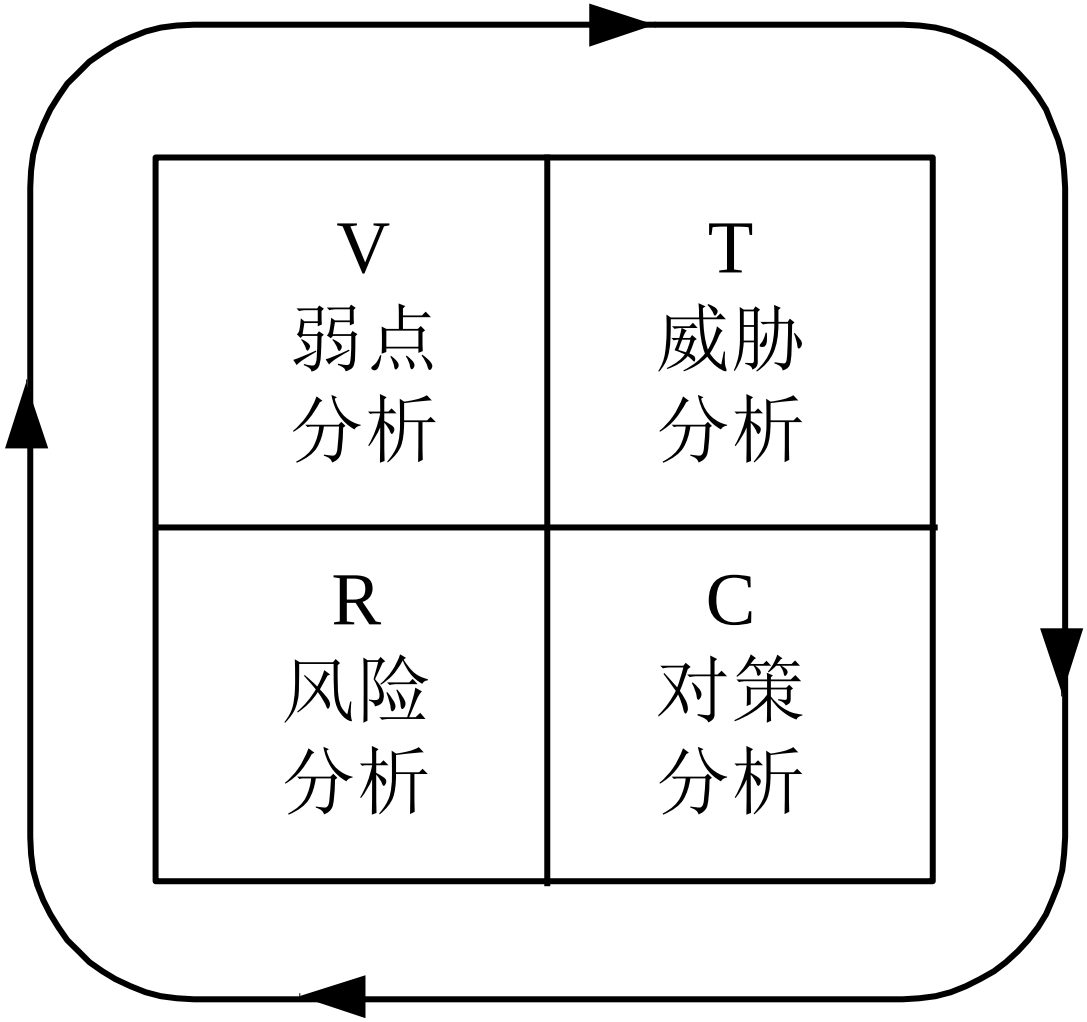
- 消息伪造
  - 未经授权冒充他人的身份
  - 未经授权以他人名义生成和分发物件



（一）信息系统安全绪论

4、信息系統的安全分析

信息系统的安全分析



弱点分析

- 对整个系统架构进行了解及测试，系统架设了哪些硬件，例如路由器(Router)、桥接器(Bridge)、网关(Gateway)及防火墙(Firewall)等；使用了哪一种操作系统，例如Linux、WinNT及Novell Network；使用了哪些通信协议，例如TCP／IP、Ethernet及ISDN等；安装了哪些应用软件，例如FTP、WWW及工资管理信息系统等；哪些人会使用本系统，授权了哪些权限给用户等。

- 管理者了解这些信息后，进而分析系统的弱点在哪里，哪些人有可能会来攻击，他们的目的是什么，以及要攻击哪些地方。

威胁分析

- 了解系统的弱点之后，接着要分析系统可能会遭受到的安全威胁及攻击。常见的入侵并影响系统安全的方式有利用电子邮件、利用Telnet远程登录、发送计算机病毒、试图得到具有高存储权限的账号、删除或移动文件等 。
- 系统管理员应随时上网浏览最新的黑客入侵信息，以防止计算机系统与网络安全危机的发生。

对策分析

- 针对这些弱点及所面临的安全威胁，应制定相应的安全策略及所需的安全机制。例如访问控制、用户认证、加密及数字签名等。

风险分析

- 不仅要定期评估及分析系统的风险，而且对于部分重要数据还必须采取进一步的防御。例如定期做备份及恢复处理等，确保当系统发生安全问题时重要数据不被损坏，从而降低问题发生时所带来的风险及损失。

安全漏洞所造成的损失

- 包括有形损失及无形损失
  - 有形损失包括硬件及软件设备、人力成本、开支成本及其他因工作延迟所造成的损失 。
  - 无形损失是指公司形象受到影响，其损失费用则无法计算。
- 通常投资在信息安全方面的费用应小于系统发生安全漏洞后所造成的损失，但要大于其损失的十分之一。
  - 例如，若预计某系统一旦发生安全事件所造成的损失为1000万元，那么所投资的成本就应该在100万到1000万元之间。

（一）信息系统安全绪论

5、安全的信息系统架构

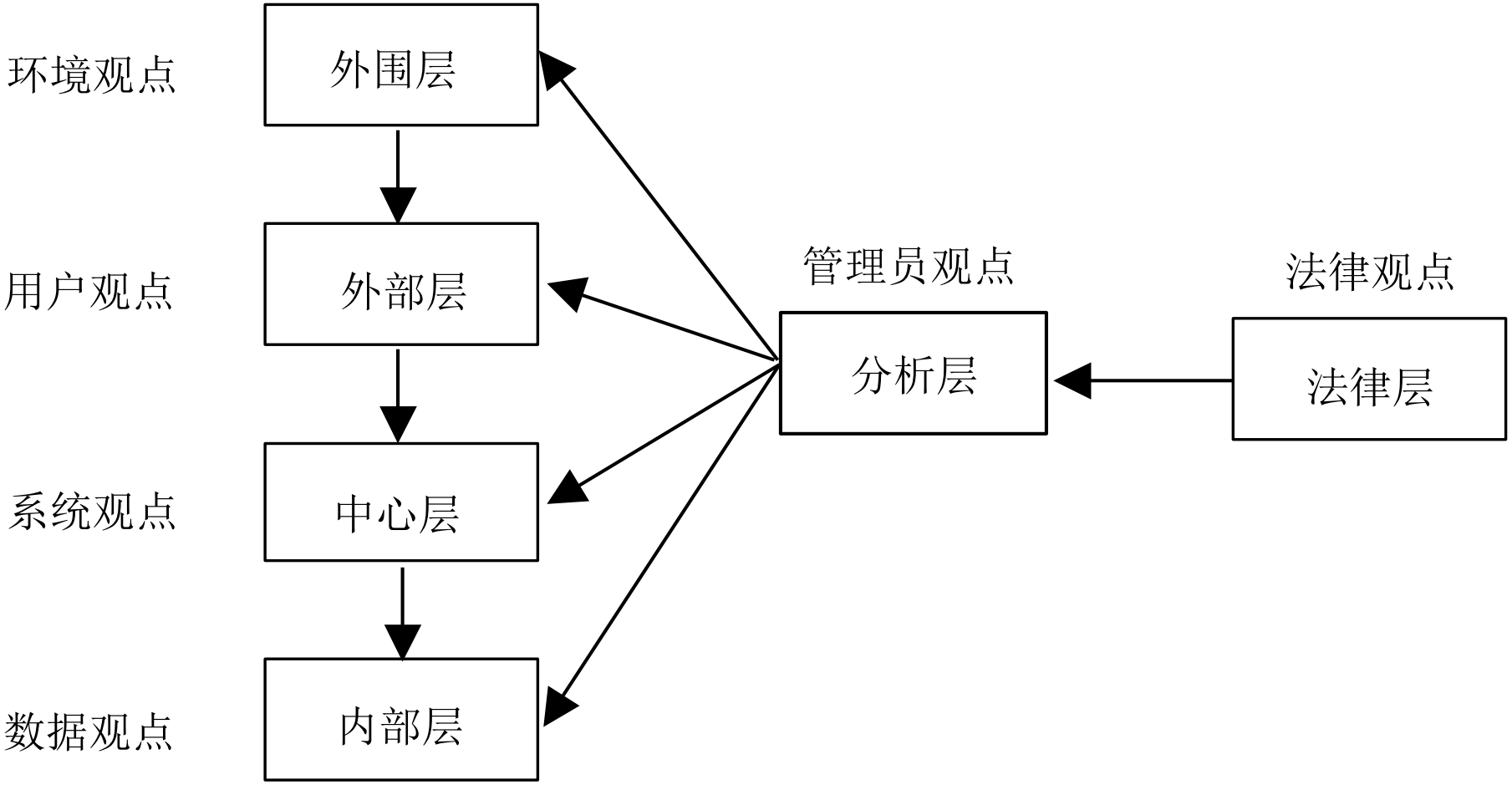
安全的信息系统架构

以信息安全角度来区分

- 外围层牵涉到有关计算机系统周边外围的环境因素。
- 外部层是用户与系统间介面层次，所牵涉到的是个别用户所能操作的系统。
- 中心层是内部层与外部层的沟通桥梁。
- 内部层牵涉到数据实际存储及管理的方式。
- 分析层牵涉到系统的管理及安全威胁的分析。
- 法律层牵涉到有关信息安全相关的法律条文。

计算机操作系统安全架构

- 以角色观点



计算机操作系统安全架构

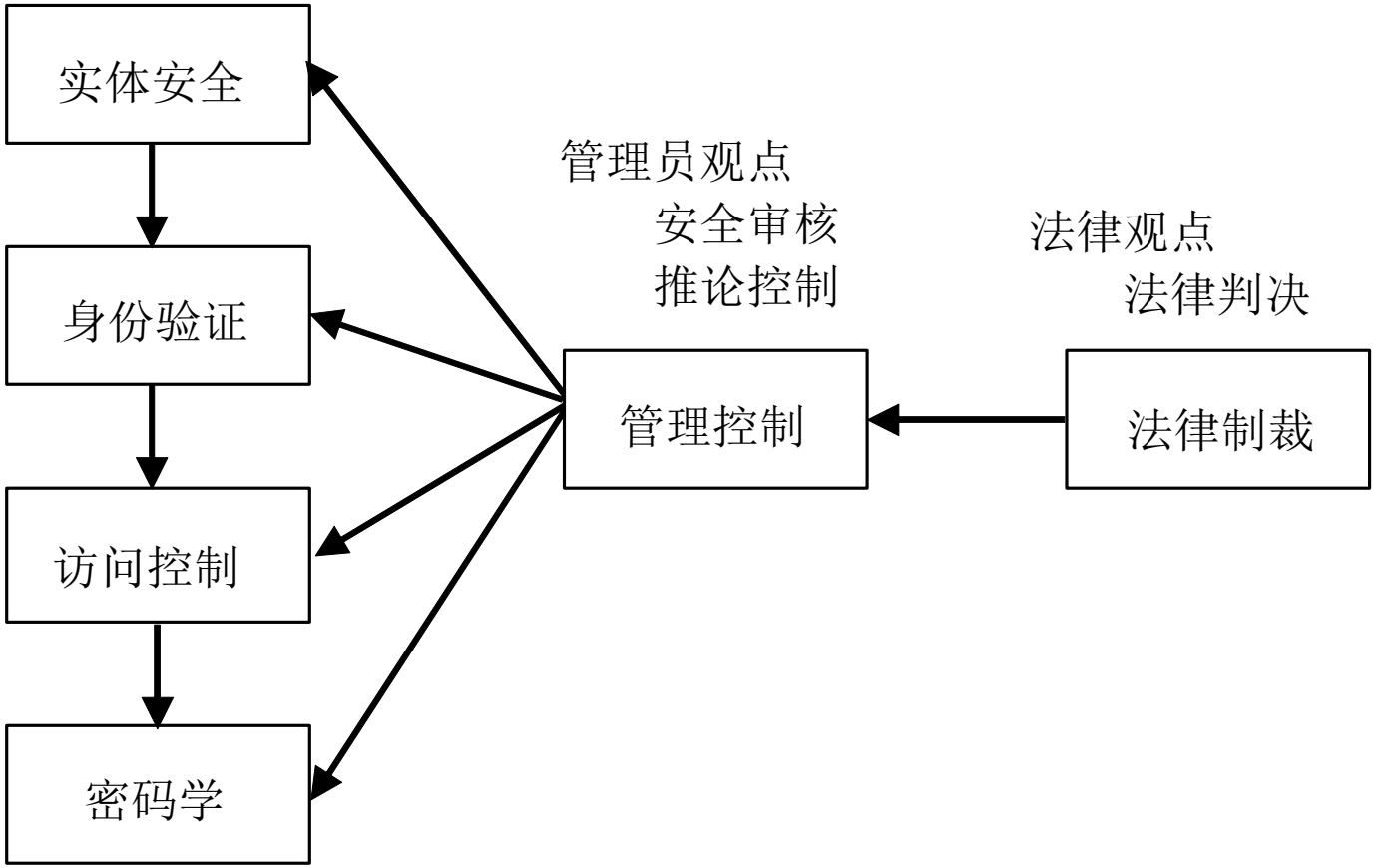
- 以技术观点

环境观点
实体安全

用户观点
通行密码
生物识别

系统观点
任意性控制
强制性控制

数据观点
加解密技术
数字签名



信息流向及颗粒性

- 数据流向
  - 一旦某信息拥有者將部分或全部权利授予他（她）人后，就很难掌握此信息。
  - 此信息的权利很可能被授予者再转授予第三者。
- 颗粒性
  - 任意性访问控制方法是将一个文件当作访问控制的基本单位。基本上，系统应该允许用户访问到数据内某一原子(Atomic)数据 。
  - 強制性访问控制或者为多层性访问控制。

谢谢！

讲课老师:王艺

1478128896@qq.com

东莞理工学院 计算机学院