管理信息系统

Management Information Systems

王谦 博士/副教授
南开大学商学院管理科学与工程系
wangqian70@nankai.edu.cn

Chapter 7

信息系统安全

学习目标

- 解释为什么信息系统容易出现系统崩溃、出错和滥用?
- 描述安全与控制的商业价值是什么?
- 描述安全与控制的组织框架有哪些组成要素?
- 描述保护信息资源最重要的工具和技术有哪些?

开篇案例

- 你上LinkedIN.com网站么？要小心！

  - 问题: 大规模数据泄漏；使用过时的安全措施。
  - 解决方案: 按照采用满足最低的行业标准做法来保护数据。例如，采用最新的哈希密码加盐方法。
  - 展现了需要按照当前的标准来持续更新企业的安全措施以应对来自数据安全的威胁。
  - 说明了计算机安全与社会网络数据安全还缺乏监管，许多公司的保护极差。

7.1 系统漏洞和被滥用

- 安全
  - 防止对信息系统非授权的访问、更改、盗窃或者物理损害的政策、步骤和技术措施
- 控制
  - 确保组织资产安全的方法、政策和组织流程，要求对资产记录要准确、可靠，对其处置符合管理标准

SOURCE: © Rafal Olechowski/Shutterstock

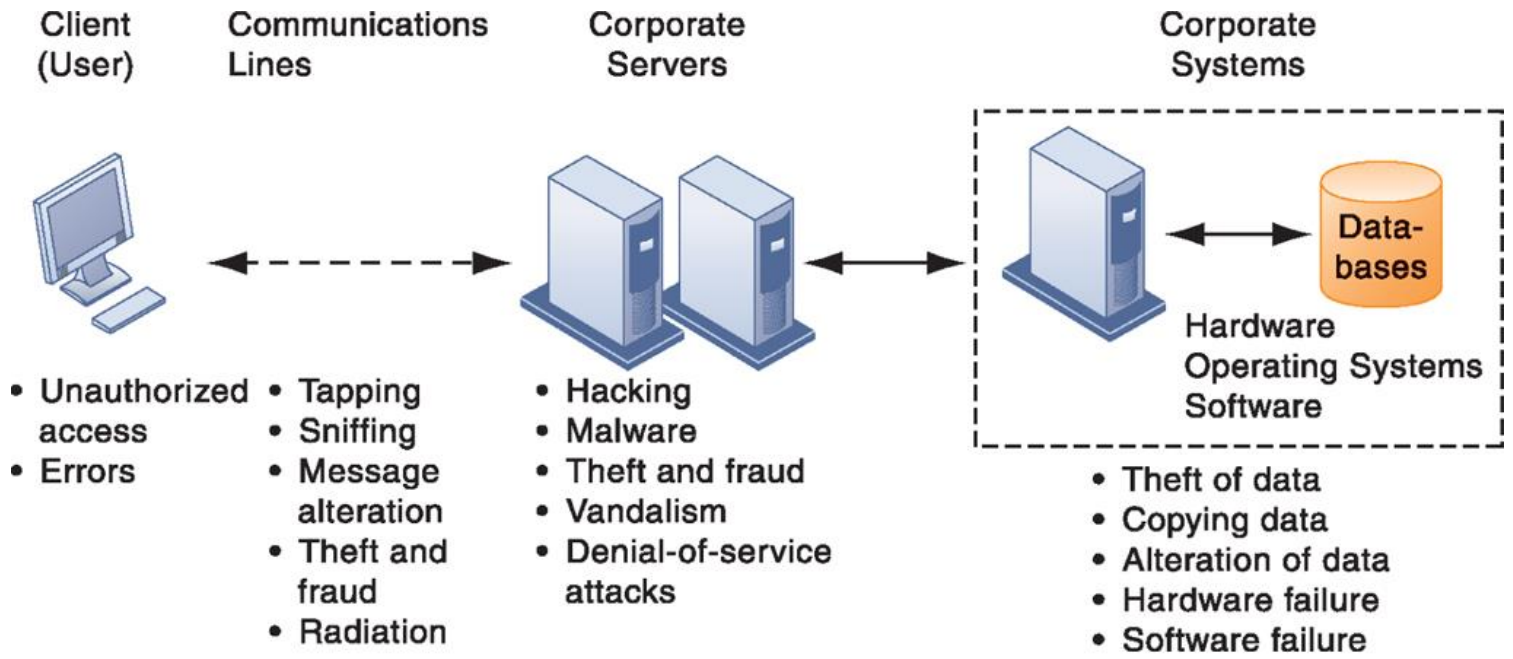
7.1 系统漏洞和被滥用

- 为什么系统容易受到破坏?
  - 网络的漏洞
  - 硬件问题（计算机硬件崩溃、配置不当、因使用不当甚至于是犯罪行为造成的损坏）
  - 软件问题（程序错误、安装不当、未经授权的更改）
  - 灾害
  - 组织控制之外的网络或者计算机的使用
  - 便携移动设备的丢失或被盗

7.1 系统漏洞和被滥用

当前安全挑战和漏洞

- 一个基于Web的应用程序体系结构通常包括Web客户机、服务器和与数据库连接的企业信息系统。每个组件都具有安全挑战和漏洞。水灾、火灾、停电及其它电气问题都会导致网络中任何连接点的中断



7.1 系统漏洞和被滥用

因特网的漏洞

- 因特网对所有人开放
- 因特网如此巨大，以致当滥用发生时会产生四处蔓延的巨大影响
- 通过调制解调器或者数字专线DSL与因特网固定连接的计算机更容易被外来者入侵，因为它们使用固定的因特网地址从而更易于黑客识别
- 未经加密的由公用因特网传输的IP语音，即VoIP（Voice over IP）
- 电子邮件，即时信息IM（instant messaging）和对等P2P（peer-to-peer）
  - 拦截
  - 附件上携带恶意软件
  - 传送有价值的交易机密

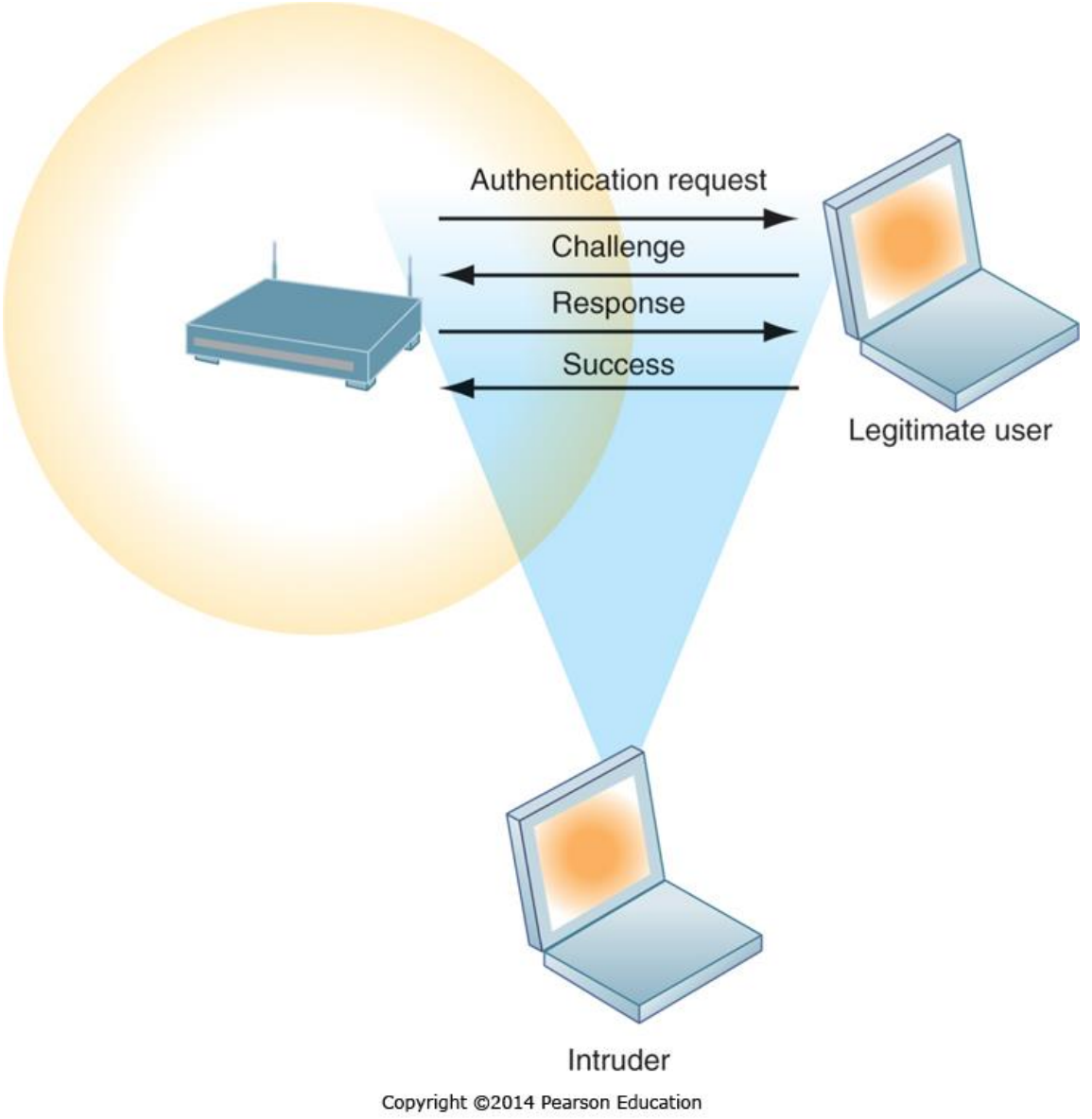
7.1 系统漏洞和被滥用

无线网络的安全挑战

- 无线频率的波段很容易被监测到
- 服务集标识SSID（service set identifier）
  - 定位识别访问点
  - 多次广播
  - 容易被入侵者的监听程序窃取
  - 驾驶攻击（war driving）
    - 窃听者在外面的建筑物或者公园里进行操纵，以拦截无线网络的流量
  - 一旦入侵者被入侵，入侵者可以通过操作系统来访问计算机的网络驱动器和文件

7.1 系统漏洞和被滥用

- Wi-Fi的安全挑战
  - 许多Wi-Fi网络容易被入侵者渗透，他们利用窃听程序来获得地址从而未经授权便访问网络中的资源。



7.1 系统漏洞和被滥用

恶意软件 *malware*

- 病毒 *virus*
  - 一种通常在用户不知情和许可的情况下，附着在其它软件程序或者数据文件上以被执行的欺诈软件程序
- 蠕虫 *worms*
  - 一种独立的计算机程序，可以在网络上将自己从一台计算机拷贝到另一台计算机
- 蠕虫和病毒的传播方式
  - 下载驱动（drive-by downloads）
  - 电子邮件或者即时信息传送的附件文件
  - Web网站及社交网络上的下载

7.1 系统漏洞和被滥用

恶意软件（继续）

- 智能手机和个人电脑一样易受攻击
  - 安全公司迈克菲（McAfee）在2012年发现了近13,000个不同类型的针对移动设备的恶意软件
- 特洛伊木马 *Trojan horse*
  - 一种软件程序，它看似良性但是会做出一些意想不到的事情
- SQL注入攻击 *SQL injection attack*
  - SQL注入攻击利用一些编程很差的Web应用软件的漏洞将恶意程序代码引入到企业的系统和网络中

7.1 系统漏洞和被滥用

恶意软件（继续）

- 间谍软件 *spyware*
  - 这些小程序将自己偷偷安装在计算机上以监视用户的上网活动和广告服务
  - 按键记录器 *key-loggers*
    - 记录下计算机键盘的每次击键以窃取软件的序列号、发动网络攻击、获得对用户电子邮件账户的访问、获取保护计算机系统的密码，或者获取如信用卡号码等个人信息
  - 其它类型
    - 重置浏览器的主页
    - 重定向搜索请求
    - 通过大量占用内存来降低计算机的性能安全公司迈克菲（McAfee）在2012年发现了近13,000个不同类型的针对移动设备的恶意软件

7.1 系统漏洞和被滥用

黑客与计算机犯罪

- 黑客（hacker）和骇客（cracker）
- 活动包含
  - 系统入侵
  - 毁坏系统
  - 恶意网络破坏行为（cyber vandalism）
    - 故意中断、毁坏，甚至摧毁一个网站或企业信息系统的行为

7.1 系统漏洞和被滥用

- 电子欺骗 *spoofing*
  - 把欺骗网站伪装成目的网站
  - 把网页链接误导入另一个与用户实际希望访问的网站不同的地址
- 嗅探器 *sniffer*
  - 一种在网络中监控信息传输的窃听程序
  - 使黑客能够从网络中任何地方盗取有价值的私有信息，包括电子邮件消息、公司文件和机密报告等

7.1 系统漏洞和被滥用

- 拒绝服务攻击 *(Denial-of-service attack, DoS attack)*
  - 黑客攻击一个网络时，向网络服务器或Web服务器发送成千上万的假通信或服务请求造成网络崩溃以至网络对合法的请求也不能及时处理
- 分布式拒绝服务攻击 *(Distributed Denial-of-service attack, DDoS attack)*
  - 使用许许多多的计算机从无数的发射点来淹没网络
  - 僵尸网
    - 由成千上万感染上恶意软件的“僵尸”个人计算机组成的网络
    - 世界上90%的垃圾邮件和80%的恶意软件都是由僵尸网传播
    - Grum僵尸网：控制了56万–84万台计算机

7.1 系统漏洞和被滥用

- 计算机犯罪 *computer crime*
  - 定义为“任何涉及利用计算机技术知识实施的刑事违法行为，可以对其调查和起诉”
  - 以计算机为犯罪目标，例如：
    - 攻破被保护的计算机保密数据
    - 未经授权进入计算机系统
  - 以计算机为犯罪工具，例如：
    - 盗取商业秘密
    - 使用电子邮件恐吓或骚扰他人

7.1 系统漏洞和被滥用

- 身份盗用 *identity theft*
  - 盗用他人关键信息（社保号、驾照号、信用卡号等）以假冒他人的犯罪
- 网络钓鱼 *phishing*
  - 仿冒合法企业设置虚假网站或发送电子邮件来获取用户的个人保密数据
- 邪恶双胞 *evil twin*
  - 一种在网络中监控信息传输的窃听程序
  - 伪装成提供可信的Wi-Fi因特网连接的无线网络

7.1 系统漏洞和被滥用

- 嫁接 *pharming*
  - 将用户引导到一个欺骗网页，即便用户在其使用的浏览器中输入了正确的网址
- 点击欺诈 *click fraud*
  - 个人被计算机程序欺骗性地点击在线广告，而没有想更多去了解或者是购买产品的主观意愿
- 全球威胁：网络恐怖主义和网络战 *cyberwarfare*

7.1 系统漏洞和被滥用

- 内部威胁：员工
  - 安全威胁常常来自于组织内部
  - 内部安全知识
  - 安全措施松散
    - 用户缺乏安全知识
  - 社交工程
    - 恶意入侵者有时会假装成公司的合法员工因需要信息而向他人骗取密码

7.1 系统漏洞和被滥用

软件漏洞

- 商业软件的缺陷造成安全漏洞
  - 隐藏的bug或程序代码缺陷
    - 较大的程序无法实现零缺陷因为根本不可能对软件进行完整测试
  - 商业软件的缺陷造成安全漏洞给网络入侵者有可乘之机
- 补丁
  - 修复软件缺陷的小程序
  - 恶意软件的产生非常迅速，在发现漏洞和得到补丁程序之前，恶意软件可能就会利用漏洞发起攻击

7.2 安全与控制的商业价值

- 失效的信息系统会导致企业产生巨大损失
- 如今的企业比任何时候都要脆弱
  - 机密的个人数据和财务数据
  - 商业秘密、新产品开发计划和营销策略
- 一个安全泄漏事件可能导致企业的市值马上大幅下降
- 安全和监管上的不足会导致要承担严厉的法律责任

7.2 安全与控制的商业价值

- 电子档案管理的法律和监管要求
  - 健康保险便利及责任法案（HIPAA）：医疗行业针对保护医疗数据和个人隐私安全作出的规定和实施措施
  - 金融服务现代化法案：规定金融机构要确保客户数据安全保密
  - 萨班斯-奥克斯利法案（Sarbanes-Oxley Act）：强制要求公司及其管理层要承担责任，确保内部使用和对外公开的财务信息的准确性和完整性

7.2 安全与控制的商业价值

电子证据

- 针对计算机系统的犯罪证据常常是以数字形式存在
  - 计算机内的数据、电子邮件、即时信息和因特网上的电子商务交易记录等方面的数据
- 正确的电子档案保存措施在应对可能发生的计算机取证请求时将会节省时间和金钱

计算机取证

- 对存储在计算机介质或从计算机介质中提取到的数据进行科学收集、审查、授权、保存和分析，使其可以在法律诉讼中作为证据使用
- 包括环境数据和隐藏数据

7.3 安全与控制基本框架的建立

- 信息系统控制
  - 人为控制和自动控制
  - 总体控制和应用软件控制

- 总体控制
  - 针对计算机程序的设计、安全和使用，以及遍布在组织IT基础设施中的一般数据文件的安全等方面的管理
  - 适用于所有与计算机应用相关的环境
  - 以建立总体控制环境为目的，由硬件、软件，以及人为等方面的措施组合而成

7.3 安全与控制基本框架的建立

- 总体控制类型
  - 软件控制
  - 硬件控制
  - 计算机运行控制
  - 数据安全控制
  - 实施控制
  - 行政控制

7.3 安全与控制基本框架的建立

应用性控制

- 针对每个计算机应用软件特有的专门控制，例如针对计算报表和订单处理
- 包括了自动措施和人为措施
- 确保只有经过认可的数据才能被应用软件完全准确地处理
- 应用性控制包括
  - 输入控制
  - 过程控制
  - 输出控制

7.3 安全与控制基本框架的建立

- 风险评估：确定如果一个活动或过程没有控制好，将会给企业带来的风险程度
  - 风险的类型
  - 一年内的发生概率
  - 潜在的损失
  - 年预期损失

TABLE 8.5 ONLINE ORDER PROCESSING RISK ASSESSMENT

EXPOSURE	PROBABILITY OF OCCURRENCE (%)	LOSS RANGE/ AVERAGE ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5,000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000–$50,000 ($25,500)	$1,275
User error	98%	$200–$40,000 ($20,100)	$19,698

7.3 安全与控制基本框架的建立

安全措施

- 由陈述信息风险、阐述可接受的安全目标以及达成这些目标的机制等构成
- 安全措施能够促使企业制定出其它一些相关措施
  - 可接受使用策略（AUP）
    - 规定使用公司的信息资源和计算机设施的可接受行为
  - 授权措施
    - 确定不同类型的用户对于信息资产的访问权限等级

7.3 安全与控制基本框架的建立

身份管理

- 由业务流程和软件工具组成，用来识别系统的合法用户，并控制他们对系统资源的访问
  - 对不同类型用户的识别和授权
  - 指定每个用户允许访问的系统或系统功能
  - 鉴定及保护用户身份的过程和技术
- 身份管理系统
  - 获取不同级别用户的访问权限

7.3 安全与控制基本框架的建立

人事系统的访问规则

- 图给出了在某个人事系统中可能使用到的两个安全配置文件或者数据安全模式样例。根据安全配置文件，用户会在要访问的系统、访问位置或要访问的数据等方面受到一定的限制

SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

7.3 安全与控制基本框架的建立

- 故障恢复规划
  - 制定出当计算和通讯服务被破坏后，能够使其恢复工作的计划
- 业务持续规划
  - 专注于经过故障冲击后企业怎样恢复其业务运行
  - 上述两类规划都需要确定企业最关键的系统
    - 进行业务影响分析来确定系统中断对业务产生的影响
    - 管理层必须确定哪些系统要最先恢复

7.3 安全与控制基本框架的建立

信息系统审计

- 对企业的总体安全环境以及针对单个信息系统的控制措施进行检查
- 安全审计对技术、步骤、文档、培训和人事等进行检查
- 完全彻底的审计甚至会模拟攻击或灾难事件来测试技术、信息系统人员和公司员工的响应情况
- 审计结果会把控制措施中的所有缺陷逐一列举出来，并评估它们发生的可能性
- 评价每种威胁对组织会产生的经济和总体影响

7.3 安全与控制基本框架的建立

控制措施缺陷清单样例

- 本图是从常见的地方商业银行的借贷系统审计报告中，截取的部分控制措施缺陷清单样本。该表单帮助审计人员记录和评估控制措施的缺陷，将结果通知管理层，并记录下管理层采取的纠正措施。

Function: Loans **Prepared by: J. Ericson** **Received by: T. Benson**
Location: Peoria, IL **Date: June 16, 2013** **Review date: June 28, 2013**

Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/13	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/13	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

7.4 保护信息资源的技术和工具

身份管理软件

- 自动保留所有用户的使用记录及其系统权限
- 包括用户身份认证、用户身份保护以及系统资源的访问控制

身份认证

- 密码系统
- 令牌
- 智能卡
- 生物身份认证

7.4 保护信息资源的技术和工具

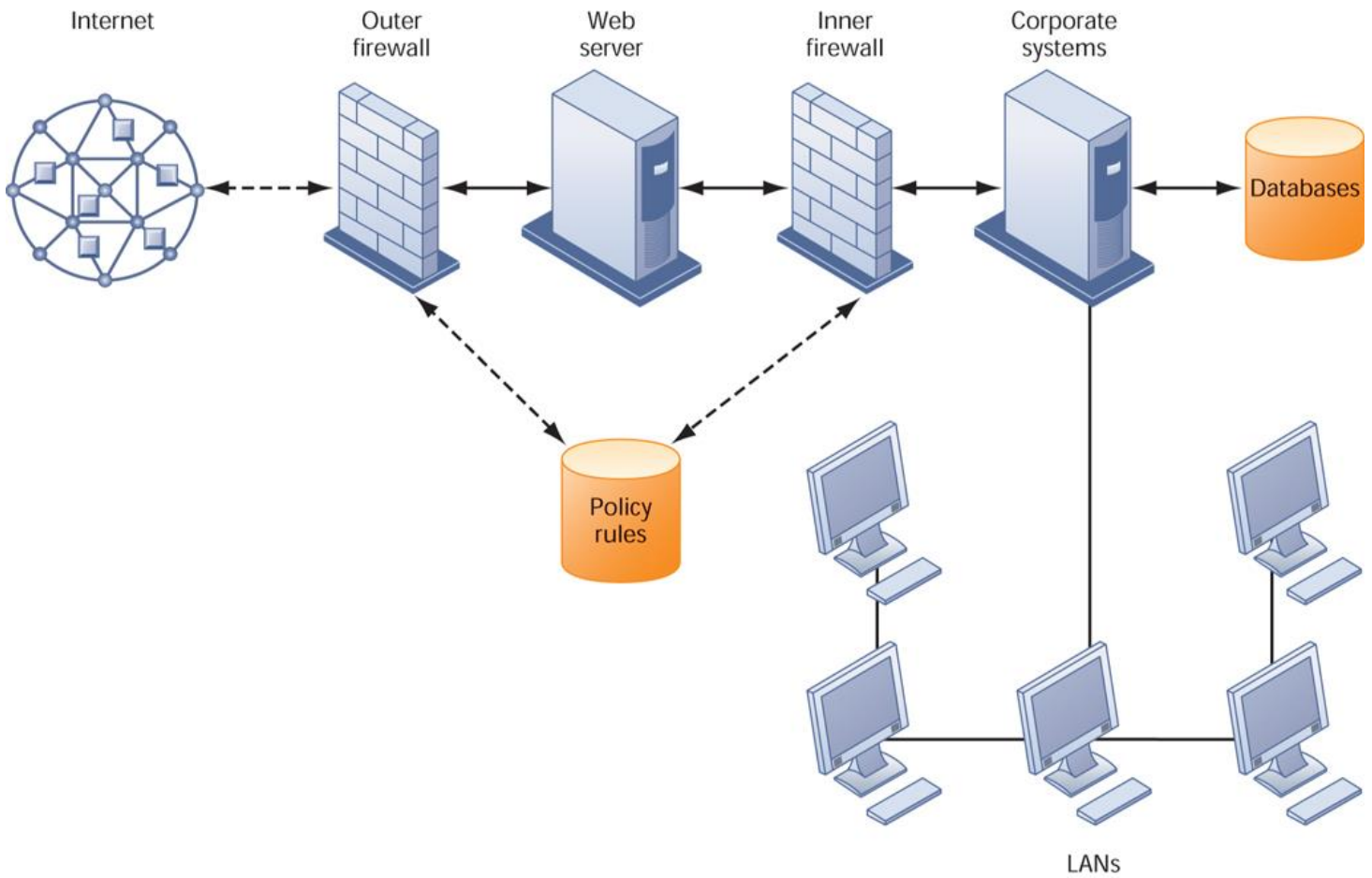
防火墙

- 一种软件和硬件的组合，用来控制传入和传出的网络流量
- 防火墙屏蔽技术包括：
  - 静态包过滤
  - 状态检测
  - 网络地址转换
  - 应用代理过滤

7.4 保护信息资源的技术和工具

企业防火墙

- 防火墙放置在公司专用网络和公共因特网或者另外的信任度不高的网络之间，用来阻止未授权的通信



7.4 保护信息资源的技术和工具

- 入侵检测系统
  - 放置在最易受攻击的连接点或者企业网络的热点节点上来检测和阻止入侵者的不断入侵
  - 检查当时发生的事件来发现正在进行的安全攻击
- 反病毒软件与反间谍软件
  - 防止、检测并删除恶意软件
  - 必须不断更新
- 一体化威胁管理系统

7.4 保护信息资源的技术和工具

无线网络安全

- WEP提供了一定的安全系数
  - 为无线网络的服务集标识（SSID）分配唯一的名字并且不广播服务集标识
  - 同虚拟专用网（VPN）技术一起使用
- Wi-Fi联盟行业贸易组织最终完成了802.11i规范（也被称为Wi-Fi保护访问2或WPA2），并且用这个更强的安全标准替代了WEP
  - 新标准使用了更长的不断变化的密钥
  - 在一个中心认证服务器上运行加密认证系统

7.4 保护信息资源的技术和工具

加密

- 一种将明码文本或数据变成暗码文本的过程。除了发送者和目的接收者以外，暗码文本不能被其他任何人阅读。
- 对网络中流量信息加密的两种方法
  - 安全套接层协议SSL（Secure Sockets Layer）及其后续的传输层安全协议TLS（Transport Layer Security）
  - 安全超文本传输协议S-HTTP（Secure Hypertext Transfer Protocol）

7.4 保护信息资源的技术和工具

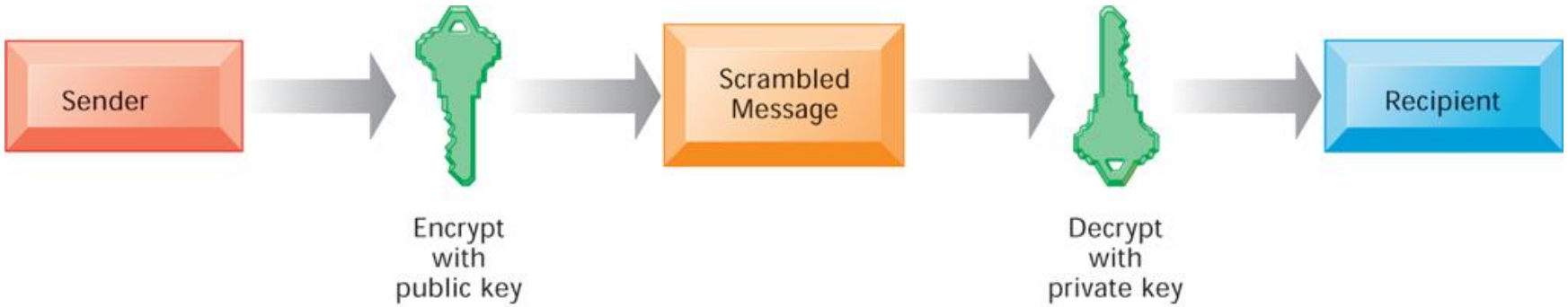
两种加密方法

- 对称密钥加密
  - 发送者和接收者通过创建一个单一密钥建立一个安全的网络会话
- 公钥加密
  - 使用两个密钥，其中一个为共享密钥（或公钥），另外一个则是完全私有的
  - 发送者利用接收者的公钥对信息加密
  - 接收者利用自己的私钥来解密

7.4 保护信息资源的技术和工具

公钥加密

- 本图公钥加密系统可看作是一系列的公钥和私钥分别在数据传输时给数据加锁而在接收数据时给数据解锁。发送者在目录中找到接受者的公钥并用它给信息加密。信息以加密的形式通过因特网或者专用网络传输。当加密信息到达时，接收者就用自己的私钥解密数据并读出信息。



7.4 保护信息资源的技术和工具

数字证书

- 为了保护在线交易，用来辨别用户身份和电子资产的一种数据文件
- 数字证书系统利用可信赖的第三方机构，称为认证中心（CA），来验证用户身份的合法性
- CA核查数字证书以验证用户的身份。数字证书信息输入CA服务器后，CA服务器会产生一个加密的数字证书，其中包括证书持有者的身份信息和一份持有者的公钥的拷贝

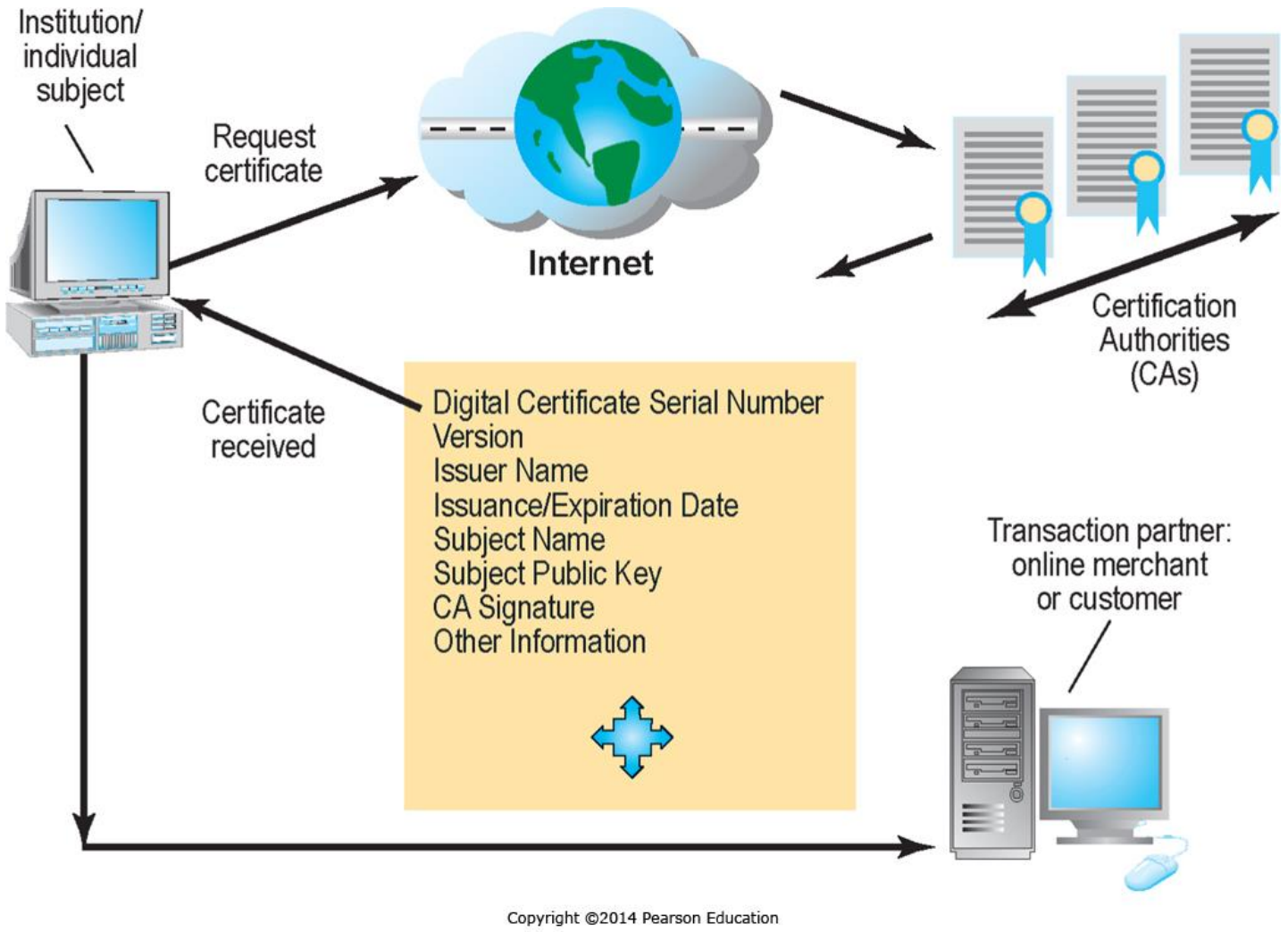
公钥加密基础设施（PKI）

- 由公钥加密技术以及数字认证中心CA组成
- 在电子商务中得到了广泛应用

7.4 保护信息资源的技术和工具

数字证书

- 本图中，数字证书帮助证实用户和电子资产的身份。通过提供安全、加密的在线通讯保护在线交易



7.4 保护信息资源的技术和工具

确保系统的可靠性

- 在线事务处理需要100%的可靠以及零宕机

容错计算机系统

- 提供连续不间断服务，例如股票市场
- 包括冗余的硬件、软件和电源保障等组成部分。这些组成部分建立起一个可提供连续不间断服务的环境

高可靠计算

- 帮助企业尽快从系统崩溃中恢复
- 尽量使宕机时间降到最低而不是完全消除

7.4 保护信息资源的技术和工具

确保系统的可靠性

- 在线事务处理需要100%的可靠以及零宕机

面向恢复的计算

- 设计能够快速恢复的系统，完善能力和工具以帮助操作人员在多部件组成的系统中查找故障源并尽快修复

网络流量控制

- 深度包检测
  - 对视屏及音乐流量进行封堵

安全管理外包

- 安全管理服务供应商（MSSP）

7.4 保护信息资源的技术和工具

云计算的安全问题

- 保护敏感数据的责任和义务仍然由数据所有者承担
- 企业必须确保云计算提供商对数据提供充分的保护
  - 数据在哪里存储
  - 满足企业的安全需求及合法的隐私保护
  - 将自己的数据与其它公司的数据隔离开
  - 外部审计和安全认证
- 服务等级协议（SLA）

7.4 保护信息资源的技术和工具

移动平台安全

- 企业应确保将移动设备的使用纳入其安全措施计划
  - 制定允许使用的移动平台和应用软件的指导原则
- 移动设备管理工具
  - 移动设备授权
  - 库存记录
  - 升级控制
  - 锁死／擦除丢失设备
  - 加密
- 将公司数据与设备中的个人信息分隔开的软件

7.4 保护信息资源的技术和工具

软件质量保障

- 软件度量：一种以定量指标的形式对系统进行客观的评价
  - 事务数量
  - 在线响应时间
  - 每小时打印的工资支票数量
  - 每百行程序代码发现的错误数量
- 尽早、定期且全面的测试
- 走查法：针对具体测试目的，挑选出一组具有所需技能的人员，对系统开发说明书和设计文档进行演示审阅
- 调试：发现并消除错误源的过程

7.4 保护信息资源的技术和工具

软件质量保障

- 软件度量：一种以定量指标的形式对系统进行客观的评价
  - 事务数量
  - 在线响应时间
  - 每小时打印的工资支票数量
  - 每百行程序代码发现的错误数量
- 尽早、定期且全面的测试
- 走查法：针对具体测试目的，挑选出一组具有所需技能的人员，对系统开发说明书和设计文档进行演示审阅
- 调试：发现并消除错误源的过程

互动讨论—技术：你的智能手机安全吗

- 请阅读互动案例，并讨论如下问题：
  - 有人说智能手机就是手中的微型计算机，深入讨论这种看法在安全方面的意义。
  - 解决智能手机安全需要考虑管理、组织和技术方面的哪些问题?
  - 智能手机的安全弱点给企业带来了哪些问题?
  - 个人和企业应该采取什么措施以使得他们的智能手机更加安全?

The End