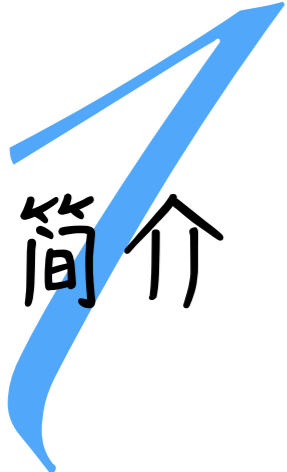


文本口令



图形口令回顾



简介



分类



PassApp



评价

- 心理学
- Deja Vu
- PassGo
- 代表产品

- 回忆-DAS
- 识别
- 线索回忆
- PassPoints

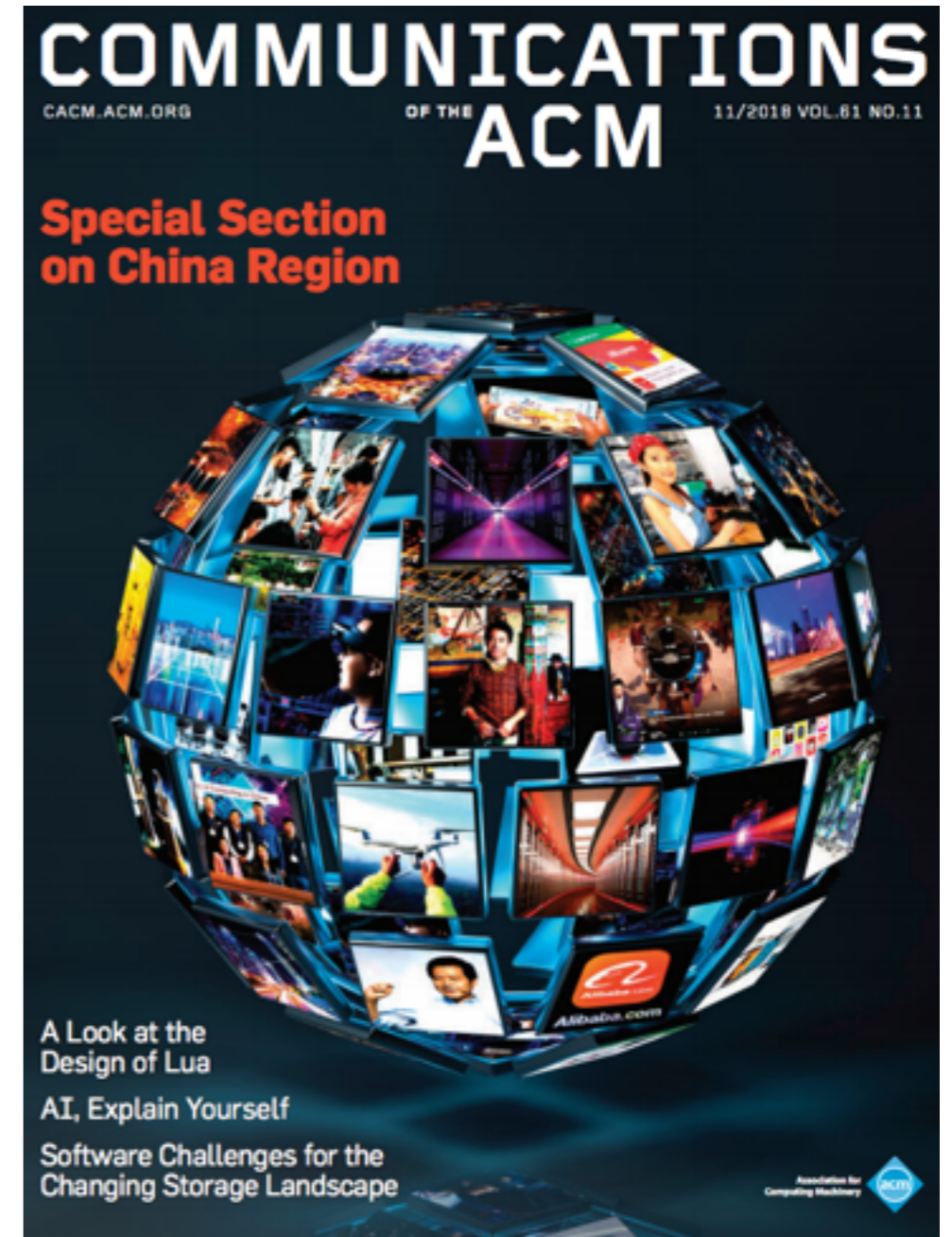
- 自传体认证
- 概念&机制
- 可用性
- 安全性

- 用户&环境
- 可用性
- 安全性
- 评估方法

本次课程内容

- 身份认证简介
- 文本口令简介
- 其余候选机制
- 理论 vs. 实践
- 防止口令泄露

<https://cacm.acm.org/>

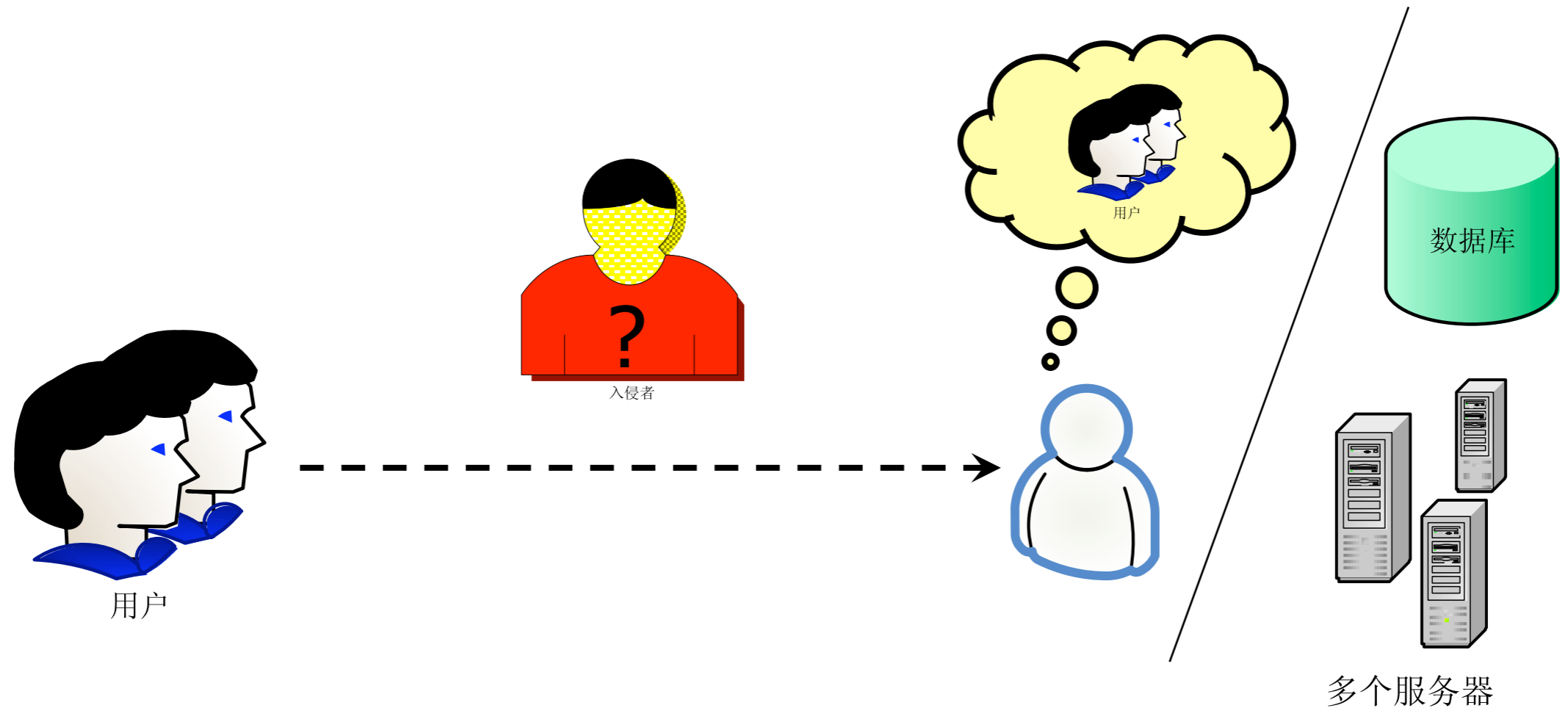


Theory on passwords has lagged practice, where large providers use back-end smarts to survive with imperfect technology.

BY JOSEPH BONNEAU, CORMAC HERLEY, PAUL C. VAN OORSCHOT, AND FRANK STAJANO

Passwords and the Evolution of Imperfect Authentication

身份认证简介



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

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

文本命令简介

- 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

- 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



56年

1960

MIT
CTSS

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

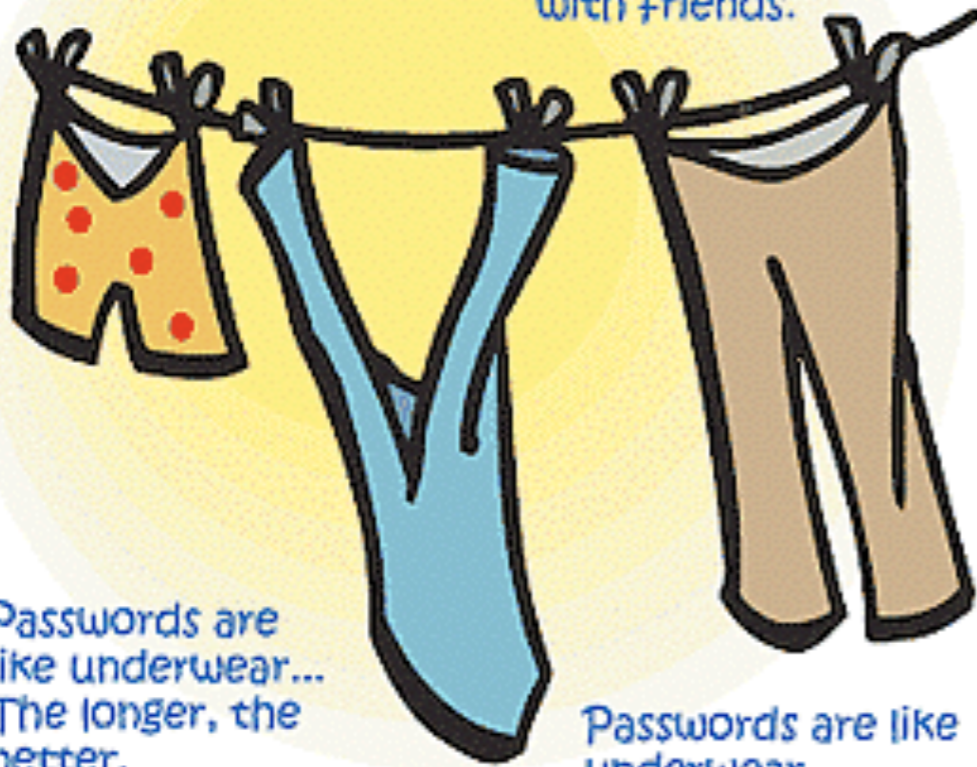


- *passphrase*、
passcode、*personal identification number*、
watchword、*access word*

Passwords Are Like Underwear

Passwords are like underwear...
Change yours often.

Passwords are like underwear...
Don't share them
with friends.



Passwords are like underwear...
The longer, the
better.

Passwords are like
underwear...
Be mysterious.

Passwords are like
underwear...
Don't leave yours
lying around.

©2001 Hallmark Licensing, Inc./Dist. by Universal Press Syndicate

I forgot the password for
the file where I keep all my
passwords.



- 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?

- 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”



VIDEOS

CXO

WINDOWS 10

CLOUD

INNOVATION

SECURITY

APP

MUST READ [SAMSUNG CUTS PROFIT FORECAST BY \\$2.3 BILLION AFTER GALAXY NOTE 7 SAGA](#)

Gates: The password is dead

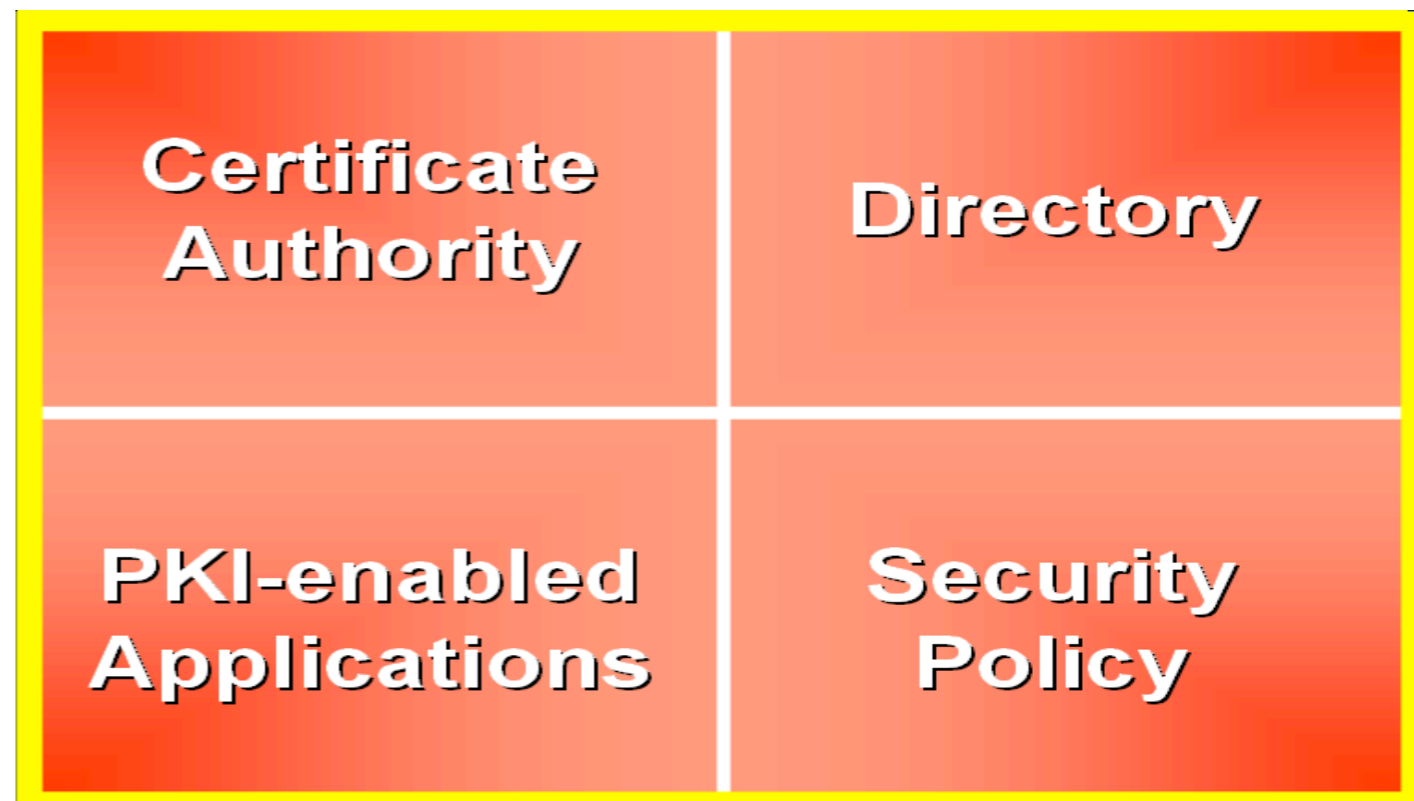
Smart cards and 64-bit are the future says Microsoft chief...

其余候选机制

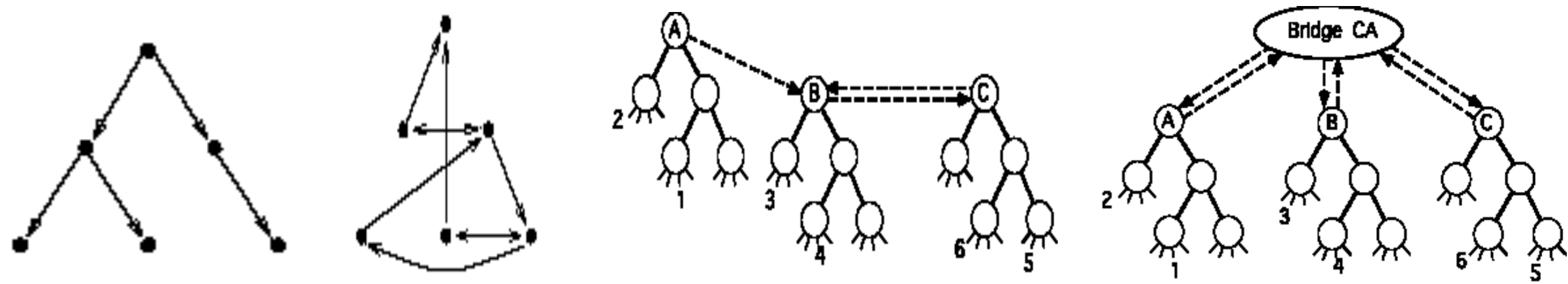
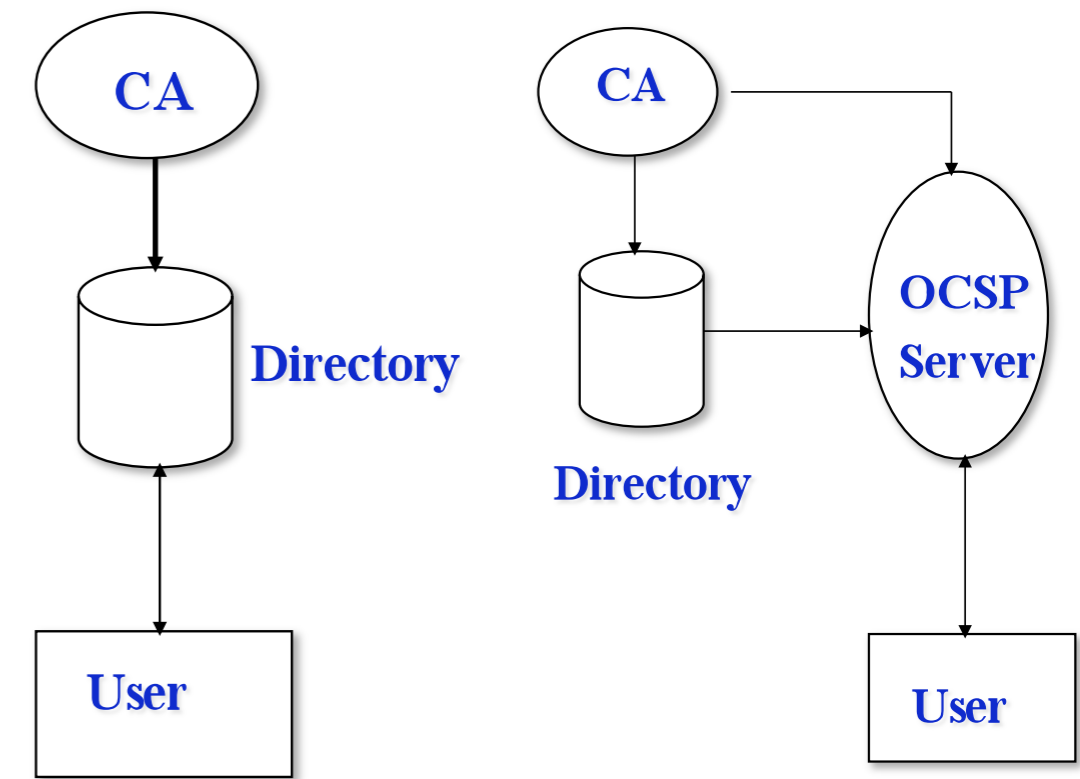
- 一系列基于**公钥密码学**之上，用来创建、管理、存储、分布和作废**证书**的软件、硬件、人员、策略和过程的**集合**。

-
- 基础：公钥密码学
 - 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**

mid-1990s

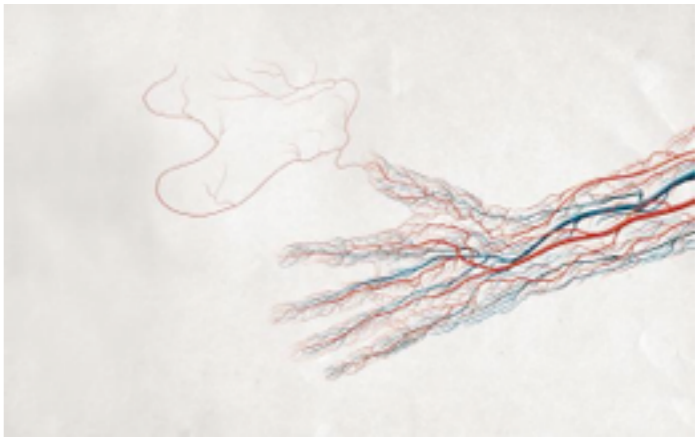
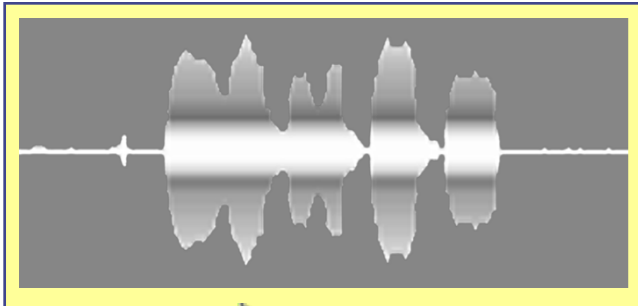
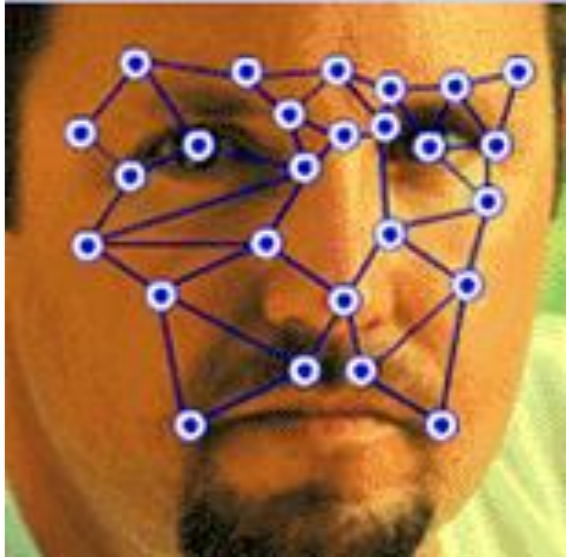
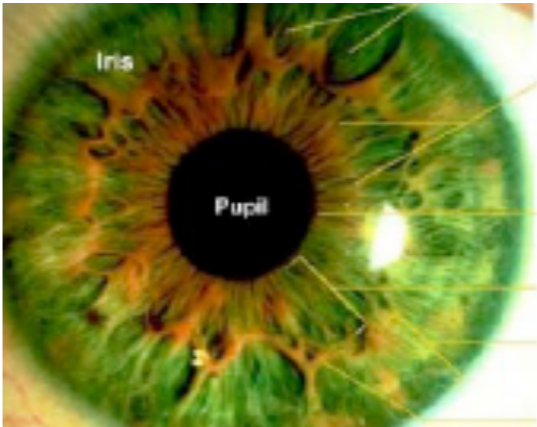
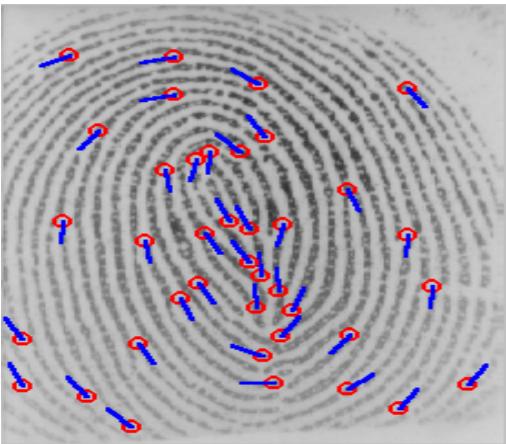


- 需要预先知道对方的公钥、需要在线服务器的支持
- 引入证书、引入可信第三方
- 密钥管理、证书管理
- 信任问题、规模问题
- 性能问题、互联互通问题



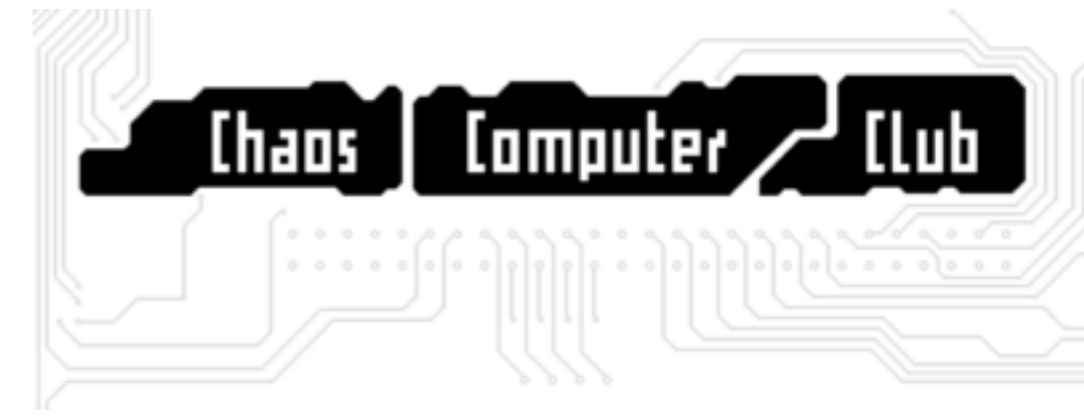
Password is Dead

Biometrics



Password is Dead

攻击指纹



Password

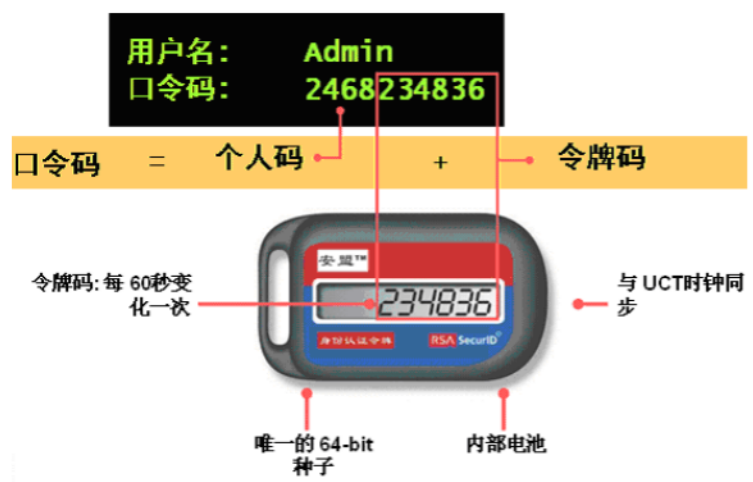
is

Imperfect

But

OTP: One Time Password

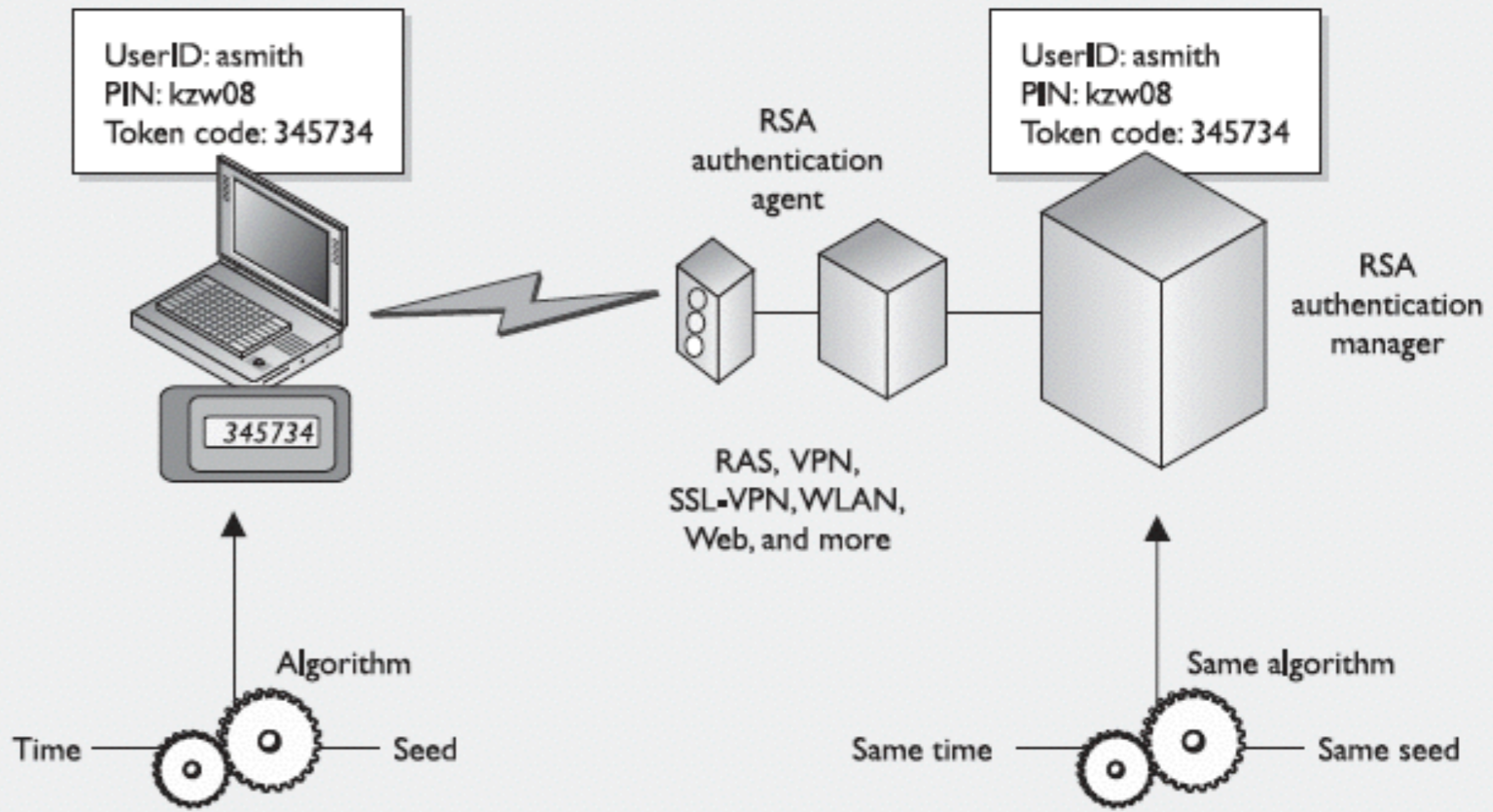
一次性(动态)口令。
是由电子令牌(Token)
等手持终端设备生成的，根据某种加密算法，产生的随某一个不断变化的参数(例如时间，事件等)不停地、没有重复变化的一种口令。



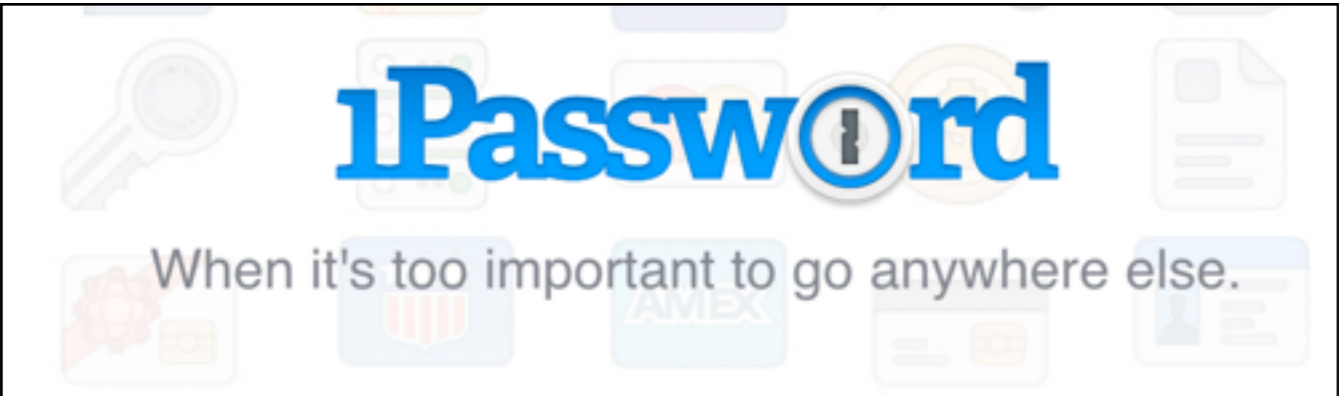
SecureID

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.

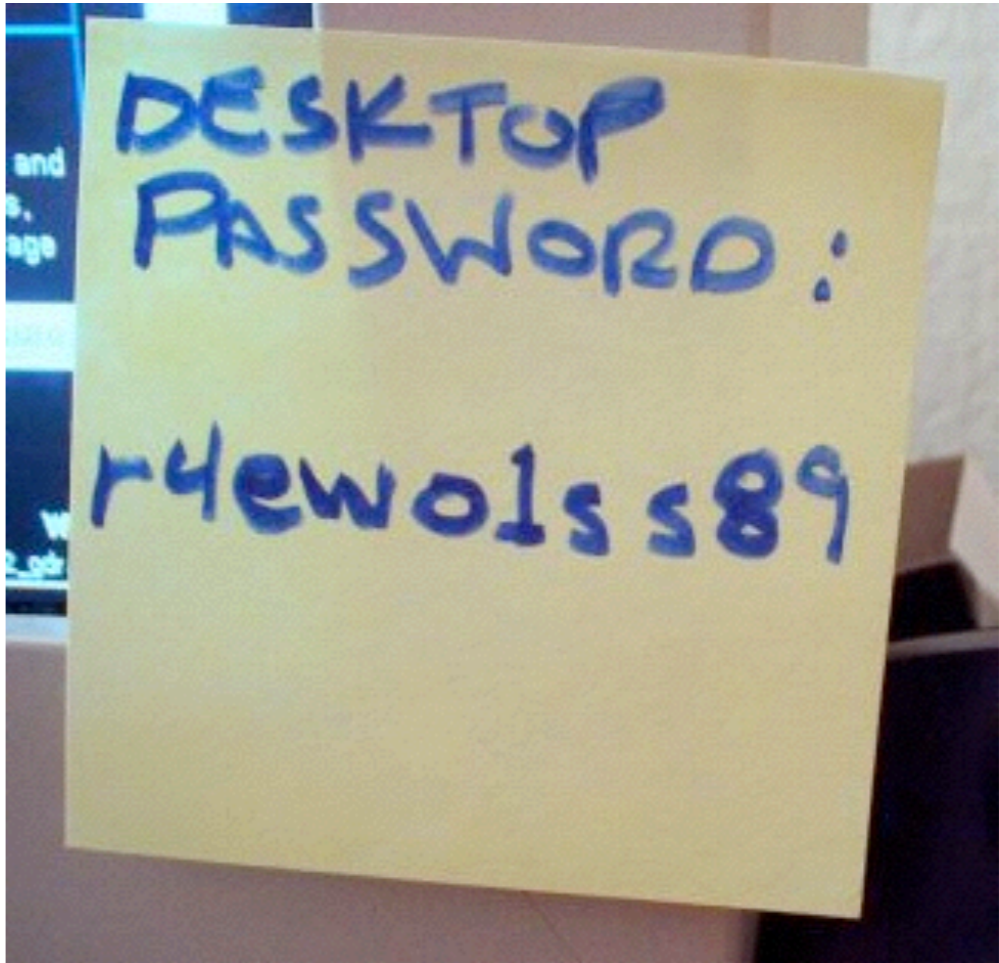
RSA SECURID TIME-SYNCHRONOUS TWO-FACTOR AUTHENTICATION



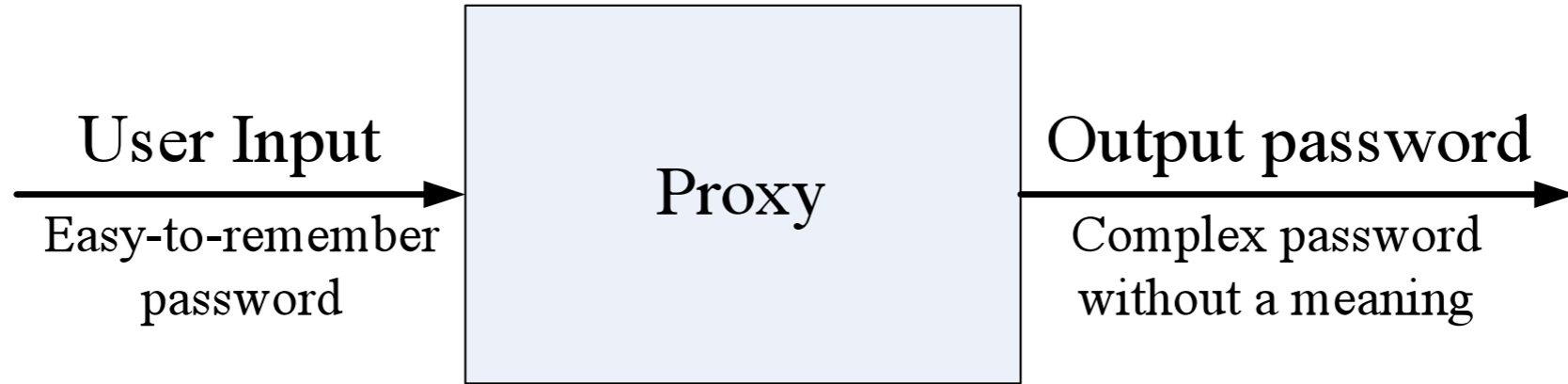
Used by permission of RSA Security, Inc., © Copyright RSA Security, Inc. 2004



- Gmail (Personal)**
Login PERSONAL
- Bank of America**
Bank Account IMPORTANT WORK
- Virgin Airmiles**
Rewards Card TRAVEL
- Business VISA**
Credit Card WORK
- Amazon.com**
Login PERSONAL



口令管理



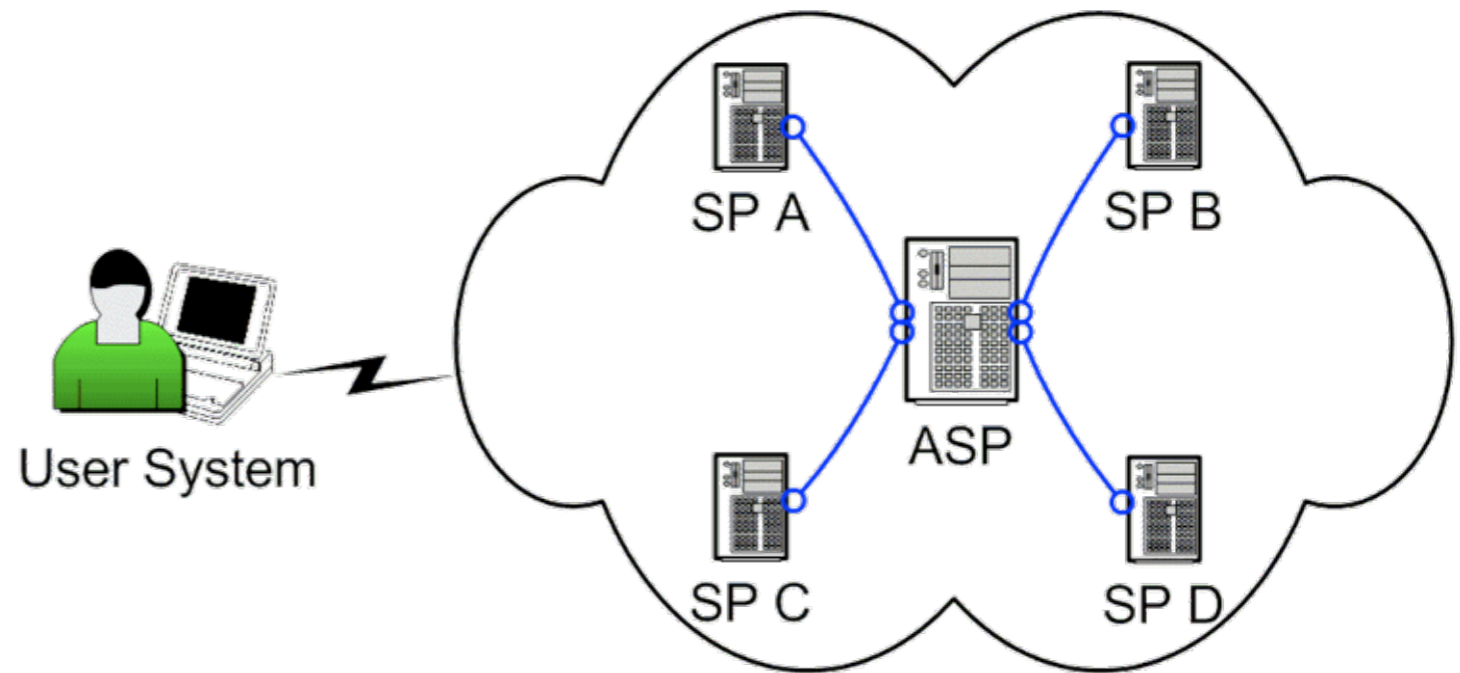
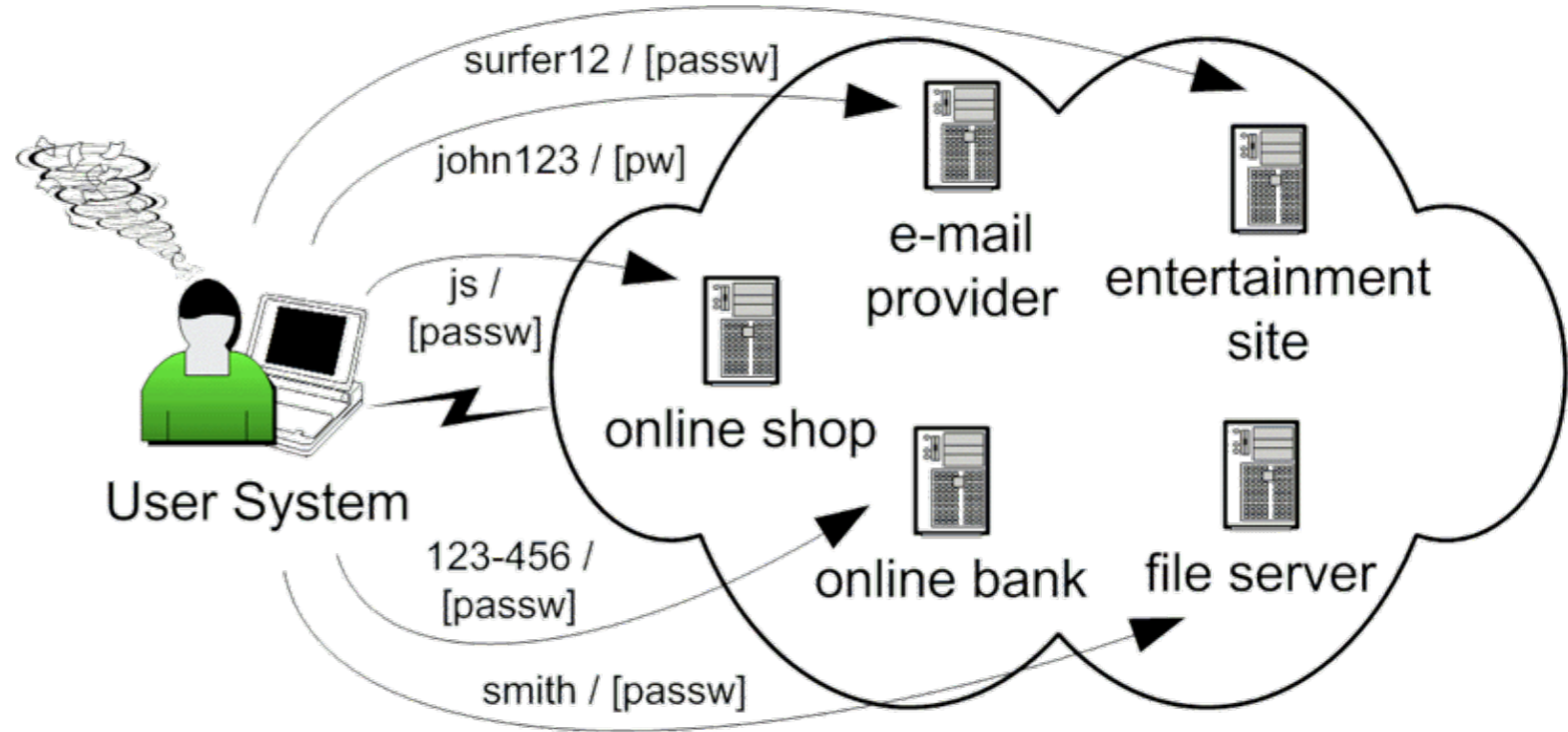
<p>pu'r'du'e'c's </p> <p>1 仆 人 毒 蛾 醋 酸 2 仆 人 3 朴 4 普 5 扑</p>	<p> 普 熱 毒 蛾 參 賽 </p>
<p>pu'ren'du'e'cu'suan </p> <p>1 仆 人 毒 蛾 醋 酸 2 仆 人 3 朴 4 普 5 扑</p>	<p> 僕 人 毒 蛾 醋 酸 </p>
<p>p'r'd'e'cu'suan </p> <p>1 仆 人 毒 蛾 醋 酸 2 騙 人 3 旁 人 4 派 人 5 平 日</p>	<p> 疲 軟 的 醋 酸 </p>

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

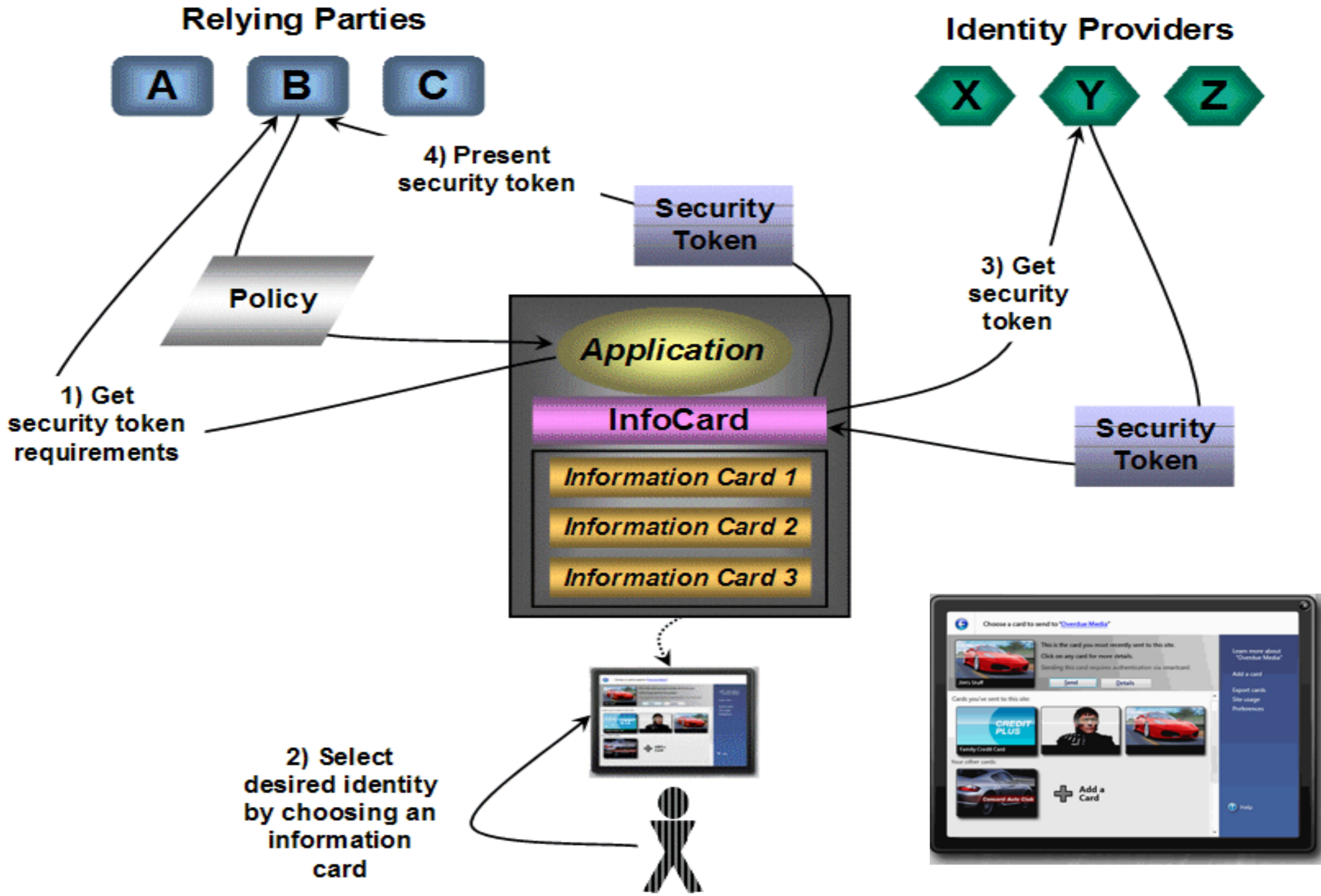
- **Single password to all resources, One Password For Everything**



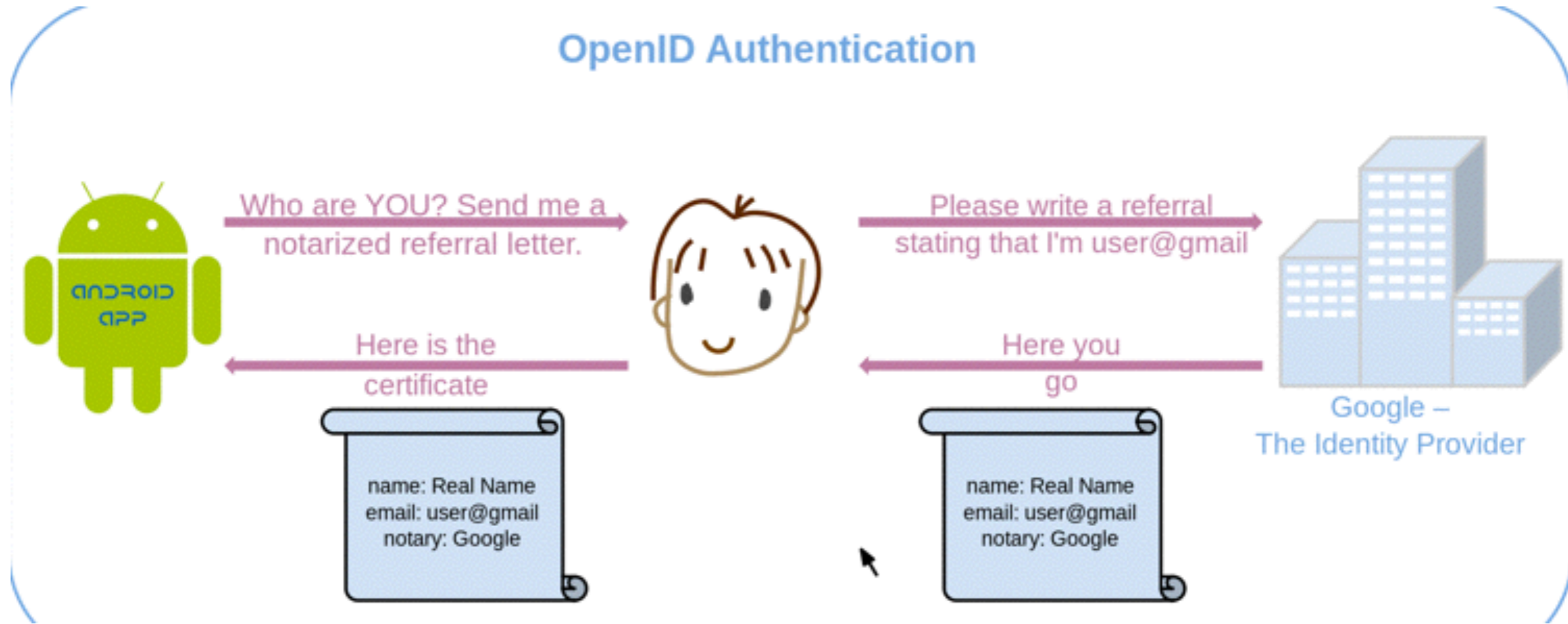
应用集成 性能瓶颈
单点失败 灵活性



CardSpace



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

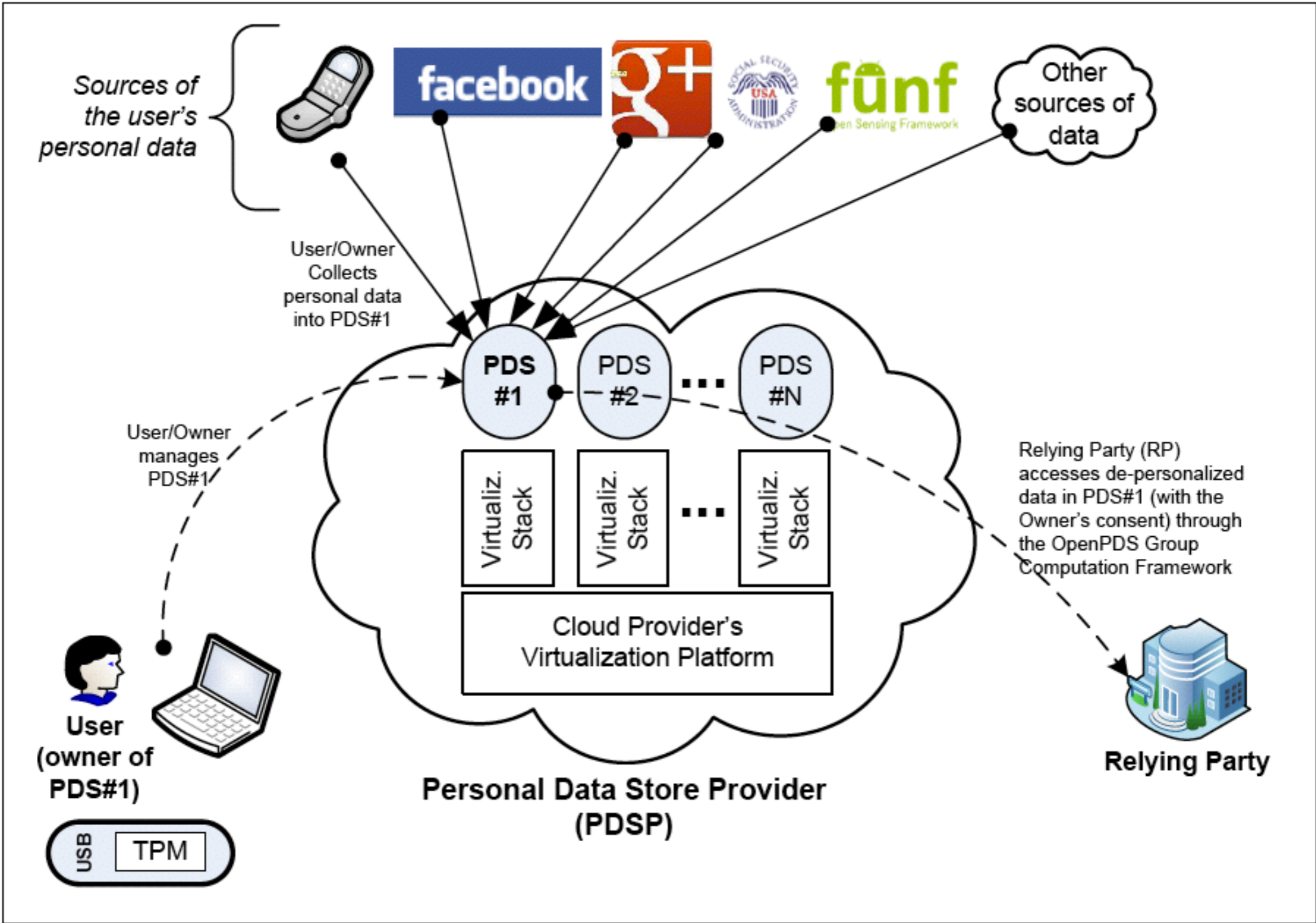


视频编辑网站可以在
接下来的2个小时内
访问我一个目录中的视频

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

Password
Others

OpenPDS



理论 vs. 实践

Theory

on Password has lagged

practice

- “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

- 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

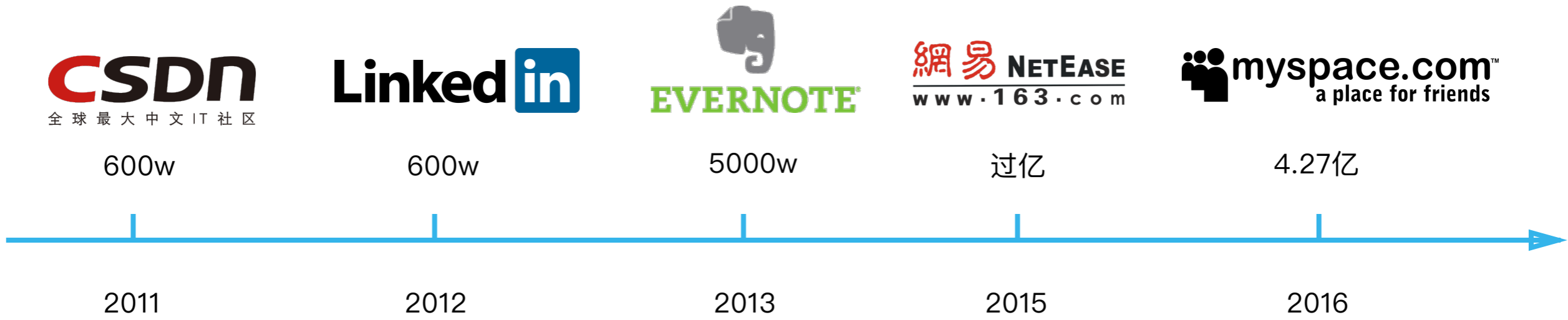
-
- *Continual authentication*
 - *Multilevel authentication*
 - *Progressive authentication*

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

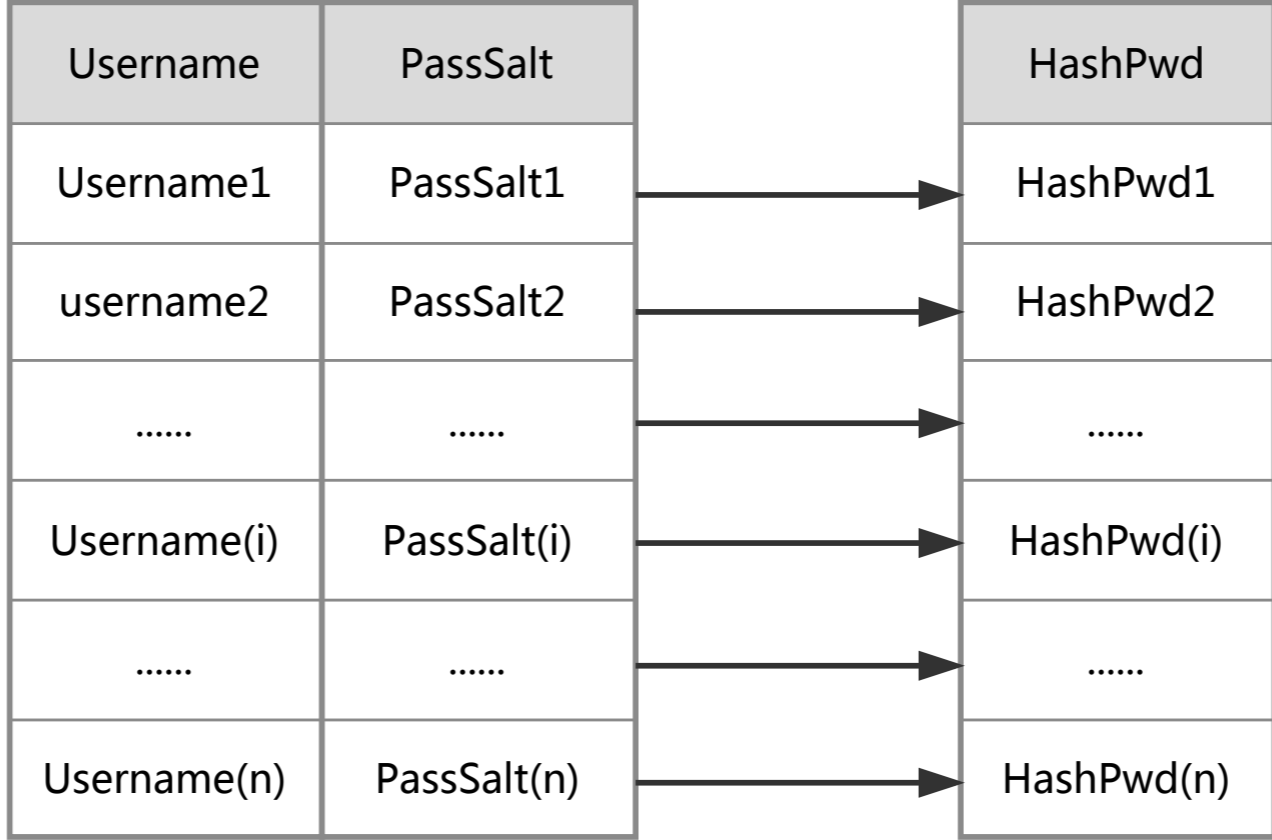
- 错误接受率 vs 错误拒绝率
- 训练数据的获取
- 更多的用户数据, 隐私
- 用户的困惑和抱怨
- 共享口令

防止口令泄露

口令泄漏



Traditional Salt Hash



Password Leakage

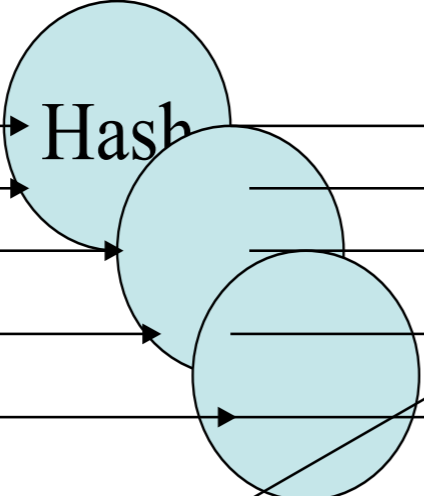
字典攻击

Index

Plain Text

7210
7211
7212
7213
7214

Effluvium
Effort
Effusive
Eft
egalitarian



Hash

er4345dg
e1aqw3
edf234
jkl244
fgt24

Index

7210
7211
7212
7213
7214

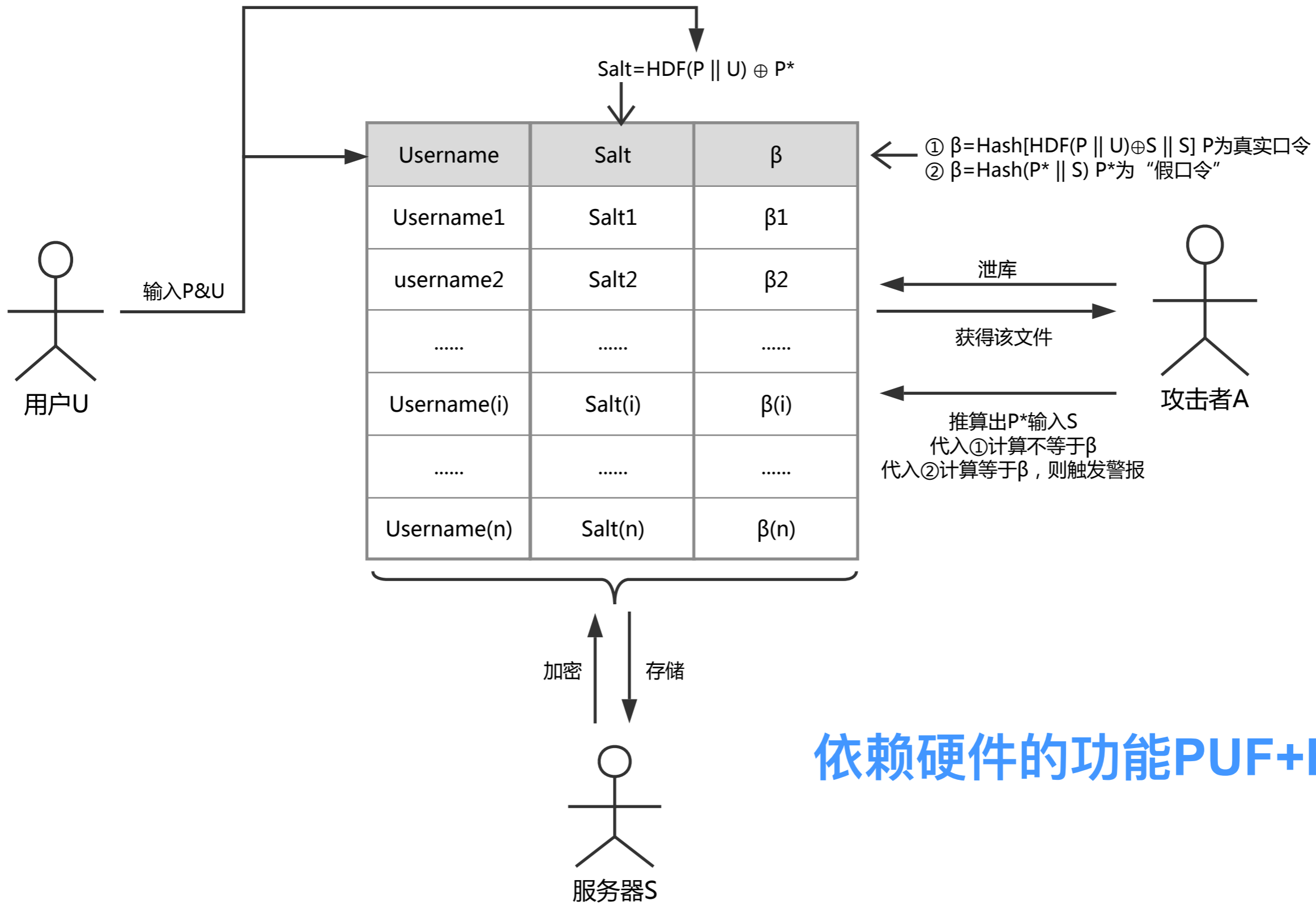
Jdoe:345ert:16:24:Cathy Roe:/home/croe:/bin/csh
Stewart:**edf234**:16:24:Mark Stewart:/home/stewart:/bin/csh
Andy:wer345t:16:24:Andy O Ram:/home/andy:/bin/csh



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

Password Leakage

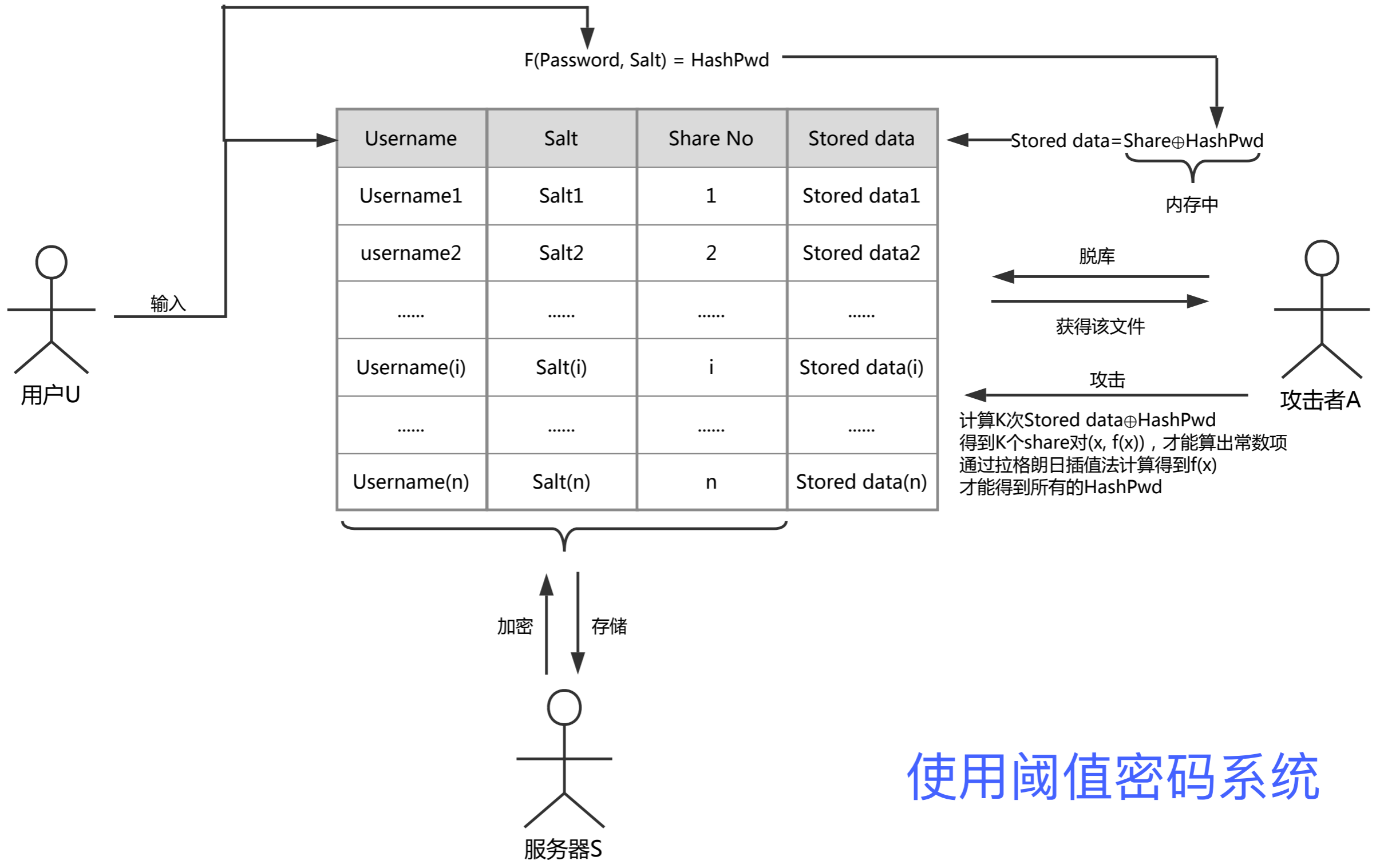
ErsatzPasswords



依赖硬件的功能 PUF+HSM

Password Leakage

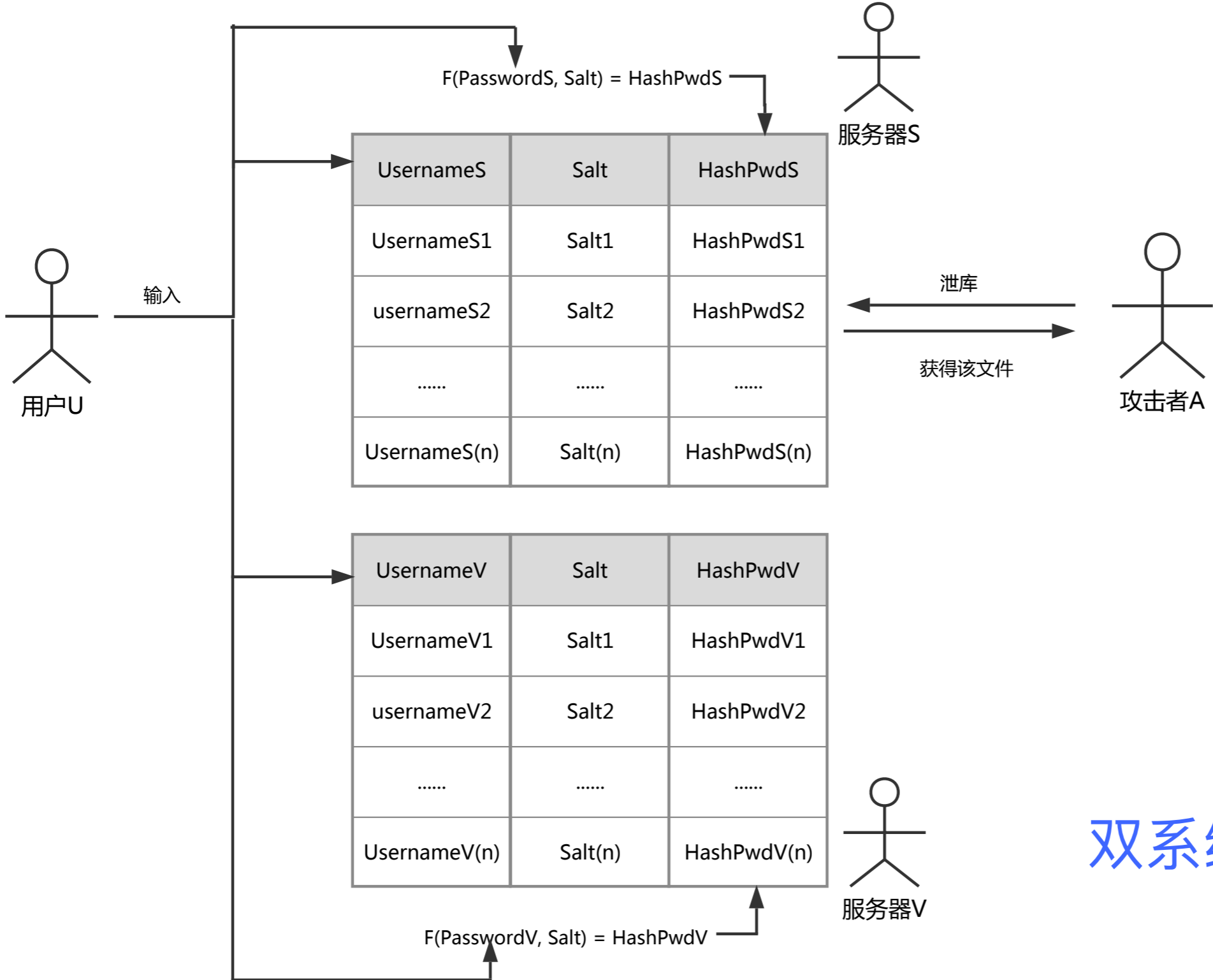
PolyPassHash



使用阈值密码系统

Password Leakage

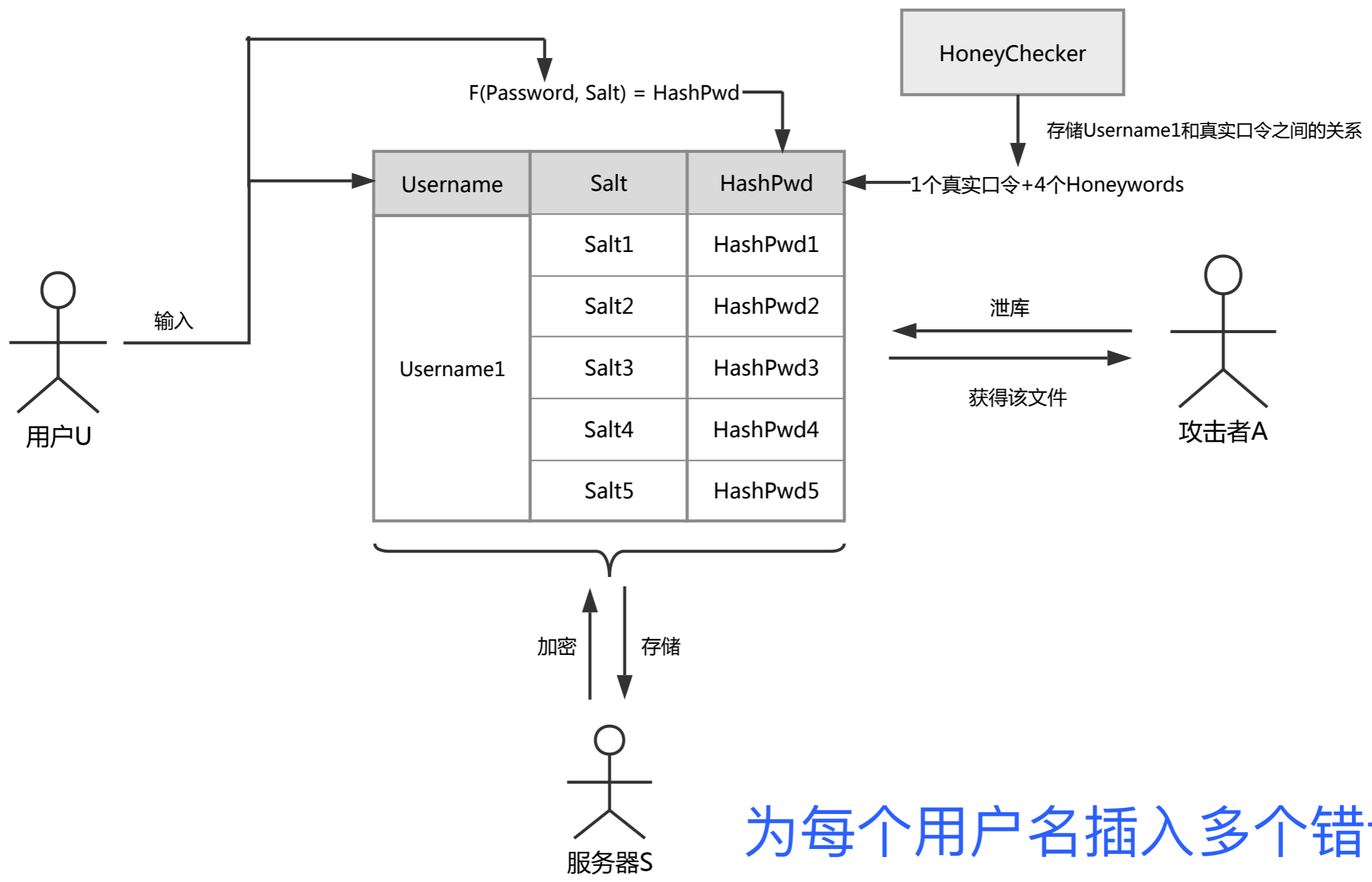
SAuth



双系统双口令认证

Password Leakage

Honeywords



为每个用户名插入多个错误的口令

提问时间！

课后作业

```
graph LR; A[阅读教材] --> B[阅读论文]; B --> C[思考]; C --> D[撰写报告];
```

阅读教材

阅读论文

思考

撰写报告

要求阅读如下文章，写阅读报告

in ACM CCS 2013

**Honeywords:
Making Password-Cracking Detectable**

Ari Juels
RSA Laboratories
Cambridge, MA, USA
ari.juels@rsa.com

Ronald L. Rivest
MIT CSAIL
Cambridge, MA, USA
rivest@mit.edu

- 1、文章概述
- 2、主要收获
- 3、存在疑问
- 4、所思所感
- 5、一篇论文

周六晚上12点
前提交

检索一篇引用Honeywords的2017-2018的论文，简单阅读，杂志的文章最好

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

<https://huipingsun.github.io>