西安电子科技大学
XIDIAN UNIVERSITY

第10章 分布式应用程序安全

《计算机安全导论》

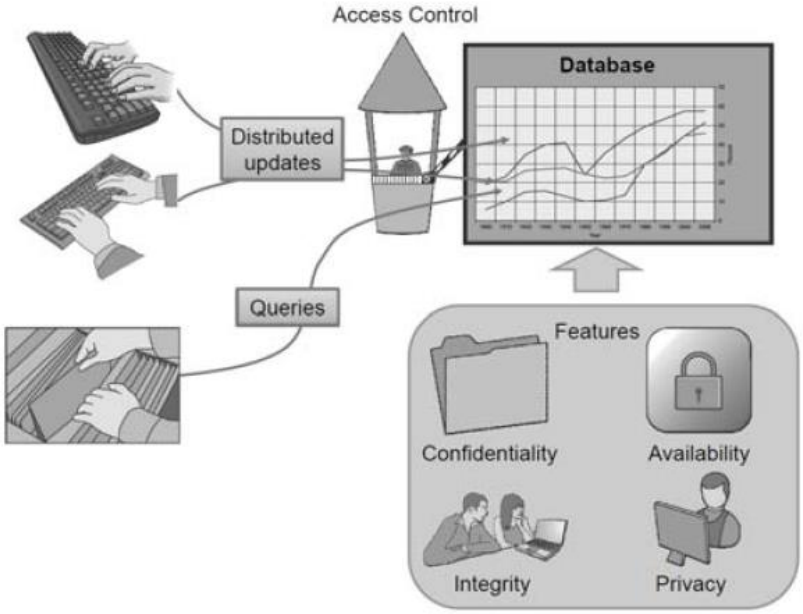
分布式应用程序的安全

- 10.1 数据库安全
- 10.2 垃圾邮件和网络犯罪
- 10.3 支付系统
- 10.4数字版权管理

数据库安全

数据库安全需求

- 需求：
  - 数据库是内部网络和Web应用程序的重要组成部分。因为在存储大量有价值的信息中，数据库扮演着重要的角色，所以恶意方为了访问这些数据，会将数据库作为攻击目标。因此，我们需要有效的方法来保护数据库安全。



表和查询

- **表和查询：**
  - 一种存储信息的常用方法是使用关系数据库 (**relational database**)
  - 在关系数据库中，将信息组织成表 (table) 的集合
  - 表的每一行是一条记录，用于存储某个实体的相关信息
  - 表的每一列是与实体相关联的属性 (**attribute**)

Num	Name	Inaugural_Age	Age_at_Death
1	George Washington	57.2	67.8
2	John Adams	61.3	90.7
3	Thomas Jefferson	57.9	83.2
4	James Madison	58.0	85.3
5	James Monroe	58.8	73.2
6	John Quincy Adams	57.6	80.6
7	Andrew Jackson	62.0	78.2
⋮	⋮	⋮	⋮
26	Theodore Roosevelt	42.9	60.2
27	William Howard Taft	51.5	72.5
28	Woodrow Wilson	56.2	67.1
29	Warren G. Harding	55.3	57.7
30	Calvin Coolidge	51.1	60.5
31	Herbert Hoover	54.6	90.2
32	Franklin D. Roosevelt	51.1	63.2
33	Harry S. Truman	60.9	88.6
34	Dwight D. Eisenhower	62.3	78.5
35	John F. Kennedy	43.6	46.5
36	Lyndon B. Johnson	55.2	64.4
37	Richard Nixon	56.0	81.3
38	Gerald Ford	61.0	93.5
39	Jimmy Carter	52.3	
40	Ronald Reagan	70.0	93.3
41	George H.W. Bush	64.6	
42	Bill Clinton	46.4	
43	George W. Bush	54.5	
44	Barack Obama	47.5	

关系数据库表Presidents存储着美国总统的数据。这个表有44条记录和4个属性。

表和查询

- **SQL查询：** 大部分数据库都使用结构化查询语言**SQL (Structured Query Language)** 来支持查询和更新，使用的命令如下：
  - SELECT：用来表示查询
  - INSERT：用来插入新纪录
  - UPDATE：用来更新已有的数据
  - DELETE：用来删除已有的记录
  - 条件语句使用WHERE，使用如 AND 和 OR 的基本布尔操作来确定满足一定条件的记录
  - UNION：将多条查询结果合并成一个单一的结果
- 可以使用这些命令的组合来执行查询，用于提取数据或更新对数据库的修改。

- **SQL查询示例 1：**
  - 对表 Presidents 执行如下的查询：SELECT * FROM Presidents WHERE Inaugural_Age < 50
  - 这个查询要找到并返回所有宣誓就职年龄小于50岁的美国总统。星号（*）指定返回符合条件记录的所有属性。查询返回结果如下表所示：

Num	Name	Inaugural_Age	Age_at_Death
11	James K. Polk	49.3	53.6
14	Franklin Pierce	48.3	64.9
18	Ulysses S. Grant	46.9	63.2
20	James A. Garfield	49.3	49.8
22	Grover Cleveland	48.0	71.3
26	Theodore Roosevelt	42.9	60.2
35	John F. Kennedy	43.6	46.5
42	Bill Clinton	46.4	
44	Barack Obama	47.5	

- **SQL查询示例 2：**
  - 还可以进行更复杂的查询，如，查询宣誓就职年龄小于50岁，上任时，又在第一任期中死亡的所有美国总统：

```
SELECT * FROM Presidents WHERE (Inaugural_Age < 50)
        AND (Age_at_Death-Inaugural_Age <4.0)
```

  - 这个查询会返回如下的记录集：

Num	Name	Inaugural_Age	Age_at_Death
20	James A. Garfield	49.3	49.8
35	John F. Kennedy	43.6	46.5

更新和两阶段提交协议

- **数据库删除：**
  - 除了使用查询从数据库中提取信息之外，授权用户也可以使用SQL命令更新数据库的内容。
  - 例如，下面的更新操作将从Presidents表中删除宣誓就职年龄小于50岁的所有美国总统的记录：

    DELETE FROM Presidents WHERE Inaugural_Age <50。

更新和两阶段提交协议

- **数据库插入：**
  - 下面的更新操作会向President表中增加一条新纪录：

    INSERT INTO Presidents

    VALUES (45, ‘Arnold Schwarzenegger’, 65.5, null)

  - 数据库可以更细粒度地执行更新，不仅仅是插入和删除整条记录，还可以修改特定记录中的某个属性值。

更新和两阶段提交协议

为了解决一致性和可靠性问题，大多数数据库在执行更新时使用**两阶段提交协议 (two-phase commit)**。操作分两个阶段顺序进行：

(1) 第一阶段是请求阶段 (request phase)，在该阶段，要确定更新所要修改的数据库的所有部分，并将这些部分标记为需要修改。这一阶段的结果要么是成功的，要么被中止。在成功时，每个修改请求都是可用的，标记被修改；在中止时，由于别人早已对其进行了标记，或者由于网络或系统出现了故障，所以不能标记所有需要修改的部分。

- 如果第一阶段被中止，则重置所有修改的请求，这样做是完全可行的，因为并未进行任何永久性的修改。
- 如果第一阶段成功完成，则协议继续第二个阶段。

更新和两阶段提交协议

- **(2) 第二阶段是提交阶段（Commit phase），**在这个阶段，对于其他修改而言，数据库是锁定的，只执行在请求阶段确定的修改序列。
  - 如果更新成功完成，则清除所有确定请求修改的标志，并释放对数据库的锁定。
  - 另一方面，如果更新操作失败，则回滚，使数据库回到完成第一阶段后的状态。
- **两阶段提交协议有助于数据库实现完整性和可用性。**

数据库访问控制

- **最小特权原则 (Least-privilege principle)：**实现适当的访问控制应遵循最小特权原则，使每个用户都拥有完成自己任务所必需的权限，但除此之外，不再拥有其他的权限。

- **特权分离原则 (Separation of privilege principle)：**实现适当的访问控制还应遵循特权分离原则，以便不同的用户具有不同的权限，这取决于他们需要执行的不同任务。

- 使用SQL的访问控制：
  - SQL定义了访问控制框架，一般用于定义数据库的权限。
  - 当创建表时，表的所有者拥有唯一的权限在表中执行操作。然后，所有者向其他用户授权，这种授权被称为**权限委托（privilege delegation）**。
  - 这些权限是非常广泛的，如对特定表进行任何操作，或更细粒度的对特定列执行SELECT查询。例如，表的所有者使用如下的SQL命令授予Alice查询表employees的权限：GRANT SELECT ON employees TO Alice。
  - 使用GRANT关键字能提供DELETE、INSERT和UPDATE等其它权限。此外，为了授予所有可用的权限时，可以使用ALL关键字。

- **权限委托(Privilege delegation)：**
  - 除了能向其他用户授予具体的权限外，表的所有者还允许其他用户来授予这些表的权限，这称为**策略授权委托 (policy authority delegation)**。
  - 具体来说，当如上述示例一样，向某用户进行授权时，授权者可以使用 WITH GRANT OPTION 子句，接收权限者能进一步委托该权限。
  - 例如，管理员为Alice创建了视图，授权Alice向其他用户委托SELECT的权限，SQL语句如下：

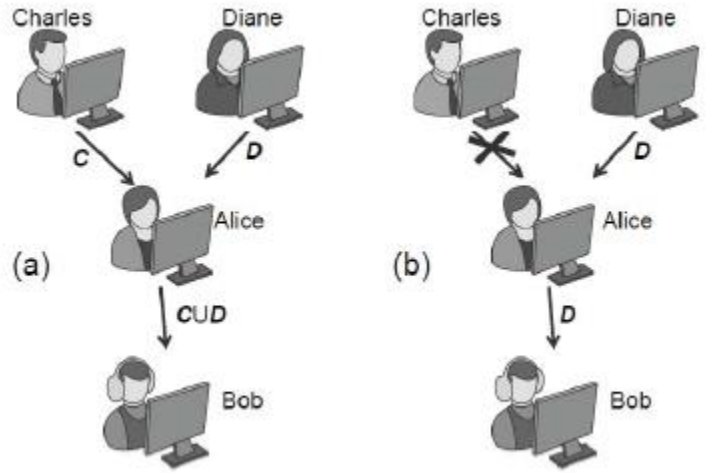
```
CREATE VIEW employees_alice AS
SELECT * FROM employees WHERE name = 'Alice';
GRANT SELECT ON employees_alice TO Alice WITH GRANT OPTION.
```

- **权限撤销(Privilege revocation)：**
  - 在数据库中，权限传播在有向图中是可视的，其中节点代表用户，有向边代表授予的权限
  - 如果Alice向Bob授予权利集A，那么画一条从Alice到Bob的有向边，标记为A
  - 用户Alice授予Bob权限后，可以有选择地撤销、删除或者重新标记从Alice到Bob的有向边，这些操作都是可视的。执行撤销的命令如下：

    REVOKE SELECE ON employees FROM Bob;

  - 这个命令会撤销授予Alice的所有SELECE权限，也会撤销Alice委派给所有人的SELECT权限。

- 权限撤销例子：



（a）首先，两个管理员Charles and Diane，分别授权Alice权限集C和D，之后，Alice将这些权限授予Bob，Bob的权限集是 C U D。

（b）如果Charles随后撤销了授予Alice的权限集C，则Bob通过Alice间接从Charles继承的权限集C也会被撤销，Bob只剩下了权限集D。

敏感数据

- **敏感数据：**
  - 除了要确保数据库相应的访问控制措施到位之外，还必须小心，存储敏感数据时，要保护用户的隐私，满足敏感数据的机密性需求。

敏感数据

- 使用加密：
  - 如果存储在数据库中的信息有机密性的需求，则不能将这些信息存储为明文，而应该存储为密文（即加密函数的输出）。
  - 在数据库中，应以加密形式保存机密文件，授权用户应该知道解密密钥，但不能将解密密钥存储于数据库中。

敏感数据

- **隐私保护：**
  - 除了采取措施来保护用户敏感信息的机密性之外，数据库所有者还应充分考虑公开隐私或授权访问敏感信息所产生的影响。
  - 如果数据库是公开的，比如说是出于研究的目的，则应删除姓名、地址、社会安全码、员工人数和学生人数等身份信息，或改用**掩码值(masking value)**，从而不提供任何身份信息。

- 推理攻击：
  - 即使删除或屏蔽掉身份信息，攻击者仍能将其他的信息与数据库结合，得到底层的数据。这种攻击被称为**推理攻击 (inference attack)**。举个例子，分析一个员工记录的数据库，它的属性有姓名、性别、ID和工资。
    - 假设，一方能访问表的脱敏版本，其中该版本的表中删除了姓名属性，用途是按性别建立工资的统计。另一方为了作报表，所拥有的表有一对属性：ID号和名字，且两者一一对应。
    - 如果两方进行过合作，则他们能很容易地推断出每个员工的工资，尽管这并非出于数据库所有者的本意。一般来说，当授予访问数据库的修改版时，管理员应该考虑在被授权者之间是否能共谋，来访问未经授权的信息。

敏感数据

- **保护数据库免受推理攻击：**为了保护数据库免受推理攻击，在公开数据库之前，可以使用如下的技术：
  - 单元抑制 (cell suppression)：在使用这种技术时，会删除数据库中的一些单元，在公开版本中只留下空白。
  - 推广 (generalization)：在使用这种技术时，公开数据库中的一些值被更常用的值所替代。
  - 加噪 (noise addition)：在使用这种技术时，在公开数据库中添加了随机值，使具有相同属性的所有记录的平均噪声为零。

- 示例：

Num	Age1	Age2
11	49.3	53.6
18	46.9	63.2
20	49.3	49.8
35	43.6	46.5
42	46.4	
44	47.5	

(a)

Num	Age1	Age2
11	49.3	
18	46.9	63.2
20	49.3	
35		
42	46.4	
44	47.5	

(b)

Num	Age1	Age2
11	45–50	50–60
18	45–50	60–75
20	45–50	45–50
35	40–45	45–50
42	45–50	
44	45–50	

(c)

Num	Age1	Age2
11	47.7	55.2
18	49.2	64.3
20	51.6	52.8
35	42.3	47.3
42	47.1	
44	48.0	

(d)

图10.4：在公开数据库中保护个人隐私的混淆技术：（a）删除个人姓名的表；（b）使用单元抑制的匿名表；（c）使用推广的匿名表；（d）使用噪声的匿名表

垃圾邮件和网络犯罪

简单邮件传输协议(SMTP)

- 简单邮件传输协议
  - 客户端通过端口25启动会话，建立TCP连接
  - 客户端向服务器发送命令
  - 服务器确认或通知错误
- 安全问题
  - 发件人未经过身份验证
  - 消息和消息头使用明文传输
  - 消息和消息头完整性没有得到保护

- SMTP会话示例

HELO mail.university.edu

MAIL FROM: president@whitehouse.gov

RCPT TO: chancellor@university.edu

DATA

From: president@whitehouse.gov

To: chancellor@university.edu

Date: April 1, 2010

Subject: Executive order

You are hereby ordered to increase the stipend of all TAs by $10,000 per year.

Sincerely,

The President of the United States.

什么是垃圾邮件？

- 垃圾邮件正式名称为 不请自来的批量电子邮件 (unsolicited bulk email)
  - 被所有主要的互联网服务提供商 (ISP) 禁止
  - 被美国直销协会 (DMA) 认为是“可接受的商业惯例”
- 不请自来的电子邮件、批量电子邮件可单独被个人、企业和组织接受
- 在将电子邮件归类为垃圾邮件时，其内容是无关紧要的，主要取决于它是否是不请自来的 、批量的
- 美国反垃圾邮件法案 (CAN-SPAM, 2004年) 要求商业垃圾邮件应满足以下要求
  - 显示退订选择权
  - 发件人标识明确，邮件主题不具有欺骗性
  - 成人标识额外规定

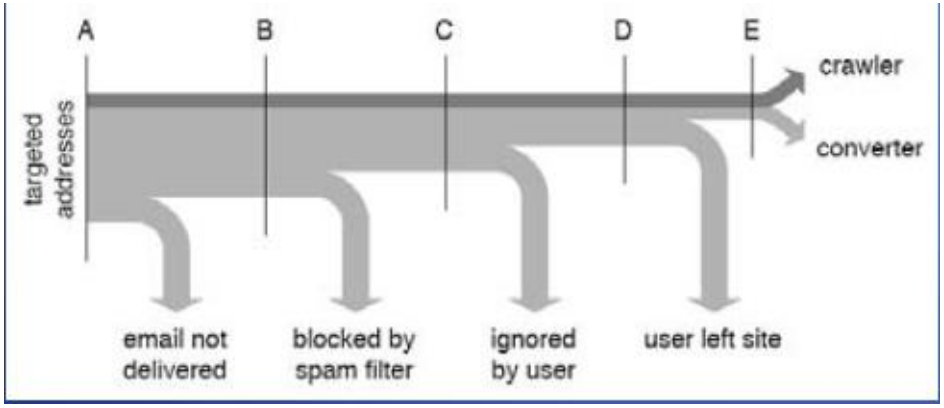
垃圾邮件的经济学

- 垃圾邮件是有利可图的，例如只需要点击垃圾邮件中的广告，就会给垃圾邮件发送者带来收益。
- 转换率是指垃圾邮件收件人执行了使邮件发送者获得收益的操作的比率。
- 尽管垃圾邮件转换率极低，但收件人的绝对数量还能使垃圾邮件发送者收回成本。

总有人会响应垃圾邮件：
尼日利亚公主想送我钱！

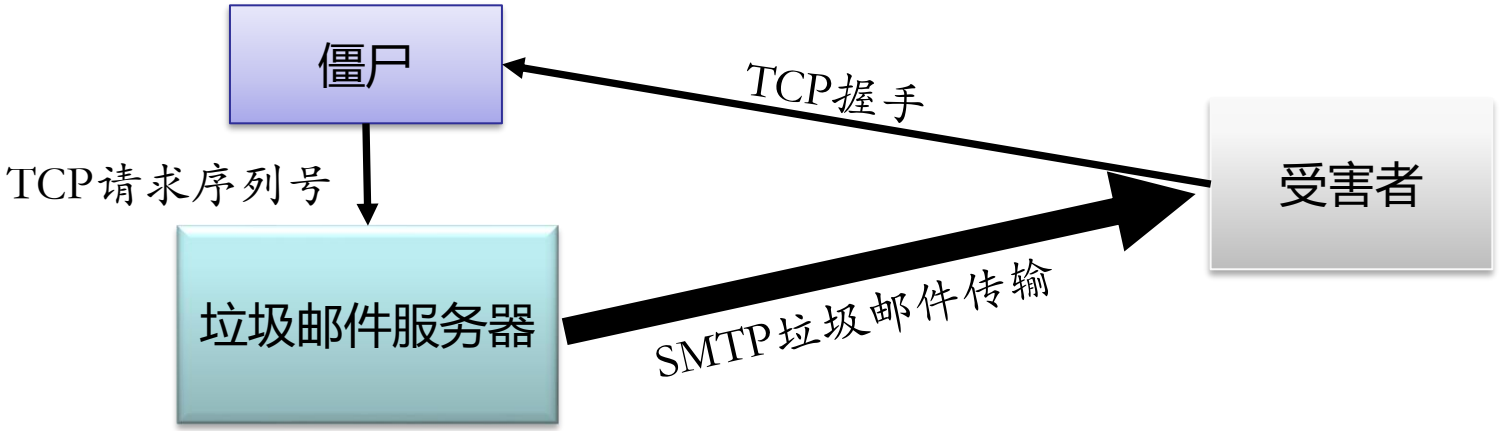
垃圾邮件的经济学

- 实例研究[Kanich + 2008]
  - 寄生僵尸网络发起“加拿大毒品”垃圾邮件
  - 通过僵尸网络进行的渗透试验结果表明发送3.5亿个信息中有28次响应(转换率是0.000008%)。



黑名单

- Spamhaus黑名单（SBL）
  - 已知的垃圾邮件源IP的即时数据库
  - 在传输之前消除大约10%的垃圾邮件
  - 规范的黑名单加入和除名流程
  - 超过6亿的电子邮件用户受SBL保护
- 如何规避黑名单
  - 强大的黑名单垃圾邮件服务器伪装成小型的未列出的僵尸服务器
  - 从僵尸服务器发起的TCP握手
  - 使用欺骗性源IP和TCP序列号从垃圾邮件服务器发送批量电子邮件

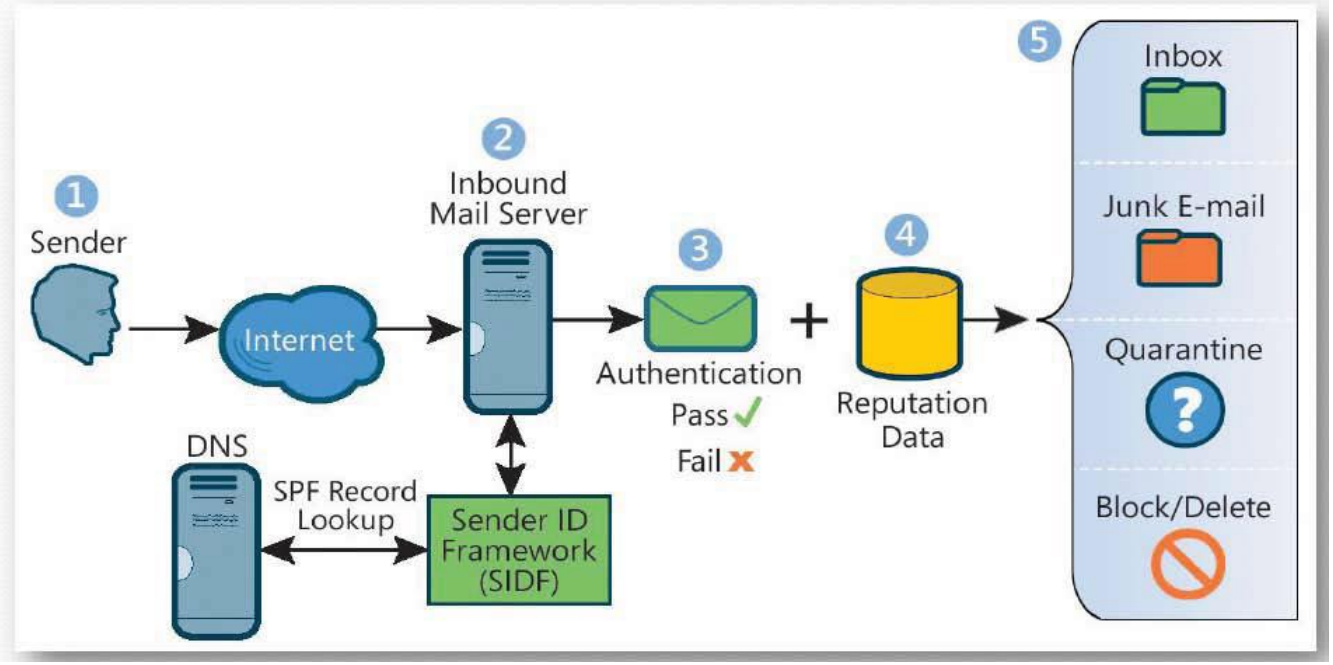


灰名单

- 另一种垃圾邮件过滤技术是灰名单，接收邮件服务器拒绝来自未知发件人的邮件。当接收来自未知发件人的邮件时，接收服务器会发送一个“临时拒绝”消息给发送方，并记录相应的信息。
- 垃圾邮件发送者通常会向数以百万计的收件人发送电子邮件，没有足够的资源来处理这些临时拒绝，并重传邮件。
- 维护一个可信发件服务器的数据库
- 简单易行且有效

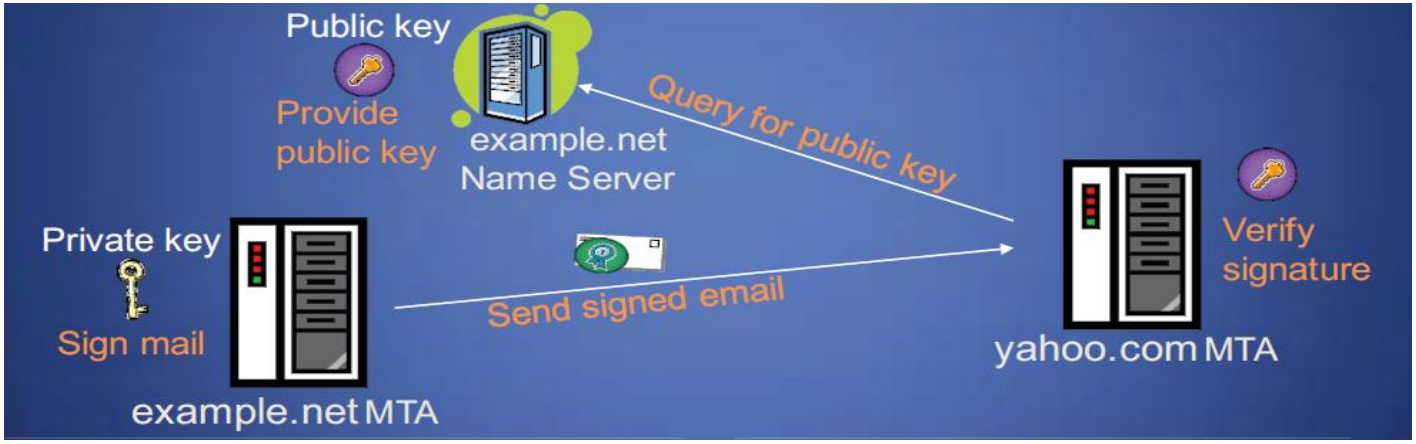
发件人ID和发件人策略框架

- 发件人策略框架(send policy framework, SPF) 可对发件人的发送邮件代理(mail transfer agent, MTA)进行身份验证，其中不使用加密技术。 接收方MTA会检查发送方MTA的IP是否在发件人域的授权IP地址列表中。
- 发件人ID框架(Sender ID framework，SIDF)与SPF类似，它也验证头中指定字段中发件人的域。



发件人的MTA身份验证：DKIM

- 域密钥标识邮件 (DomainKeys Identified Mail, DKIM) 是一种用于验证发送邮件传输代理的方法
- 在DKIM中，签名实体（通常是发件人的MTA（邮件传送代理，Mail Transfer Agent））向消息中增加签名，表明消息的签名实体所在的域
- 公钥存储在DNS的文本记录中
- 通常与其他垃圾邮件过滤方法配合使用



域关键字签名: a=rsa-sha1;
s=mail;d=example.net;
c=simple; q=dns;b=Fg…5J

验证结果: example.net
from=bob@example.net;
domainkeys=pass;

SPF vs. DKIM

发件人策略框架 (SPF)

- 用于发送MTA身份验证
- 基于通道
- 实施简单
- 不能保护消息正文的完整性
- 不支持邮件的转发
- 易受DNS缓存中毒攻击
- 易受IP源地址伪造攻击

域密钥标识邮件 (DKIM)

- 用于发送MTA身份验证
- 基于对象
- 加密保证
- 保护消息完整性
- 支持邮件转发
- 易受DNS缓存中毒攻击

网络犯罪

- 网络犯罪定义
  - 赛门铁克（Symantec）公司的定义：

网络犯罪是使用计算机、网络或硬件设备犯下的任何罪行。 计算机或设备可以是犯罪的代理人，犯罪的促进者或犯罪的目标。 犯罪可以单独在计算机上进行，也可以在其他地方进行。

- 网络犯罪的推动因素
  - 软件漏洞
  - 在线购物和在线访问金融账户
  - 执法不严或执法腐败的国家

信用卡

- 信用卡信息
  - 支持保密功能
  - 可与多个商家共享
  - 经常被不安全地传送
  - 信用卡号码的熵值较低（前四位数字表示金融机构）
- 优点
  - 对于用户，银行和商家都简单易行
- 缺点
  - 易发生欺诈
- 折中考虑
  - 没有便利的安全措施
  - 对客户和商家是无害的
  - 通过交易费用来弥补银行被欺诈带来的损失

常见的信用卡欺诈

- 购买热门商品并转售
  - 需要快递配送地址
  - 需要转售业务
  - 通常货物在国外转运
- 购买金融产品
  - 旅行支票
  - 礼品卡
  - 电子黄金
  - 为了避免撤销所需的额外转换
- 购买现金等价物
  - 西联汇款
  - 外币

防范信用卡诈骗

- 一次性信用卡号码
  - 可从多家发卡行获得(例如，AmEx, Citibank)
  - 不适用于可预约的交易
  - 用户花费的时间长
  - 申请退款流程繁琐
  - 适用于高价值交易或不受信任的商家
- 监控交易
  - 每笔交易进行时均通过电子邮件或短信告知持卡人
  - 与持卡人保持联系以捕捉潜在的危害事件
- 交易时启动密码输入
  - 与ATM卡的PIN码类似
  - 很难做到在仅与银行共享密码的情况下将验证结果发送给商家

银行账户

- 帐户信息
  - 应该被保密
  - 与商家，客户和朋友共享
  - 存款和取款的帐号相同
- 典型的银行交易
  - 支票
  - ATM
  - 电子汇款

- 美国的银行业务
  - 帐户名称
  - 纳税人识别号（TIN）
  - 支票可由客户或第三方生成
  - 对于金额低于$30K的交易，未验证其签名
  - 由美联储监管的自动清算所系统(ACH)支持跨行转账和存取款
  - 当账户A和B的TIN相同时，ACH允许从账户A发起从账户B到账户A的入境转账

常见的银行欺诈

- **伪造支票：**
  - 用磁性油墨打印机伪造支票
  - 虚假身份证
  - 低金额交易时通常不经过审查
- **电子汇款：**
  - 发送传真给银行要求电子汇款
  - 最有效的方法是汇钱到国外
- **创建恶意账户：**
  - 创建账户A冒充账户B的所有者
  - 发起从B到A的ACH交易
  - 通过ATM或者电汇提现

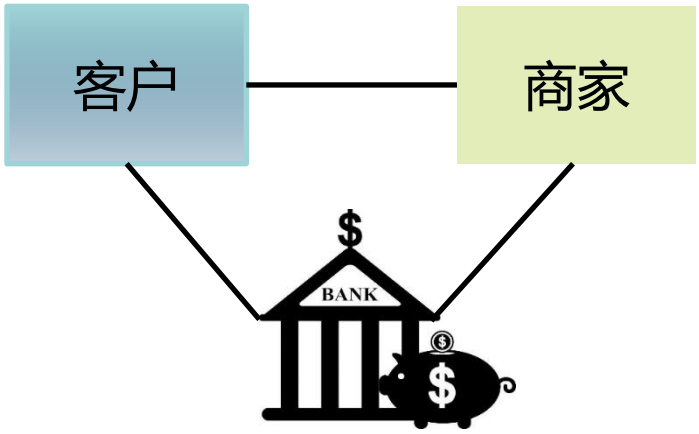
防范银行欺诈

- **多重身份认证：**
  - 通过硬件令牌生成 一次一密 密码
  - 定制私人镜像或链接防范钓鱼网站
  - 通过电子邮件/短信发送到注册地址以获取借记交易的密码
- **账户所有权验证：**
  - 将账户与ACH转账相关联需要提供该账户的交易明细
- **账户限制：**
  - 例如，只接受信用卡交易
- **监控银行交易：**
  - 每笔交易后的通过电子邮件/短信通知
- **取消网银：**
  - 限制通过网银的欺诈行为

支付系统

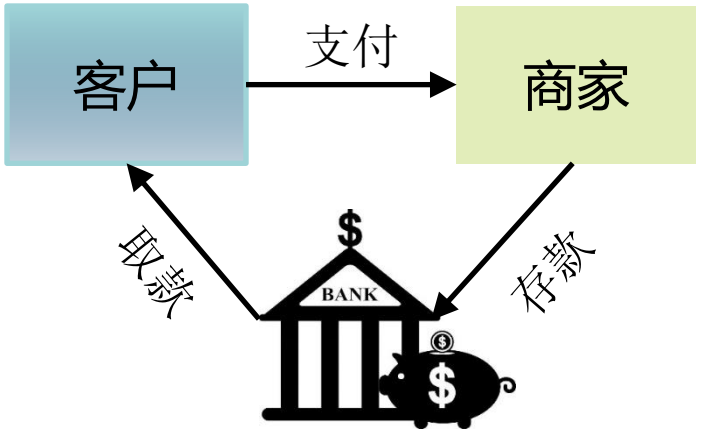
电子支付方案

- 电子支付方案是一种多方协议(multi-party protocols)
- 支付工具由电子货币(electronic coin)充当，它具有固定价值，可与传统货币交换
- 参与方包括：
  - 支付方 (客户)
  - 收款方 (商家)
  - 银行



电子支付方案 – 交易

- 电子支付方案中的交易通常包括：
  - 客户从银行取款
  - 客户支付电子货币给商家
  - 商家在银行存入电子货币
- 线上方案：
  - 银行参与支付交易
- 离线方案：
  - 银行不参与支付交易

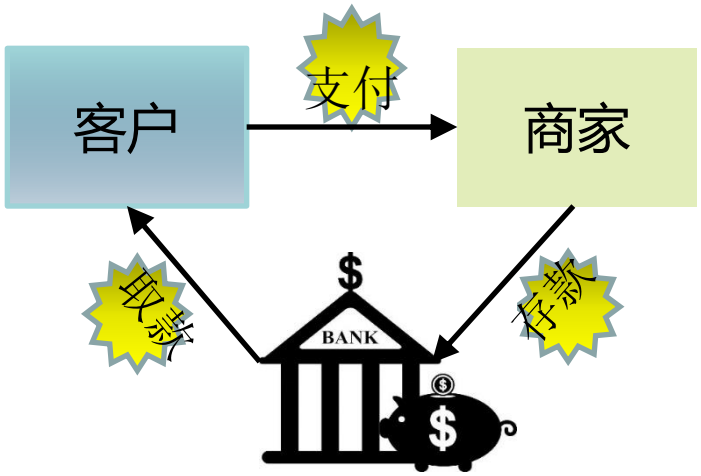


电子支付方案 – 目标

- **完整性：**
  - 电子货币不能被伪造或复制
  - 合法交易能够兑现
- **问责制：**
  - 交易进行后不能否认交易
  - 有效地解决交易纠纷
- **隐私：**
  - 有些参与方的身份不能揭示给其他参与方
  - 电子货币不能追踪到付款人或收款人，与使用实际现金一样

包含数字签名的支付

- 电子货币是一个随机标识符，并且银行在用取款时会对其数字签名
- 商家会验证数字签字并存储货币
- 银行承认有效货币的存款
- 存在的安全和隐私问题:
  - 顾客可复制货币，进行双重支付
  - 银行会了解客户和商家的每一笔交易



私密支付方案

- 盲签名允许签名者在不知道消息本身的情况下对消息进行签名
- 基础的数字现金方案:
  - 银行对客户提取的货币进行盲签名
  - 商家验证签名并存入货币
  - 银行无法将货币与客户关联起来

RSA盲签名

- 使用RSA密码系统能实现简单高效的盲签名方案
- 考虑下列RSA签名方案:
  - 公共模数 N
  - 公共加密指数 e 和公共加密哈希函数 h
  - 解密指数 d
- 银行可以在不知情的情况下为任何交易项生成签名
- 银行必须保证是在正确金额的有效货币上签名

RSA盲签名协议

- 客户选取秘密的随机值 x 和 r
  - 货币标识符 x
  - 随机数 r 与 N 互质
- 客户将值提交给银行
  - $y = r^e h(x) \bmod N$
- 银行对 y 值进行签名
  - $\sigma(y) = y^d \bmod N$
- 客户能从$\sigma(y)$推导出 x 的签名 $\sigma(x)$
  - $\sigma(x) = \sigma(y) r^{-1} \bmod N$
- 证明
  - $\sigma(y) / r \bmod \mathrm{N} = r^{ed-1} h(x) \bmod N = h(x)d \bmod N = \sigma(x)$

对钱币进行盲签名

- 为了确保是对有效的货币而非其他的内容进行签名，银行要求生成 k 个钱币，并为每个钱币生成加密散列
- 银行随机选择 1 个钱币
- 银行要求客户向其揭示其余的 k-1个钱币
- 银行验证选定的 k-1 个钱币的散列
- 银行在剩余的钱币上创建盲签名
- 银行签名的钱币是有效的概率为 1- 1/k

防止双重支付

- **在线协议（联机系统中）：**
  - 在支付过程中，银行保持在线，实时撤销已使用的钱币
- **离线协议（离线系统中）：**
  - 每个提款的钱币都包含客户身份的加密信息
  - 每个存款的钱币都包含商家身份的加密信息
  - 双重支付将导致欺骗者的身份被披露出来

秘密分享

- 一个秘密字符串 x 可以被划分为以下的随机值 y 和 z：
  - 选择一个随机数 y
  - $z = y \oplus x$
- 字符串 x 可以通过 y 和 z 进行重构：
  - $x = y \oplus z$
  - 秘密份额 y 和 z 都是随机值并且都被称为 x 的秘密份额
  - 任一秘密份额都不会揭示关于秘密值 x 的任何信息

钱币（Coins）

- 令 h 表示密码学哈希函数
- 给定一个秘密值 x 和关于 x 的承诺 (commitment) 信息(a, b):
  - $a = h(y)$
  - $b = h(z)$
  - y 和 z 是x的秘密份额
- ID是标识客户的字符串 (如姓名、地址等)
- 银行向客户发行的钱币中包括:
  - 钱币标识符 x
  - 关于ID的 n 对承诺信息(a_1, b_2) , … , (a_n, b_n)
- 钱币本身没有揭示客户的身份信息

取款

- 客户生成并向银行提交 k 个钱币
- 银行随机选择 k-1 枚钱币
- 银行要求客户向其披露所选定的 k-1 个钱币的承诺的秘密份额
- 银行在剩余的硬币上创建一个盲签名
- 银行签名的钱币是有效的概率是 $1 - 1/k$

支付

- 客户向商家提交钱币 $\{x, [(a_1, b_2), \ldots, (a_n, b_n)]\}$
- 商家验证钱币上的签名
- 商家发送给客户一个随机的二进制向量 $s_1, \ldots, s_n$, 称为选择器。
- 客户向商家揭示由选择器所选定的秘密份额，即，客户向商家发送一组字符串 $P_1, \ldots, P_n$:

$$h(P_i) = a_i \ \textbf{if}\ s_i = 0$$

$$h(P_i) = b_i \ \textbf{if}\ s_i = 1$$

存款及安全性分析

- 存款
  - 商人将钱币和字符串 $P_1, \ldots, P_n$ 提交给银行进行存款
  - 银行验证签名并且记录钱币和相应字符串的对应关系
- 安全性分析
  - 两个商家提供的选择器相同的概率是 $1/2^n$
  - 因此，如果客户将1个钱币进行双重支付，那么银行发现该客户身份的概率为 $1-1/2^n$
  - 客户想要在不被银行发现的情况进行双重支付的唯一办法是找到一个Hash函数的碰撞。
- 该方案虽然不能阻止双重支付的发生，但是可以以较高的概率检测并追踪到双重支付者的身份信息。

参考文献

- The electronic cash scheme presented in this lecture is based on the work by David Chaum http://www.chaum.com/
- D. Chaum, A. Fiat, and M. Naor. Untraceable Electronic Cash, in Proc. CRYPTO 1988. http://citeseer.ist.psu.edu/421212.html
- S. Goldwasser and M. Bellare. Lecture Notes on Cryptography [Section 12.5] http://wwwcse.ucsd.edu/users/mihir/papers/gb.html

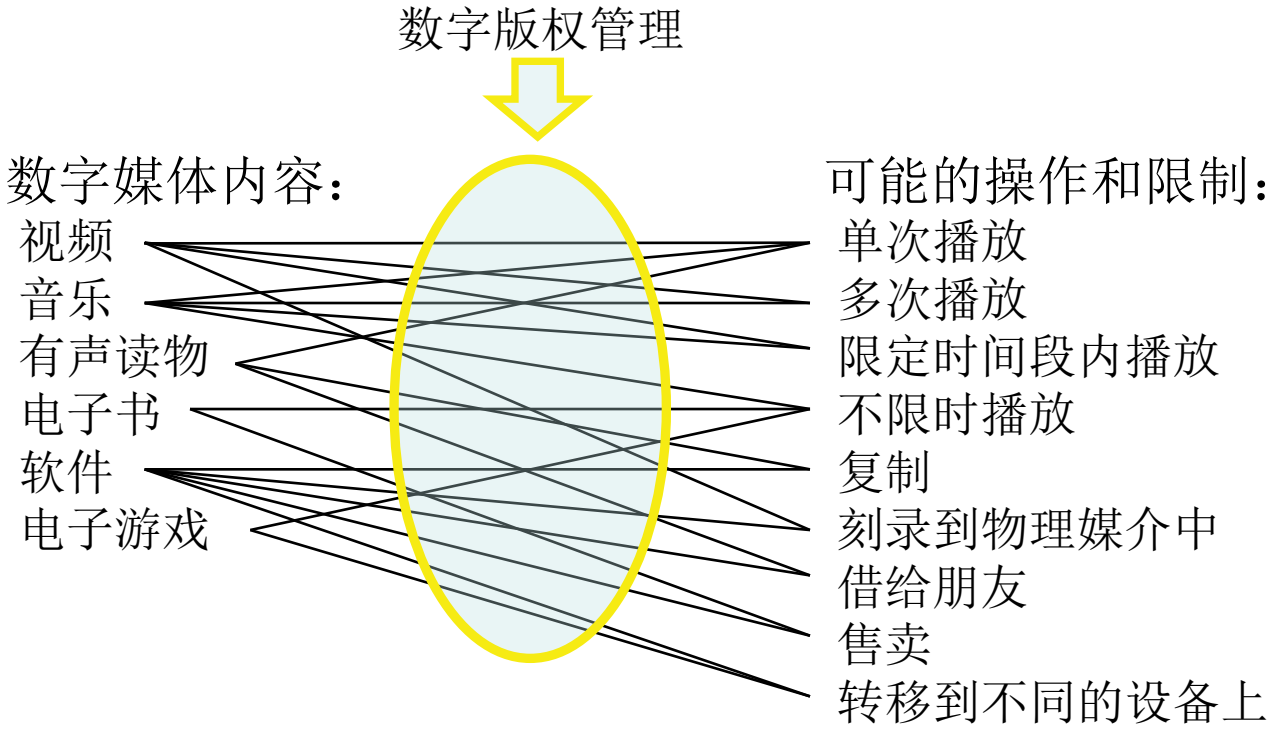
数字版权管理

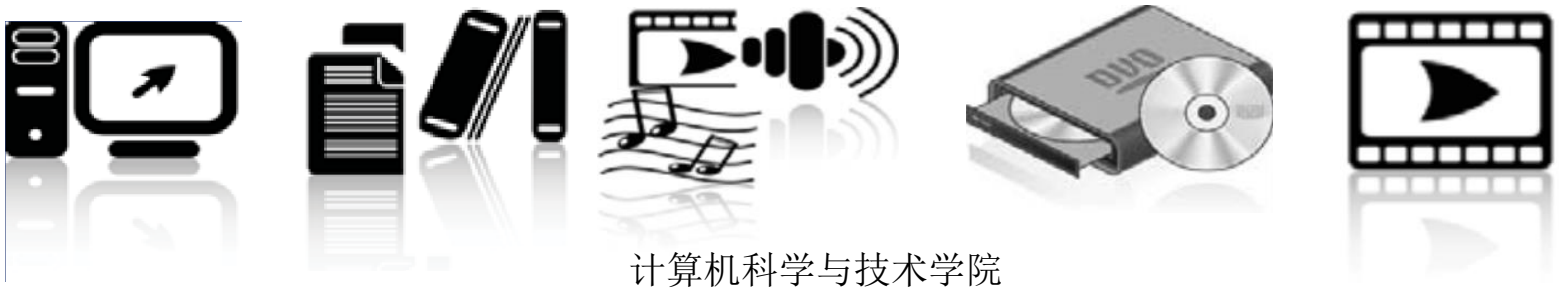
介绍

- 数字版权管理 (Digital Rights Management, DRM) 是指能限制用户使用数字内容的做法，常用于数字媒体，如DVD、下载的音乐和许可的软件
- DRM防止非法更改、分享、复制、打印以及无授权设备查看数字媒体
- 版权所有者需要DRM来防止因非法分发其受版权保护的作品而导致的收入损失

DRM内容和操作

- 数字版权管理涵盖了许多功能





早期的美国版权法

- 美国宪法第1条第8节
  - “国会拥有权力……为促进科学和实用技艺的进步，对作家和发明家的著作和发明，在一定期限内给予专利权的保障”
- 1790年版权法案
  - “在美国境内印刷的任何地图，图表，书籍的作者，作为公民……应享有印刷，转载，出版和出售此类地图，图表的专利权和自由”
  - 公民可以拥有书籍，图表或地图的专利时长为14年- 如果届时仍在世，可以续约14年
  - 非公民和其他国家的作品不受保护
  - 其他的法律应根据本法案做适当修订

1976年版权法

- 保障文学作品，音乐作品，戏剧作品，舞蹈作品，图形作品，电影和录音（1990年增加的建筑作品）的版权
- 版权所有者拥有复制或创作原创衍生作品、出售或出租复制品、公开表演、公开展示的独家权利
- 作者可以保留28年的版权，最多可再延长28年
- 法案第107节至第118节对版权所有者的权利进行限制 - 被称为合理使用原则

合理使用原则

- 复制特定作品用于某些目的被认为是合理使用
  - 批评，评论，新闻报道，教学和研究

- 在确定是否合理使用时会考虑四个因素[17 U.S.C. §106]
  1. 使用的目的和性质：是用于商业性质还是用于非营利性教育;
  2. 受版权保护作品的性质;
  3. 与受版权保护作品的数量和实质内容相关;
  4. 对受版权保护作品的使用产生的潜在市场或价值

索尼 vs. 环球影城

- 20世纪70年代，索尼发明了Betamax，一种类似于家用录像系统(VHS) 的磁带录制格式
- 可用于录制受版权保护的公共广播制品
- 与此同时，一些电影制片厂发明了激光录像磁盘(Discovision)，它可以在数次播放后自行销毁
- 1976年环球影城和迪士尼就造成的所有利润损失起诉索尼，并试图禁止其使用磁带录像机（VTR）
- 加利福尼亚中心区的地方法院驳回了索赔，理由是非商业性地使用录像机被视为合理使用
- 第九巡回上诉法院撤销了该裁决，并要求索尼承担协助侵犯版权的责任

索尼 vs. 环球影城（续）

- 1984年，最高法院必须就此问题做出决定 - 向公众出售VTR是否助长了公共广播制品的版权被侵犯?

- 最高法院最终裁定 “ 将VTR出售给公众并不构成对版权的侵犯 ”
  - 得出的结论是，大多数公共广播制品的版权所有者都不介意公众将他们的广播制品录制在 Betamax 磁带上
  - Betamax 被裁定遵循了合理使用原则

- 案件经常被之后的版权诉讼案件借鉴，包括Napster案

Dmitry Skylarov和Ed Felten

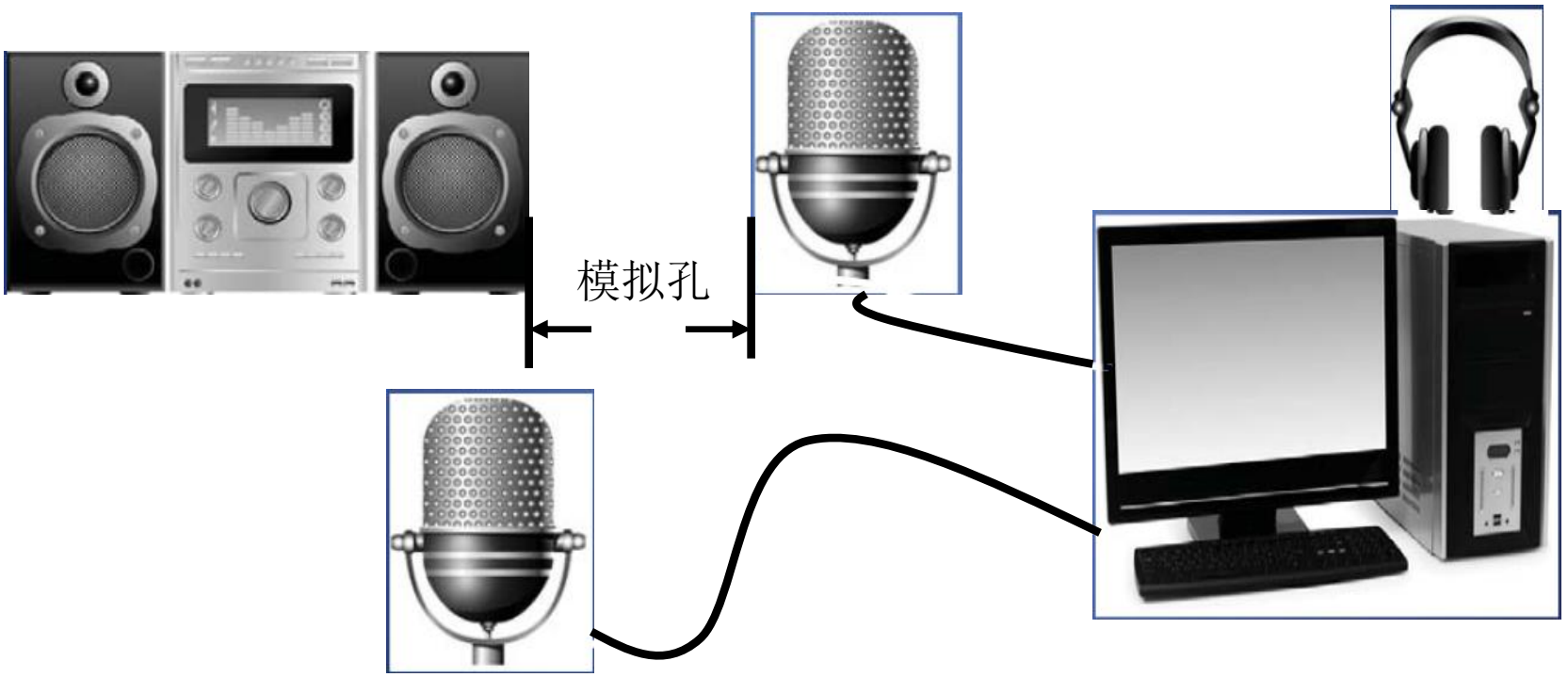
- Dmitry Skylarov
  - 为俄罗斯的Elcomsoft公司工作，创建了将Adobe安全电子书转换为无保护PDF的产品（在俄罗斯是合法的）
  - 在美国，Skylarov因违反DMCA而被捕入狱
  - 最终Elcomsoft公司被起诉，Skylarov被释放
- 普林斯顿大学 Edward Felten教授
  - 2000年，音乐著作权保护协会 (SDMI) 邀请研究人员尝试攻破他们的水印技术
  - Felten和他的团队成功移除了水印，并写出论文打算发表在会议上
  - SDMI和RIAA威胁要对Felten采取法律行动
  - Felten将论文从会议撤稿，但向外界公布了他所受到的威胁
  - 在电子前线基金会的帮助下，Felten起诉了RIAA和SDMI
  - SDMI和RIAA撤回了他们的威胁
  - Felten最终在另一个会议上发表了该论文

复制保护的方法

- **加密狗（Dongle）**
  - 可插拔式硬件设备，包含运行软件所需的密码
- **产品密钥**
  - 在安装软件时必须输入
  - 在线检查密钥的重复使用情况
  - 通过硬件和操作系统的指纹将许可证绑定到固定的设备上
- **手机激活**
  - 一对一的交互机制更具威慑性

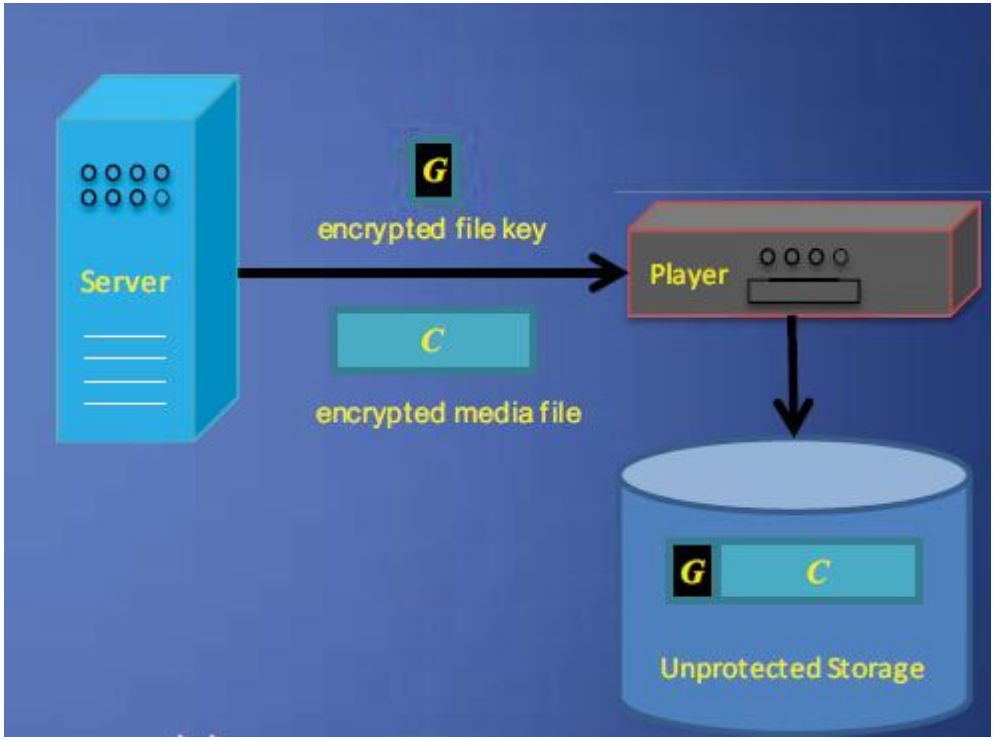
模拟漏洞

- 每个复制保护机制都存在“模拟漏洞”的风险，即在播放时记录其内容



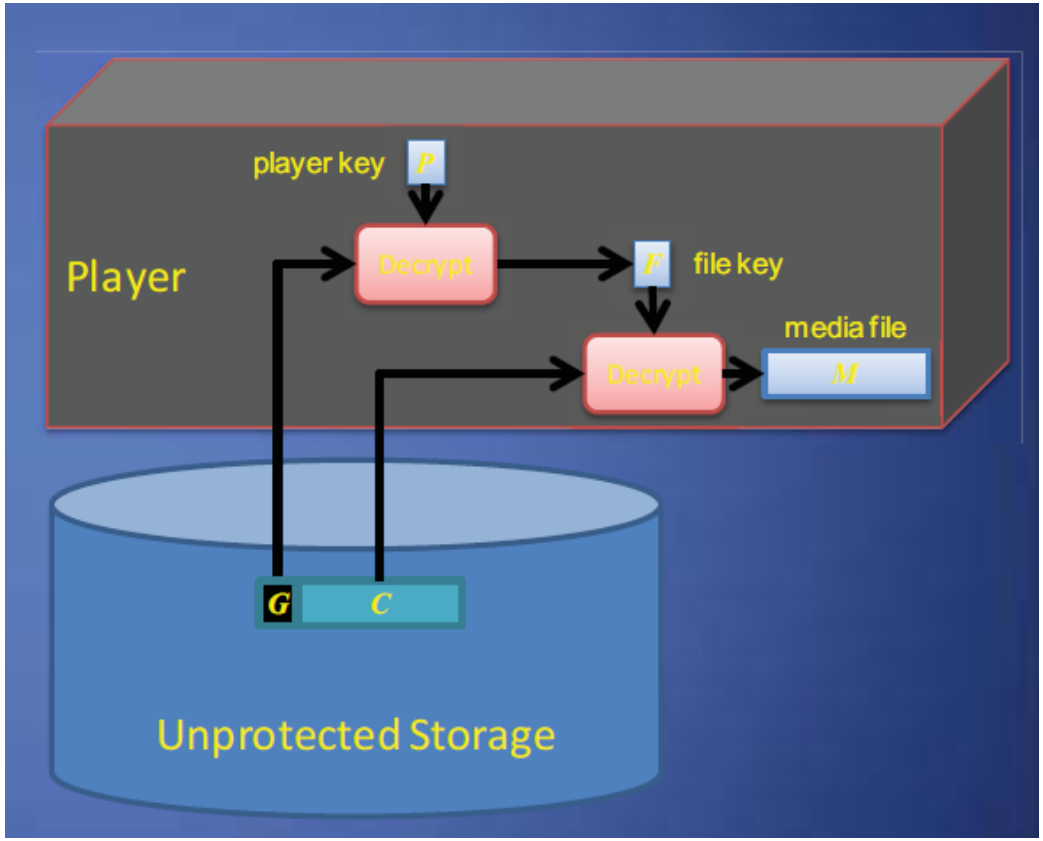
用于媒体文件的DRM方案

- **步骤1：**
  - 媒体服务器向播放器发送用文件密钥加密的媒体文件和用播放器密钥加密的文件密钥



DRM媒体文件示例

- **步骤 2：**
  - 播放器先用播放器密钥解密文件密钥，然后使用文件密钥解密媒体文件。

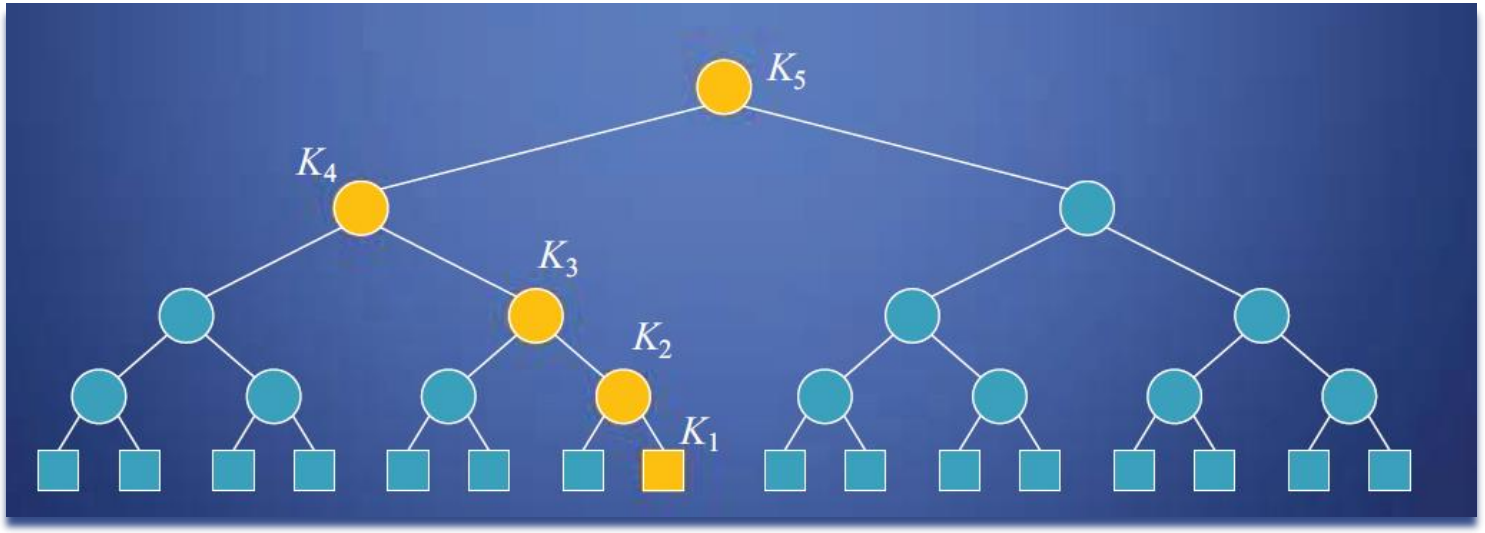


叛徒追踪

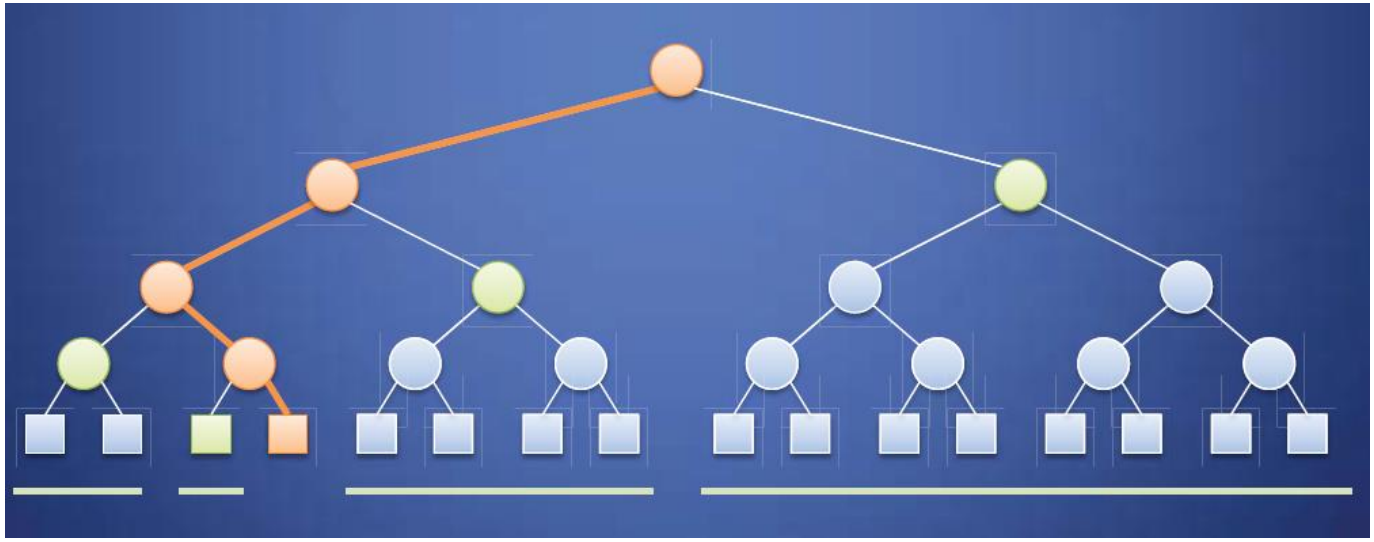
- 控制器将受保护的内容分发到多个设备
- 设备与控制器共享一个公共的对称密钥
- 每个内容项都使用共享密钥加密并广播到所有设备
- 某些设备（叛徒）被克隆或被用于非法复制和分发受保护的内容
- 问题：
  - 识别叛徒
  - 剔除叛徒

逻辑密钥树

- 逻辑密钥树
  - 是平衡二叉树，树的每个节点都与一个对称加密密钥相关联
  - 将设备与叶子节点关联，每个设备上存储着从叶子到根路径上的所有密钥
  - 用节点 v 的密钥加密的内容可以被 v 的子树中的所有设备解密

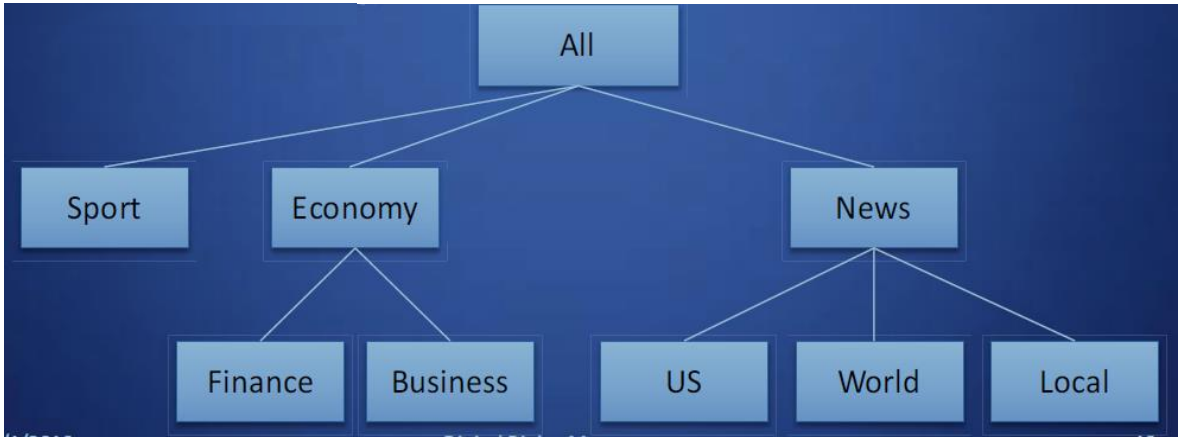


- 设备的撤销
  - 如果设备需要被撤销，则必须更改此设备已知的密钥，并分发新的密钥
  - 新密钥的分发可以通过广播对数级数量的加密消息来完成



加密的广播消息

- **加密广播**
  - 内容包含了各种层次结构的订阅包
  - 广播之前，每个内容项都用单一的对称密钥进行加密
  - 被授权查看该内容项的订阅者应该拥有解密该项的密钥
  - 每个节点的密钥可以被用来计算该节点的子孙节点的密钥
  - 密钥分配问题



CD/DVD 保护

- **CD/DVD 保护**
  - 大多数CD/DVD都是受保护的，因此它们不能被拷贝
  - CD是易损坏的，因此需要备份
  - 在大多数国家，可以合法备份你拥有的CD——但禁止出售
  - 大多数保护技术使用密钥来加密文件，并将密钥作为数字签名添加到光盘上
  - 几乎所有的加密技术都被破解了

CD/DVD 保护

- CD/DVD 保护
  - 从技术上讲，要完全阻止用户复制他们购买的媒体文件是不可能的
    - 按位复制软件
    - 使用麦克风记录音频
    - 用摄像机录制视频
    - 使用扫描仪复制文本
  - 给予足够的时间和资源，任何媒体文件都可被复制
  - 大多数公司意识到他们不能阻止专业人员的复制行为，但他们试图阻止普通用户的复制行为

商用加壳软件SafeDisc

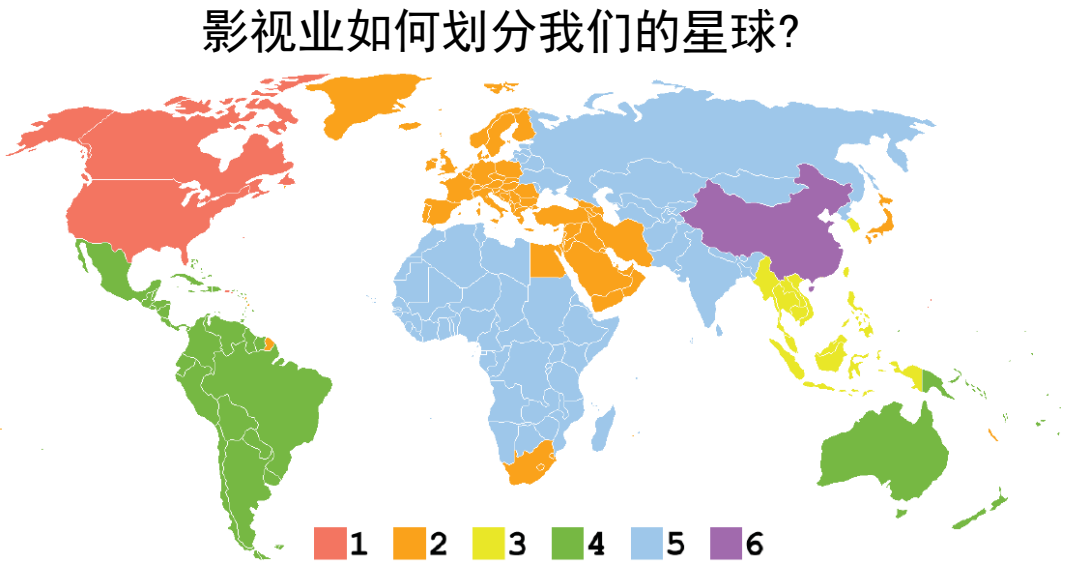
- **商用加壳软件 SafeDisc V1/V2**
  - 由MacroVision公司开发的复制保护软件
  - 自1999年起应用于游戏加密市场
  - 容易被破解
    - 可以通过1:1 光盘拷贝复制程序到其他光盘
    - 可用的安全破解补丁: Generic SafeDisc Patch, Daemon Tools
    - 可执行的解密器：unSafeDisc，DumPalyerx

DVD拷贝保护

- **DVD拷贝保护**
  - 传统的用于音频和视频刻录的媒介（如磁带，VHS磁带）使用不同的标准NTSC，PAL，SECAM …
  - 盗版并不是太大的问题，因为拷贝产品的质量会逐渐下降。
  - 随着数字录音和高分辨率视频的出现，DVD拷贝保护对电影业来说是一个大的挑战。
  - 事实上，DVD发明后大约过了2年，DVD电影才得以上架。部分原因正是考虑到需要制定了合理的DVD版权保护方案。

DVD区域码

- DVD区域码是由美国八大影业所共同制定的，为了保护各地区电影放映时的权益。将全世界分成六个区域，并且限定每个区域中流通的DVD光盘必须设定影片区域码。



数字版权管理架构

- **数字版权管理架构**
  - 由DVD复制保护技术工作组(CPTWG)、IBM、Intel、Matsushita、Toshiba提出。
  - 主要思路：Alice向Bob出售视频，为了防止Bob将视频转发给其他人，Alice希望Bob只能通过可信设备来访问视频资源。

- **可信设备**
  - 可信设备由可信制造商制造加工。
  - 如果制造商已经加入了Copy Control Association(CCA)，则它是受信任的。
  - 受信任的设备会被分配一个（保密的）播放器密钥。
  - 受信任的制造商必须与CCA签订协议，从根本上防止它制造出可能破坏复制保护机制的设备。
  - 自2000年以来，制造商必须生产符合RPC2（区域回放控制）的DVD 光碟机驱动设备。

内容扰乱系统

- 内容扰乱系统(Content Scrambling System, CSS)
  - 在大多数情况下，DVD（视频磁盘）受CSS方案的保护。直观上看，使用磁盘密钥 k 加密视频内容。
  - 在受CSS保护的DVD的导入区，磁盘的密钥 k 被加密了大约400次，每次都使用不同的播放器密钥。
  - 使用第 i 个播放密钥的DVD播放机将读取该导入区的第 i 个条目，然后使用播放密钥 k_i 解密这个条目，以获得磁盘密钥 k。

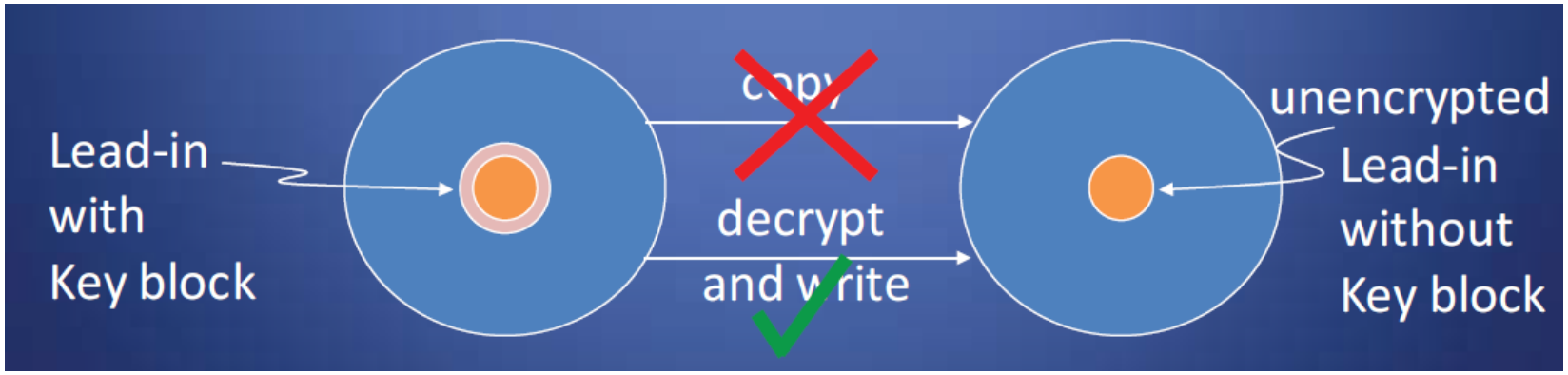
内容扰乱系统

- 内容扰乱系统(Content Scrambling System)

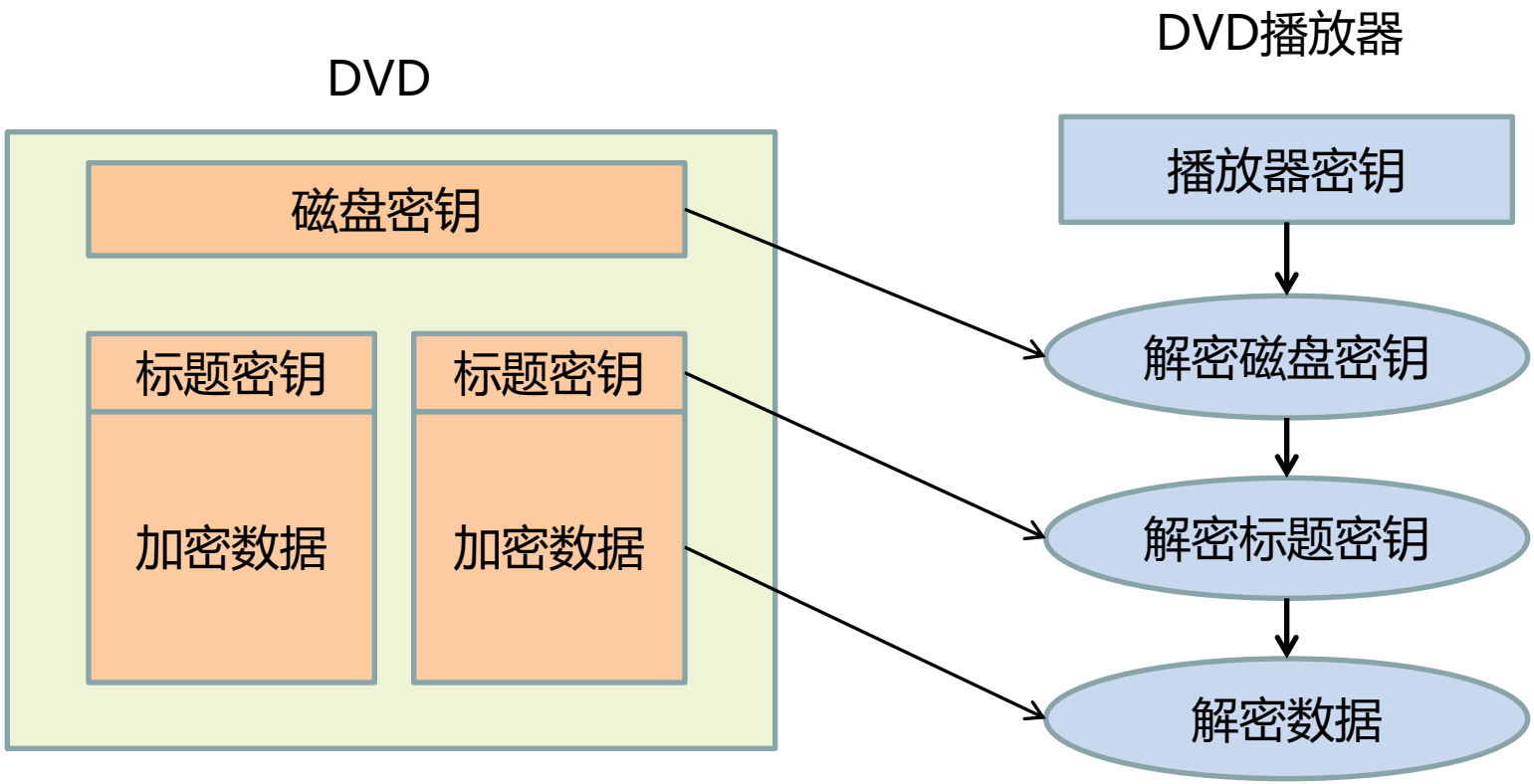
– 在播放影片时，视频内容将被实时解密。

– 使用普通DVD刻录机拷贝时将不会包含密钥块，磁盘将不能播放。

– 如果有人使用特殊工具解密了视频，那么就有可能使用导入的密钥块对盗版视频来进行解密或者绕过CSS。



- **DVD播放**


DVD播放器
DVD
播放器密钥
磁盘密钥
解密磁盘密钥
标题密钥
标题密钥
加密数据
加密数据
解密标题密钥
解密数据

内容扰乱系统密钥

- 内容扰乱系统密钥
  - 鉴权密钥
  - 用于双向认证
  - 会话密钥
  - 认证期间协商
  - 在将内容在不受保护的总线上传输之前用于加密标题和磁盘密钥
  - 监听防范
  - 播放器密钥
  - 由“DVD复制管理协会”授权给DVD播放器制造商
    - 存储在播放器内
    - 用于验证播放器
    - 用于解密磁盘密钥
  - 磁盘密钥
  - 用于解密标题密钥
  - 标题密钥
  - 该密钥与扇区密钥相异或，然后用于加密扇区内的数据
  - 扇区密钥
  - 每个扇区有128位明文头
  - 每个扇区头的80 – 84位包含一个用于在扇区内编码数据的附加密钥

解密内容扰乱系统(DeCSS)

- **解密内容扰乱系统(DeCSS)**
  - 1999年由Jon Johansen提出
  - 可以解密CSS并且允许复制文件到硬盘驱动器
  - 当时，关于CSS算法的知识还很少
  - DeCSS附带的源代码显示了破解CSS是容易的
  - 被作为一种技术用于创建可以运行在linux上的开源DVD播放器。
  - 首先是一长串DVD解密程序
  - Johansen被DVD-CCA起诉，但案件最终被撤销
    - 在DeCSS公布之前，大规模盗版行为就已经发生了
    - DVD刻录机无法写入CSS所写的区域
    - 大多数DVD拷贝都是使用特殊设备逐位复制的

高级访问内容系统

- 高级访问内容系统 (Advanced Access Content System， AACS)
  - DRM的新标准，允许有限共享和复制下一代DVD
    - 由Microsoft, Sony, Disney, IBM, Matsushita, and Warner Brothers等公司开发
    - 用于蓝光光碟
  - 方法
    - 基于广播加密技术
    - 可以撤销盗版者权限

作业

- R
- C