Information Security Engineering

2017.10.11

文本口令

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

课程项目 - 分组和选题

- 01: 语音识别认证（李晖、杜思佳、储贤、曹路）
- 02: Face认证（吴勃志、汪蕴哲、杨法偿、孙媛）
- 03: PINSlide（任昆鹏、陈炘、卜天童、马明仪）
- 04: 基于汉字的图形口令（陈波波、胡鸿、吴诗晨、杨晨）
- 05: 公共WIFI安全（杨寒冬、康雨城、郭梦瑶、邓宇凡）
- 06: 文本验证码攻击（王道鹏、代革命、陈李昊、王帅）
- 07: 图片＋滑块CAPTCHA（龙东恒、宋文浩、谢贤彬、许佳）
- 08: 图形验证码的设计与破解（许志鹏、陈菊芳、李子康）
- 09: 图形验证码的设计与攻击（曾显峰、周力、马炀、黄钰淇）

课程项目 – 选题汇报

- 10月25日，01-05组项目选题汇报；
- 10月24日晚上11点前提交一个文字版的项目开题报告，项目选题汇报PPT，提交到github；
- 项目开题报告和项目选题汇报PPT，必须包括选题背景、产品现状、研究现状、主要思路、项目分工、项目计划；
- 组内成员必须每人都汇报，每个人三分钟（最多3页Slide），每个组最少5分钟Q&A；
- 上一组负责下一组的主持，包括开场介绍、每个人的时间控制、Q&A等，本组的同学记录问题和回答，课下整理成开题记录。
- 11月1日，06-09组项目选题汇报，要求和步骤同上；

课程内容

- 图形口令评价
- 身份认证简介
- 文本口令现状
- 例子：防口令泄漏机制

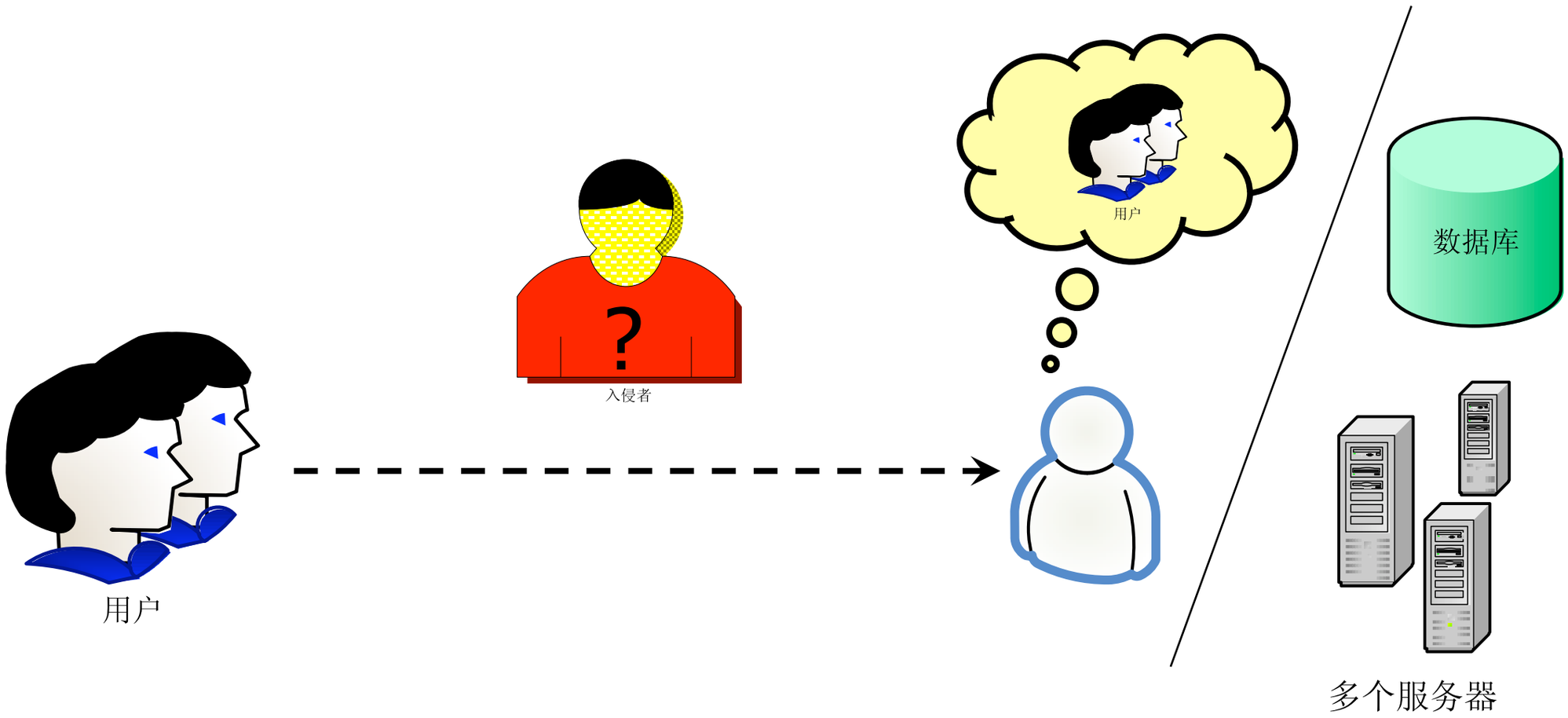
尽管存在大量的其余选择

文本口令

依然是最常用的认证机制

Authentication

身份认证



身份认证因子

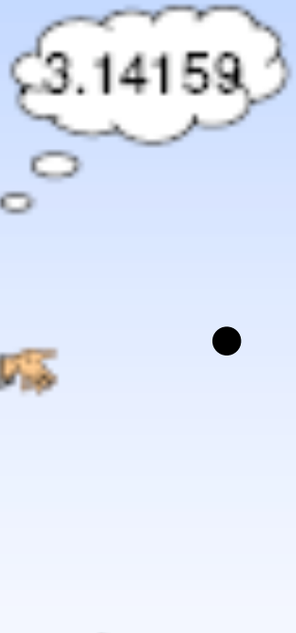
Security Level

- Something you have
  - OTP
  - Smart Card
  - USB Token
  - Mobile Phone

Something you have

- Something you are /can do
  - Fingerprint
  - Voice

Something you are



Something you know

- Something you know
  - Password
  - Image
  - Answer

Method

Text Password

文本口令

- 文本口令是研究与使用最为广泛的身份认证方法，最常用的形式：用户名＋口令
- 选择原则：易于记忆，难于猜中或者发现，抗分析能力强

Table 1. Password characteristics.

Password characteristic	Security focus	Usability focus
Length	Longer	Shorter
Composition	Heterogeneous characters	Homogeneous characters
Uniqueness	Forbid reuse	Common passwords
Change frequency	Often	Seldom

Text Password 文本口令

- 为了证实标识或者获得存取资源的许可而用于身份认证的一个秘密的字或者一串字符

https://www.wired.com/2012/01/computer-password/

56年

1960

MIT CTSS

- *passphrase、passcode、personal identification number、watchword、access word*

Text Password 文本口令

Text Password

文本口令优缺点

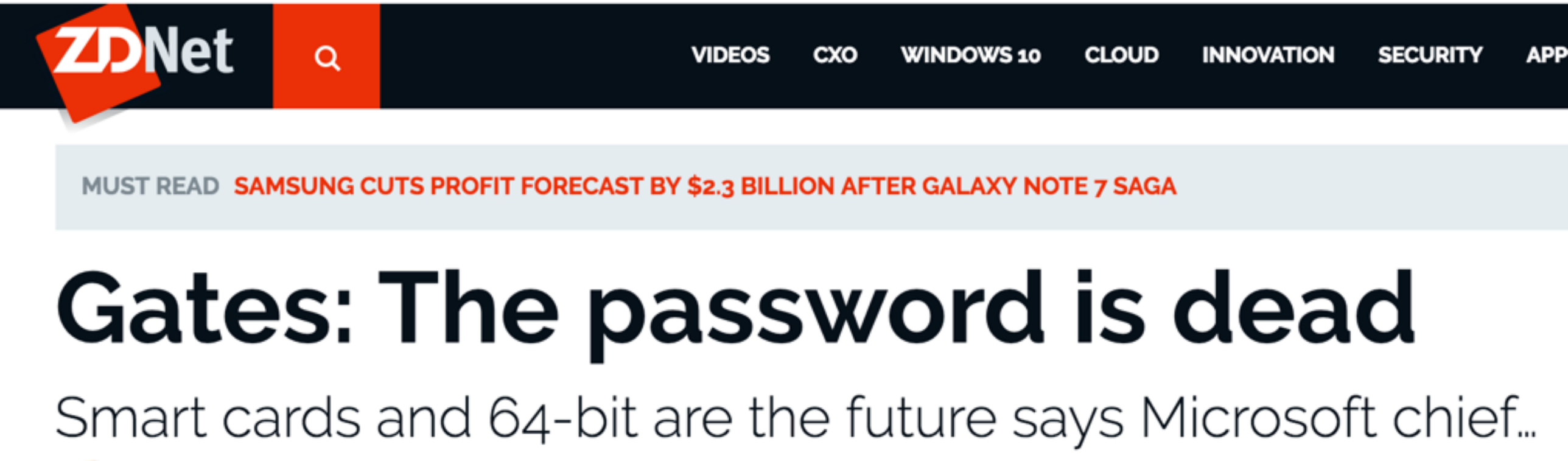
- 容易使用
- 价格便宜
- 用户熟悉
- 隐私保护
- 携带方便

- 记忆困难
- 容易预测
- 多个账户
- 再次使用
- 可用影响

Password is Dead?

历史

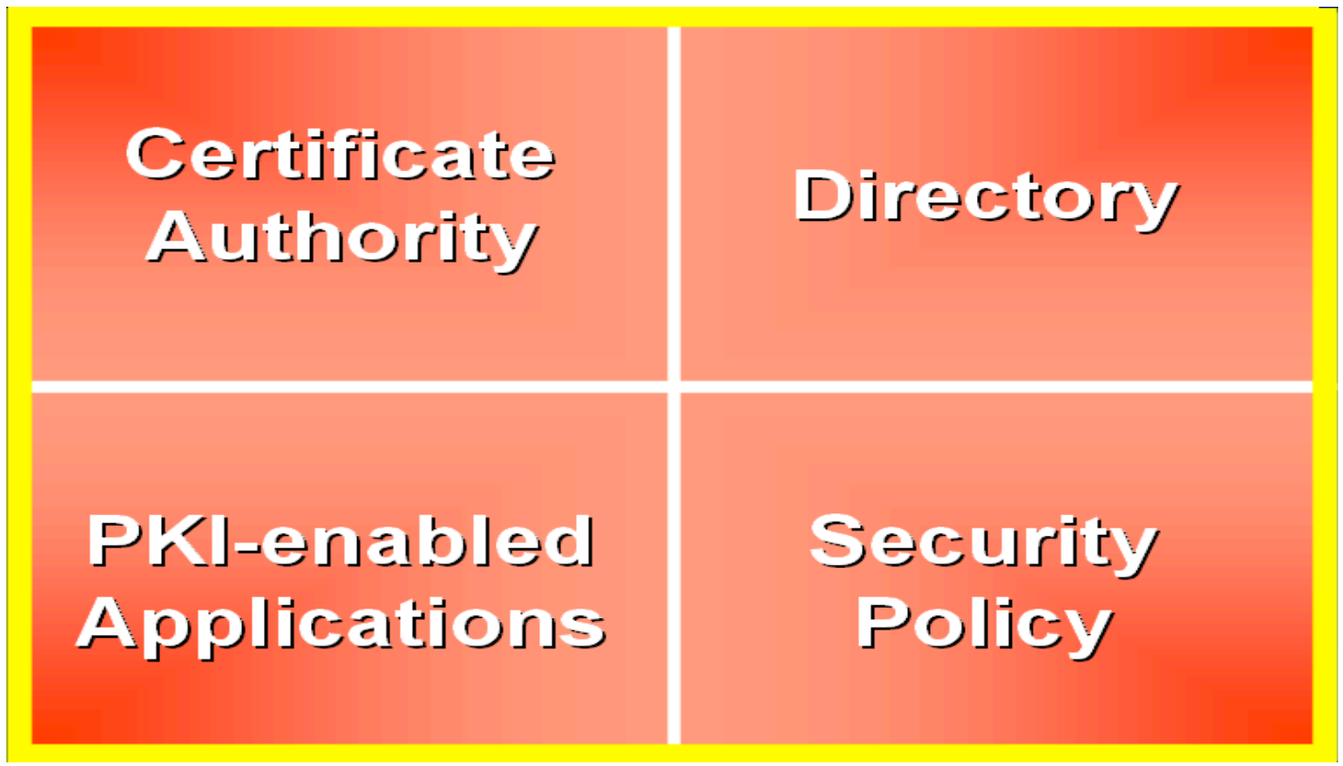
- *1960: MIT CTSS*
- *1970: MULTICS，Hash存储*
- *1979: crypt()，hash＋salting*
- *1985: Green Book*
- *1985: NIST FIPS 112*
- *2004: Bill Gates, "the password is dead"*



PKC & PKI

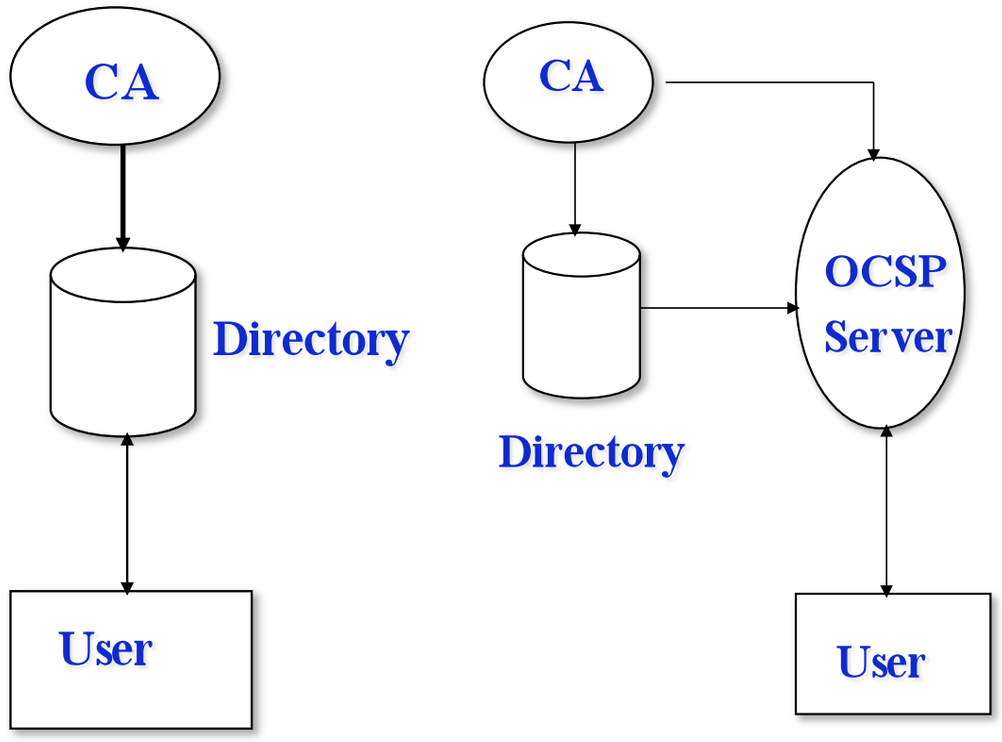
- 一系列基于公钥密码学之上，用来创建、管理、存储、分布和作废证书的软件、硬件、人员、策略和过程的集合。

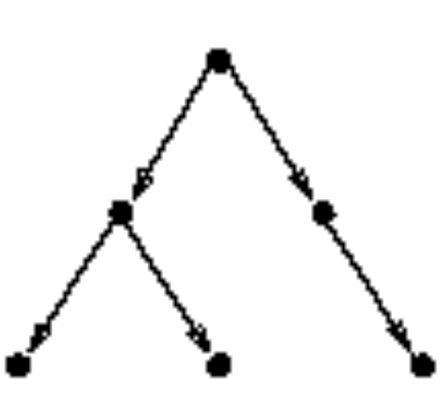
- 基础：公钥密码学 ***mid-1990s***
- 动作：创建、管理、存储、分布和作废证书
- 包含：软件、硬件、人员、策略和过程
- 目的：表示和管理信任关系

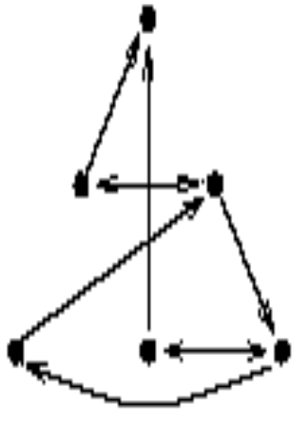


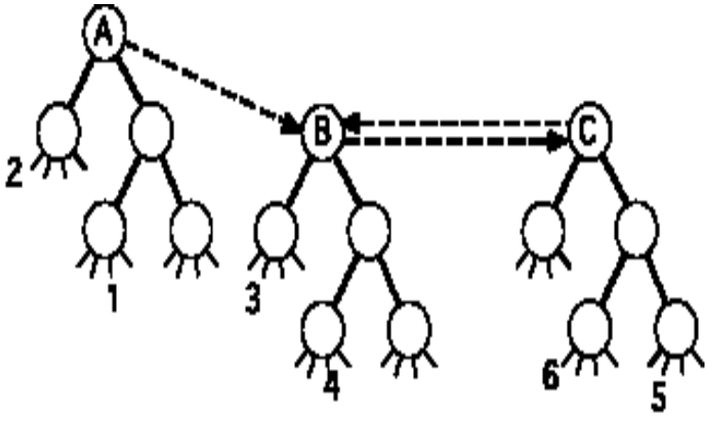
PKC & PKI

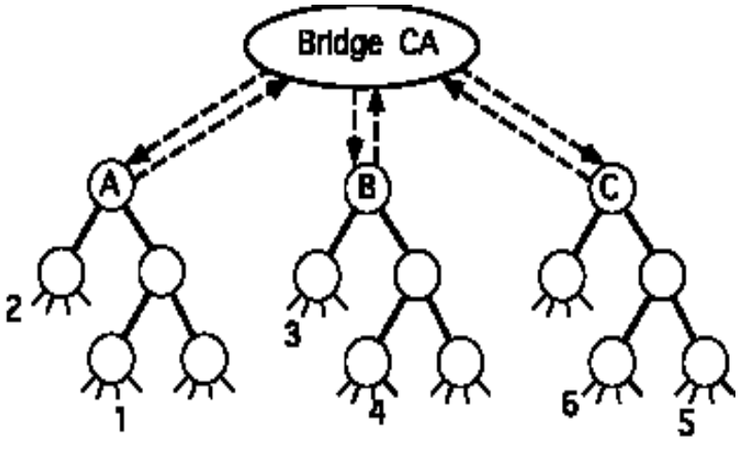
- 需要预先知道对方的公钥、需要在线服务器的支持
- 引入证书、引入可信第三方
- 密钥管理、证书管理
- 信任问题、规模问题
- 性能问题、互联互通问题





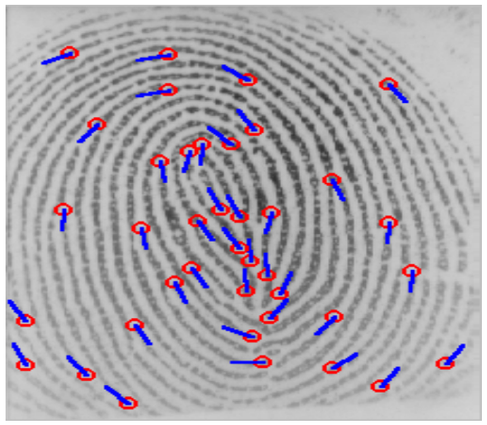


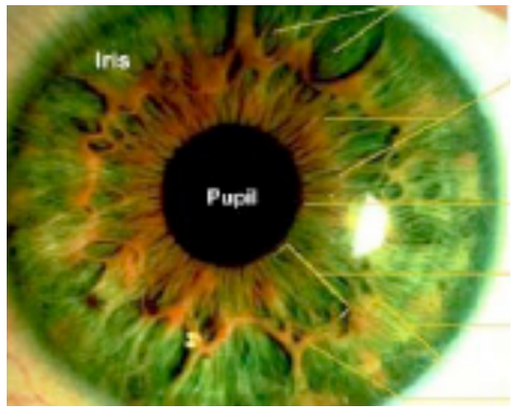


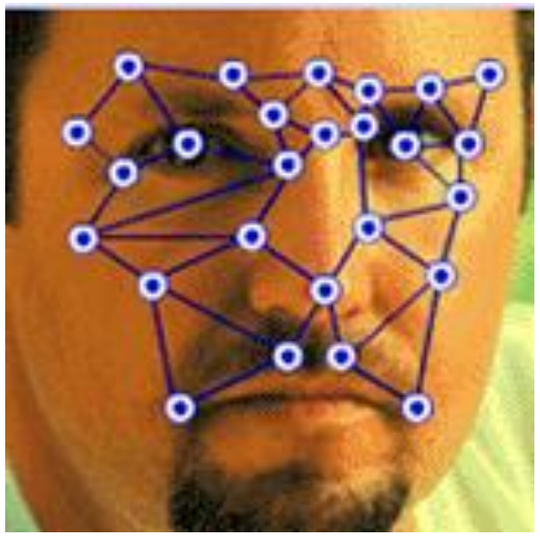


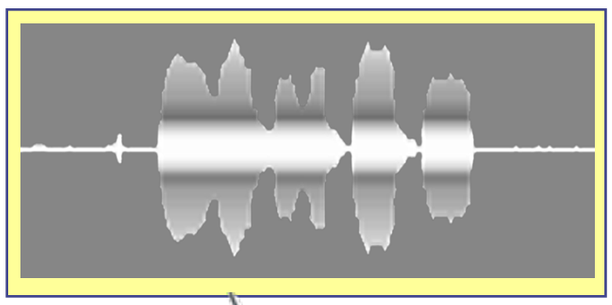
Password is Dead

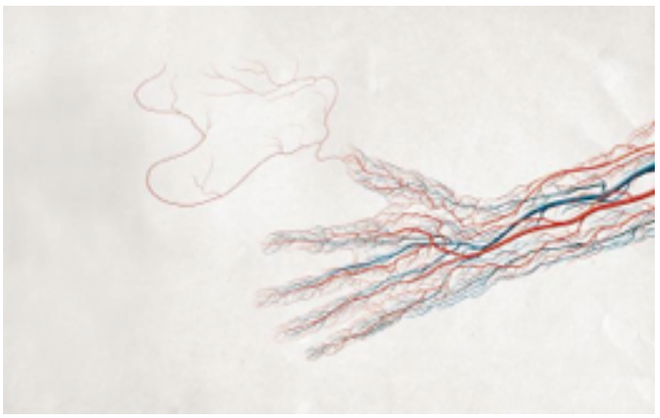
Biometrics

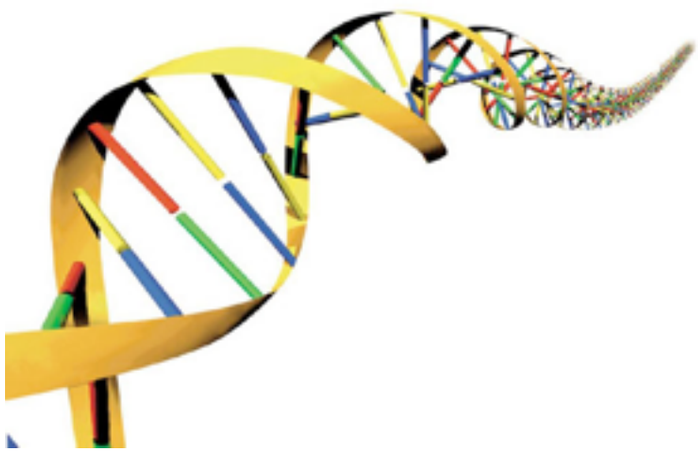












Password is Dead

攻击指纹

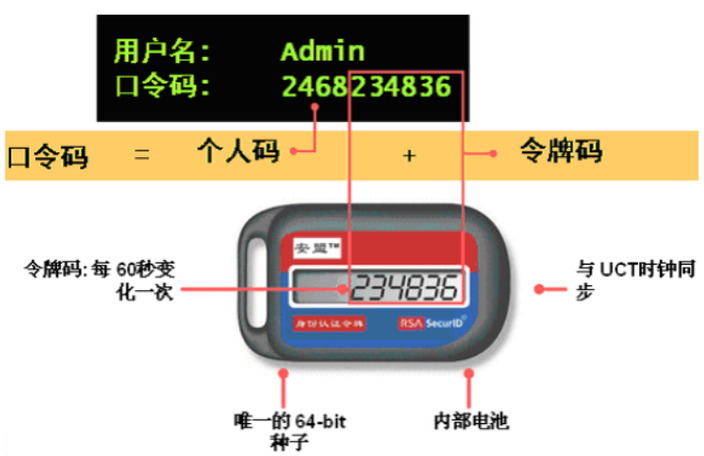
Chaos Computer Club

Password is Imperfect

But ... ...

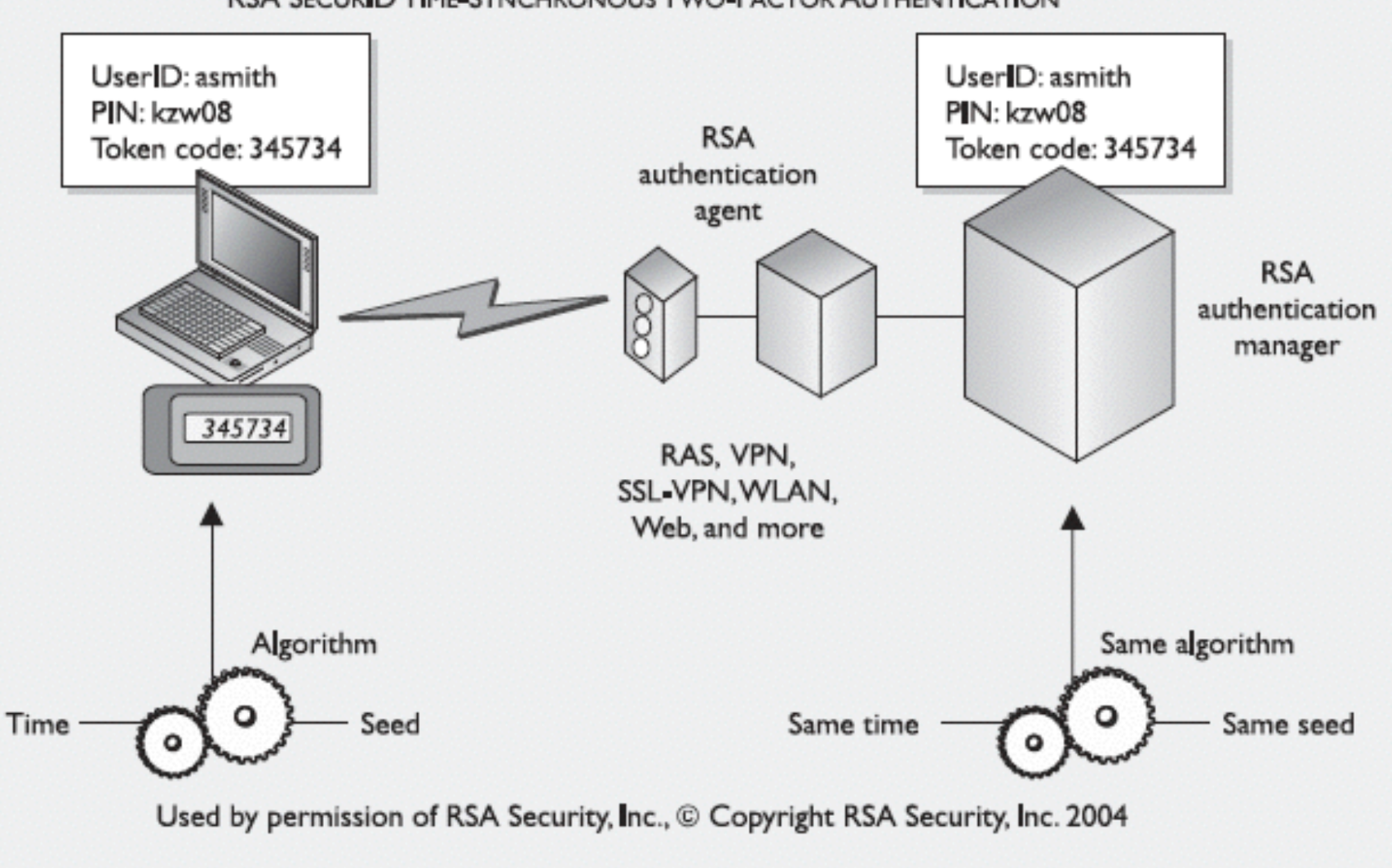
OTP: One Time Password

一次性(动态)口令。是由电子令牌(Token)等手持终端设备生成的，根据某种加密算法，产生的随某一个不断变化的参数(例如时间，事件等)不停地、没有重复变化的一种口令。



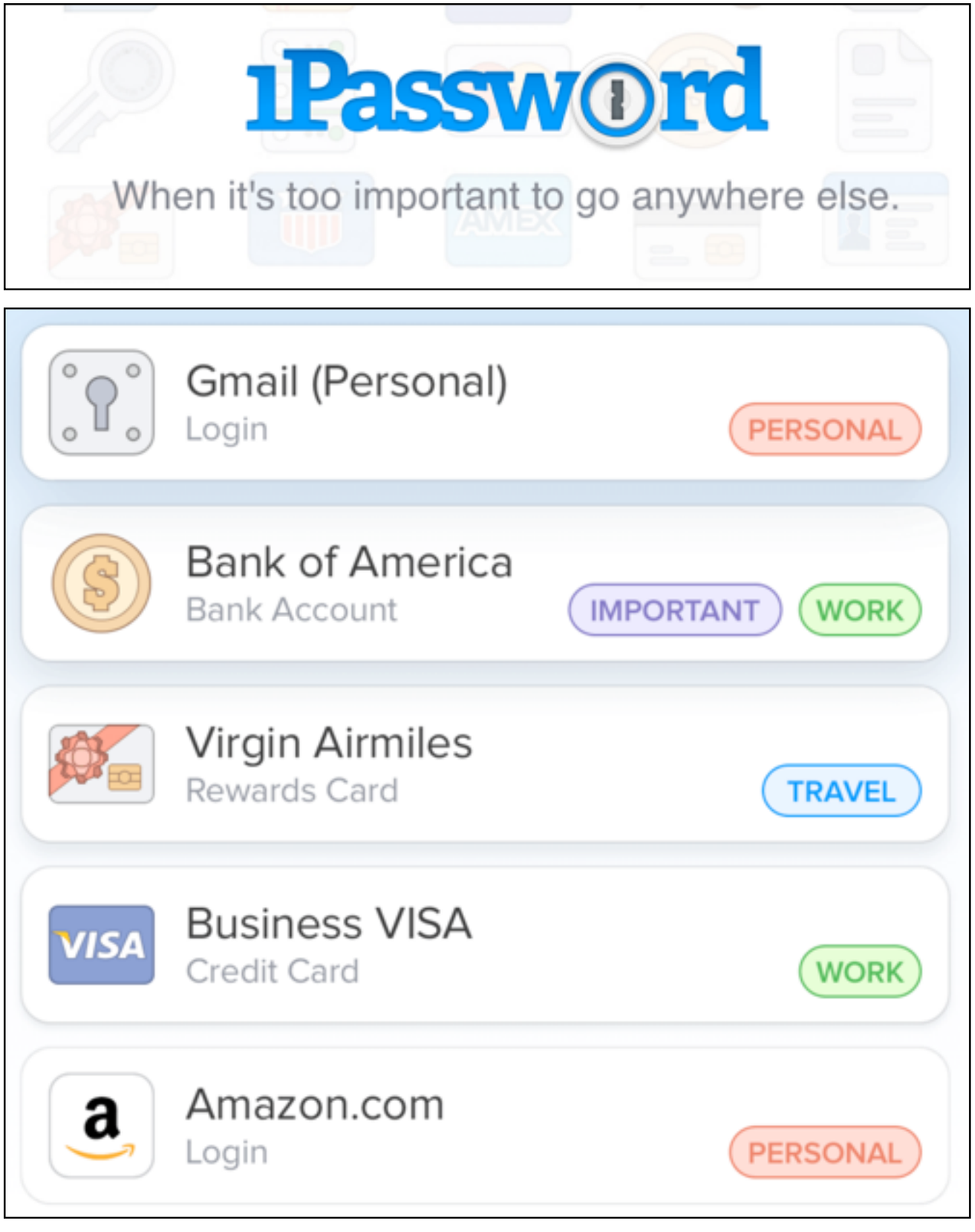
SecureID

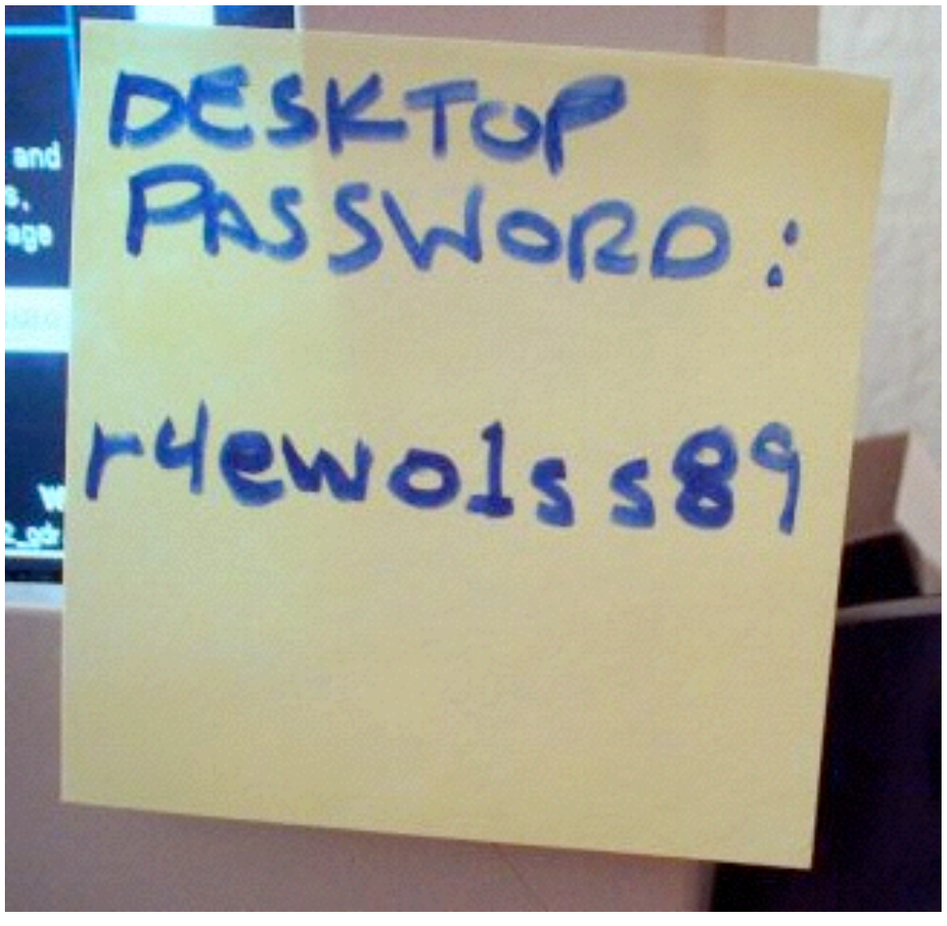
SecureID, from RSA Security, Inc., is one of the most widely used time-based tokens. One version of the product generates the one-time password by using a mathematical function on the time, date, and ID of the token card. Another version of the product requires a PIN to be entered into the token device.



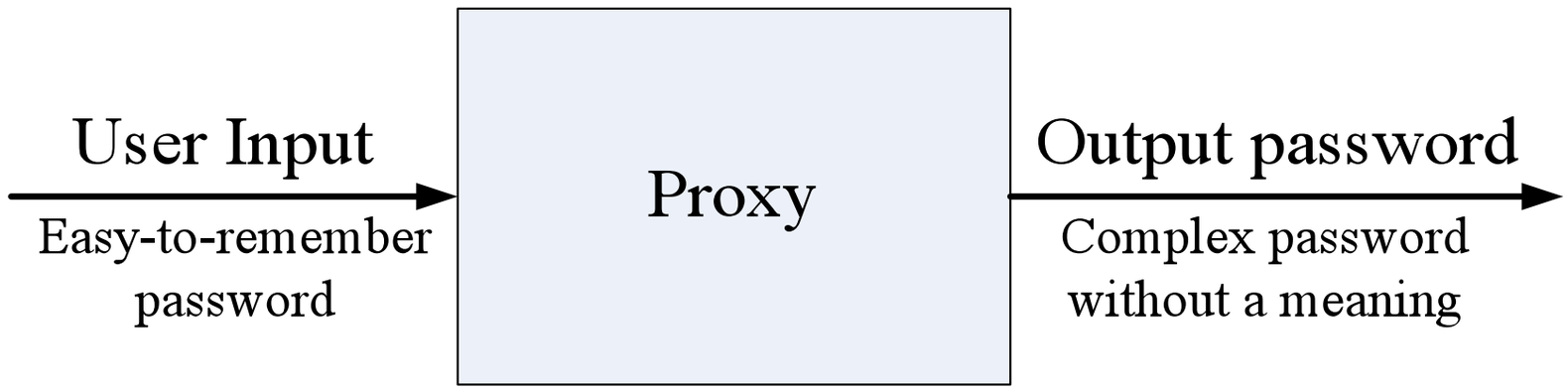
Password
Others

口令管理





口令管理



pu'r'du'e'c's 1仆人毒蛾醋酸 2仆人 3朴 4普 5扑	普熱毒蛾參賽
pu'ren'du'e'cu'suan 1仆人毒蛾醋酸 2仆人 3朴 4普 5扑	僕人毒蛾醋酸
p'r'd'e'cu'suan 1仆人毒蛾醋酸 2骗人 3旁人 4派人 5平日	疲軟的醋酸

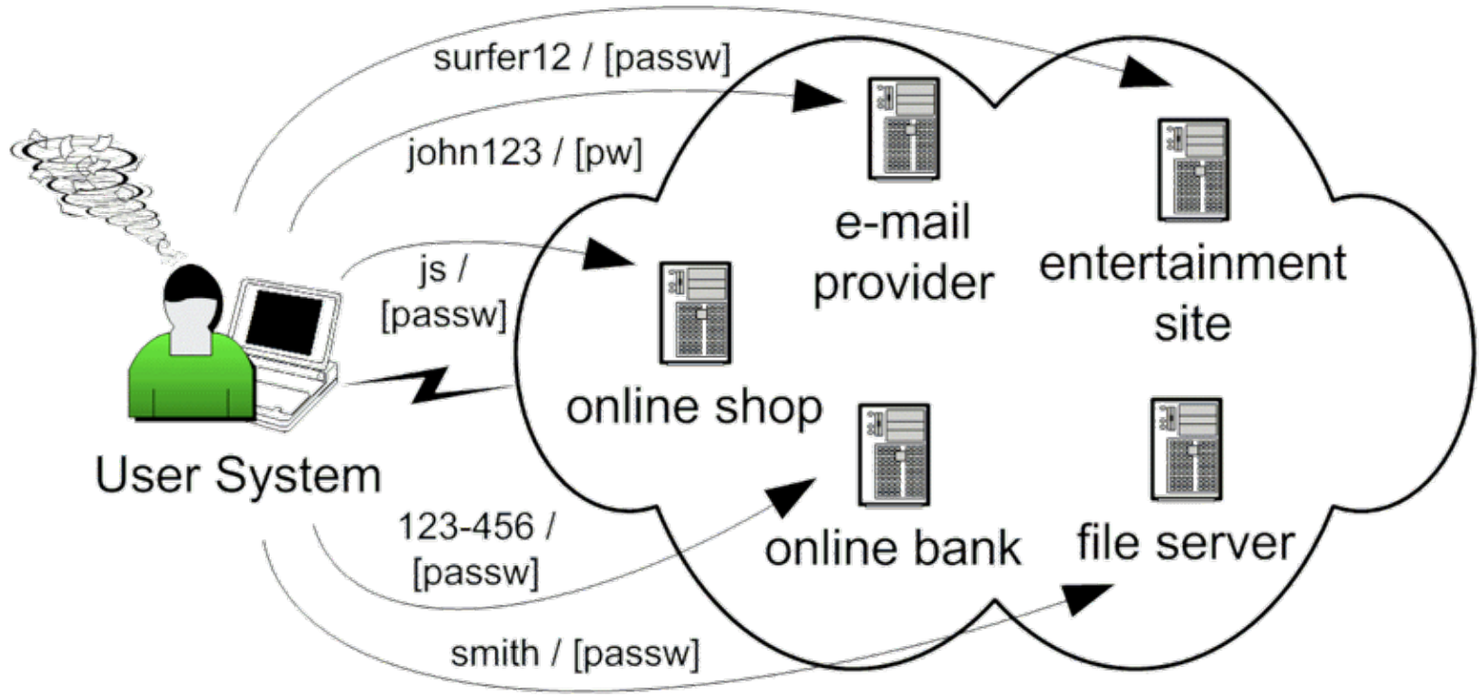
1a 2a
1b 2b
1c 2c

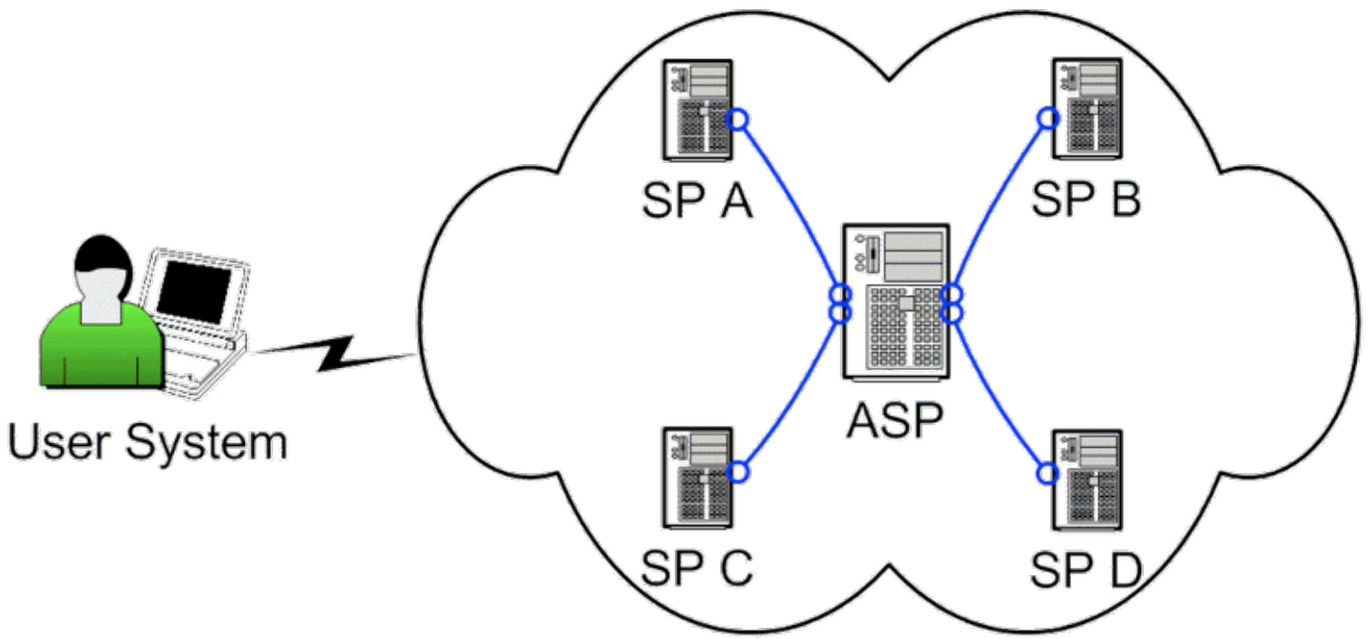
SSO

- ***Single password to all resources, One Password For Everything***

facebook

OpenID

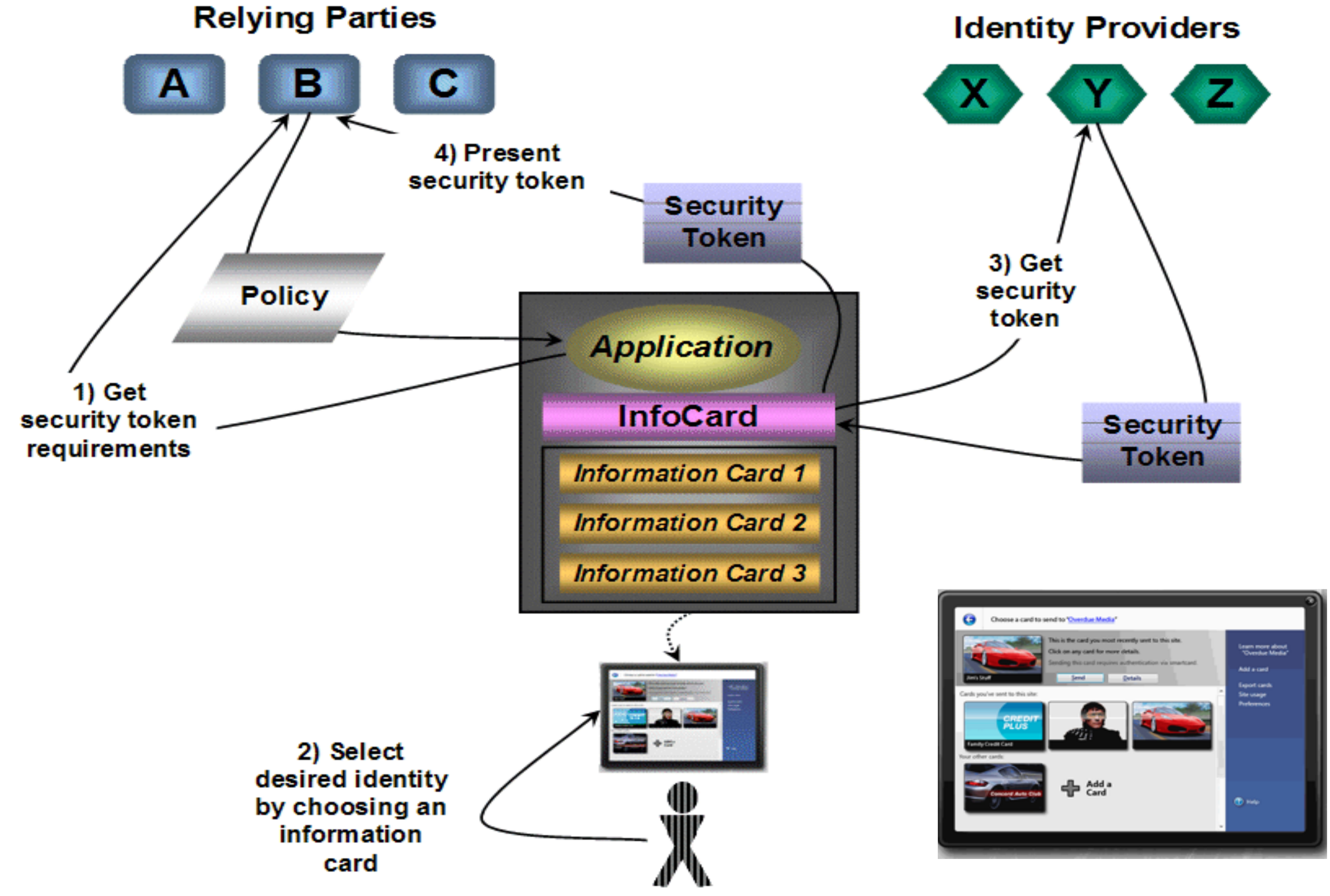




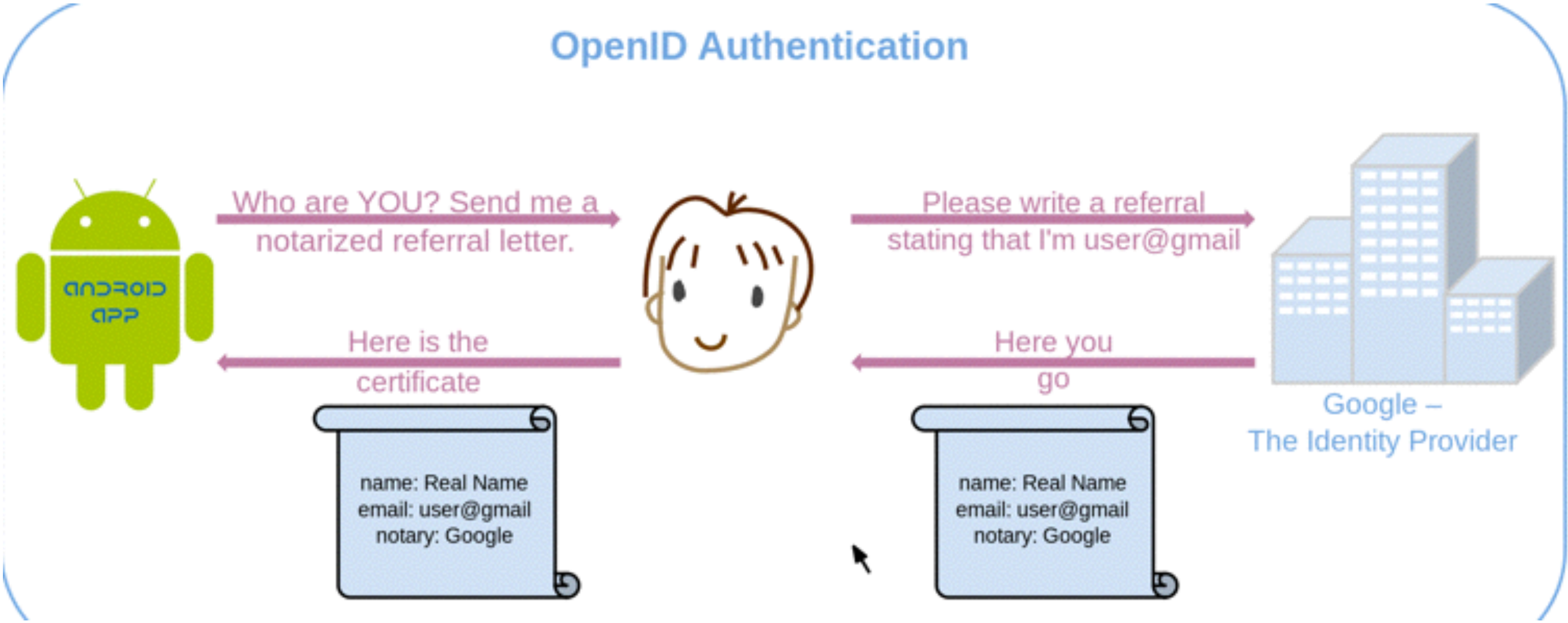
应用集成 性能瓶颈

单点失败 灵活性

CardSpace


Relying Parties
A
B
C
Identity Providers
X
Y
Z
4) Present security token
Security Token
Policy
Application
InfoCard
Information Card 1
Information Card 2
Information Card 3
3) Get security token
1) Get security token requirements
Security Token
2) Select desired identity by choosing an information card
Add a Card

OpenID



OpenID

轻量级IDM、基于URI

OAuth

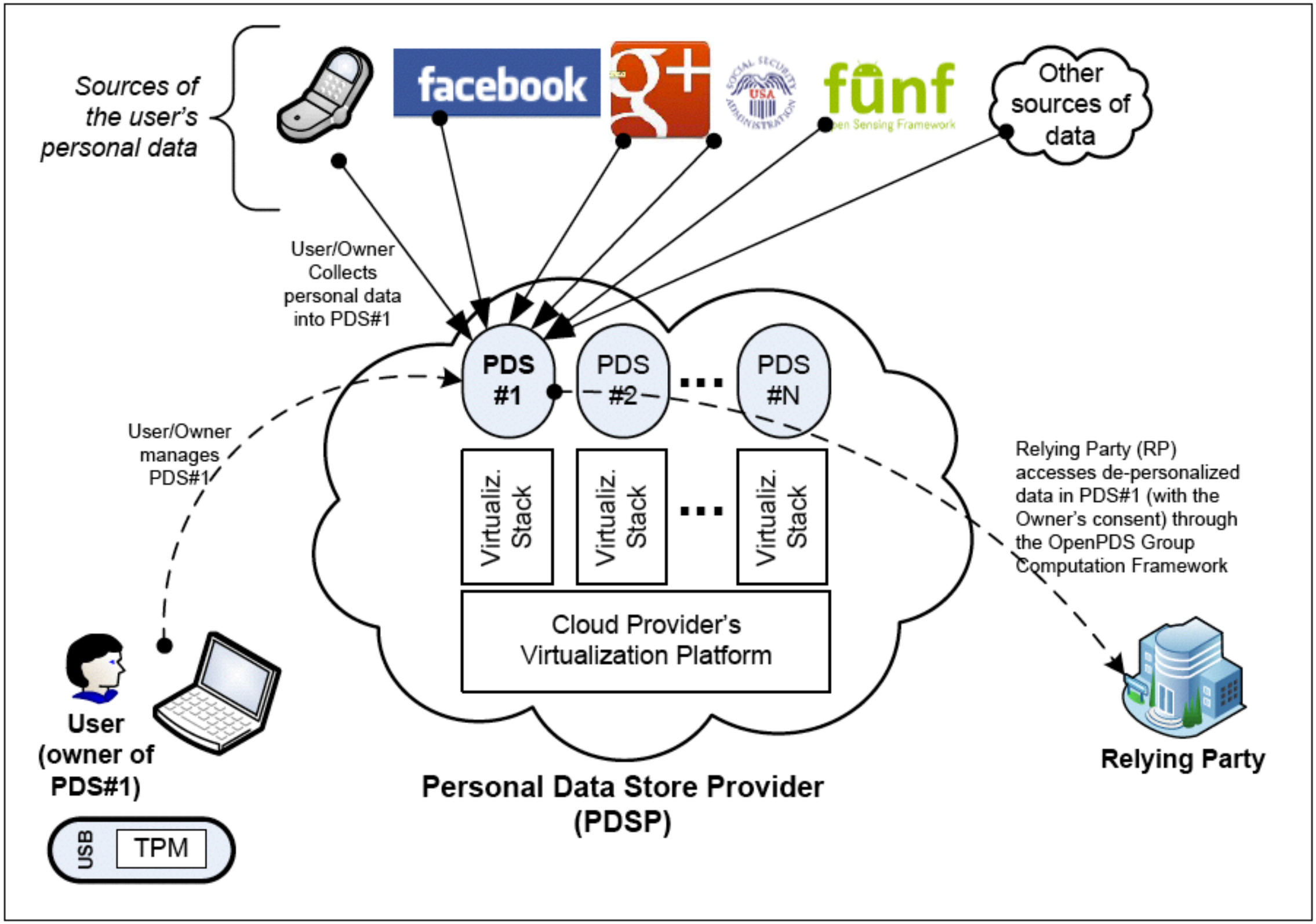
- OAuth是一个开放标准，允许用户让第三方应用访问该用户在某一个网站上存储的私密的资源（如照片、视频、联系人列表），而无须将用户名和密码提供给第三方应用
- Oauth允许用户提供一个令牌，而不是用户名和密码来访问他们存放在特定服务提供者的数据。每一个令牌授权一个特定的网站
- 是OpenID的一个补充

视频编辑网站可以在
接下来的2个小时内
访问我一个目录中的视频

Dropbox
Facebook
Flickr
Google
Instagram
LinkedIn
Microsoft
QQ
PayPal
Salesforce
Sina Weibp
Twitter
Yahoo

Password
Others

OpenPDS



Theory

on Password has lagged practice

口令建议和要求

- *"Since many user-created password are particularly easy to guess, all passwords should be machine-generated"*
- *Users "shall be instructed to use a password selected at random, if possible, or to select one that is not related to their personal identity, history, or environment"*
- *"Pick something you cannot remember, and do not write it down"*
- *Independence when choosing multiple passwords*
- … …

Users are also typically the most difficult component to model

Impossible for human to follow

口令强度

- 口令的理论空间 *vs* 口令的实际空间
- 长度、构成元素、重复、相关性
- 安全性 *vs* 可用性
- 竞争性 *vs* 非竞争性
- 口令*checker vs blacklists*
- *offline vs online attack*
- 口令泄漏
- 三次失败锁定
- 提高强度的代价和收益

Web Authentication as Classification

Authentication as Classification

新的口令模型

- *2000s:* 基于风险的模型，口令作为一个*signal*
- 其余*signal*：*Ip*地址、地理位置、浏览器信息、*cookies*、登录时间、口令输入方式和特征、申请资源
- 认证的结果不是一个*0/1*，而是一个估计值

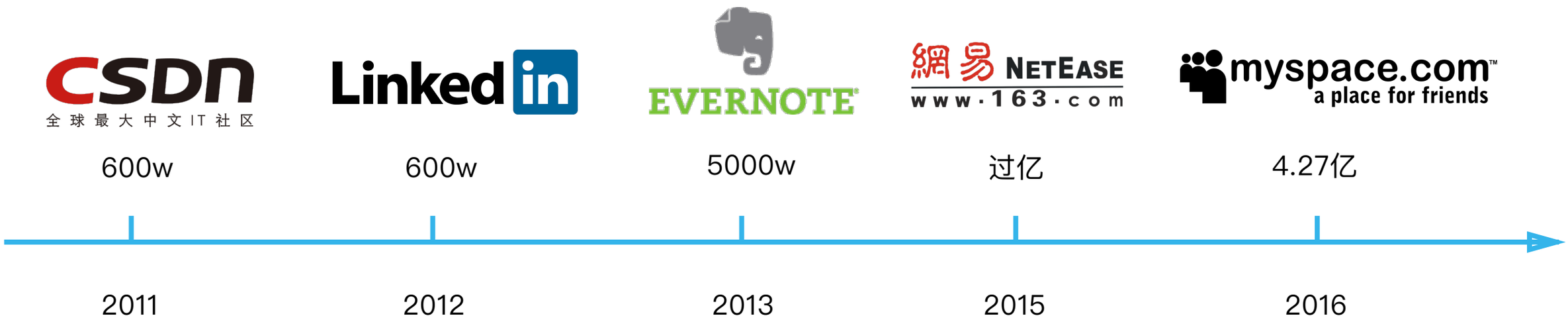
- *Continual authentication*
- *Multilevel authentication*
- *Progressive authentication*

- *winner-take-all*
- *two sided market*

- 错误接受率 *vs* 错误拒绝率
- 训练数据的获取
- 更多的用户数据，隐私
- 用户的困惑和抱怨
- 共享口令

Password Leakage

口令泄漏



Traditional Salt Hash

Username	PassSalt	HashPwd
Username1	PassSalt1	HashPwd1
username2	PassSalt2	HashPwd2
.....	.....	.....
Username(i)	PassSalt(i)	HashPwd(i)
.....	.....	.....
Username(n)	PassSalt(n)	HashPwd(n)

字典攻击

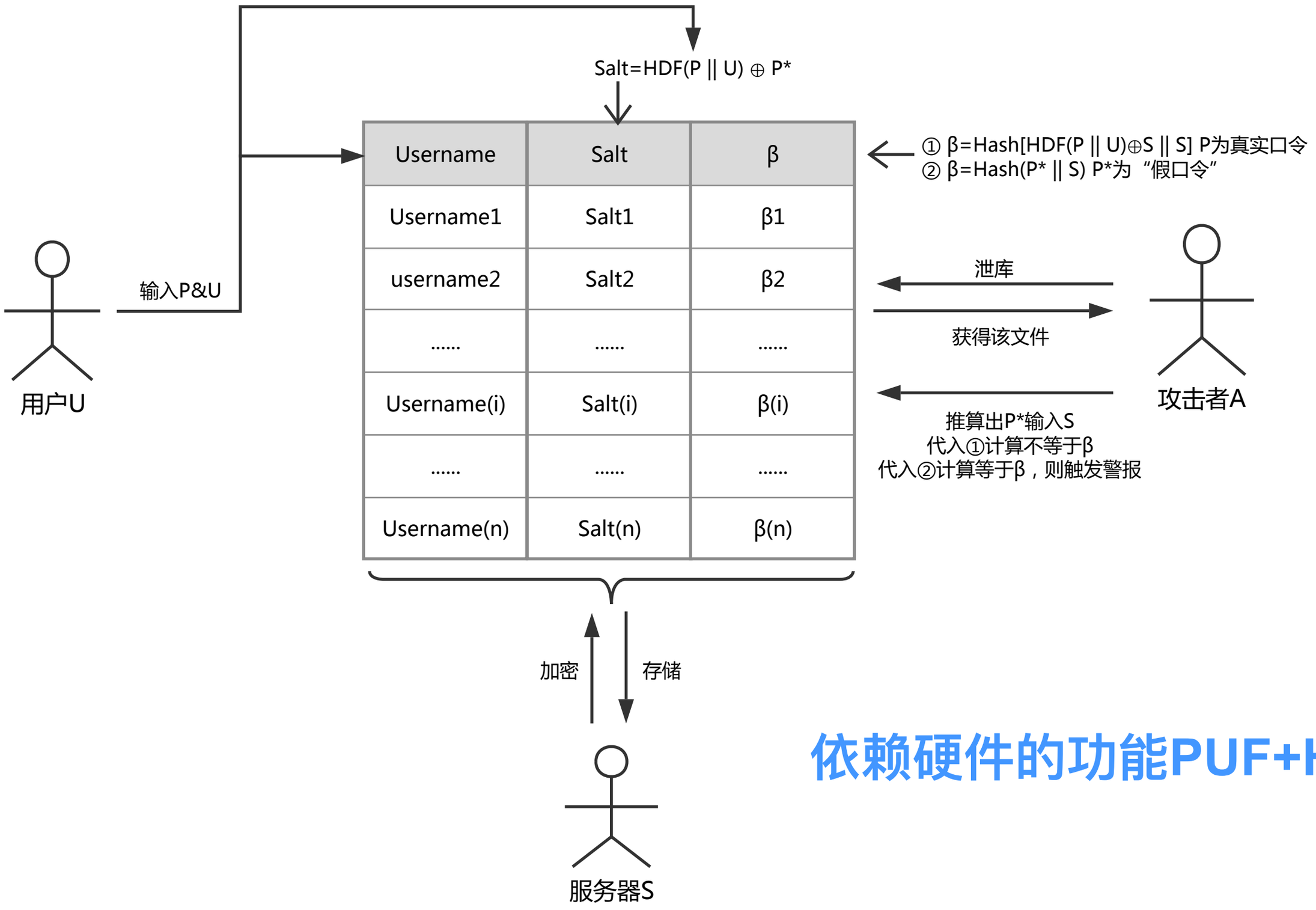
Index	Plain Text		Hash	Index
7210	Effluvium		er4345dg	7210
7211	Effort	Hash	e1qqw3	7211
7212	Effusive		edf234	7212
7213	Eft		jkl244	7213
7214	egalitarian		fgt24	7214

Jdoe:345et:16:24:Cathy Roe:/home/croe:/bin/csh
Stewart:edf234:16:24:Mark Stewart:/home/stewart:/bin/csh
Andy:wer345t:16:24:Andy O Ram:/home/andy:/bin/csh

password1	abc123	myspace1	password
Blink182	**qwerty1**	fuckyou	123abc
baseball1	football1	123456	soccer
monkey1	liverpool1	princess1	**jordan23**
slipknot1	superman1	iloveyou1	**monkey**

Password Leakage

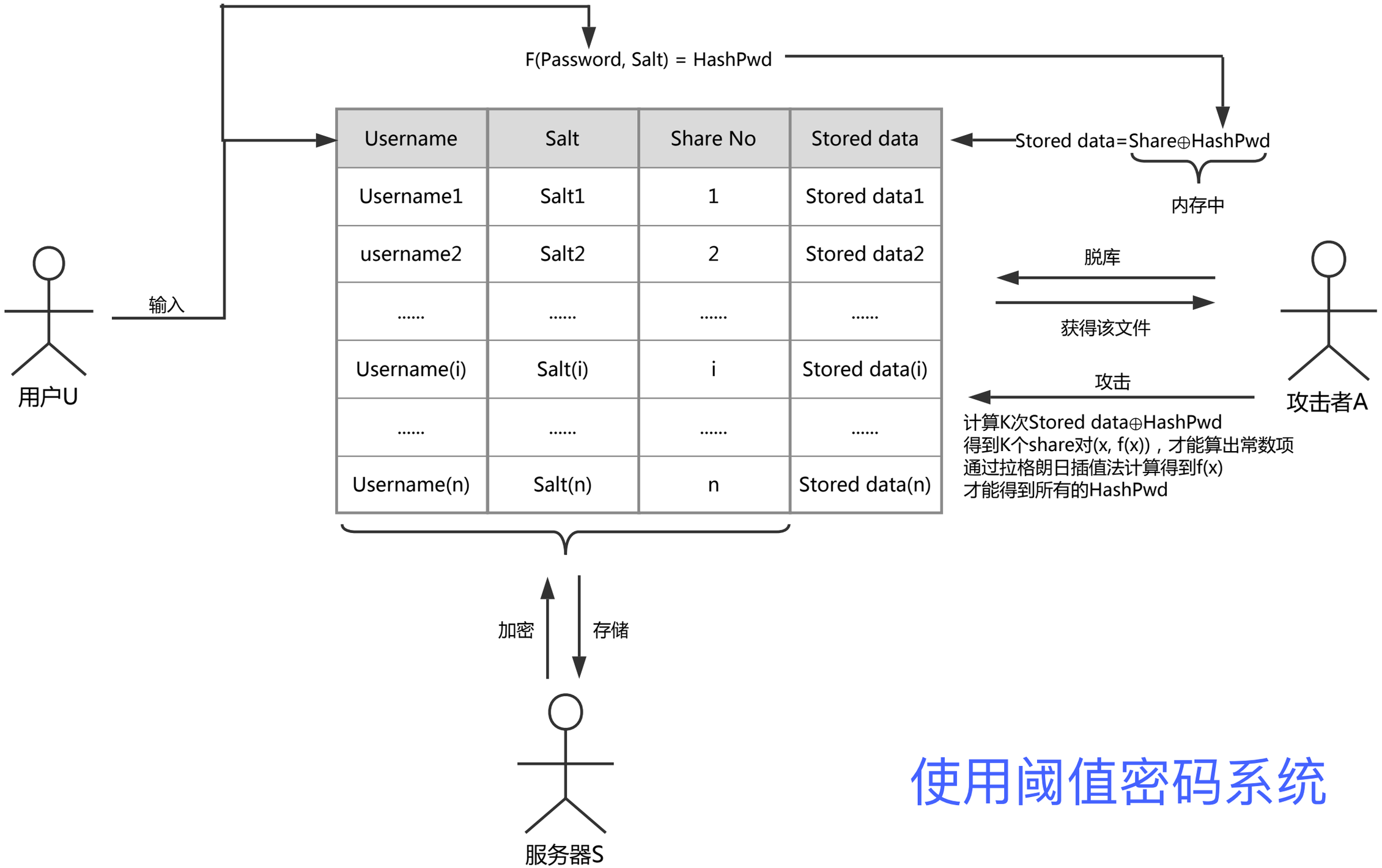
ErsatzPasswords



依赖硬件的功能PUF+HSM

Password Leakage

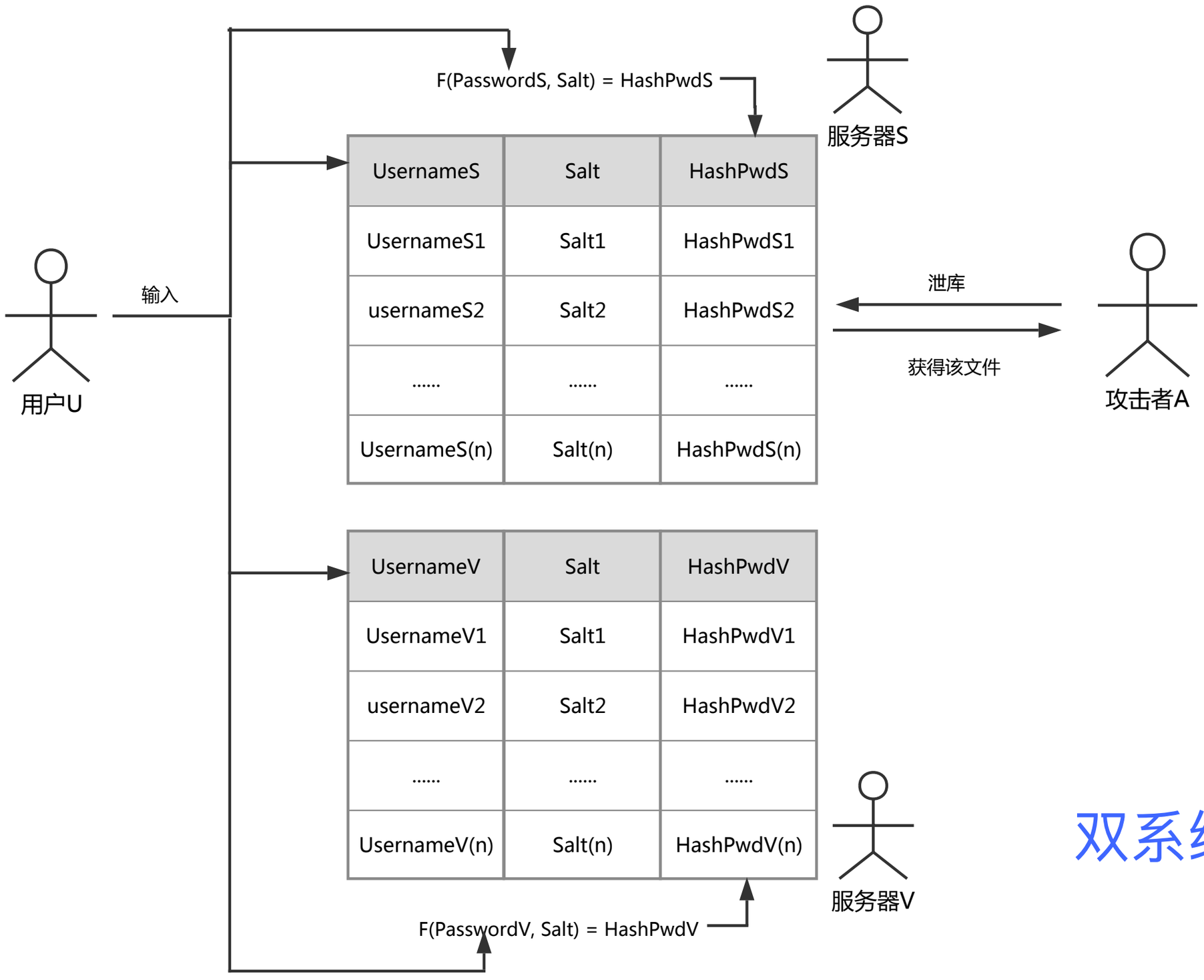
PolyPassHash



使用阈值密码系统

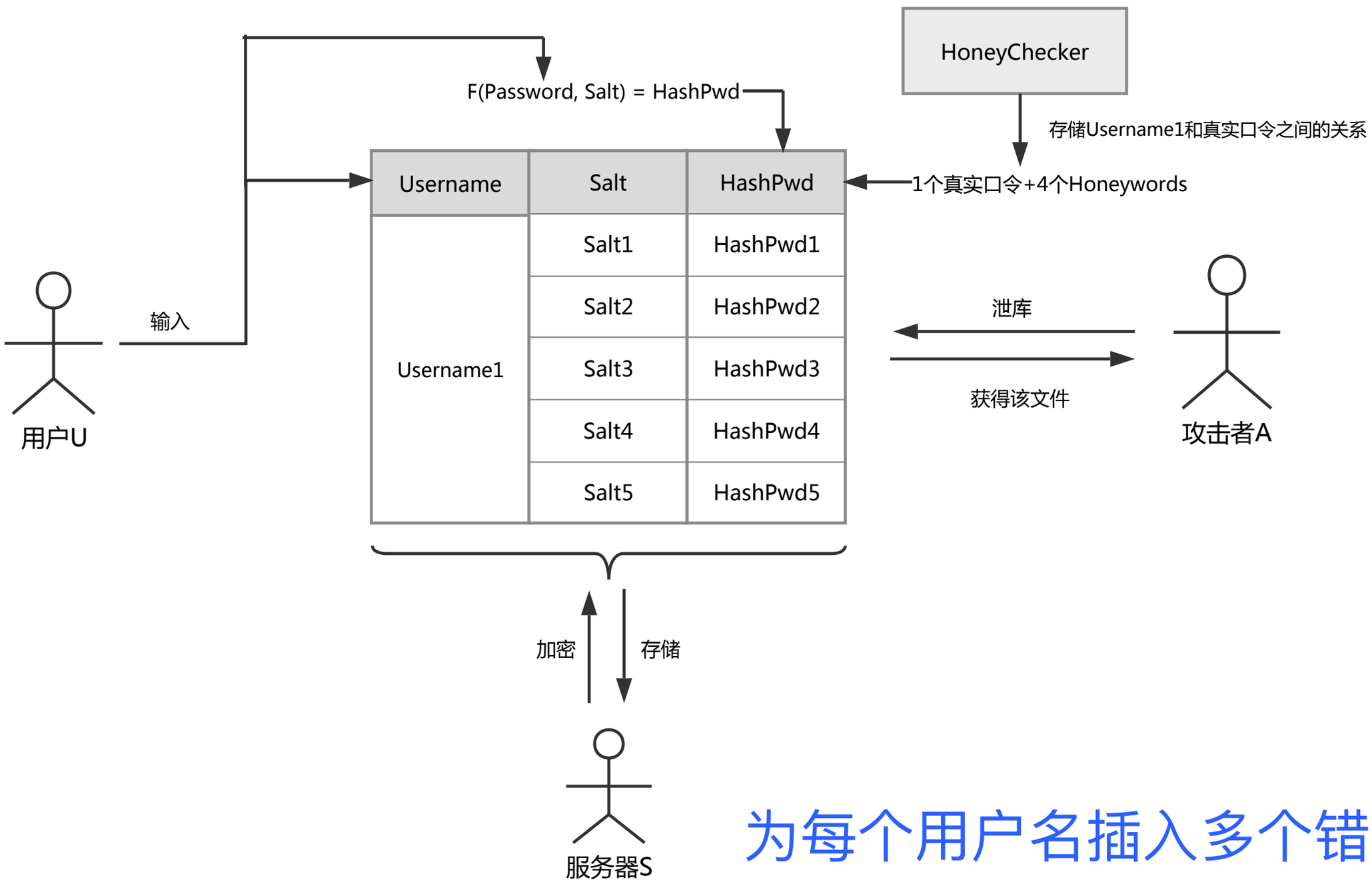
Password Leakage

SAuth



双系统双口令认证

Honeywords



为每个用户名插入多个错误的口令

Homework 课后作业

- 要求阅读如下论文：

➡ *Ari Juels et al. Honeywords: Making Password-Cracking Detectable. In Proc. CCS'2013.*

要求看： *Introduction*、 *Technical Description*、 *Related Work*、 *Open Problems*、 *Discussion and Conclusion*

下次上课测试！

谢谢！

孙惠平

sunhp@ss.pku.edu.cn