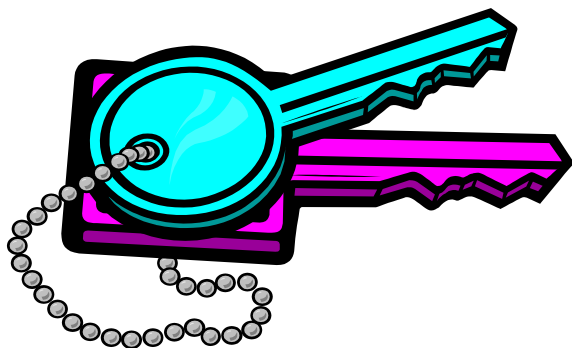


第三章 网络安全



网络空间安全概论



大纲

1

口令认证与入侵检测

2

挑战应答认证

3

隐私保护

4

防火墙

5

PKI



1 口令认证与网络入侵

- 基本思想

- 用户和系统共享相同的秘密口令（通行字 password）

- 问题

- 如何存储口令？
 - 系统如何检查口令？
 - 猜测口令的难度有多大？

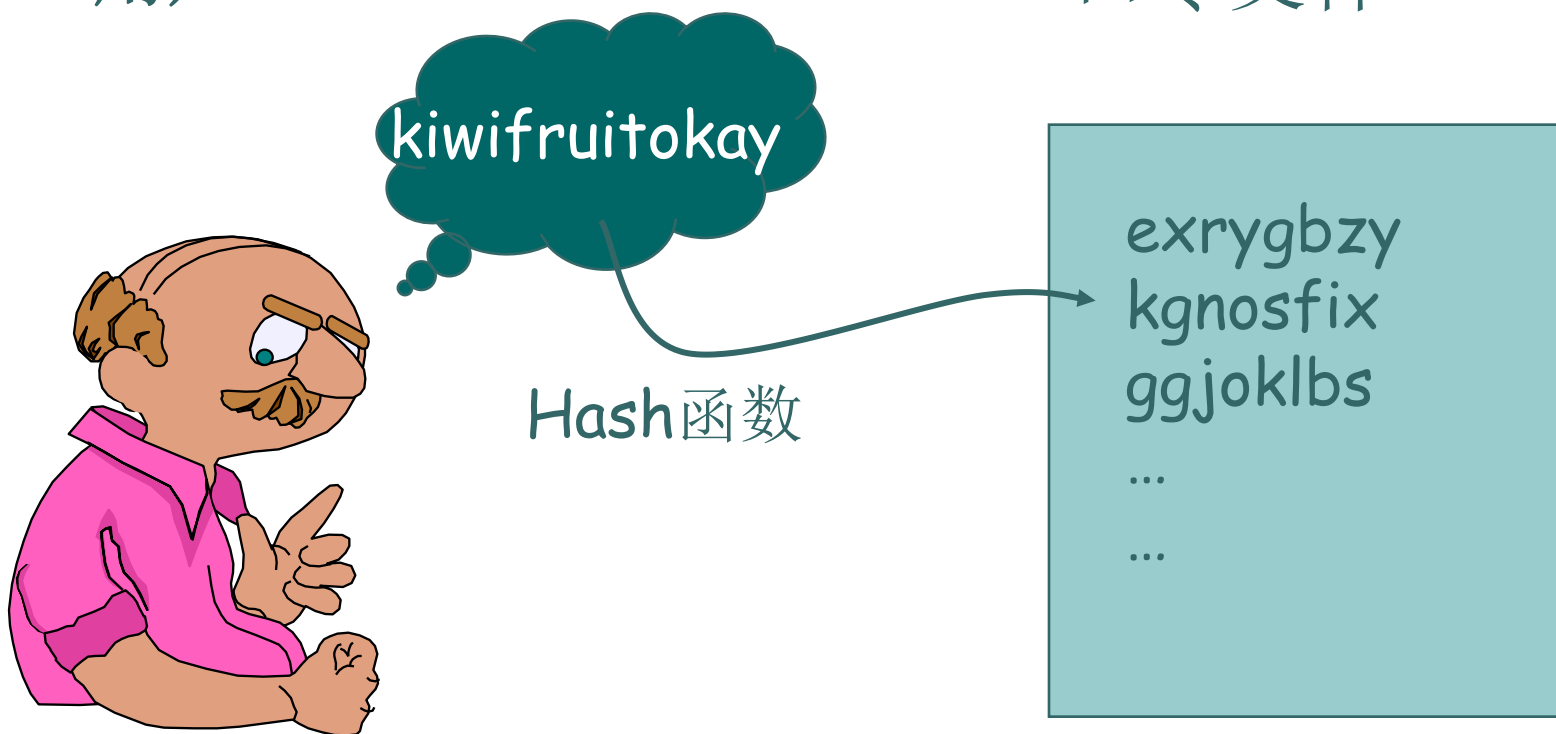
由于网络的开放性，保密口令文件很困难，最理想的情况是即使拥有口令文件也不能得到口令



口令存储机制

用户

口令文件



- Hash函数 h : 字符串 \rightarrow 字符串
 - 给定 $h(\text{口令})$, 难以反向得到口令
- 用户口令以哈希值存储 $h(\text{口令})$
- 当用户输入口令
 - 系统计算口令的哈希值
 - 与口令文件中存储的哈希值相比较
- 磁盘中不存储口令原文



猜测口令的方法

- 尝试系统提供的标准账户和默认口令
- 尝试**1~3**个字符的短口令
- 尝试电子词典里的所有单词(**60,000**个词汇量)
- 收集用户的个人信息，如：爱好，姓名，生日等
- 尝试用户的电话号码，身份证号码，住址等
- 尝试用户所有证件的号码
- 使用特洛伊木马逃避访问控制限制
- 窃听用户和主机间的通信线路

预防方法: 选择好的口令选择策略，至少**8**个字符，至少一个大写字母，一个小写字母，一个数字和一个标点符号(如: **Ij4Gf4Se%f#**)



字典攻击

- 典型的口令字典
 - 1,000,000个通用口令词条
 - 姓名, 宠物名, 常见词
 - 假设每秒猜测尝试10个词
 - 成功的字典攻击最多需要100,000秒 = 28个小时, 平均14个小时
- 如果口令字随机
 - 假设口令为6个字符
 - 大写/小写字母, 数字, 32个符号
 - 689,869,781,056 种组合的口令字(94^6)
 - 穷举攻击成功平均需要1093年



网络入侵的步骤

1. 扫描网络
 - 定位目标主机的**IP**地址
 - 使用何种操作系统
 - 哪些**TCP/UDP**端口是开放的 (可以被服务器监听)
2. 针对开放端口运行漏洞利用脚本
3. 获得访问**suid shell**程序的权限 (拥有**root**管理员权限)
4. 从黑客网站下载针对特定操作系统版本的文件，以拥有未来访问该机器的权限，并且不会被系统审计程序记录

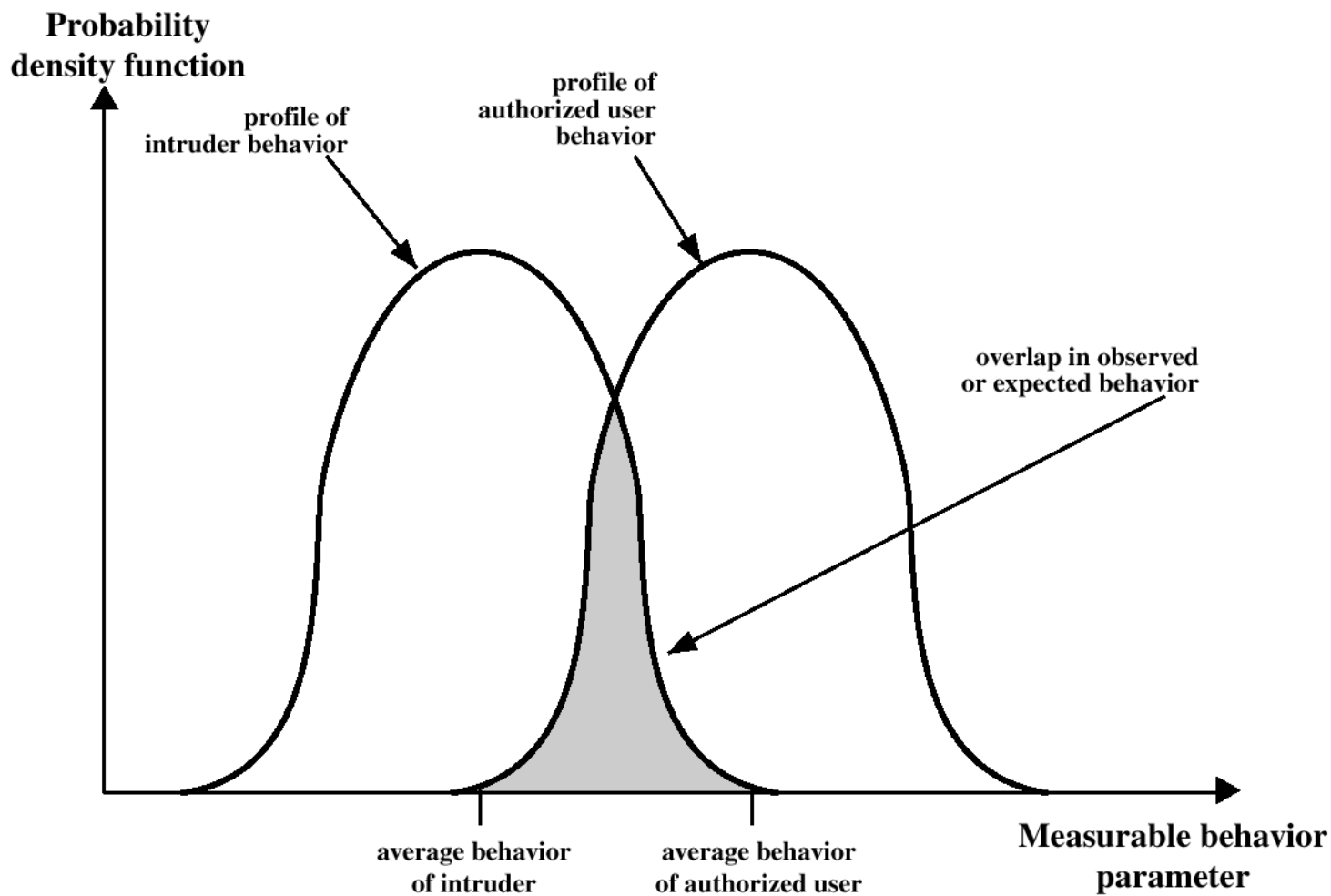


入侵检测

- 计算机系统的第二道防线
 - 入侵者能及时被系统识别和驱逐
 - 有效的入侵检测系统能防止入侵
 - 入侵检测系统能收集关于入侵技术的信息，用于加强入侵防护设施



入侵者和授权用户的行为轮廓



入侵者和授权用户的行为轮廓

- 放宽对入侵的定义将导致**误报**——
将授权用户识别为入侵者
- 收紧对入侵的定义将导致**漏报**——
将入侵者识别为授权用户





入侵检测

○ 误用检测

- 定义现有入侵模式的特征值以进行识别
- 难以检测新型未知入侵

○ 异常检测

- 定义行为正常模式轮廓
- 判定入侵和正常行为的偏差值
- 能检测新型未知入侵



入侵检测指标

- 每天或每个时段的登录频率
- 在不同地点的登录频率
- 最后一次登录时间
- 登录的口令错误
- 执行频率
- 执行失效
- 读/写/创建/删除频率
- 读/写/创建/删除失效次数



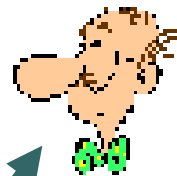
2 挑战应答认证

目标: Bob希望Alice向其“证明”她的身份

协议1.0: Alice说“I am Alice”



“I am Alice”

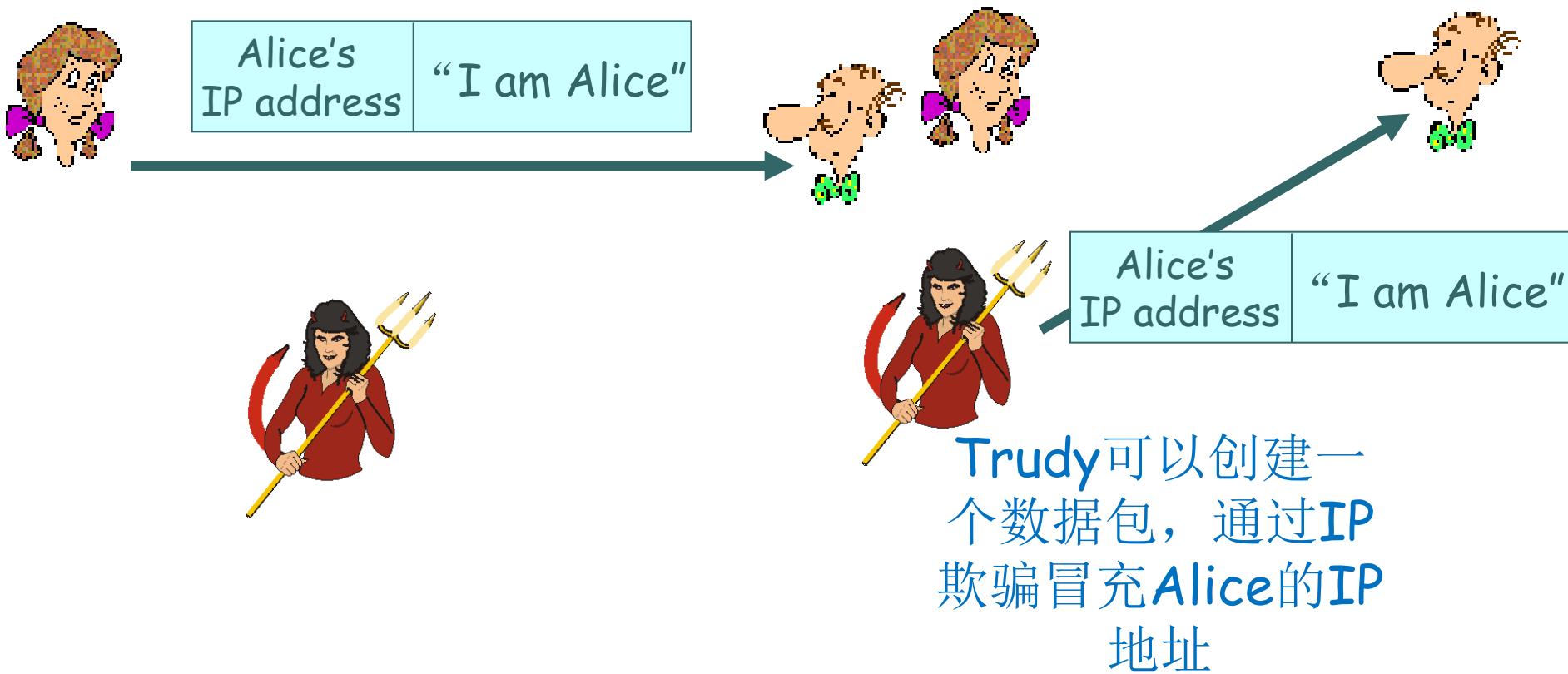


“I am Alice”

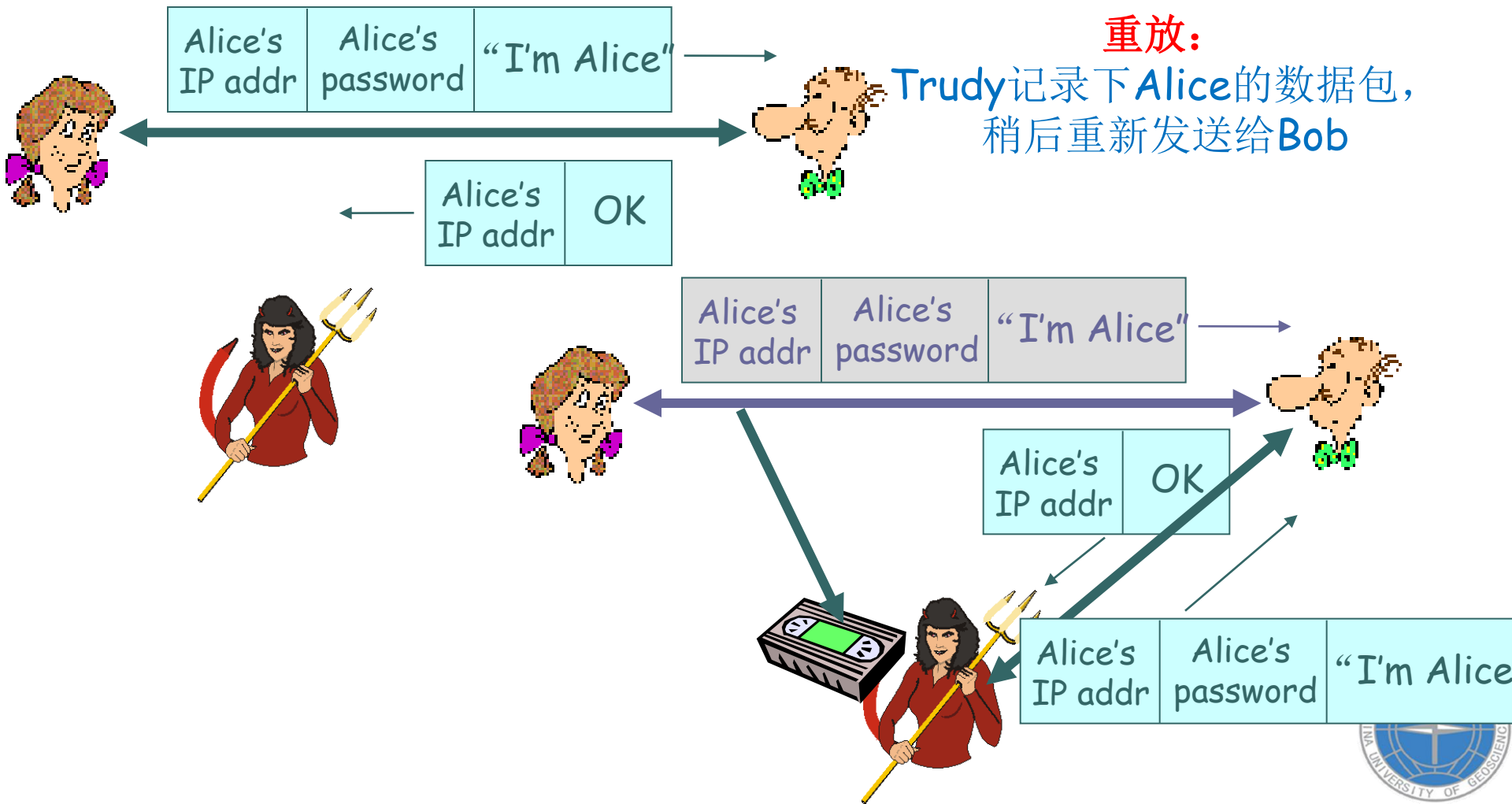
在网络中，Bob不能“看见” Alice，所以Trudy可以声称她自己是Alice



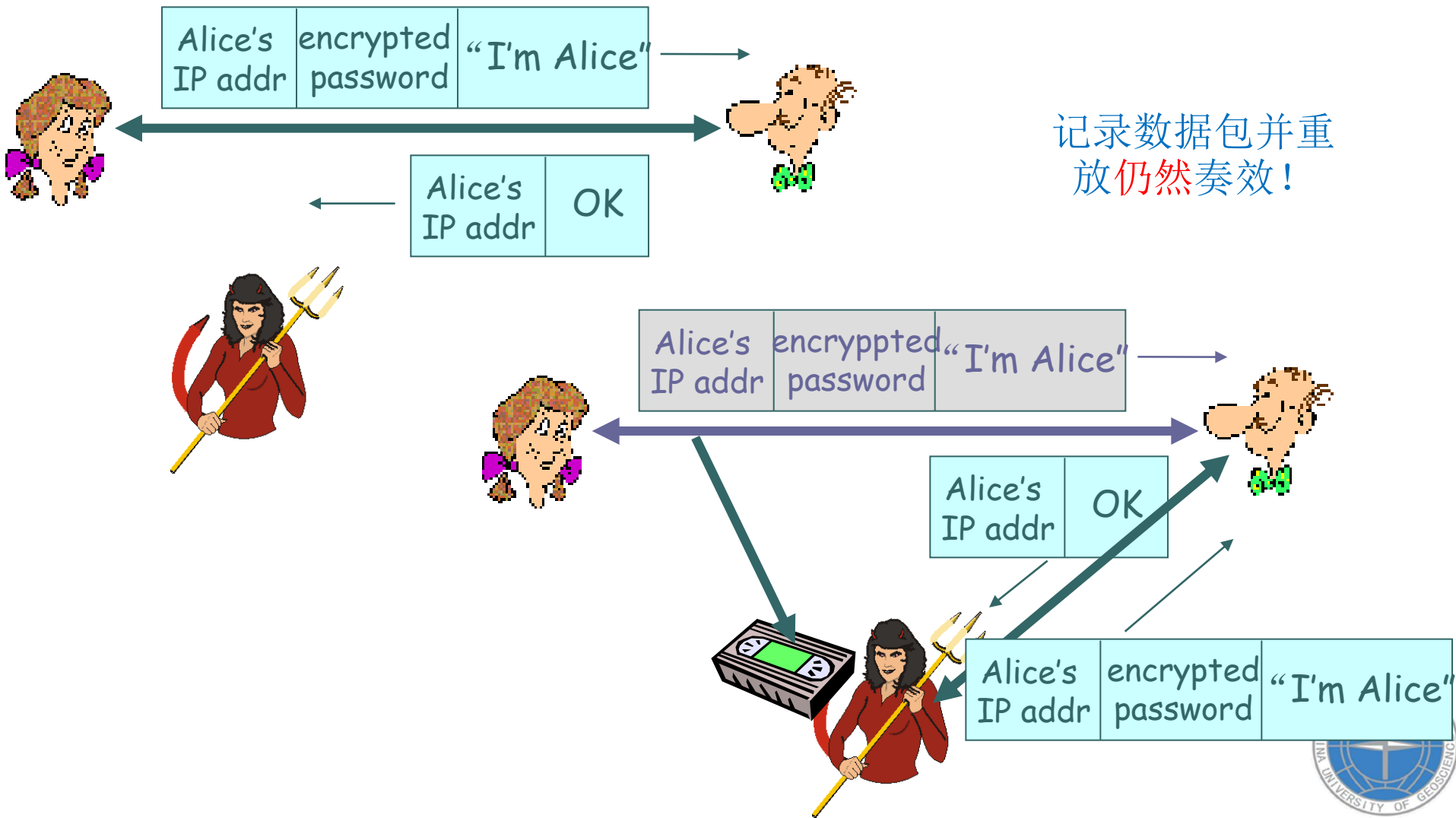
协议2.0: Alice在一个包含自己源IP地址的IP包中说
“I am Alice”



协议3.0: Alice说“I am Alice”并发送她的秘密口令来
“证明”自己



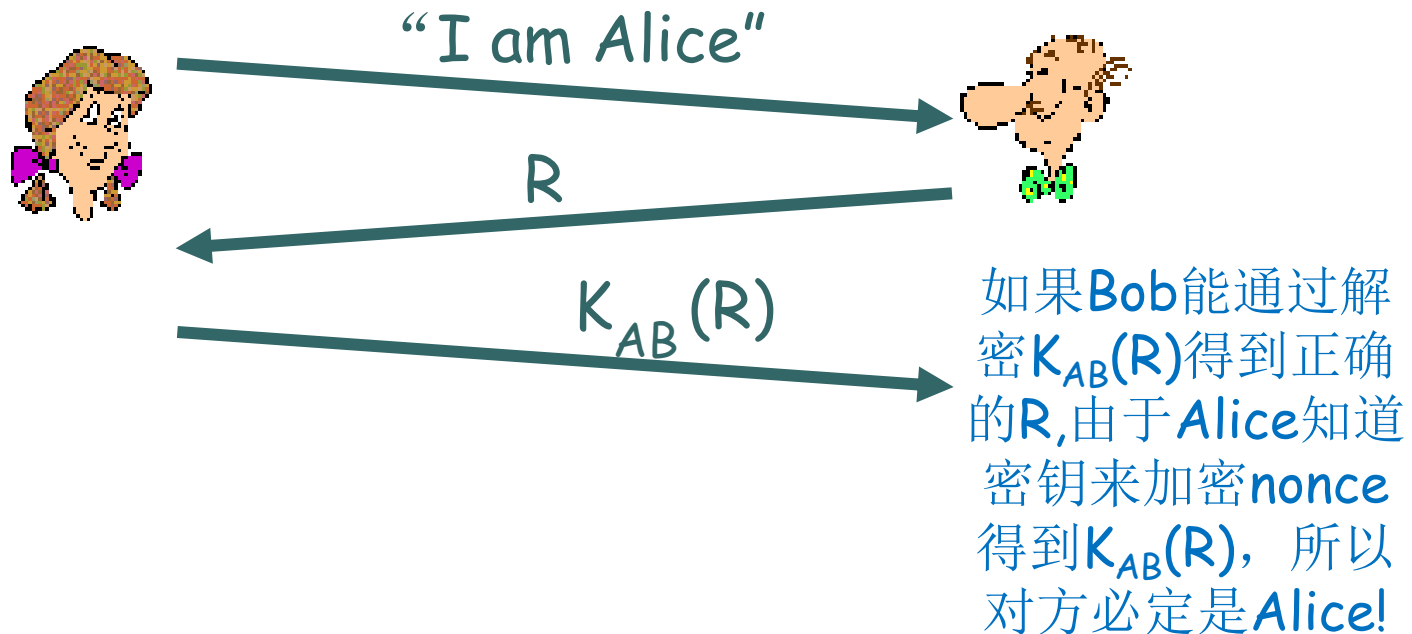
协议3.1: Alice说“I am Alice”并发送她加密的秘密口令来
“证明”自己



目标: 避免重放攻击

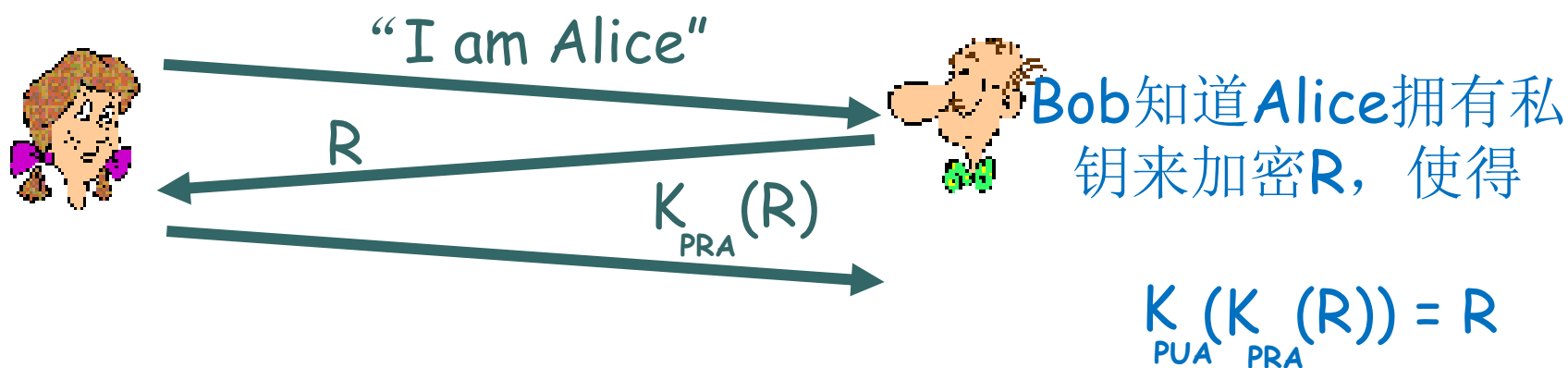
Nonce: 只使用一次的数字(R)

ap4.0: 为了证明Alice“活着”，Bob向Alice发送**nonce**--- R (随机数). Alice必须返回(应答), 用双方共享的秘密钥加密



协议4.0需要事先传输共享对称密钥

协议5.0: 使用公钥密码



3 隐私保护

- 隐私定义
 - 隐私是可确认特定个人（或团体）身份或其特征，但个人（或团体）不愿被暴露的敏感信息
- 隐私分类
 - 财务隐私
 - 互联网隐私
 - 医疗隐私
 - 政治隐私
 - 信息隐私



● ● ● | 针对隐私的链接攻击

- 链接攻击是从发布的数据表中获取隐私数据的常见方法。其基本思想为：攻击者通过对发布的数据和其他渠道获取的外部数据进行链接操作，以推理出隐私数据，从而造成隐私泄露。



链接攻击实例

Race	Visit Date	Hospitalization	ZIP	Birthday	Sex	Total charge	Disease
Black	2016.3.8	In	430074	1995.3.8	Male	20g	Flu
Black	2016.3.8	Out	430073	1995.3.8	Male	30g	Cancer
Yellow	2016.10.2	In	430082	1996.6.2	Male	10g	Obesity
Yellow	2016.2.1	In	430083	1996.7.5	Male	20g	Gastritis
White	2016.3.1	Out	430080	1998.3.3	Female	0g	HIV
White	2016.7.2	In	430081	1998.4.1	Female	35g	Cancer

表1 医疗数据表



链接攻击实例

Name	Race	Date Registered	Address	ZIP	Birthday	Sex	Party Affiliation
Paul	Black	2016.9.1	CUG	430074	1995.3.8	Male	YES
Bob	Black	2016.9.1	CUG	430073	1995.3.8	Male	NO
David	Yellow	2016.9.6	WHU	430082	1996.6.2	Male	YES
Tom	Yellow	2016.9.5	CUG	430083	1996.7.5	Male	NO
Jane	White	2016.9.6	HUST	430080	1998.3.3	Female	YES
Alice	White	2016.9.1	WHU	430081	1998.4.1	Female	YES

表2 选民数据表



链接攻击实例

Name	Race	Zip	Birth	Sex	Disease
Paul	Black	430074	1995.3.8	Male	Flu
Bob	Black	430073	1995.3.8	Male	Cancer
David	Yellow	430082	1996.6.2	Male	Obesity
Tom	Yellow	430083	1996.7.5	Male	Gastritis
Jane	White	430080	1998.3.3	Female	HIV
Alice	White	430081	1998.4.1	Female	Cancer

表3 链接攻击得到的数据表



K-匿名研究意义

随着公开信息的数据共享的隐私保护研究越来越深入，K-匿名技术成为基于隐私保护的数据发掘的相关研究的重要保障，应用于医疗系统、数据挖掘、视图发布等领域。



K-匿名相关定义

1.标识符

标识符可直接表示出个体身份的属性，如身份证号、社保号、姓名等。一般在数据发布前将显式标识符属性屏蔽、删除或加密，达到保护这些私有信息的目的。

2.准标识符

准标识符是指与其他外部数据表进行链接以标识个体身份的属性或属性组合，如性别、出生日期、邮政编码等。准标识符的选择取决于进行链接的外部数据表。



K-匿名相关定义

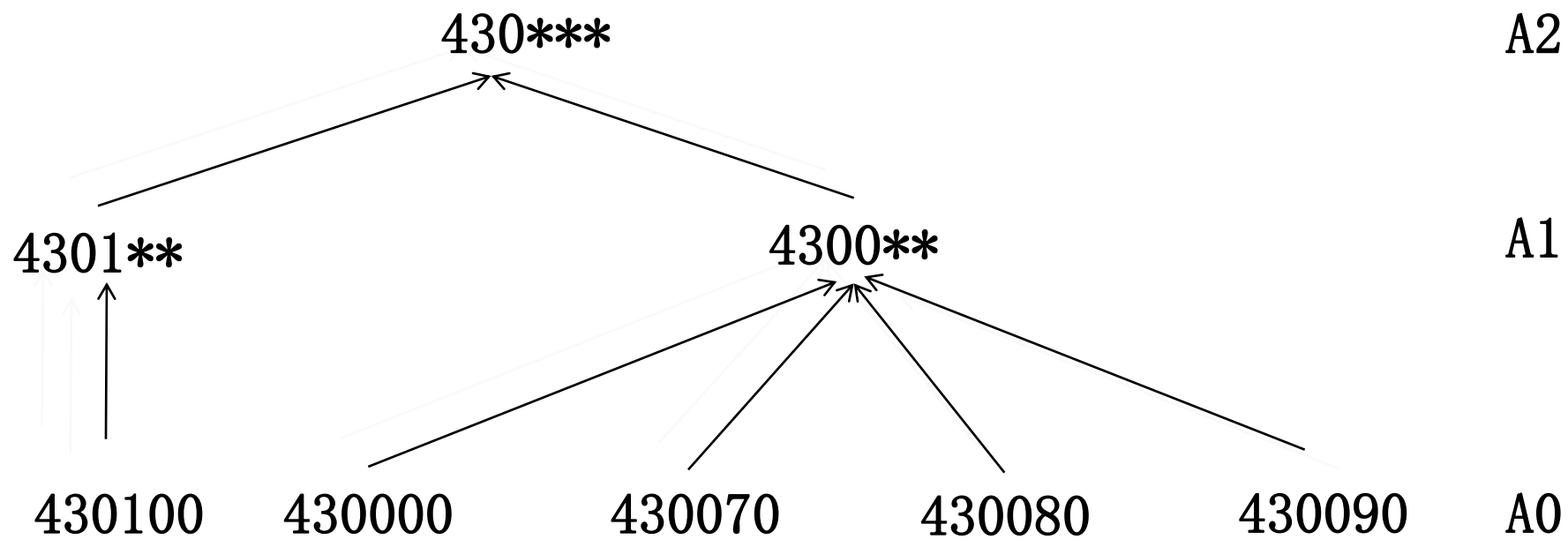
3.K-匿名

K-匿名通过概括和隐匿技术，发布精度较低的数据，使得每条记录至少与数据表中其他**K-1** 条记录具有完全相同的准标识符属性值，从而减少链接攻击所导致的隐私泄露。

4.泛化

泛化是对数据进行更概括、更抽象的描述。将具体的数据抽象化，使攻击者更难攻击。





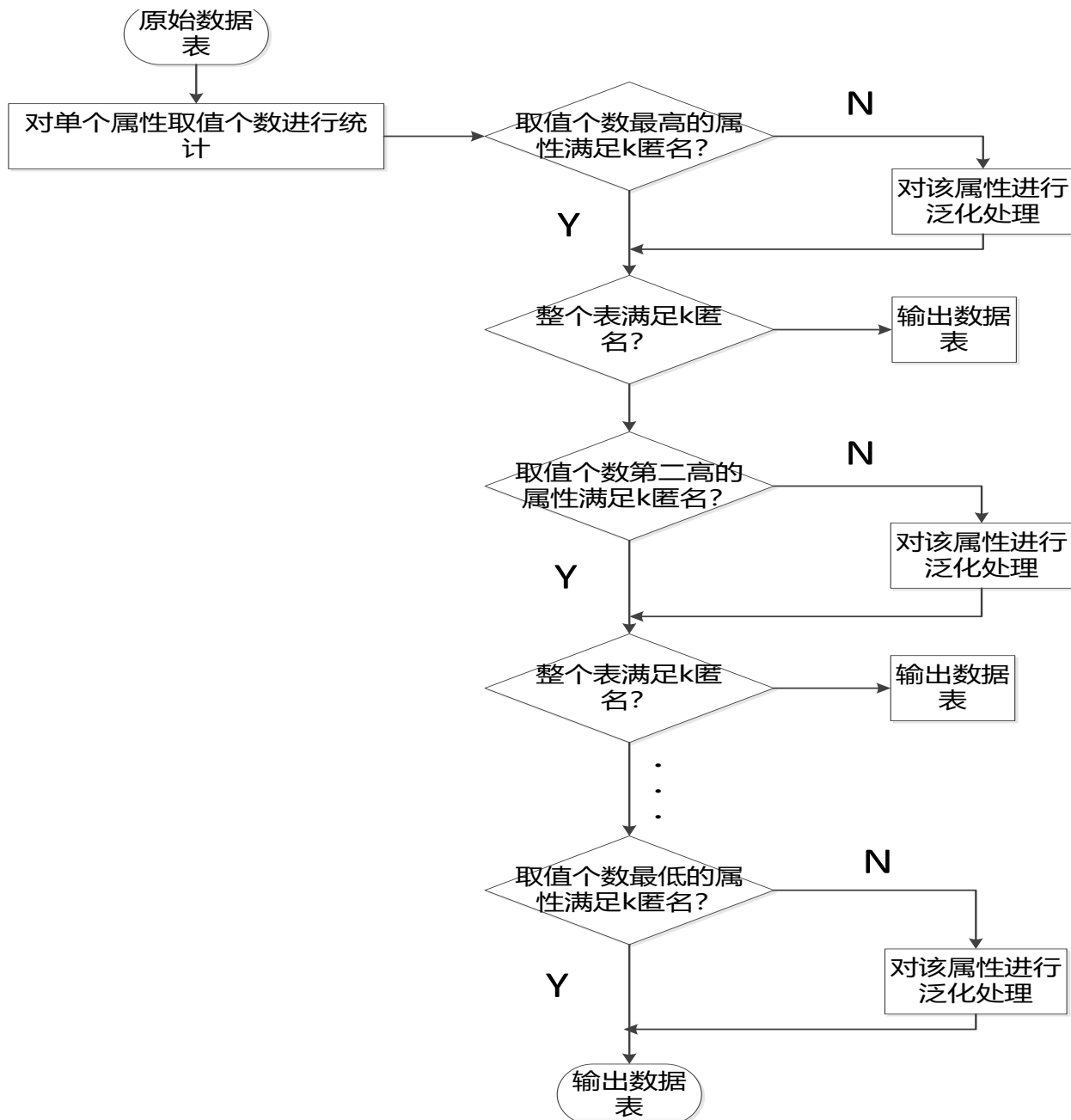
Zipcode的泛化过程



K-匿名算法——Datafly

主要思想是：每次计算都只选择某一个属性值来泛化，被选中的这某一属性的值域集合的基数在其他剩余属性中是最大的，重复之前的步骤直到选取完准标识符属性。





Datafly算法实例

- 1.根据进行链接的表1，表2可知，准标识符为**Race, ZIP, Birthday, Sex**,分别统计每个属性的种类个数，即基数为**3, 6, 5, 2**。
- 2.根据现实需求确定**K**的值，此处令**K=2**。
- 3.对基数最大的**ZIP**属性判断是否满足**2-匿名**，不满足则进行泛化。
- 4.对剩余基数最大的**Birthday**属性判断是否满足**2-匿名**，不满足则进行泛化。
- 5.对剩余基数最大的**Race**属性判断是否满足**2-匿名**，不满足则进行泛化。
- 6.对剩余基数最大的**Sex**属性判断是否满足**2-匿名**，不满足则进行泛化。



Datafly 算法实例

Race	Visit Date	Hospitalization	ZIP	Birthday	Sex	Total charge	Disease
Black	2016.3.8	In	43007*	1995.3.8	Male	20g	Flu
Black	2016.3.8	Out	43007*	1995.3.8	Male	30g	Cancer
Yellow	2016.10.2	In	43008*	1996.6.2	Male	10g	Obesity
Yellow	2016.2.1	In	43008*	1996.7.5	Male	20g	Gastritis
White	2016.3.1	Out	43008*	1998.3.3	Female	0g	HIV
White	2016.7.2	In	43008*	1998.4.1	Female	35g	Cancer

表4 对表1进行ZIP泛化



Datafly 算法实例

Race	Visit Date	Hospitalization	ZIP	Birthday	Sex	Total charge	Disease
Black	2016.3.8	In	43007*	1995	Male	20g	Flu
Black	2016.3.8	Out	43007*	1995	Male	30g	Cancer
Yellow	2016.10.2	In	43008*	1996	Male	10g	Obesity
Yellow	2016.2.1	In	43008*	1996	Male	20g	Gastritis
White	2016.3.1	Out	43008*	1998	Female	0g	HIV
White	2016.7.2	In	43008*	1998	Female	35g	Cancer

表5 对表4进行Birthday泛化



Datafly 算法实例

Race	Visit Date	Hospitalization	ZIP	Birthday	Sex	Total charge	Disease
Black	2016.3.8	In	43007*	1995	Male	20g	Flu
Black	2016.3.8	Out	43007*	1995	Male	30g	Cancer
Yellow	2016.10.2	In	43008*	1996	Male	10g	Obesity
Yellow	2016.2.1	In	43008*	1996	Male	20g	Gastritis
White	2016.3.1	Out	43008*	1998	Female	0g	HIV
White	2016.7.2	In	43008*	1998	Female	35g	Cancer

表6 对表5进行Race泛化



Datafly算法实例

Race	Visit Date	Hospitalization	ZIP	Birthday	Sex	Total charge	Disease
Black	2016.3.8	In	43007*	1995	Male	20g	Flu
Black	2016.3.8	Out	43007*	1995	Male	30g	Cancer
Yellow	2016.10.2	In	43008*	1996	Male	10g	Obesity
Yellow	2016.2.1	In	43008*	1996	Male	20g	Gastritis
White	2016.3.1	Out	43008*	1998	Female	0g	HIV
White	2016.7.2	In	43008*	1998	Female	35g	Cancer

表7 对表6进行Sex泛化



Datafly 算法实例

Name	Race	Date Registered	Adress	ZIP	Birthday	Sex	Party Affiliation
Paul	Black	2016.9.1	CUG	43007*	1995	Male	YES
Bob	Black	2016.9.1	CUG	43007*	1995	Male	NO
David	Yellow	2016.9.6	WHU	43008*	1996	Male	YES
Tom	Yellow	2016.9.5	CUG	43008*	1996	Male	NO
Jane	White	2016.9.6	HUST	43008*	1998	Female	YES
Alice	White	2016.9.1	WHU	43008*	1998	Female	YES

表8 对表2进行泛化



Datafly 算法实例

Name	Race	Zip	Birth	Sex	Disease
Paul/Bob	Black	43007*	1995	Male	Flu
Paul/Bob	Black	43007*	1995	Male	Cancer
David/Tom	Yellow	43008*	1996	Male	Obesity
David/Tom	Yellow	43008*	1996	Male	Gastritis
Jane/Alice	White	43008*	1998	Female	HIV
Jane/Alice	White	43008*	1998	Female	Cancer

表9 对表7和表8进行链接攻击

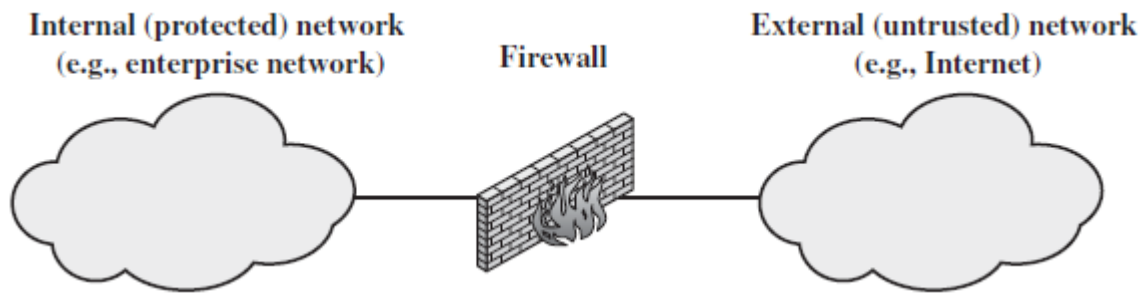



4 防火墙

○ 定义

一种有效的安全技术，用于保护本地系统或网络通过**WAN (Wide Area Network, 广域网)**或**Internet**对外访问时免受基于网络的安全威胁





- 
- 防火墙设计准则
 - 防火墙特征
 - 防火墙缺陷
 - 防火墙种类
 - 防火墙配置



● ● ● | 防火墙设计准则

- 信息系统经历了持续变革，从小的局域网(Local Area Network)到Internet连接
- 在所有工作站和服务器的上都配置强安全防护不现实



● ● ● | 防火墙设计准则

- 防火墙被安装在驻地网络和**Internet**之间
- 目标:
 - 建立可控连接
 - 保护驻地网络免受**Internet**端的攻击
 - 提供单一阻塞点



防火墙特征

○ 设计目标:

- 双向的网络流量必须通过防火墙(除非通过防火墙, 否则所有对驻地网络的访问将被物理阻塞)
- 只有被本地安全策略允许的授权流量能通过防火墙
- 防火墙自身对渗透免疫(使用具有安全OS的可信系统)



防火墙特征

四种通用技术:

- 服务控制
 - 决定访问**Internet**的服务类型
- 方向控制
 - 决定允许通过服务的方向
- 用户控制
 - 控制尝试访问的用户
- 行为控制
 - 控制特定服务的行为（如过滤**Email**）





防火墙缺陷

- 不能防御绕过防火墙的攻击
- 不能防御内部攻击
- 不能查杀病毒文件



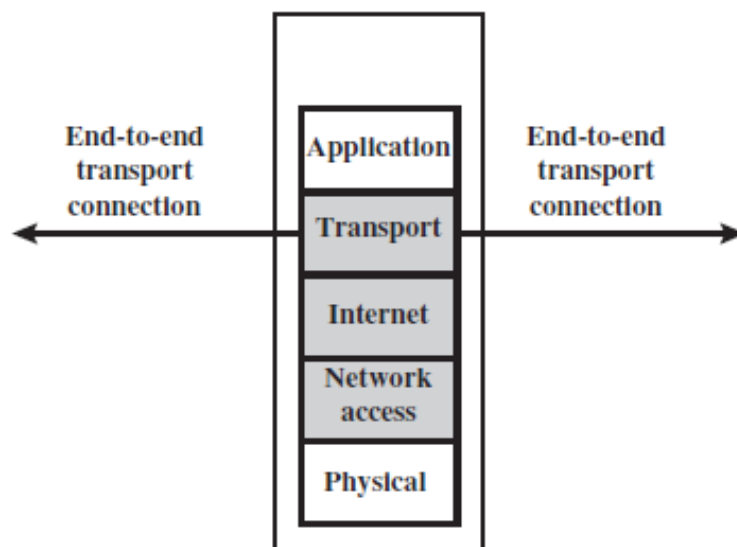
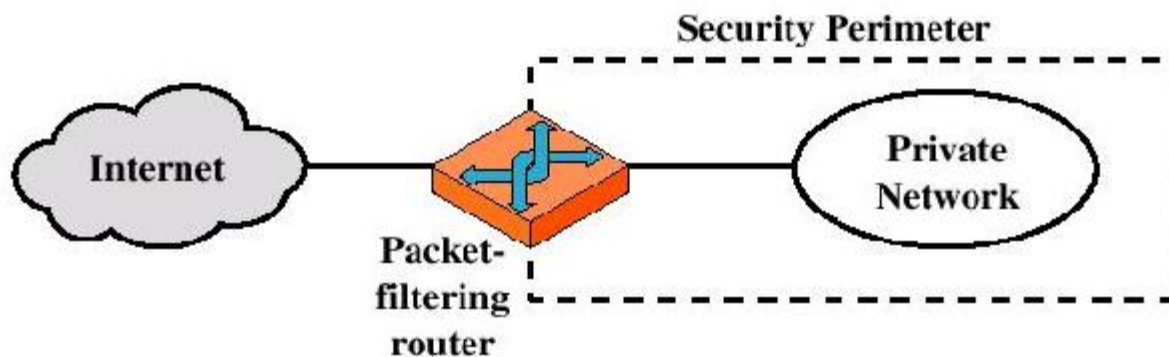
● ● ● | 防火墙种类

- Packet-filtering routers 包过滤路由器
- Application-level gateways 应用层网关



防火墙种类

包过滤路由器



包过滤路由器

- 对**TCP/IP**包设置一系列规则，根据规则转发或丢弃数据包
- 包过滤对双向数据包都有效
- 两种默认策略（丢弃**or**转发）



包过滤路由器

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port



包过滤路由器

- 优点:

- 简单
- 对用户透明
- 快速

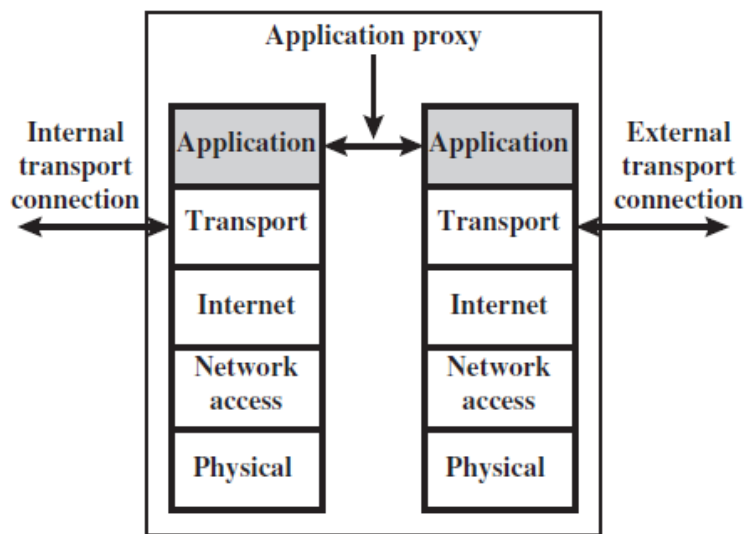
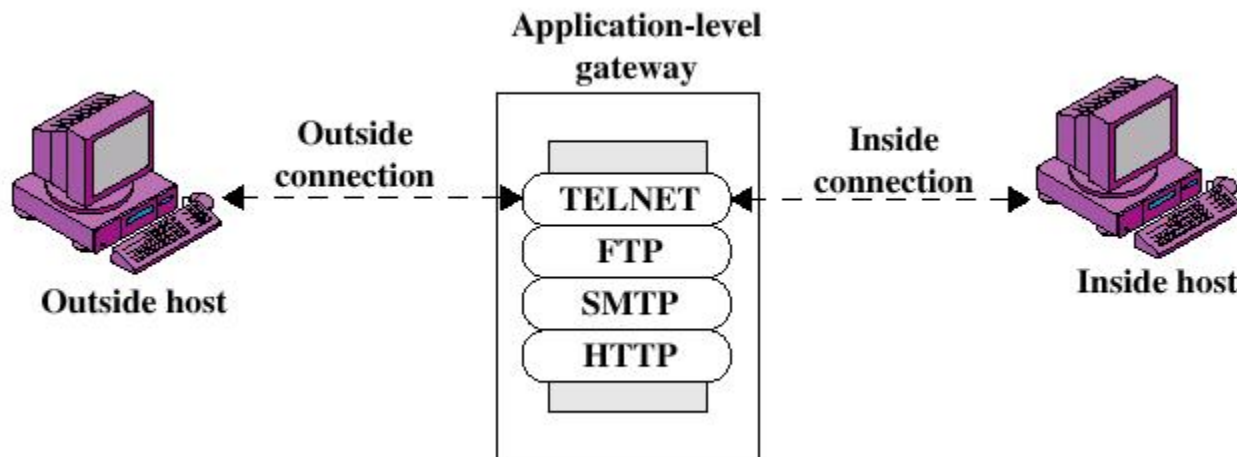
- 缺点:

- 难以设置复杂的包过滤规则
- 缺乏认证



防火墙种类

应用级网关



应用级网关

- 也称为代理服务器
- 作为应用级流量的中继
- 用户通过向远程主机提交账号和口令建立应用级连接



应用级网关

○ 优点:

- 比包过滤路由器更安全
- 只需审查少量特定应用流量
- 易于审计

○ 缺点:

- 所有流量均会通过代理服务器，因此代理服务器可能成为性能瓶颈



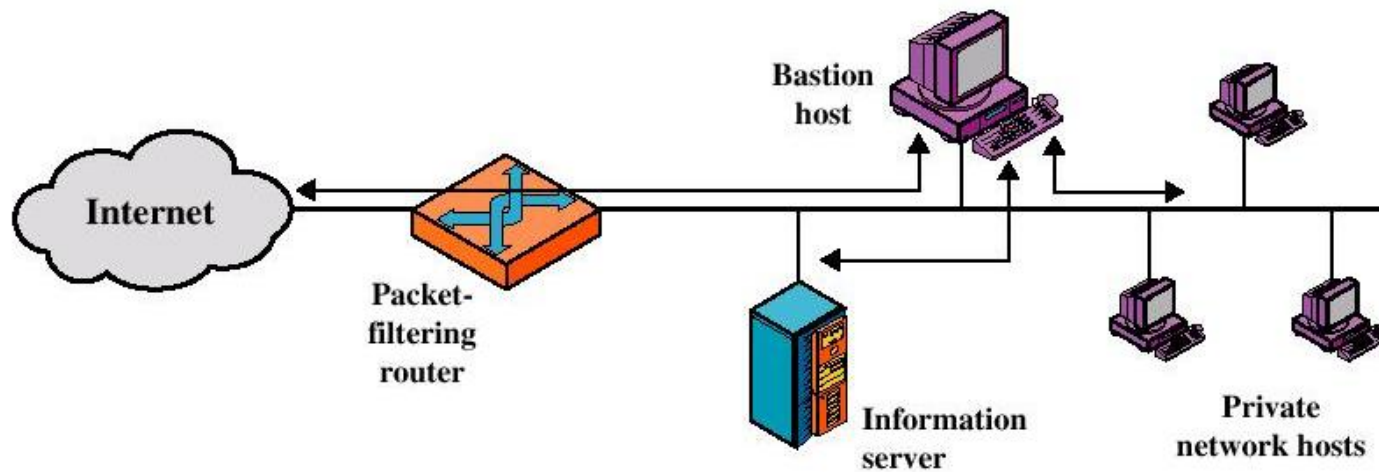
防火墙配置

- 除了单独使用包过滤路由器或应用级网关，还有更为复杂的防火墙配置
- 三种配置
 - 单宿堡垒主机
 - 双宿堡垒主机
 - 屏蔽子网防火墙



防火墙配置

屏蔽主机防火墙 (单宿堡垒主机)



防火墙配置

- 防火墙包括两个系统：
 - 包过滤路由器：只有进出堡垒主机的流量允许通过路由器
 - 堡垒主机：执行认证和代理功能



单宿堡垒主机

- 比单一配置更安全：
 - 综合了包过滤路由器和应用级网关
 - 攻击者必须渗透两个系统



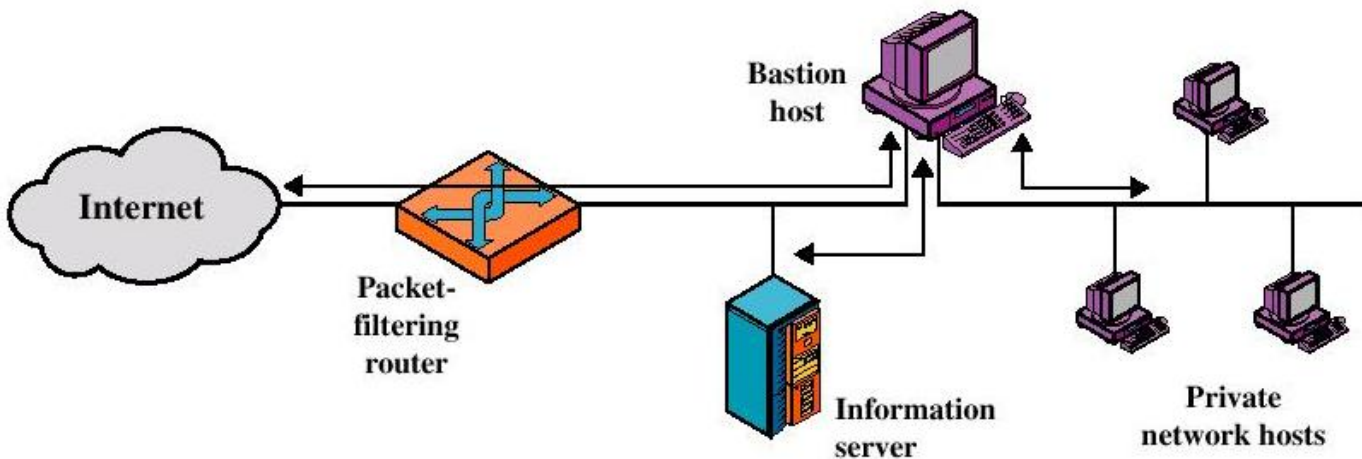
单宿堡垒主机

- 提供直接**Internet**访问的便利（将**Web**服务器放在包过滤路由器和应用级网关之间）
- 如果包过滤路由器被攻破，则堡垒主机被绕过



防火墙配置

屏蔽主机防火墙(双宿堡垒主机)



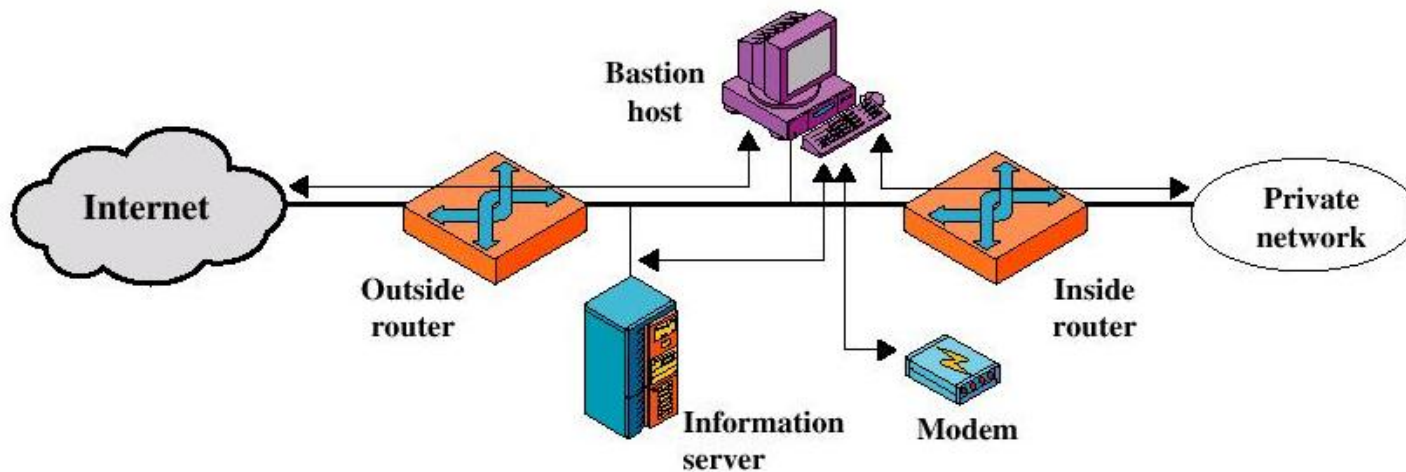
双宿堡垒主机

- 双网卡隔离驻地网络和**Internet**
- **Internet**和驻地网络之间的流量必须经过堡垒主机



防火墙配置

屏蔽子网防火墙



屏蔽子网防火墙

- 在三种配置中最安全
- 使用两个包过滤路由器
- 形成独立子网



屏蔽子网防火墙

- 三重防护攻击者
- 外部路由器隔离了屏蔽子网和 **Internet**，对于 **Internet** 来说，内部驻地网络不存在
- 内部路由器隔离了屏蔽子网和驻地网络，驻地网络不能构造对 **Internet** 的直接访问



5 PKI

- PR---秘密: 保密性, 完整性&真实性
- PU---公开: 完整性 & 真实性
- PU和用户身份的对应关系用数字签名来保护



● ● ● | 密钥分配

- 用数字签名保证PKDB中PU的真实性和完整性
- 证书：可信实体对用户的身份和PU进行签名
- CA(Certification Authority, 认证中心): 对PU进行签名的可信实体



● ● ● | X.509 认证服务

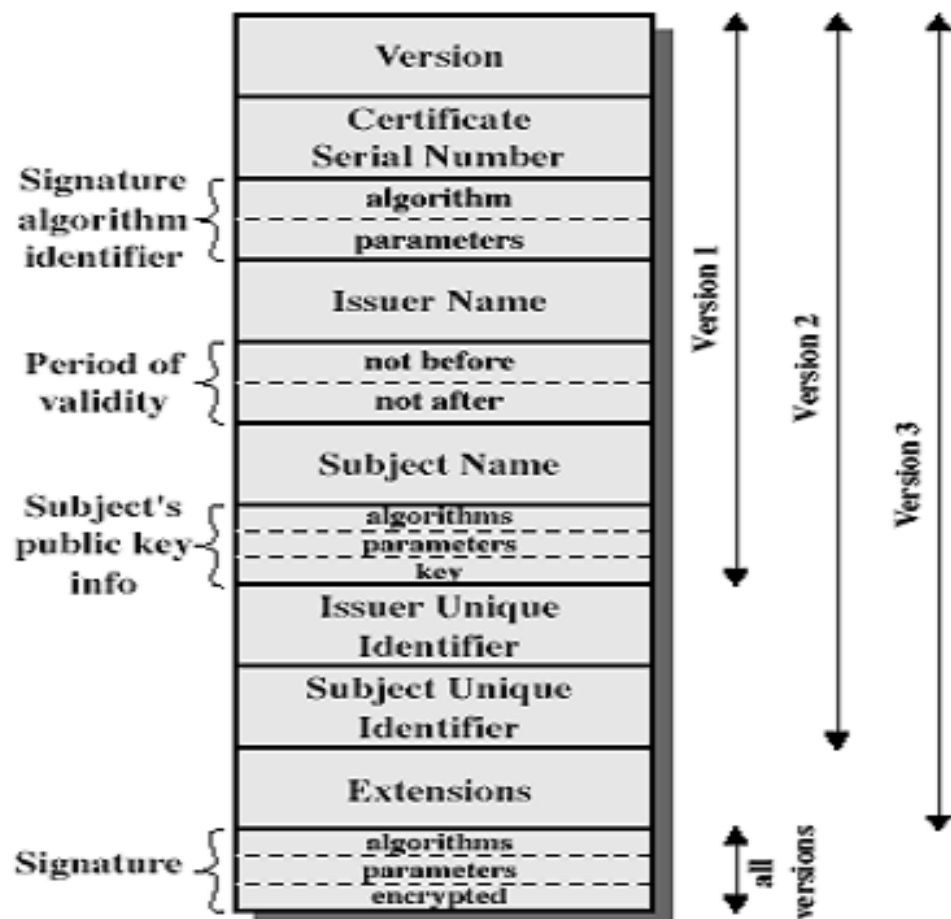
- 定义认证服务的框架
 - 目录存储公钥证书
 - 包含用户公钥
 - **CA**用其私钥**PR**进行数字签名
- 使用公钥加密和数字签名
 - 算法无需指定，一般推荐使用**RSA**
- 公钥证书是**PU**的可信载体，安全分配**PU**，用于电子商务和电子政务



X.509公钥证书

- 由**CA**颁布，包括：
 - 版本号 (V1, V2, or V3)
 - 序列号 (在同一**CA**下唯一): 识别证书
 - 签名算法标识符
 - 颁布者X.500名 (**CA**名)
 - 有效期 (自 - 至日期)
 - 主体X.500名 (所有者名)
 - 主体公钥信息 (算法, 参数, 密钥)
 - 颁布者唯一标识符 (v2+)
 - 主体唯一标识符 (v2+)
 - 扩展域 (v3)
 - 签名 (对证书所有域的哈希值进行签名)
- **CA** << **A** >> 表示**CA**用 PR_{CA} 对**A**的 PU_A 进行签名得到的证书





(a) X.509 Certificate

● ● ● | 证书获取

- 任何可以访问**CA**的用户都可以获取其上的证书
- 只有**CA**可以修改证书
- 由于不能伪造，证书可以放在公开目录上



● ● ● | 证书验证

- 用户获取**CA证书**以得到**CA**公钥，来验证其他用户证书中公钥的安全性
- **CA**证书通过**自签**或**上级CA**签署



CA层次结构

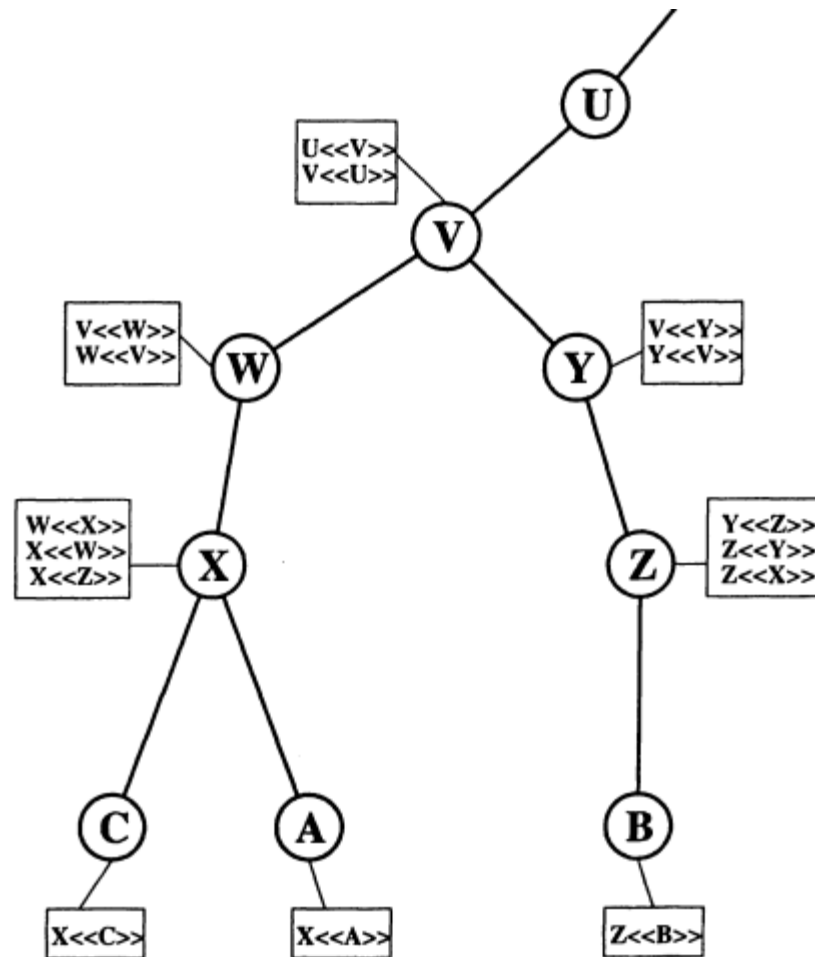
- 如果两个用户属于同一个**CA**，则他们都知道**CA**的证书，否则需要考虑**CA**间的层次关系
- 使用层次结构的证书链接关系来验证其他**CA**证书的有效性
- 每个用户信任其父证书，**CA**之间的信任关系依赖于他们之间互相颁布的证书



交叉认证

- 给定 $X1 \ll A \gg$, $X2 \ll B \gg$, $A \& B$ 如何相互认证证书?
 - $X1X2$ 相互颁布证书
 - A 认证证书链 $X1 \ll X2 \gg X2 \ll B \gg$
 - B 认证证书链 $X2 \ll X1 \gg X1 \ll A \gg$





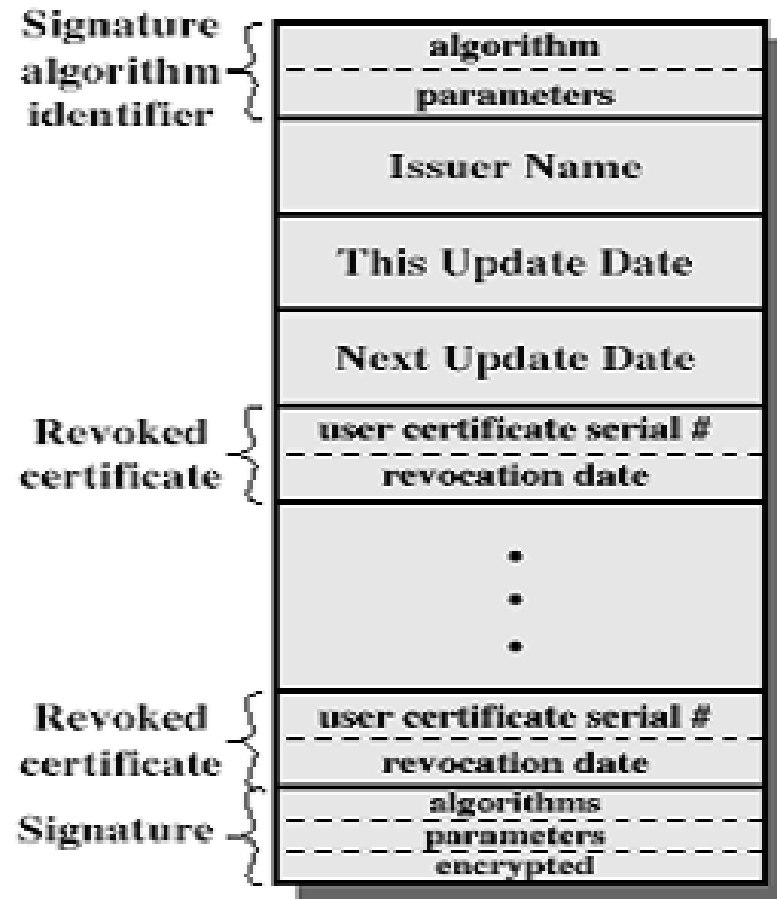
X.509 Hierarchy: A Hypothetical Example.



● ● ● | 证书撤销

- 证书都有有效期
- 以下情况可能在到期前撤销证书：
 - 用户的私钥被破坏或泄露
 - 用户不再被**CA**信任
 - **CA**的证书被破坏
- **CA**通过数字签名维护被撤销证书的列表
 - the Certificate Revocation List (CRL)
- 用户需要定期更新**CRL**，在使用每个证书前检查其是否已经撤销
- 缓存**CRL**以加速使用





(b) Certificate Revocation List



● ● ● | PKI (Public Key Infrastructure) 公钥基础设施

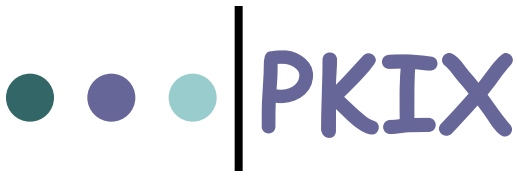
- 包含硬件、软件、人、策略和相应处置的系统，用来创建、管理、存储、分配、使用、撤销和销毁数字证书（PU）
- 目标：分配PU
- 信任通过证书来传递



● ● ● | PKIX组件

- 端实体
- CA
- RA (Register Authority, 注册机构, 可选)
- CRL发布点(可选)
- 证书库(证书 & CRL)





- 用户注册
- 用户初始化
 - 密钥对产生和分配
- 认证
 - 证书产生
- 公私密钥对的备份和恢复
 - 对于加密，存储PU和PR
 - 对于签名，只存储PU
- 密钥对自动更新 (正常)
- 证书撤销请求(异常)
- 交叉认证
 - CA为其他CA颁布证书





| 2021 |

Thank you...