文本口令

北京大學 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

Text Password

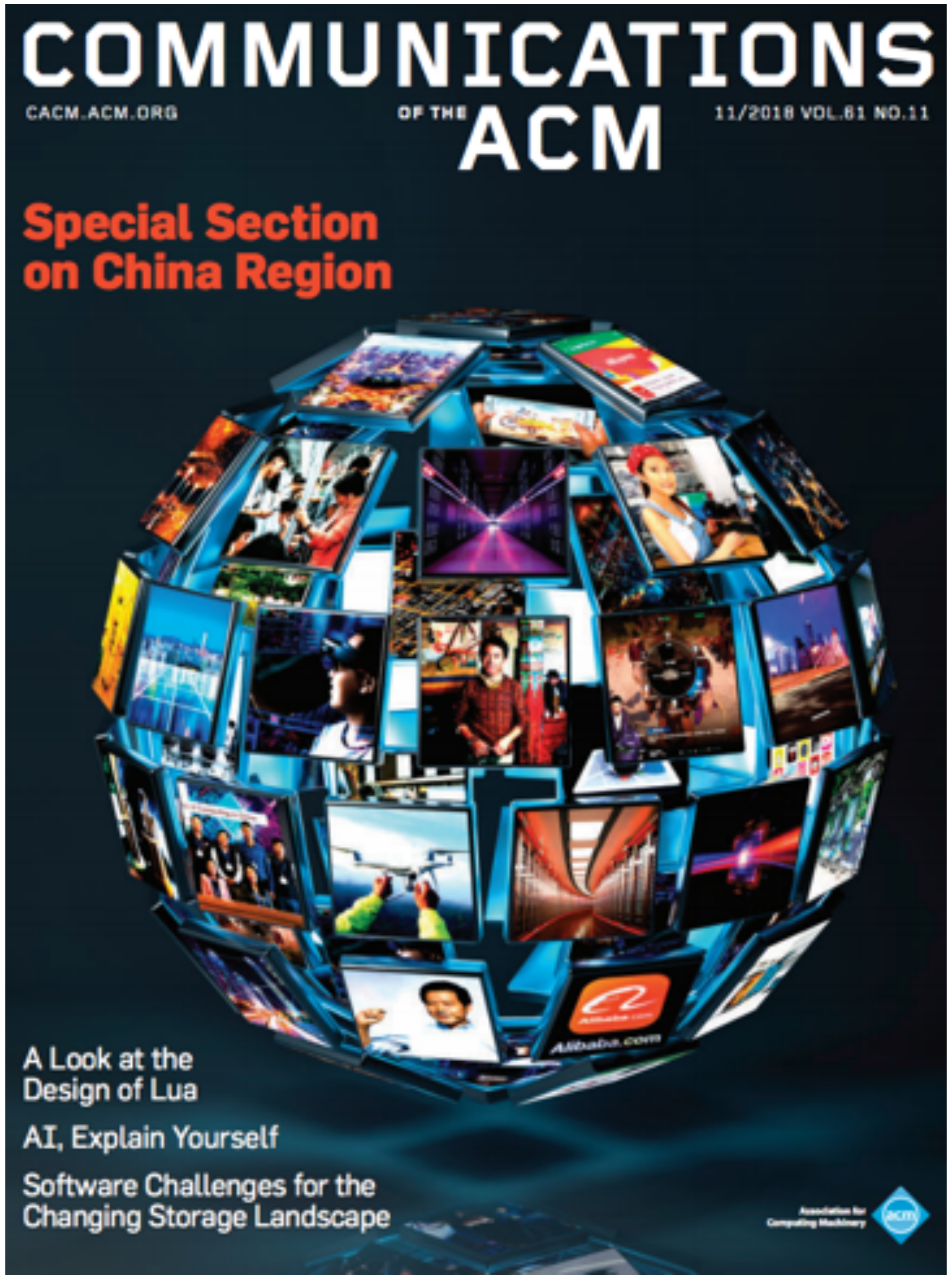
图形口令回顾

1 简介	2 分类	3 PassApp	4 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/



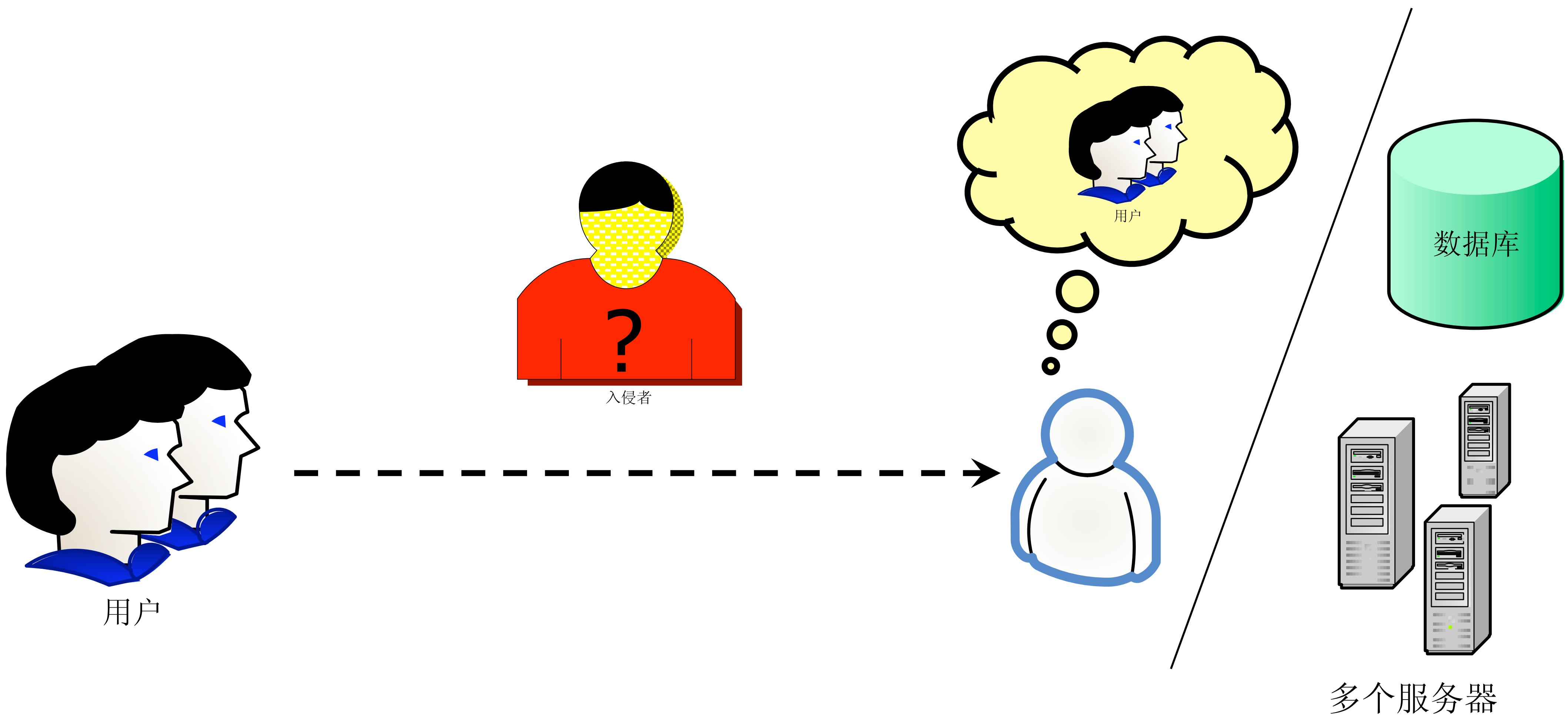
Theory on passwords has lagged practice, where large providers use back-end smarts to survive with imperfect technology.

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

Authentication 身份认证



身份认证因子

- Something you are /can do
  - Fingerprint
  - Voice

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

- Something you know
  - Password
  - Image
  - Answer

Security Level

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

文本口令简介

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

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

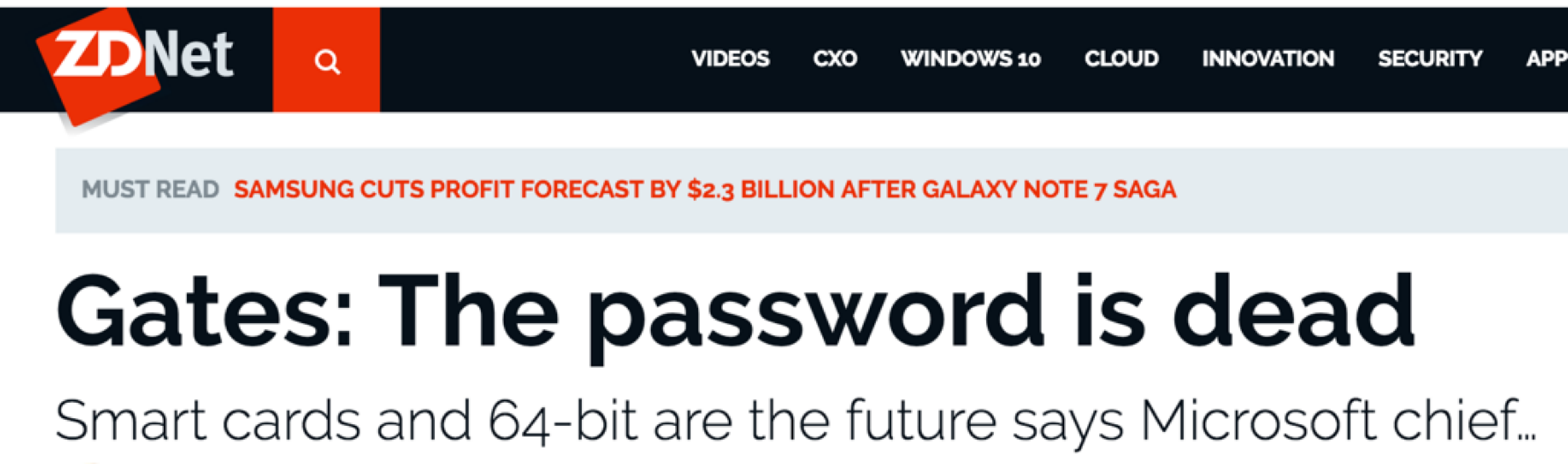
is

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”*



其余候选机制

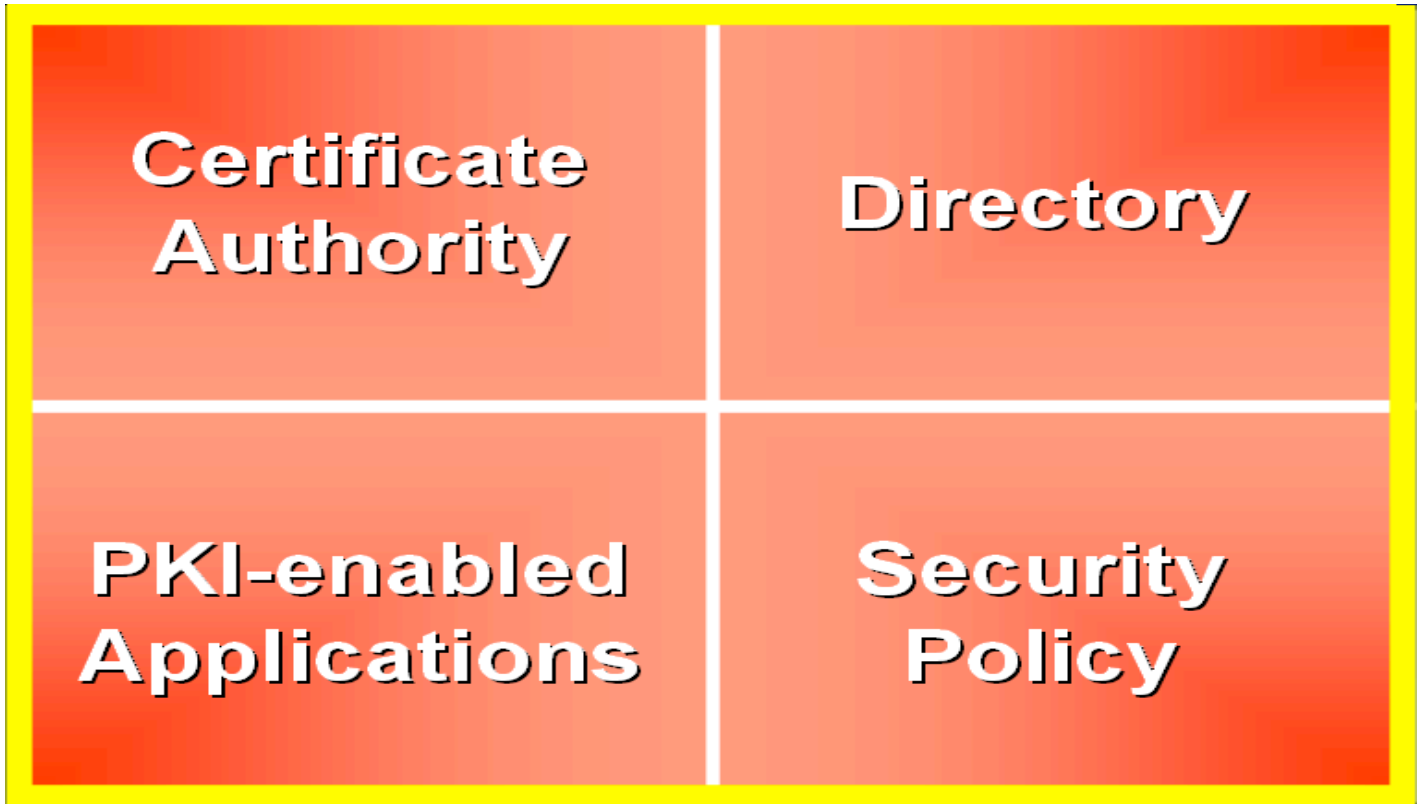
PKC & PKI

- 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。

---

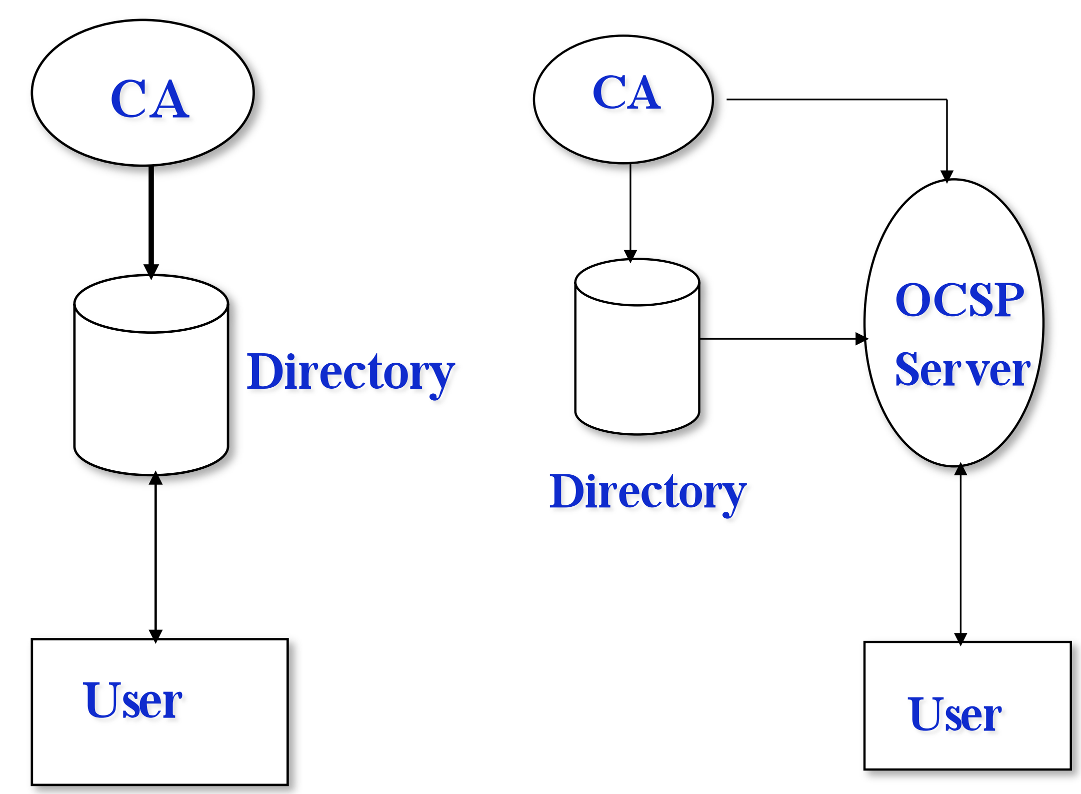
mid-1990s

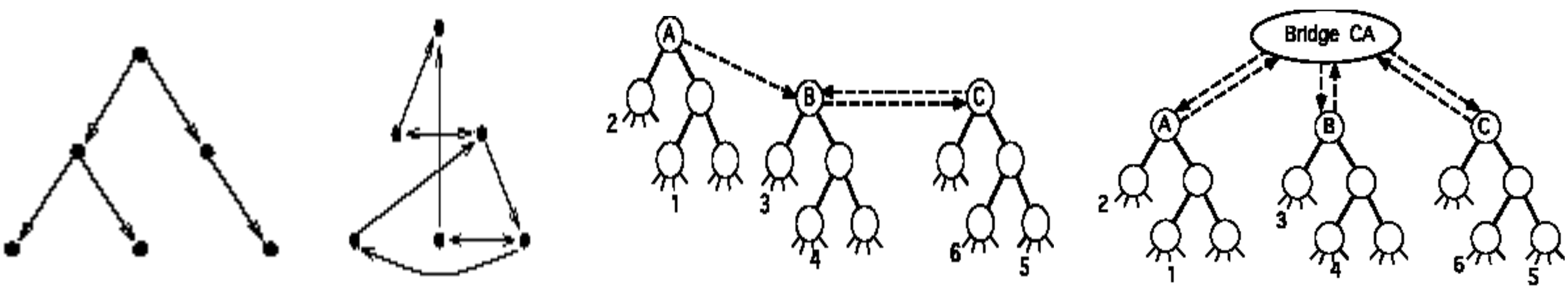
- 基础：公钥密码学
- 动作：创建、管理、存储、分布和作废证书
- 包含：软件、硬件、人员、策略和过程
- 目的：表示和管理信任关系



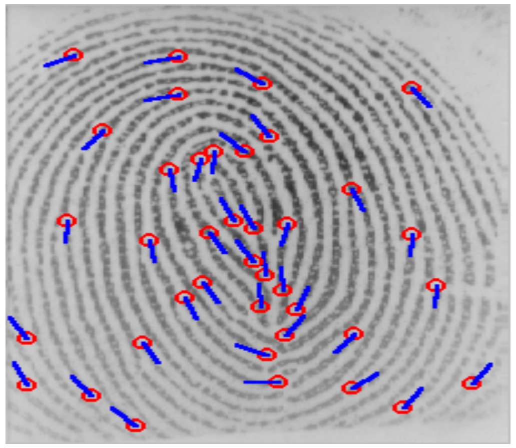
PKC & PKI

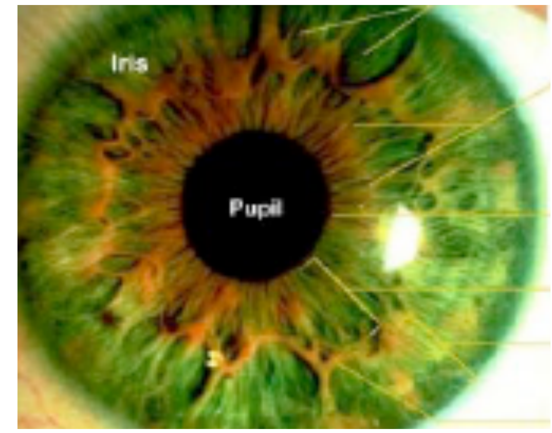
- 需要预先知道对方的公钥、需要在线服务器的支持
- 引入证书、引入可信第三方
- 密钥管理、证书管理
- 信任问题、规模问题
- 性能问题、互联互通问题

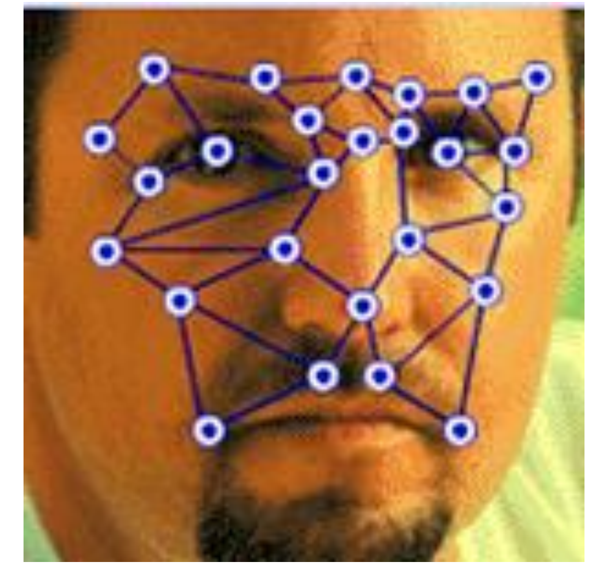


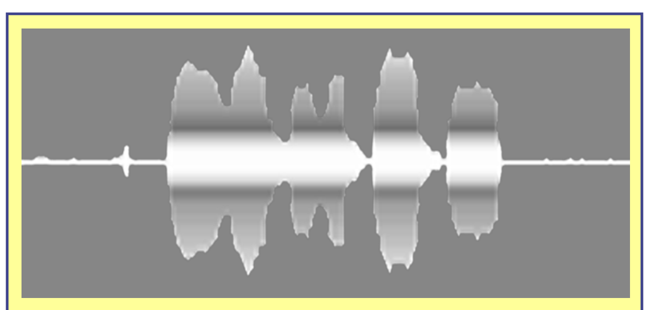


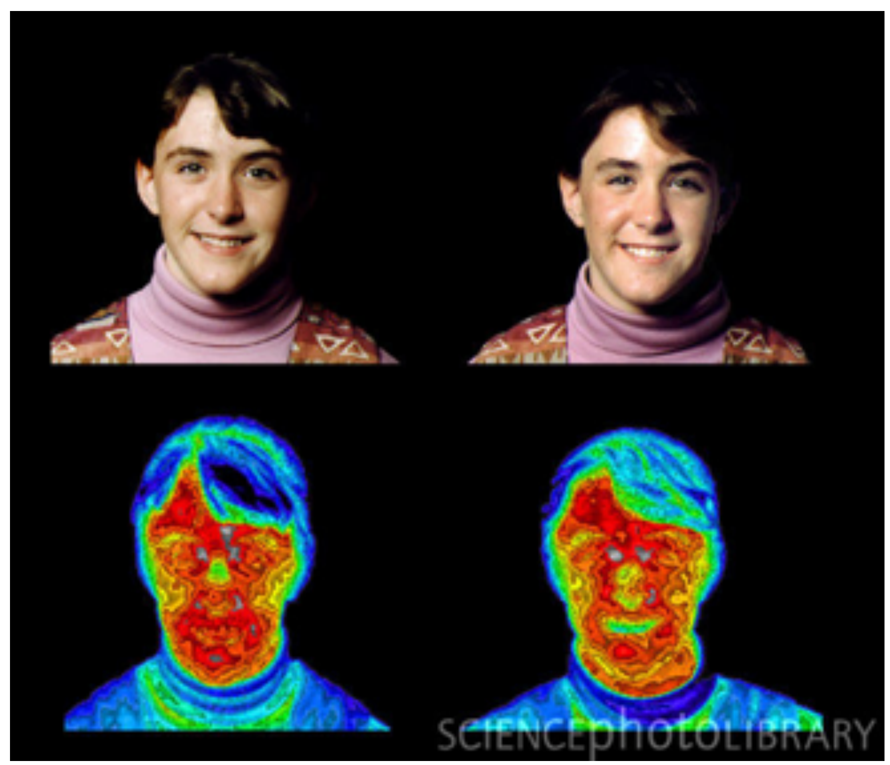
Biometrics

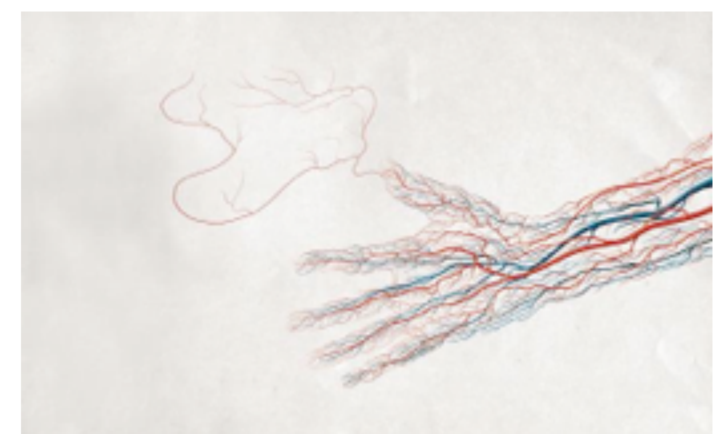


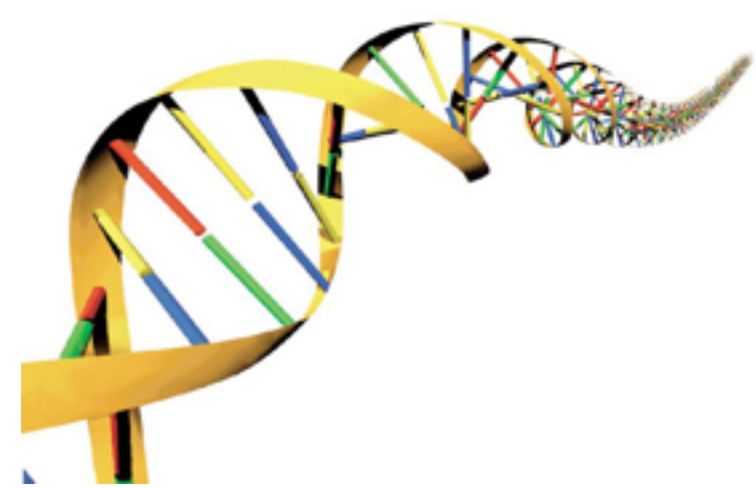






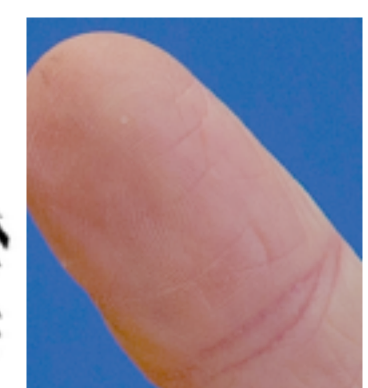






攻击指纹

Chaos Computer Club



Password

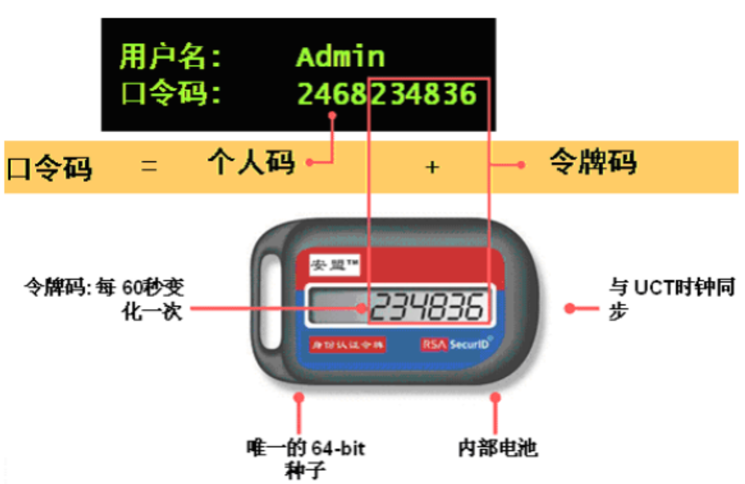
is

Imperfect

But … …

OTP: One Time Password

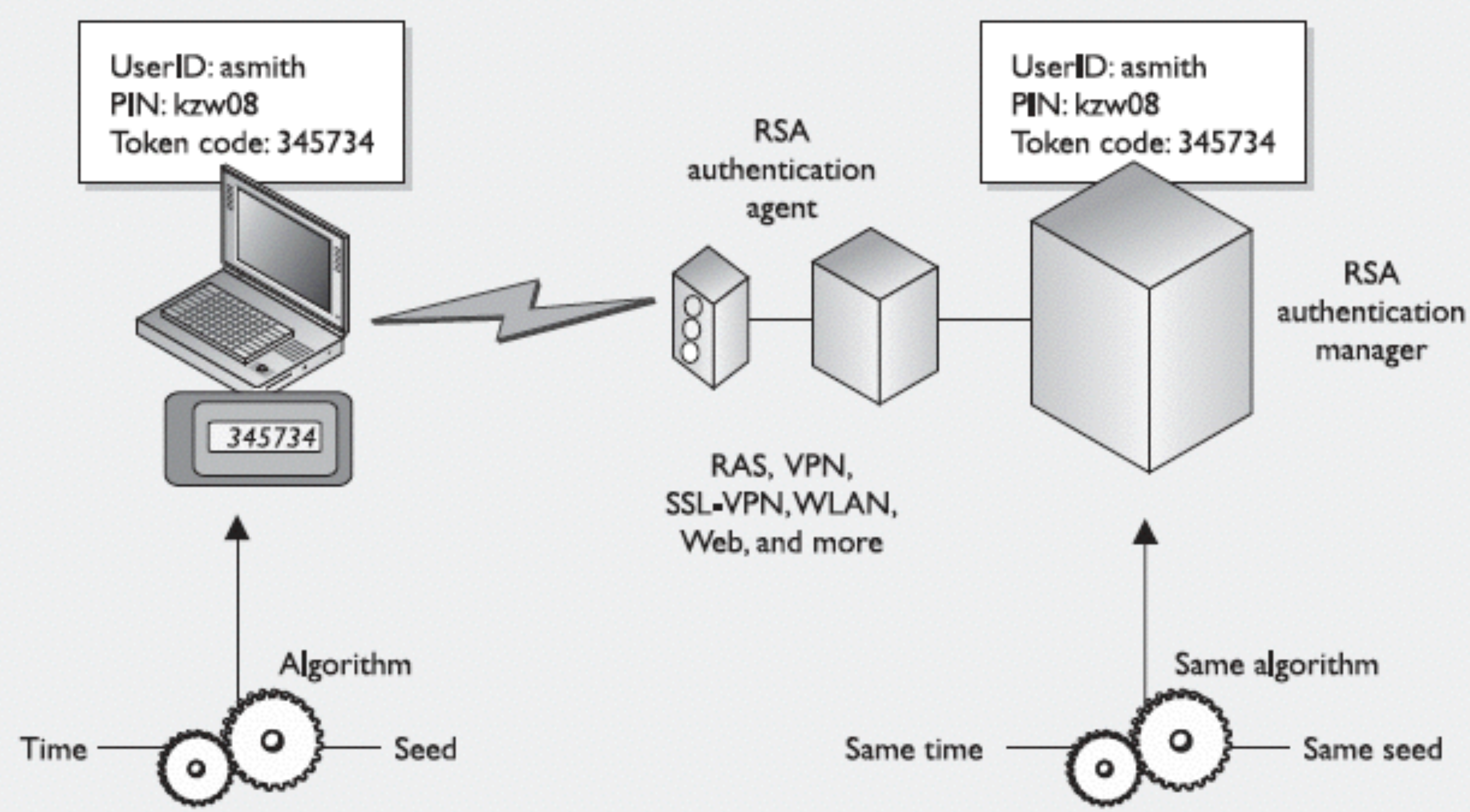
一次性(动态)口令。是由电子令牌(Token)等手持终端设备生成的，根据某种加密算法，产生的随某一个不断变化的参数(例如时间，事件等)不停地、没有重复变化的一种口令。



SecureID

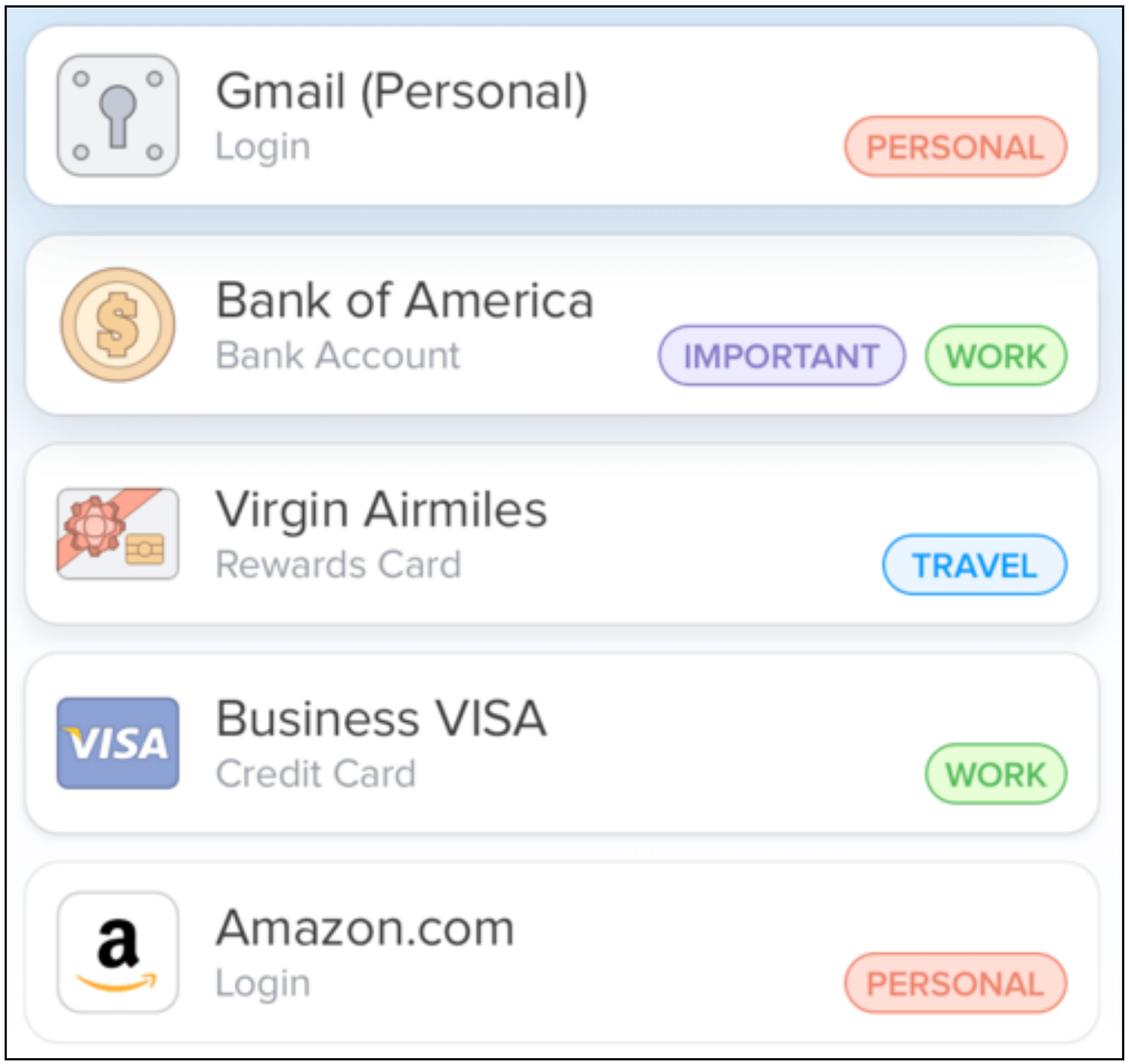
SecureID, from RSA Security, Inc., is one of the most widely used time-based tokens. One version of the product generates the one-time password by using a mathematical function on the time, date, and ID of the token card. Another version of the product requires a PIN to be entered into the token device.

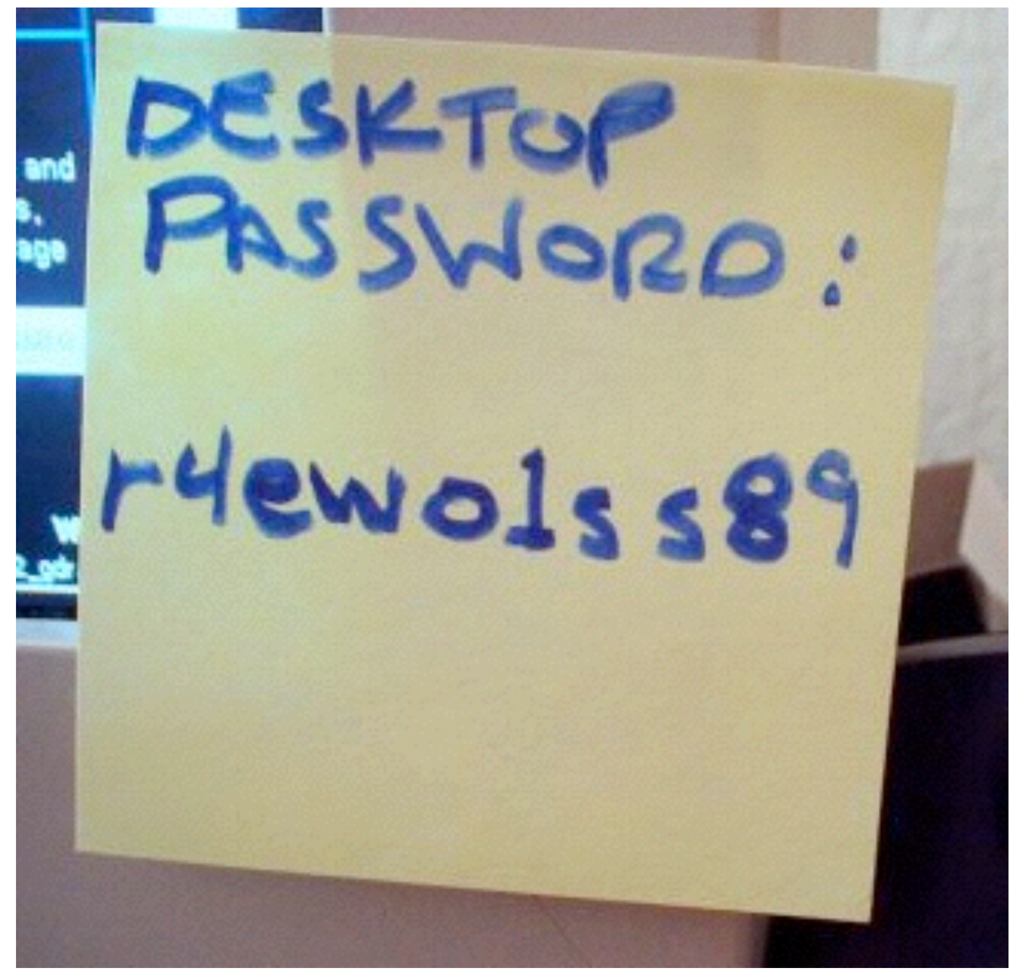
RSA SECURID TIME-SYNCHRONOUS TWO-FACTOR AUTHENTICATION



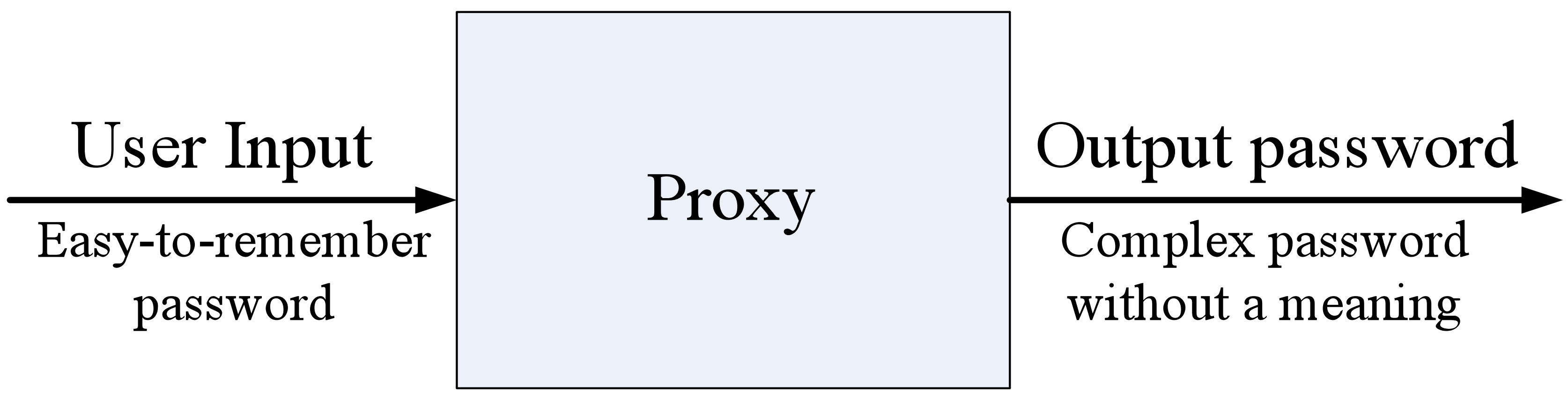
口令管理


1Password
When it's too important to go anywhere else.


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


DESKTOP
PASSWORD:
r4ewolss89

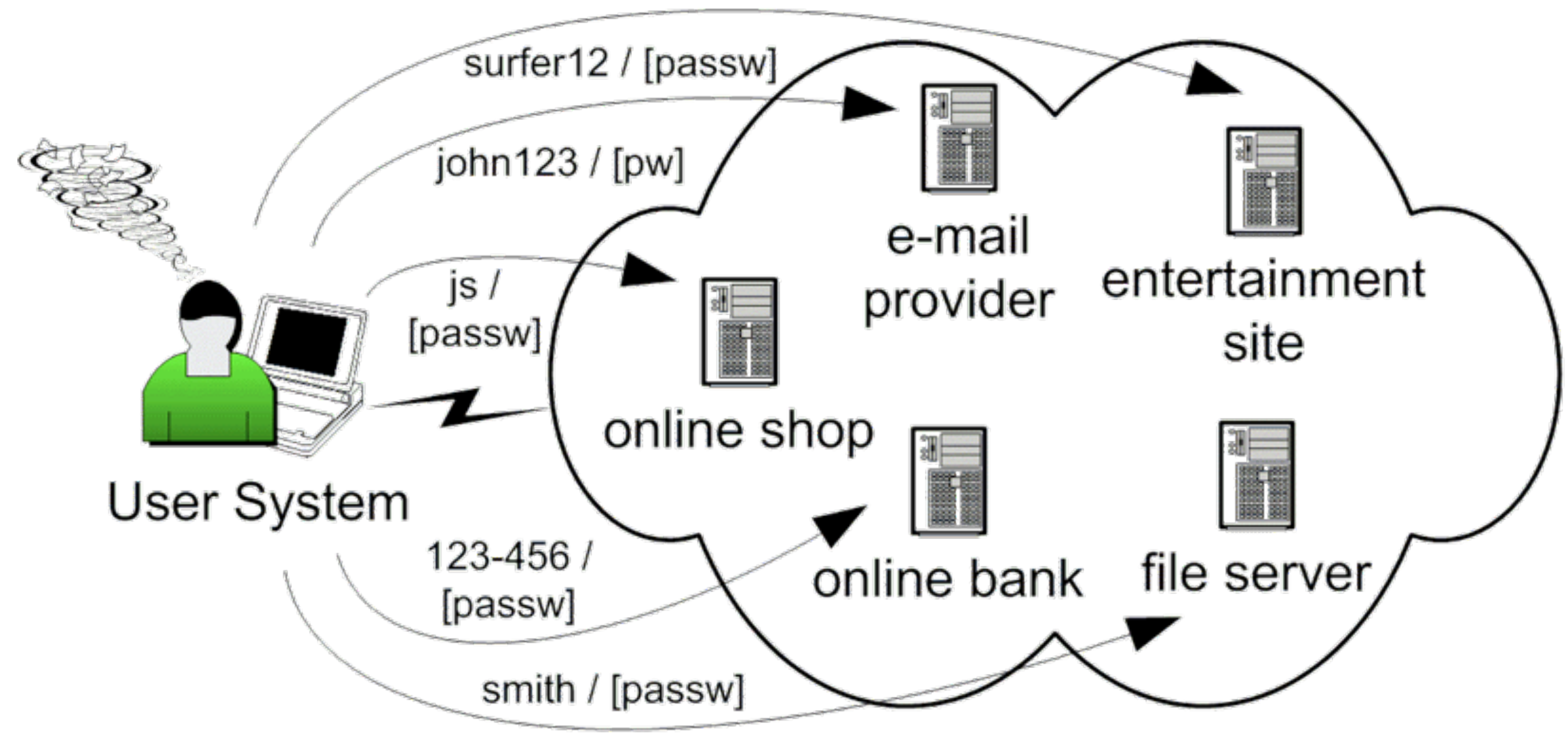
口令管理

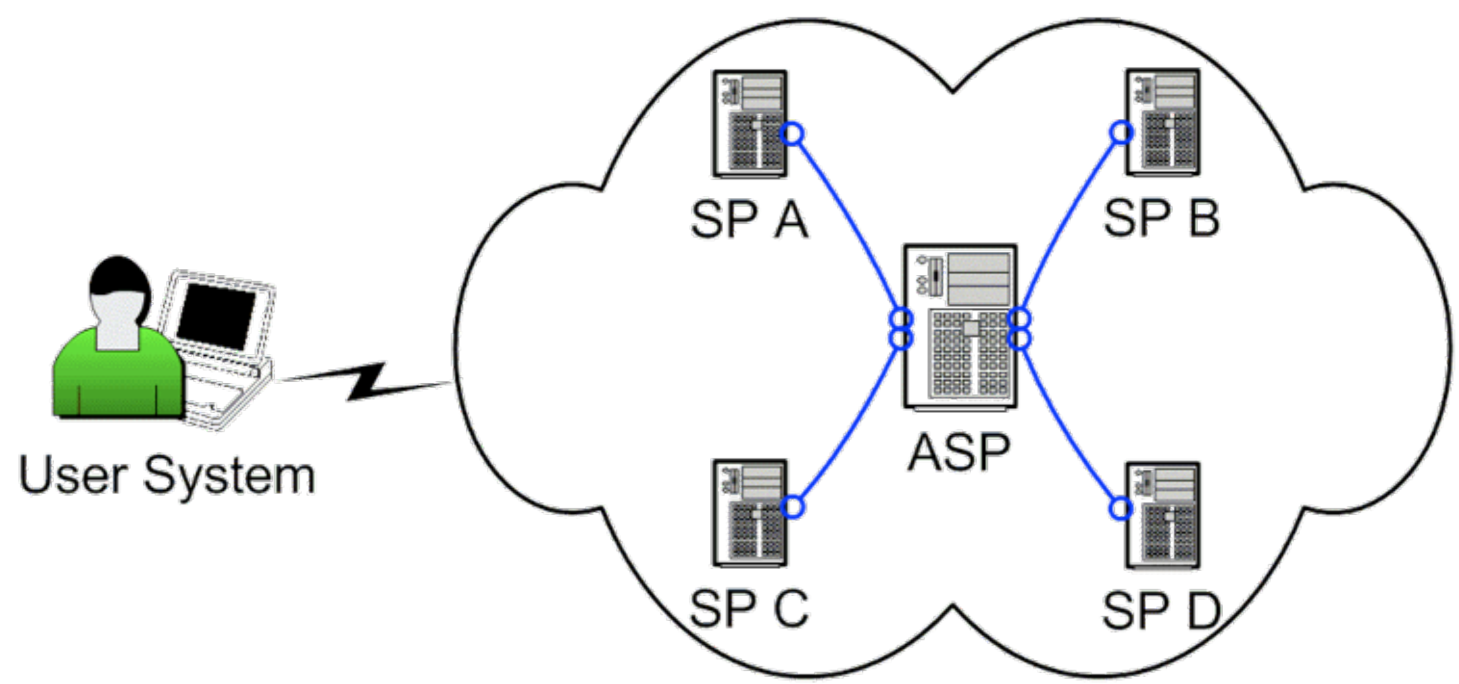

User Input
Easy-to-remember password
Proxy
Output password
Complex password without a meaning


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

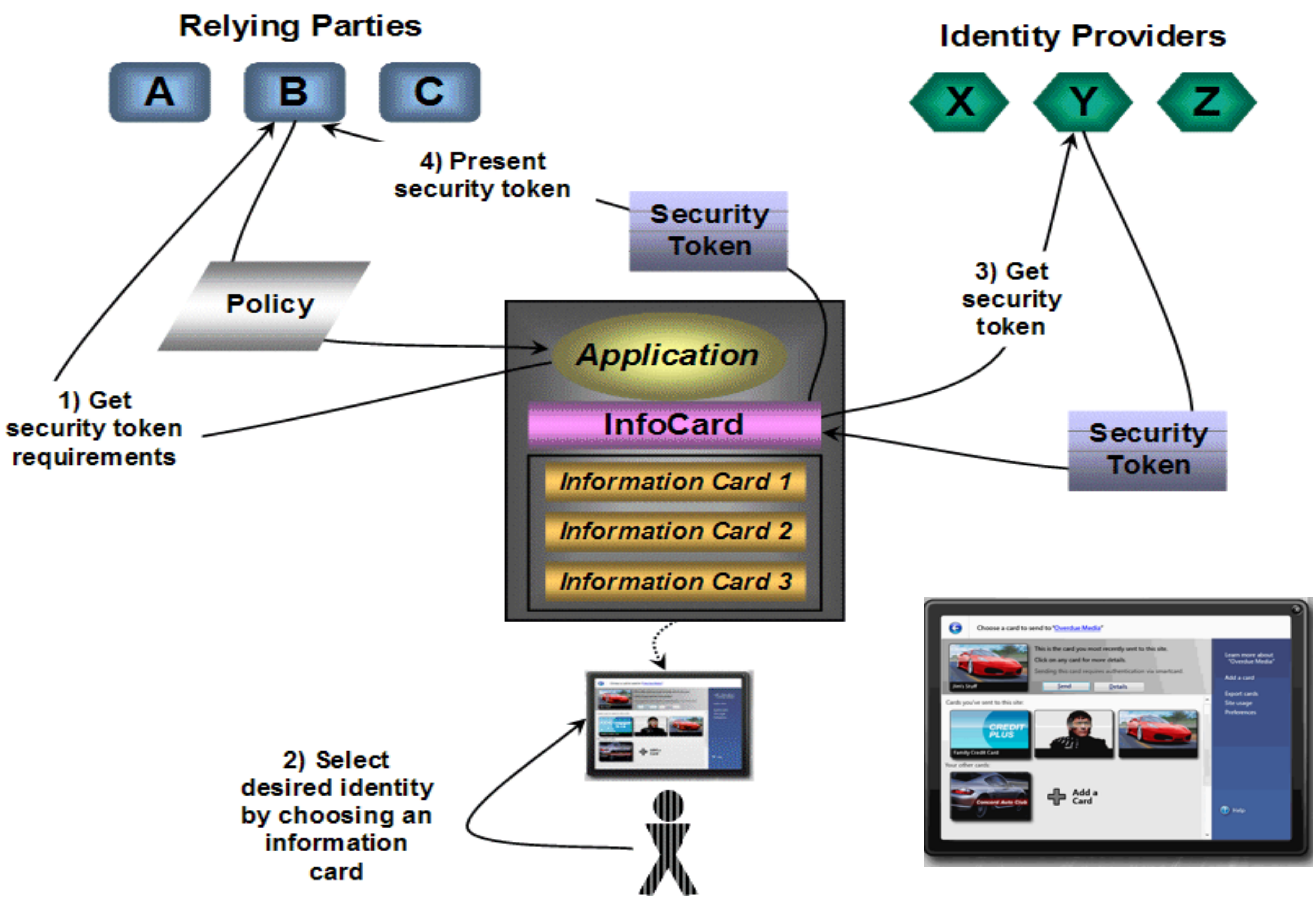
- *Single password to all resources, One Password For Everything*



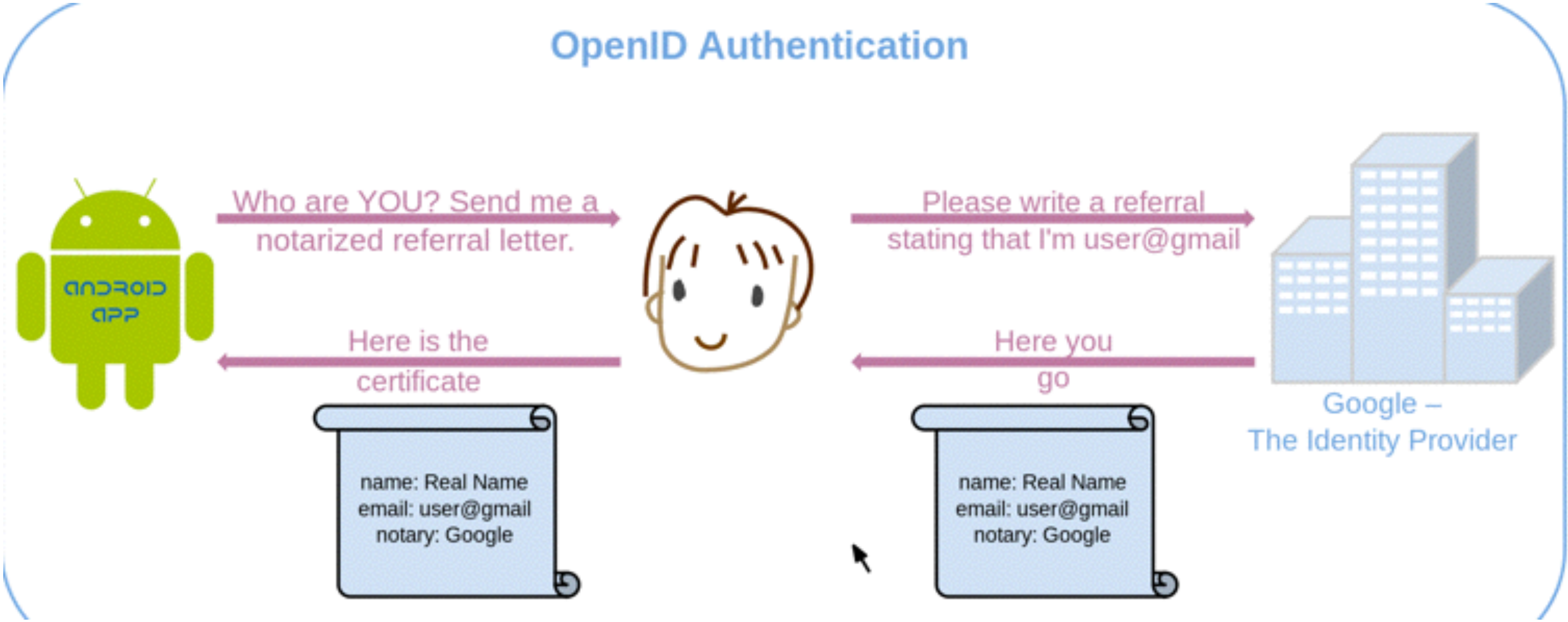


应用集成 性能瓶颈
单点失败 灵活性

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
Security Token
1) Get security token requirements
2) Select desired identity by choosing an information card

OpenID



轻量级IDM、基于URI

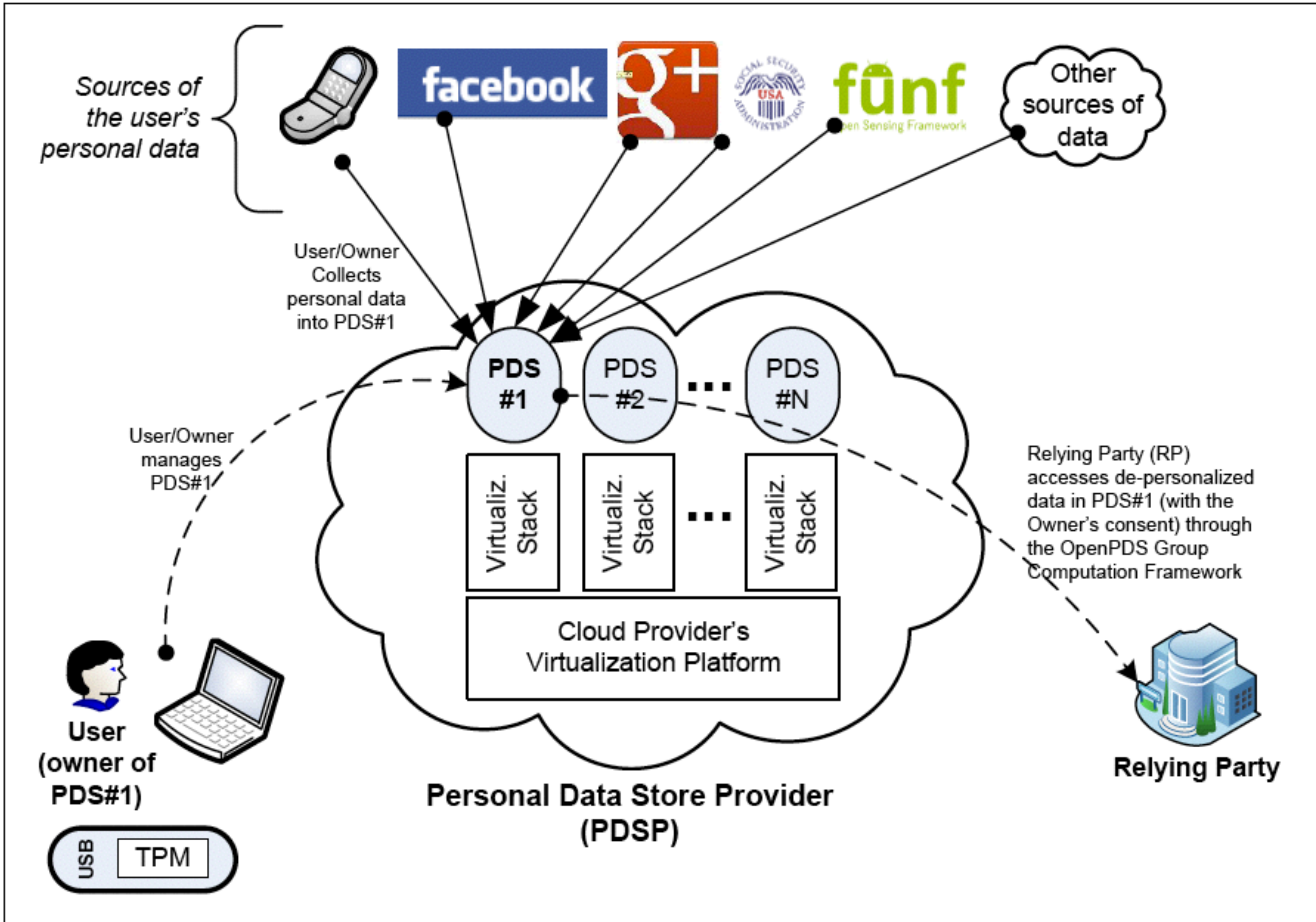
OAuth

- 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

OpenPDS


Sources of the user's personal data
facebook
Other sources of data
User/Owner Collects personal data into PDS#1
PDS #1
PDS #2
PDS #N
Virtualiz. Stack
Virtualiz. Stack
Virtualiz. Stack
Cloud Provider's Virtualization Platform
User/Owner manages PDS#1
Relying Party (RP) accesses de-personalized data in PDS#1 (with the Owner's consent) through the OpenPDS Group Computation Framework
User (owner of PDS#1)
USB
TPM
Personal Data Store Provider (PDSP)
Relying Party

理论 vs. 实践

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

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

防止口令泄露

Password Leakage

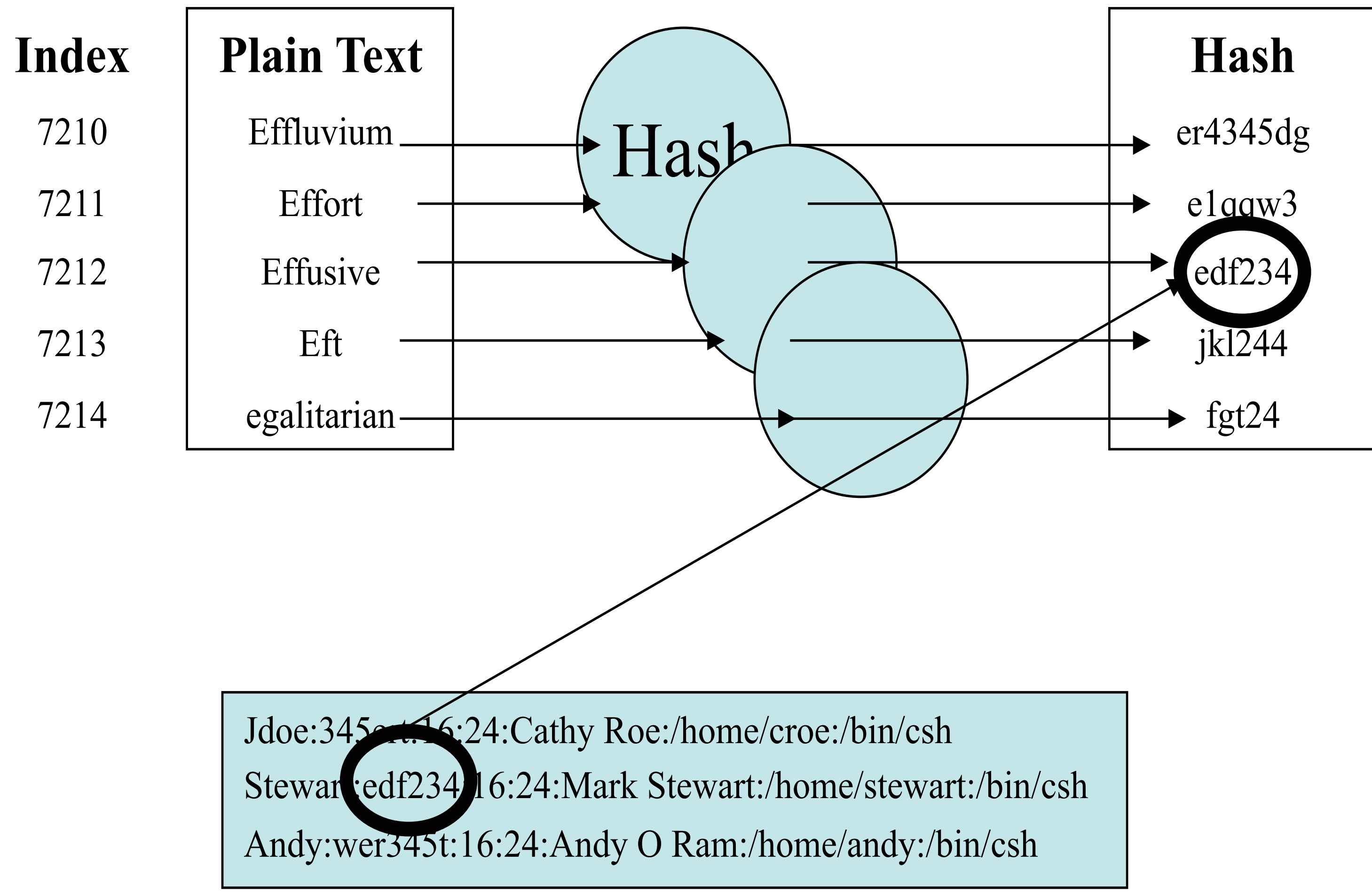
口令泄漏

CSDN	LinkedIn	EVERNOTE	網易 NETEASE	myspace.com
600w	600w	5000w	过亿	4.27亿
2011	2012	2013	2015	2016

Traditional Salt Hash

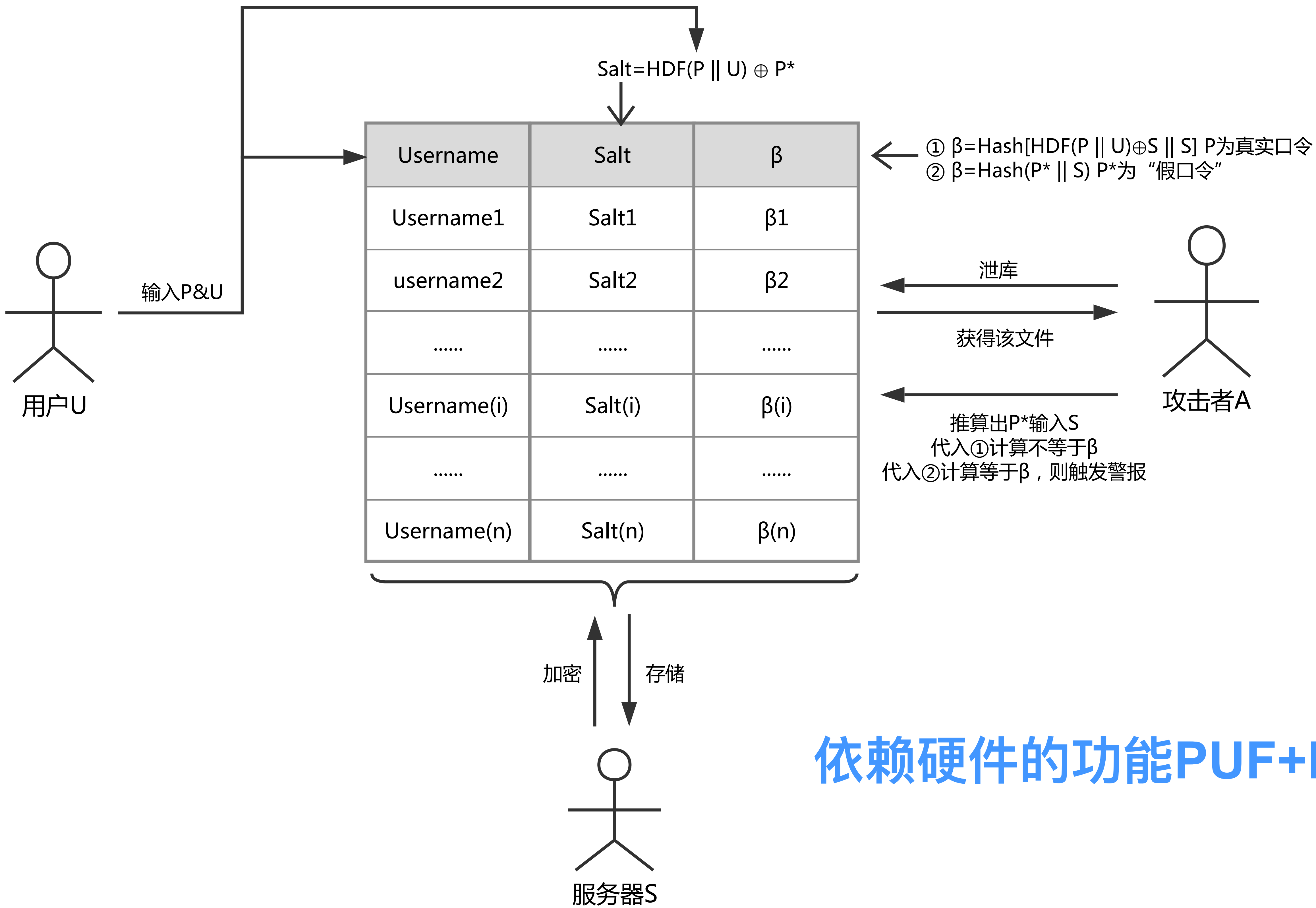
Username	PassSalt	→	HashPwd
Username1	PassSalt1	→	HashPwd1
username2	PassSalt2	→	HashPwd2
......	......	→	......
Username(i)	PassSalt(i)	→	HashPwd(i)
......	......	→	......
Username(n)	PassSalt(n)	→	HashPwd(n)

字典攻击



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

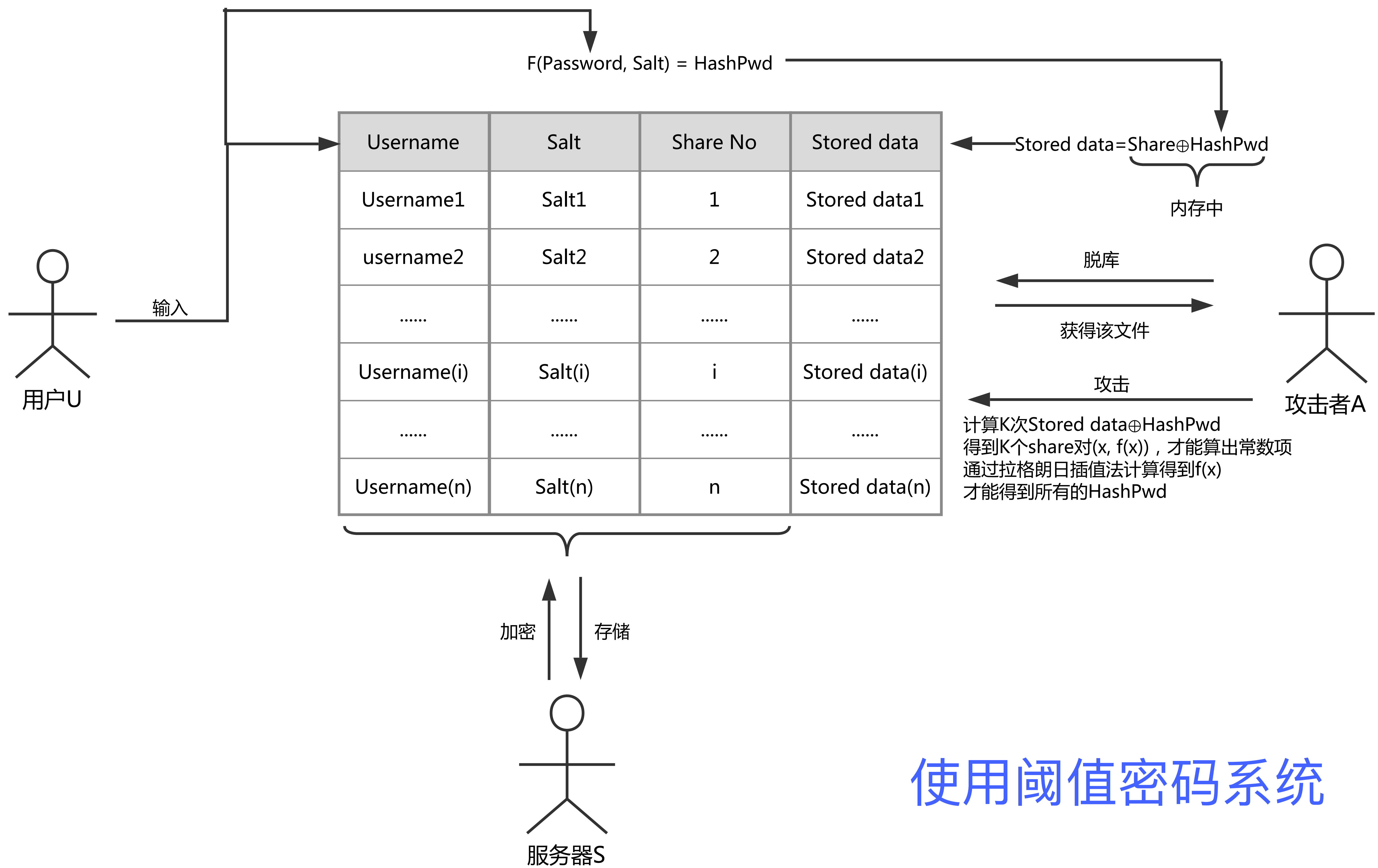
ErsatzPasswords



Username	Salt	β
Username1	Salt1	β1
username2	Salt2	β2
……	……	……
Username(i)	Salt(i)	β(i)
……	……	……
Username(n)	Salt(n)	β(n)

依赖硬件的功能PUF+HSM

PolyPassHash

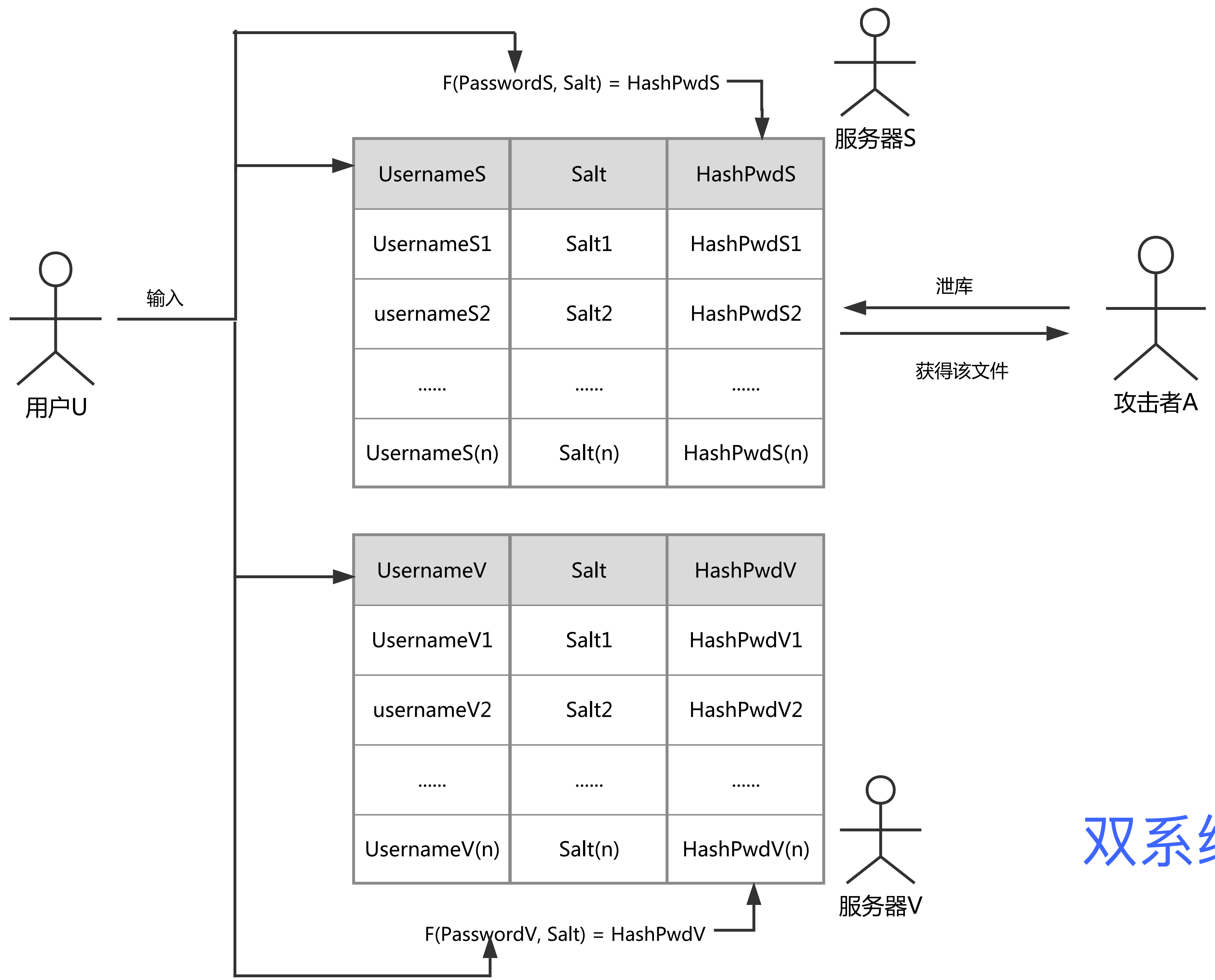


Username	Salt	Share No	Stored data
Username1	Salt1	1	Stored data1
username2	Salt2	2	Stored data2
……	……	……	……
Username(i)	Salt(i)	i	Stored data(i)
……	……	……	……
Username(n)	Salt(n)	n	Stored data(n)

使用阈值密码系统

Password Leakage

SAuth

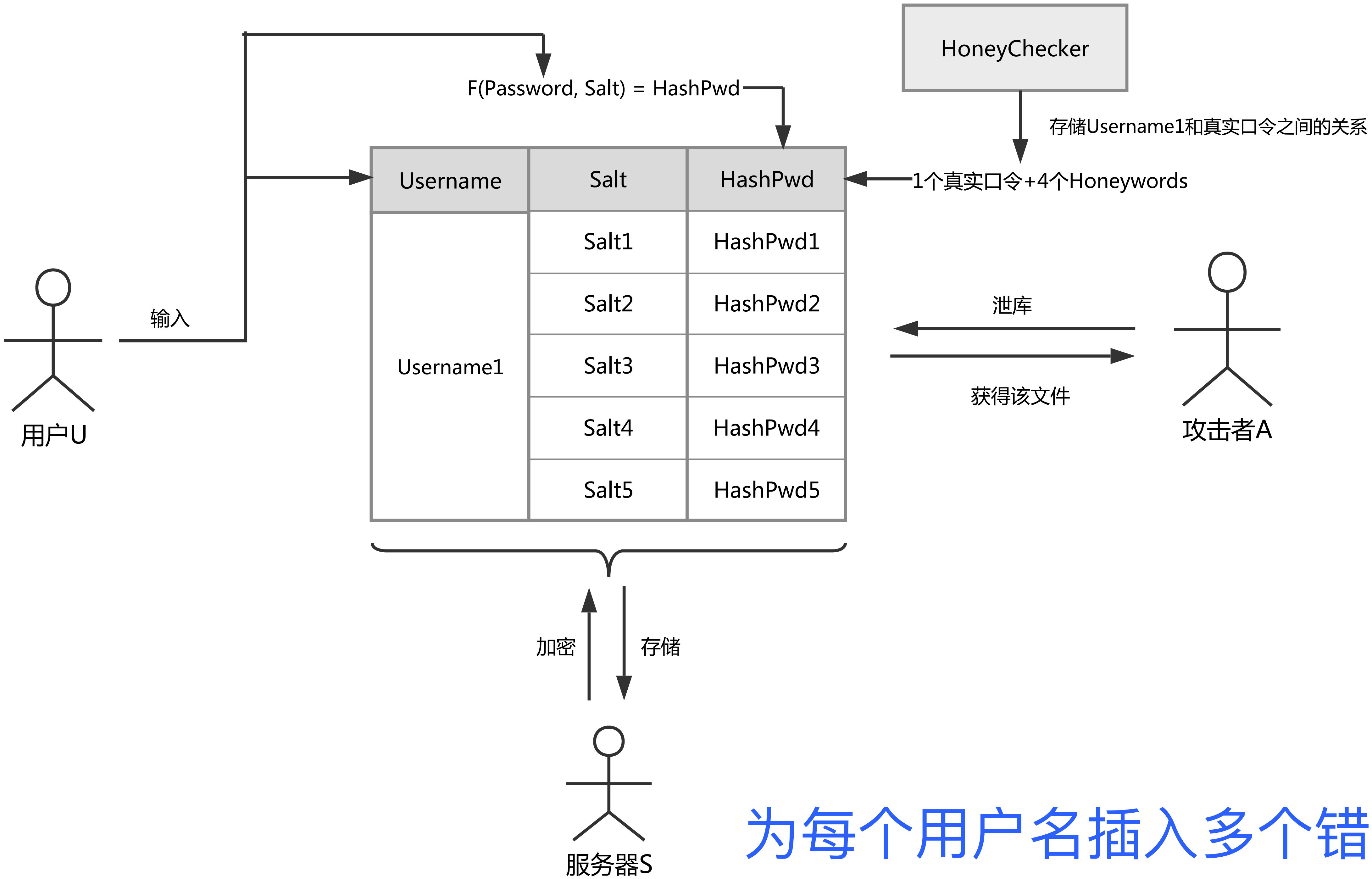


UsernameS	Salt	HashPwdS
UsernameS1	Salt1	HashPwdS1
usernameS2	Salt2	HashPwdS2
……	……	……
UsernameS(n)	Salt(n)	HashPwdS(n)

UsernameV	Salt	HashPwdV
UsernameV1	Salt1	HashPwdV1
usernameV2	Salt2	HashPwdV2
……	……	……
UsernameV(n)	Salt(n)	HashPwdV(n)

双系统双口令认证

Honeywords



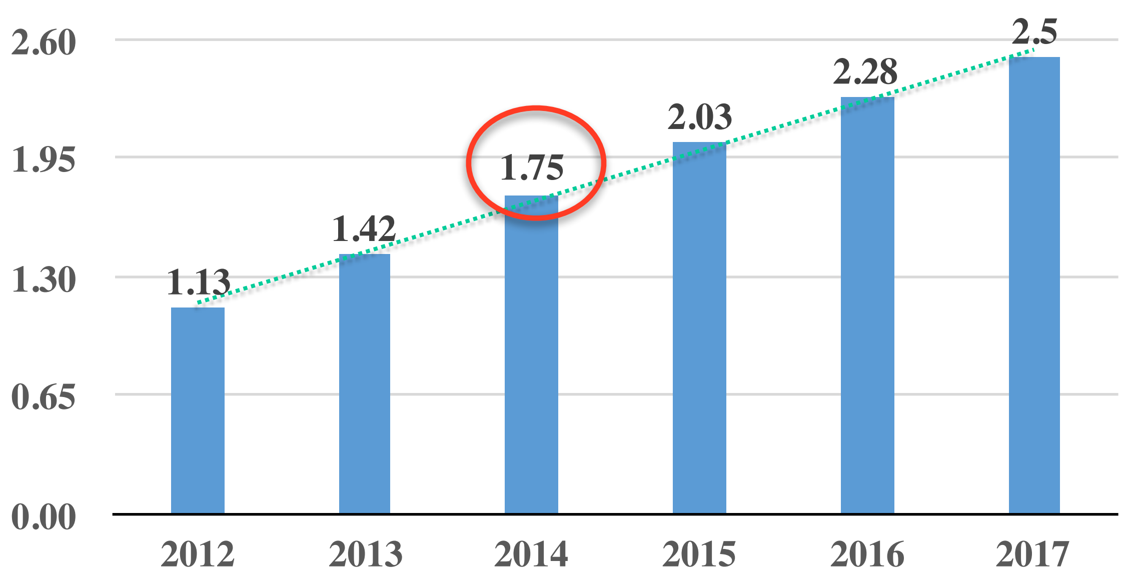
为每个用户名插入多个错误的口令

SlidePIN:

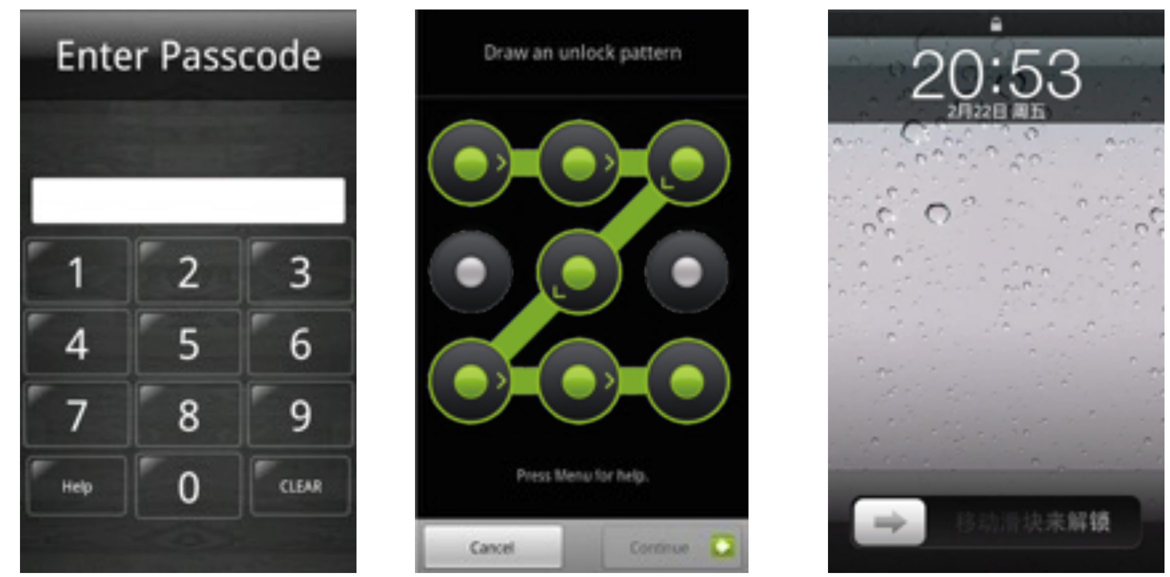
Slide-based PIN Entry Mechanism on Smartphones

SlidePIN 背景

www.eMarketer.com



4 digits PIN PatternLock No



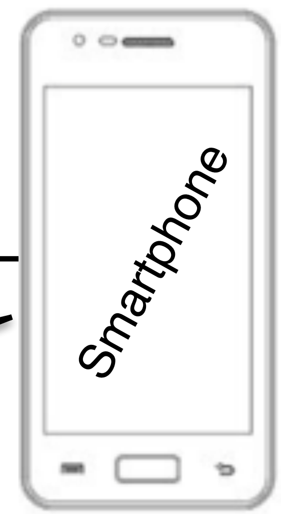
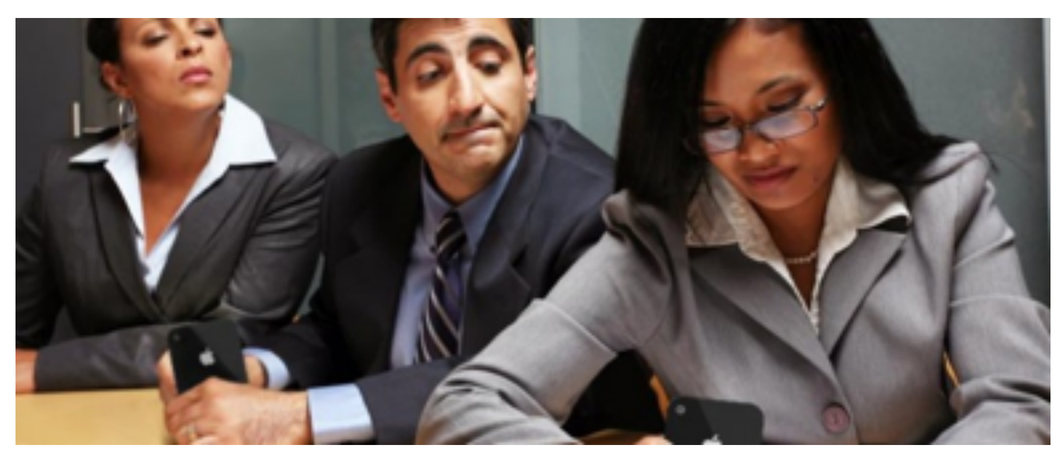


Photo Audio Video
SMS Call Email
Payment Location
SNS Blog IM
… …

http://www.mireview.com/blog/wp-content/uploads/2013/03/timthumb.jpg

Shoulder surfing attack



什么是肩窥攻击

- 肩窥攻击（Shoulder Surfing）也称为窥视攻击，是一种利用直接观察就可以得到所需要信息的攻击技术，是社会工程的一种，对于基于知识的身份认证机制有着非常大的威胁，特别对于文本密码、图形密码和隐私问题这三个最主要的认证机制。

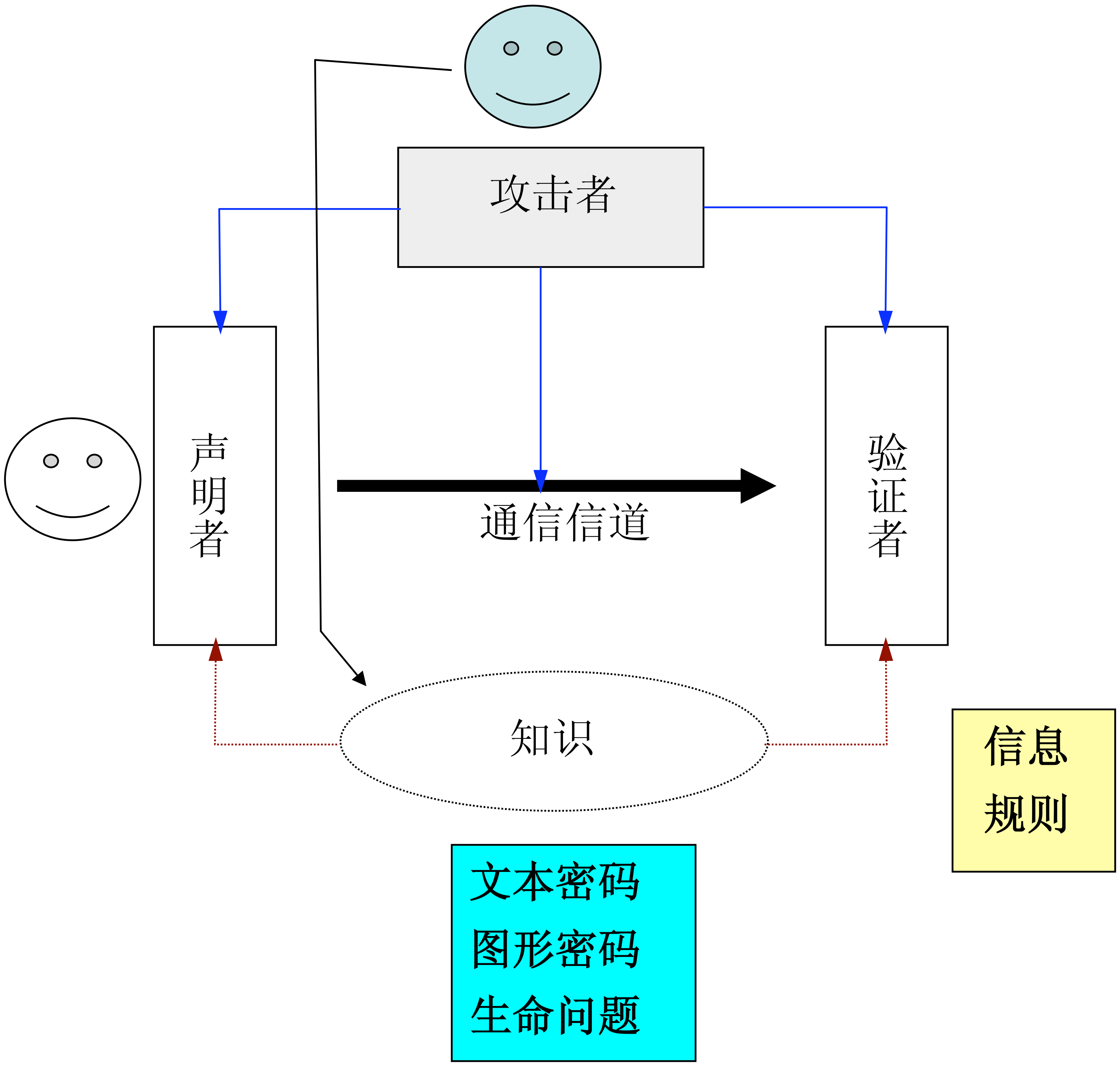
- 肩窥攻击一般发生在相对临近的环境中，特别是在比较拥挤的地方，在这种环境中攻击者可以很容易的看见临近的一些人所填写的标单、在ATM机器上录入的PIN、在公用电话上使用的电话卡、在屏幕上显示得各种信息等。当然在摄像头、望远镜、录像机等设备的支持下，肩窥也能发生在非常远的距离。

- 肩窥攻击基本上有四种形式：临近偷看、使用设备、声学跟踪、电磁泄露。

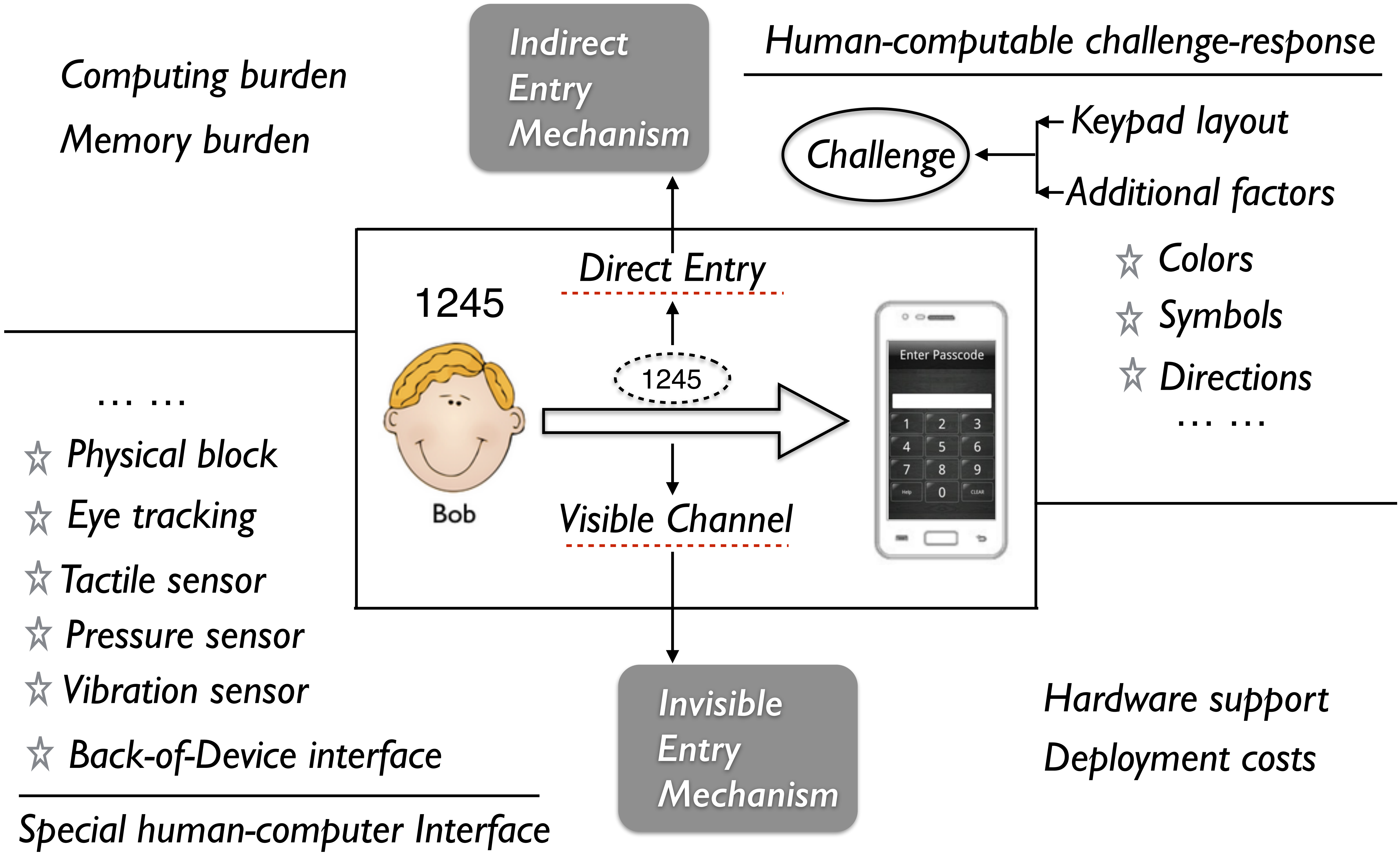
- 该类攻击被人提及已有20多年的历史，但一直没有引起足够的重视，现有的相关研究和论文还不太多。但是随着移动网络和移动计算的发展，越来越得到了重视。

SlidePIN

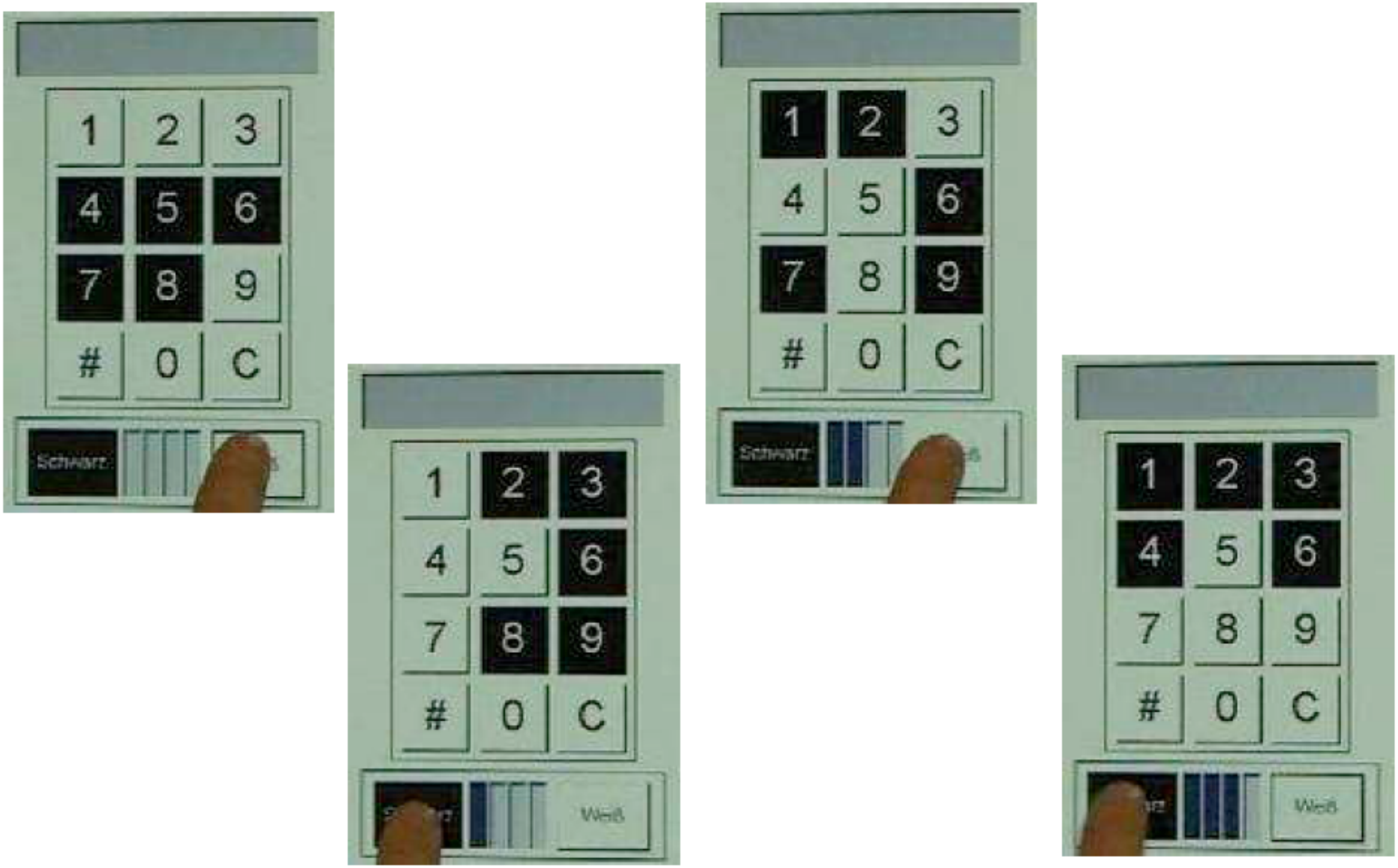
肩窥攻击产生原因



相关工作


Computing burden
Memory burden
Indirect Entry Mechanism
Human-computable challenge-response
Challenge
Keypad layout
Additional factors
☆ Colors
☆ Symbols
☆ Directions
… …
1245
Bob
Direct Entry
1245
Visible Channel
Enter Passcode
1 2 3
4 5 6
7 8 9
0
… …
☆ Physical block
☆ Eye tracking
☆ Tactile sensor
☆ Pressure sensor
☆ Vibration sensor
☆ Back-of-Device interface
Special human-computer Interface
Invisible Entry Mechanism
Hardware support
Deployment costs

PINEntry



A PINEntry Method Resilient Against Shoulder Surfing@ CCS 2004

ColorPIN

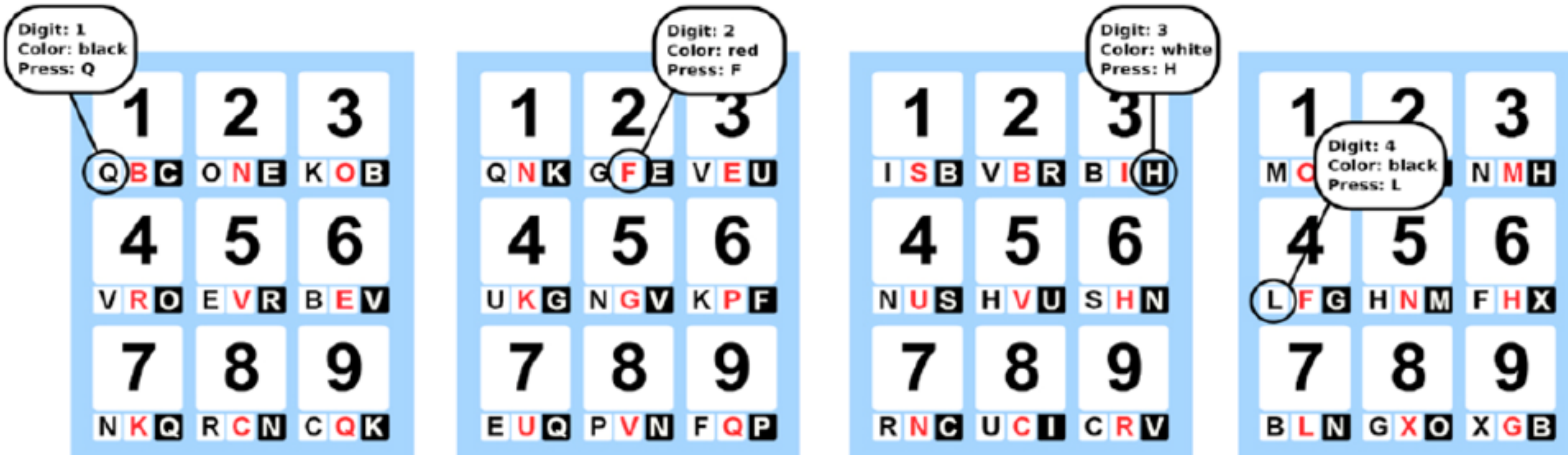


Figure 1: Exemplary PIN entry with ColorPIN. To input the PIN 1(black) 2(red) 3(white) 4(black) the user inputs the letters "QFHL". After each key press, letter assignment changes randomly.

ColorPIN-Securing PIN entry through indirect input @ CHI 2010

BoD AuthE

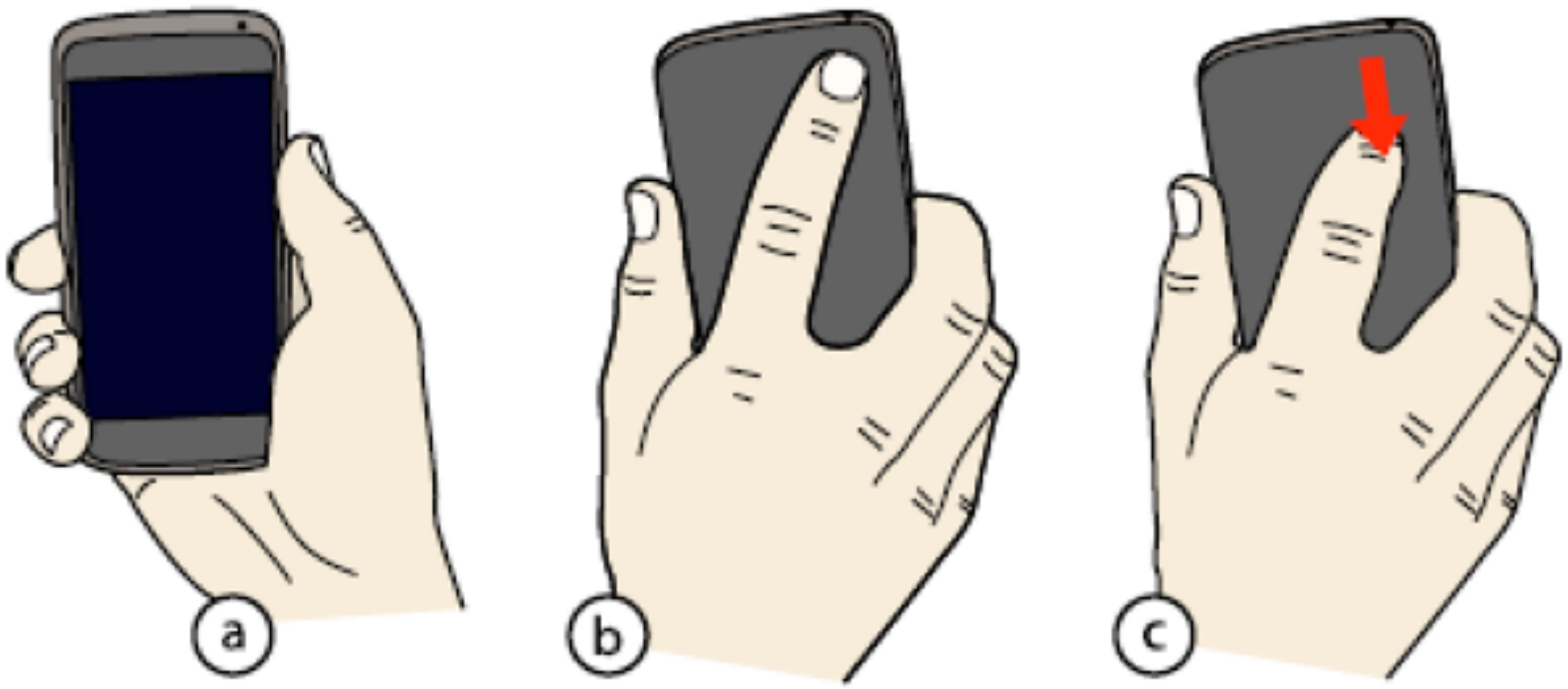
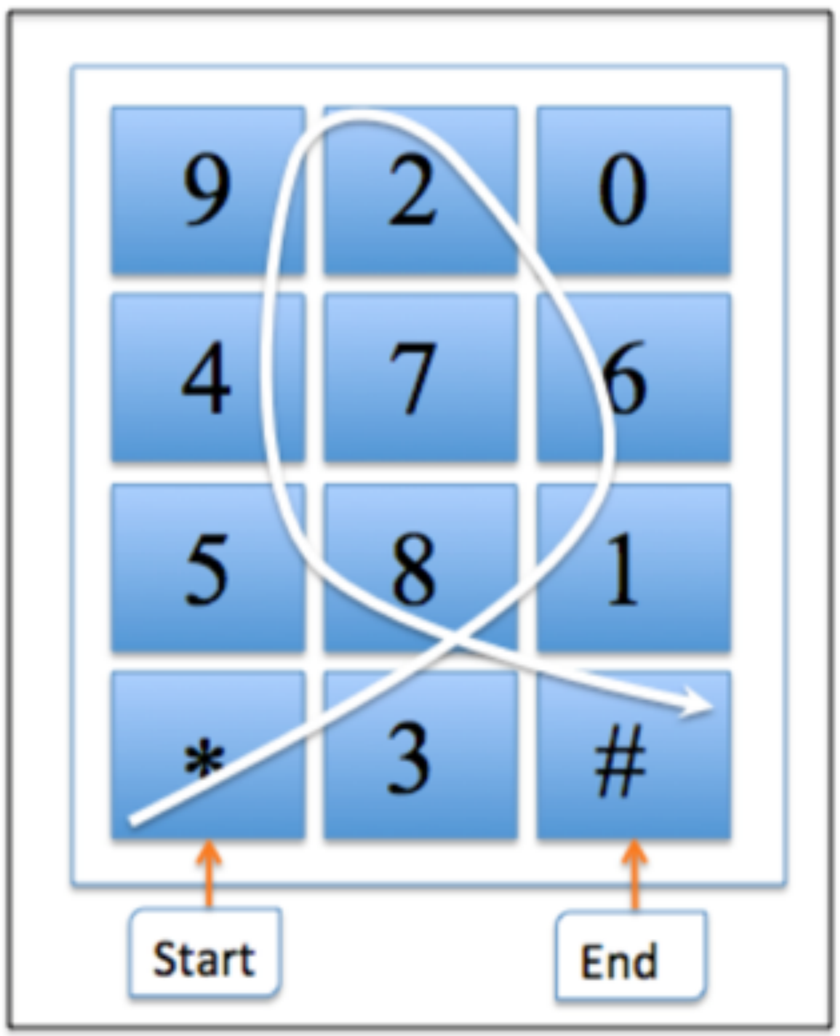


Figure 1. BoD (Back-of-Device) Shapes authentication concept. a) Typical hand posture when using one-handed input for authentication. b) The user authenticates by performing a row of simple shapes on the back. c) Example of a user performing a single-stroke shape ("Down").

Back-of-Device Authentication on Smartphones @ CHI 2013

SlidePIN概念

Slide-based PIN Entry Mechanism

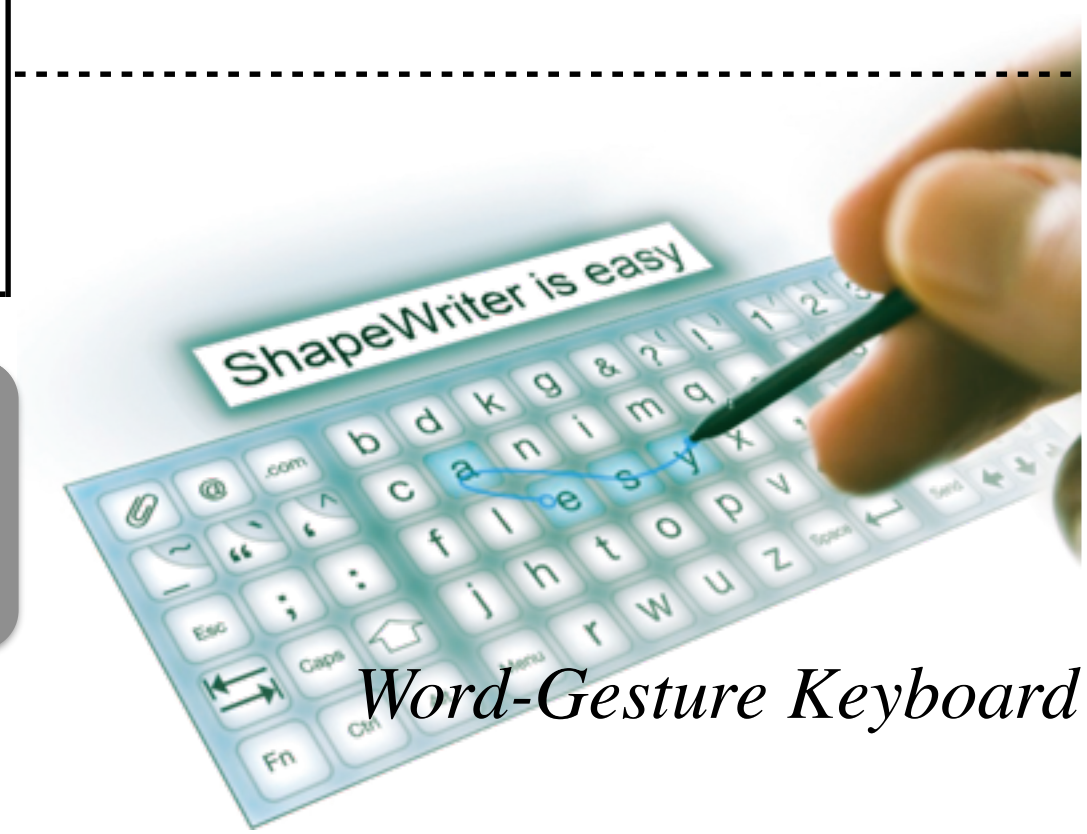


PIN	1245
SlidePIN	*381629458#

Random Keypad

Input with random numeric keypad is more secure

Slide



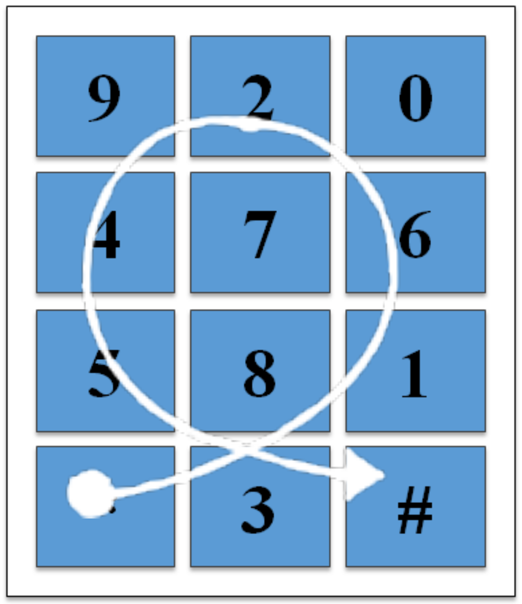
Word-Gesture Keyboard

Slide input is faster

Slide input is more secure

模型分析

PIN: 1245



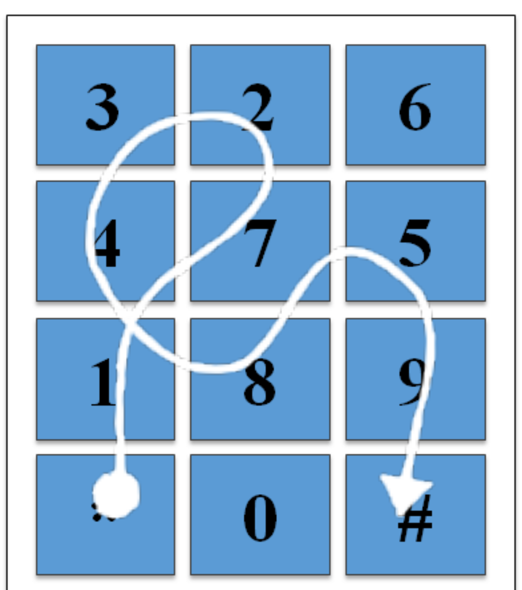
Layout 1

Trajectory 1

↓

Sequence 1

*381629458#



Layout 2

Trajectory 2

↓

Sequence 2

*1472341859#

Slide Map Function

F (PIN, Layout) → Sequence

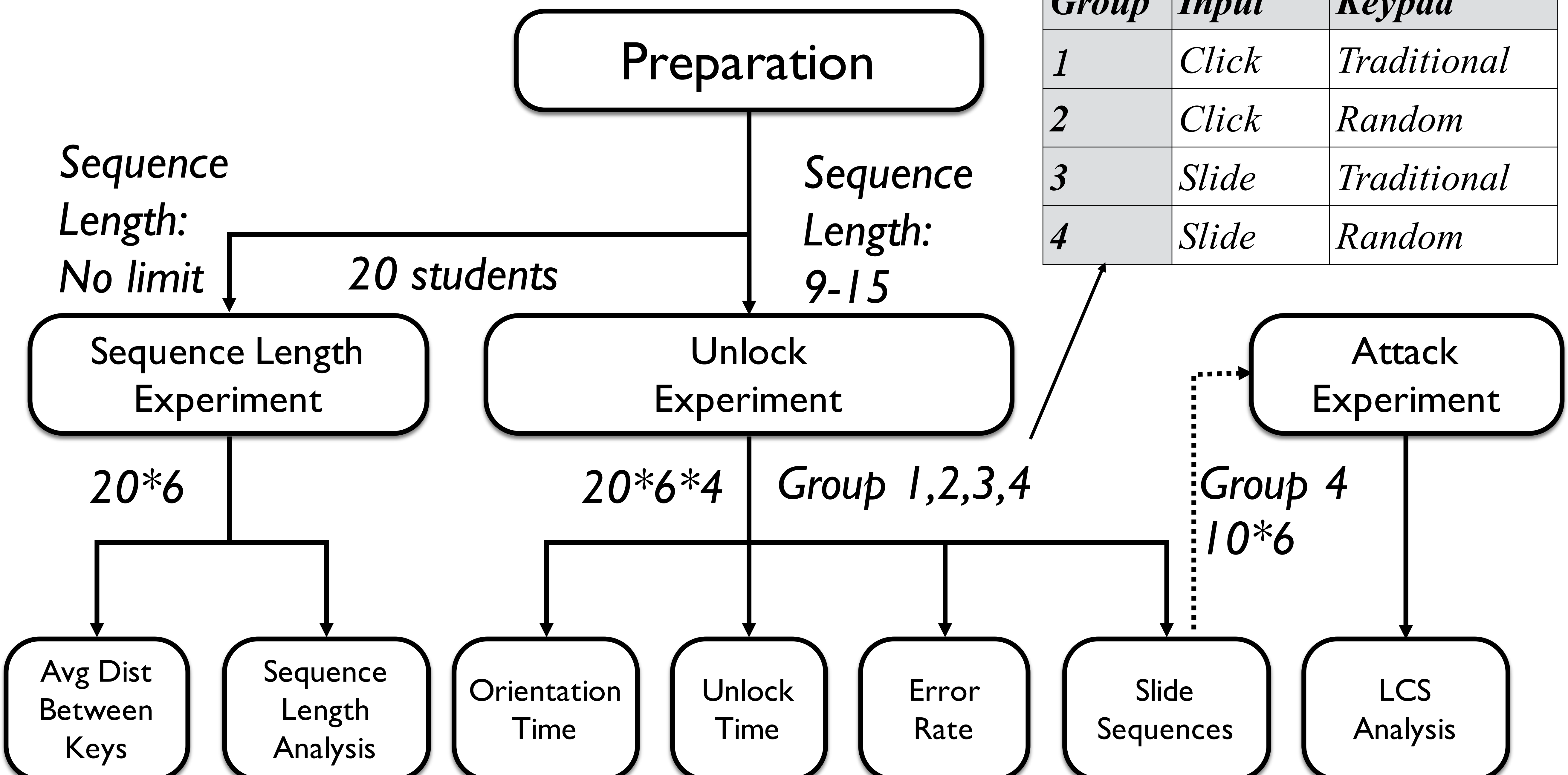
Attack Function

One-Time: F^{-1}(Sequence 1) → PIN

Multi-Time: F^{-1}(Sequence 1, Sequence 2, … … Sequence n) → PIN

实验设计

Group	*Input*	*Keypad*
1	*Click*	*Traditional*
2	*Click*	*Random*
3	*Slide*	*Traditional*
4	*Slide*	*Random*



序列长度分析

Too long | * 0123456789 0123456789 0123456789 0123456789 #

Why

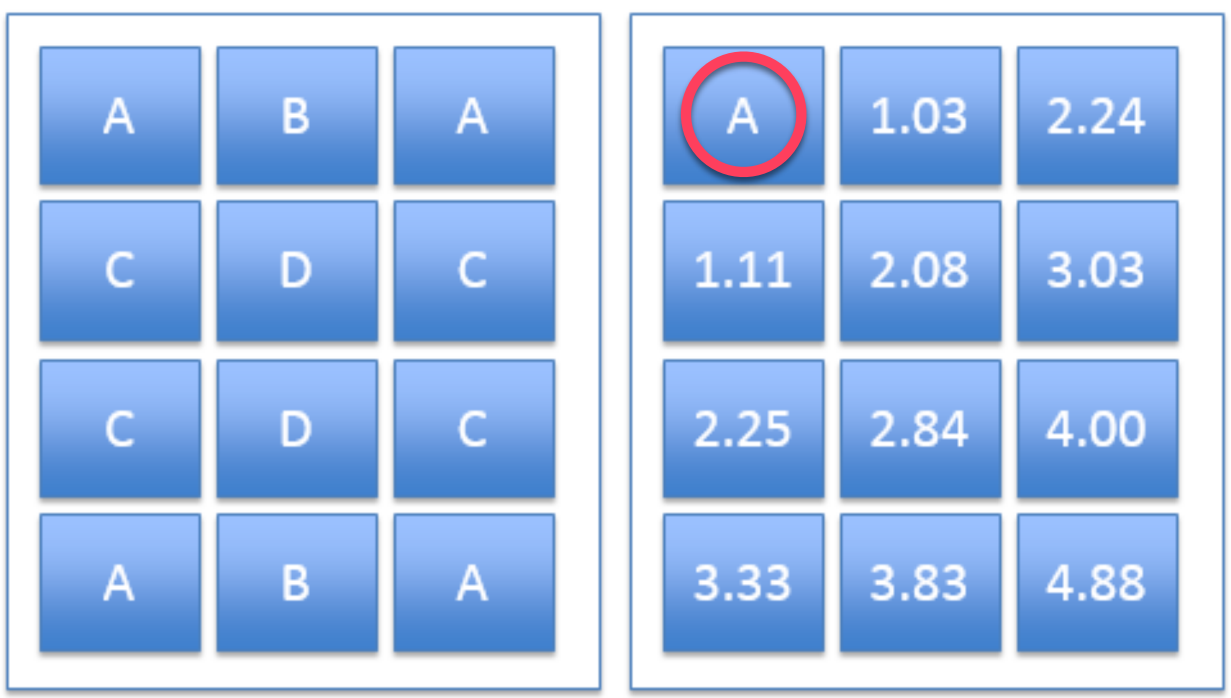
*3816279450#

*381629450#

Too short | *31629450#

How

20 students
** 6 times*



(a) (b)

Estimate of Distance between Keys

D(A)=(1.03+2.24+1.11+2.08+3.03+2.25+2.84+4.00+3.33+3.83+4.88) /11≈2.78

序列长度分析

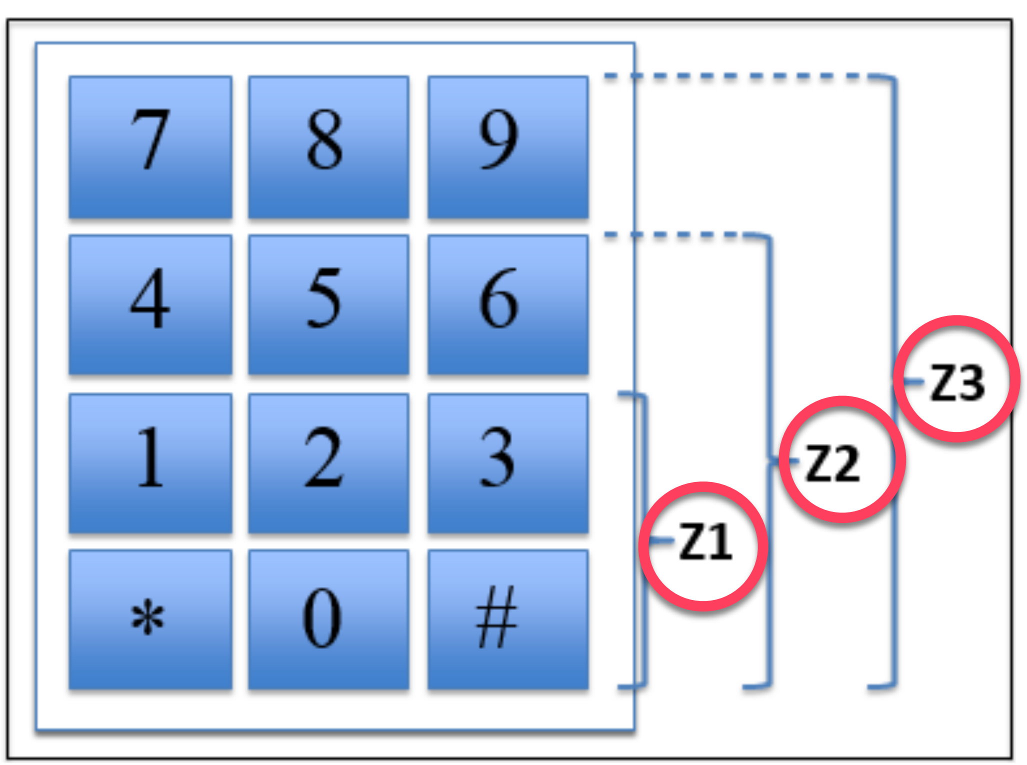
(a) (b) (c)

$D(B) = 2.38$

$D(C) = 2.25$

$D(D) = 1.87$

$Davg = (D(A)*2+D(B)*2) +D(C)*4+D(D)*2) / 10 \approx 2.31$



$P(Z3) = 1$ $D(Z3) = 11.55$

$P(Z2) = 1/6$ $D(Z2) = 10.82$

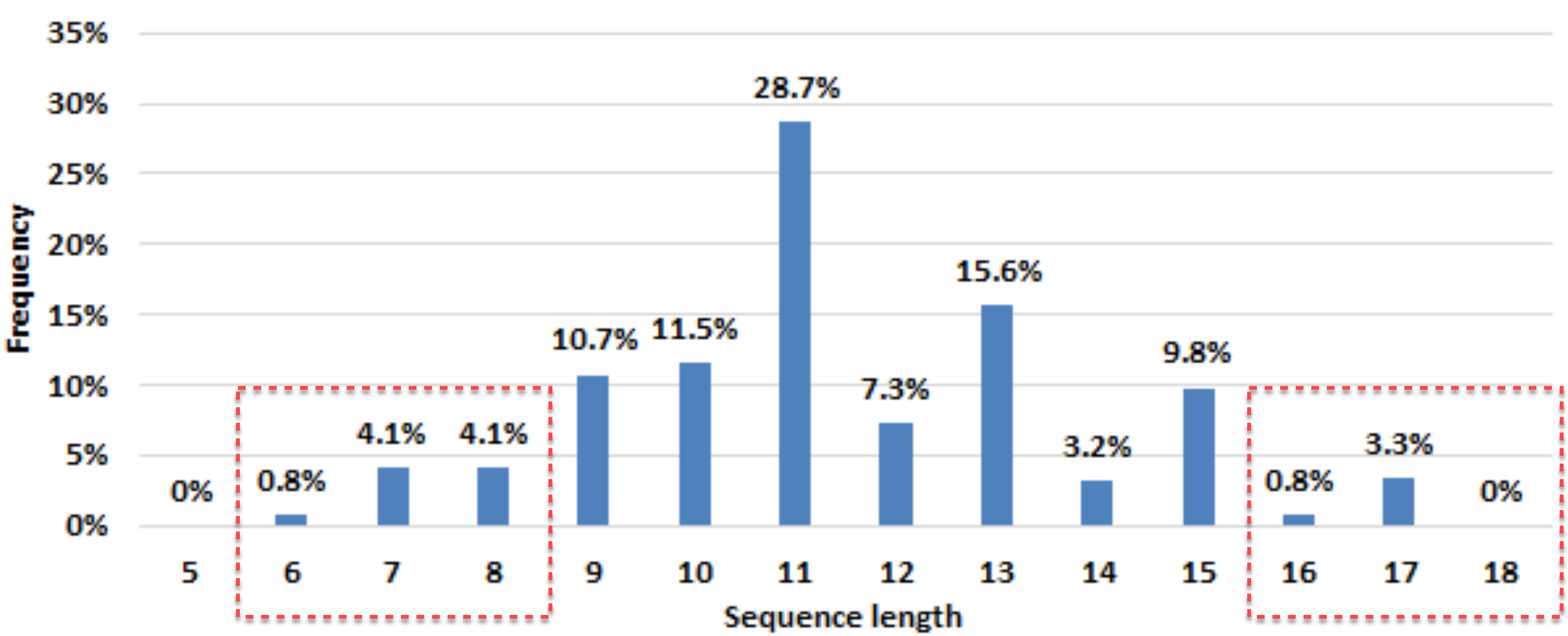
$P(Z1) = 1/200$ $D(Z1) = 8.08$

$8.08 * 1.87 \approx 15.11$

9 - 15

序列长度分析

- *Estimate of Sequence Length*
  - ✶ *Mean value of sequence length: 11.55 vs 11.46*
  - ✶ *Lower threshold of sequence length: 9*
  - ✶ *Upper threshold of sequence length: 15*



安全性分析

- *Shoulder surfing attack*

One-Time

Sequence Length	*9*	*10*	*11*	*12*	*13*	*14*	*15*
PIN	*126*	*210*	*330*	*495*	*715*	*1001*	*1365*

Multi-Time

Times	*u1*	*u2*	*u3*	*u4*	*u5*	*u6*	*u7*	*u8*	*u9*	*u10*
2	*6*	*6*	*6*	*6*	*7*	*6*	*6*	*7*	*6*	*4*
3	*5*	*5*	*4*	*4*	*4*	*4*	*4*	*5*	*4*	
4	*4*	*4*						*4*		

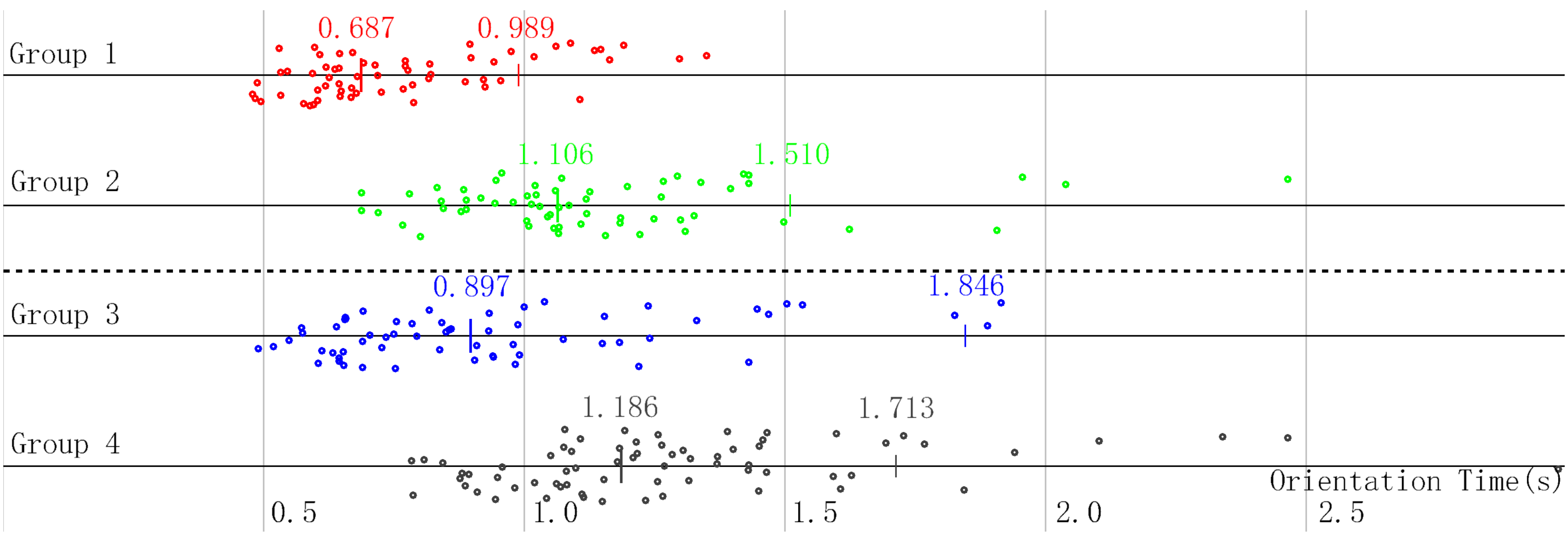
- *Guessing attack*
  - ✴ *Brute force attack*
  - ✴ *Dictionary attack*

- *Replay attack*
  - ✴ *Random numeric keypad*

可用性分析

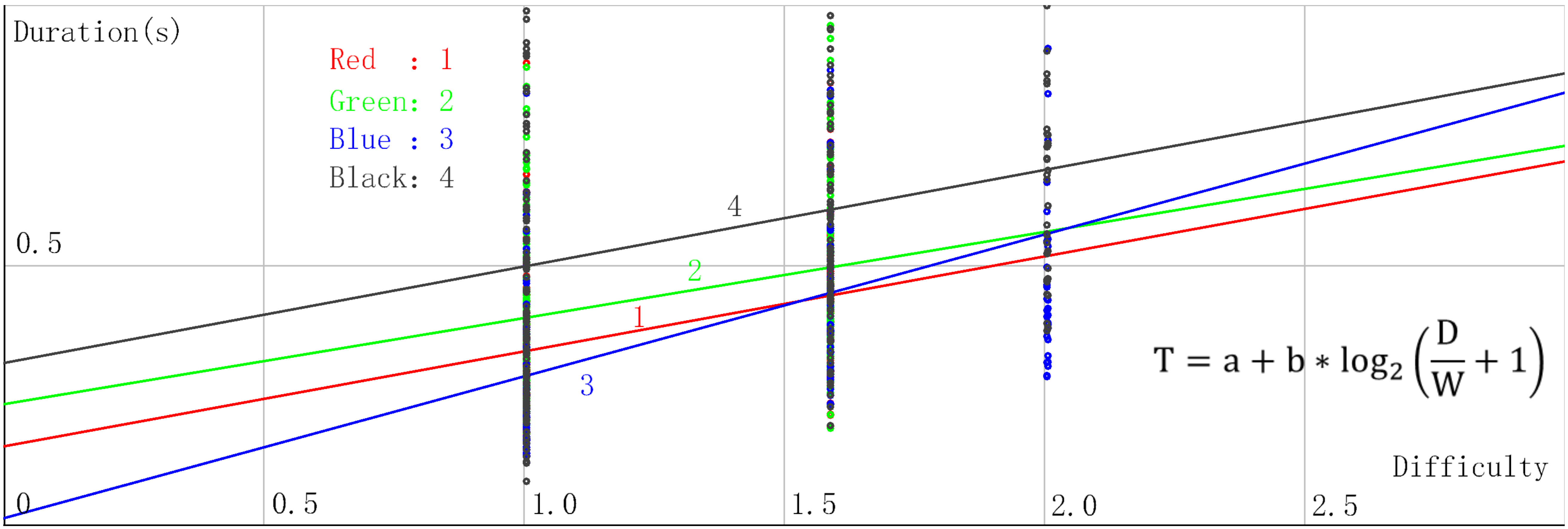
- *Orientation time*

Groups	Average	Standard Deviation	Threshold Value
1	0.687	0.133	0.989
2	1.064	0.199	1.510
3	0.798	0.293	1.846
4	1.186	0.225	1.713



可用性分析

- *Unlock time*
  - ✴ *Sliding is faster*
  - ✴ *Input sequences become longer*
  - ✴ *Random number keypad increases unlock time*



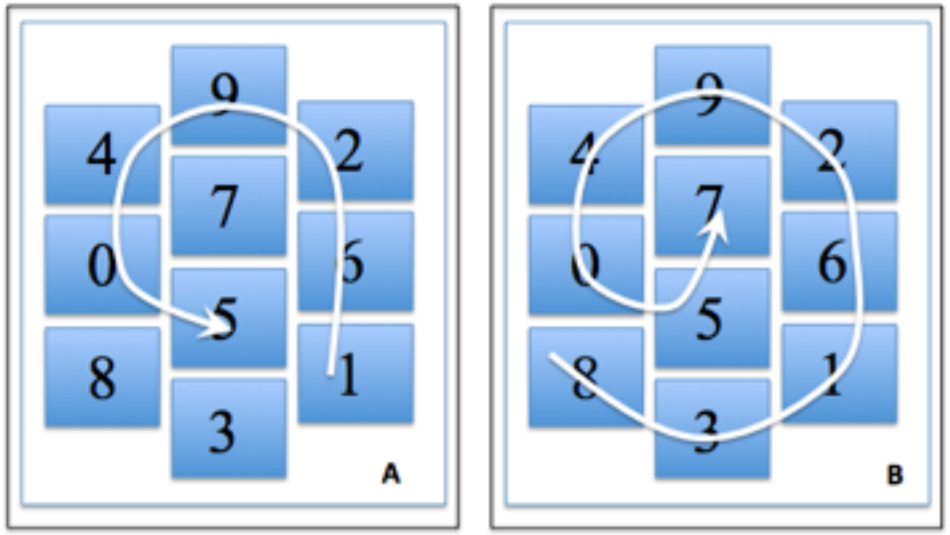
可用性分析

- Error rate
  - *Sequence length limit*
  - *Start point and end point*
  - *Not familiar enough*

Groups	*Error Rate*
1	*1.67%*
2	*3.33%*
3	*7.69%*
4	*13.04%*

- Cost of learning
  - *SlidePIN is built based on 4-digits PIN*
  - *SlidePIN is easy to use*
  - *SlidePIN is interesting to use*

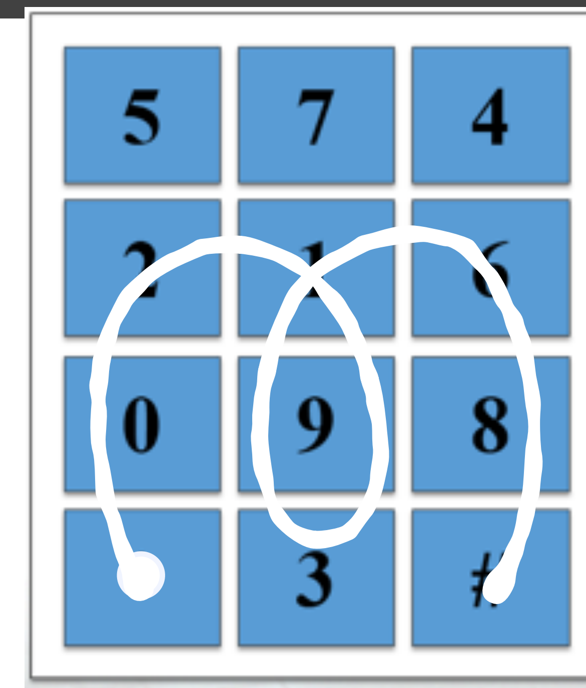
讨论



PIN: 1245

PIN: 2118

*021939168#



1: Fixed start point and end point

2: Same adjacent Digits

3: PIN storage

Device ID or SIM ID

↓

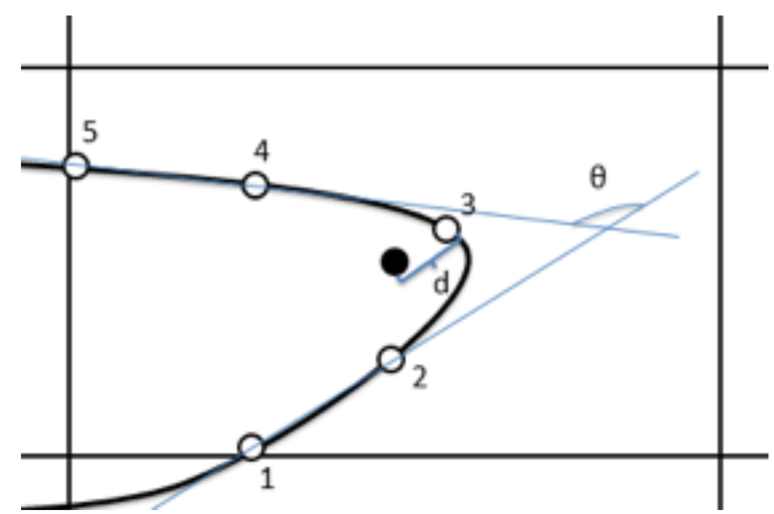
Key

↓ encrypt

PIN

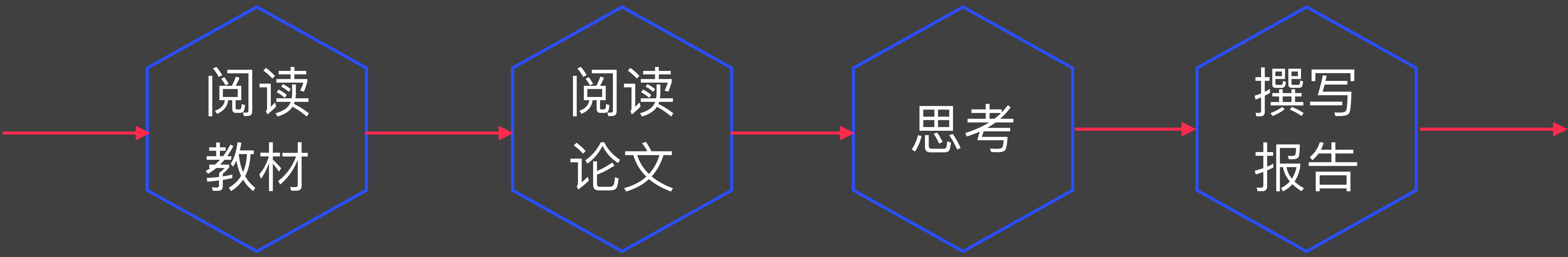
4: Smudge attack

5: Attack based on Features



提问时间！

课后作业



Homework

课后作业

要求阅读如下文章，写阅读报告

Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns

Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz
Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany
{firstname.lastname}@rub.de

ACM CCS'2013

检索一篇引用该论文的2018以后的论文，简单阅读

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

10月18日晚上12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io