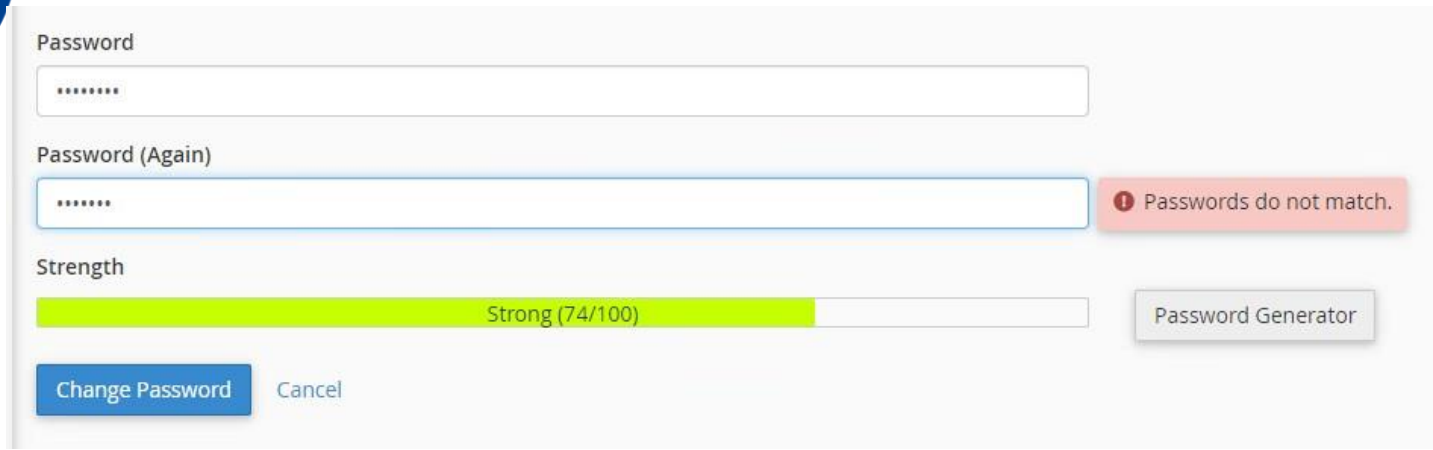
认证

李澄清

2024年3月9日

www.chengqingli.com


Password
Password (Again)
Passwords do not match.
Strength
Strong (74/100)
Password Generator
Change Password
Cancel


非接触式IC卡
RFID
中国建设银行
China Construction Bank
支持刷脸取款

认证


ON THE INTERNET
nobody knows you're a dog


Wait, she's really a human??
ICANHASCHEEZBURGER.COM


B2
B1
1 2 3
4 5 6
7 8 9
* 0 #

AI诈骗

警惕！AI诈骗正在全国爆发，科技公司老板被骗430万

包头警方日前发布一起利用人工智能（AI）实施电信诈骗的典型案例，福州市某科技公司法人代表郭先生10分钟内被骗430万元。AI技术改变诈骗方式，诈骗成功率接近100%。

高度逼真: 可精准地模拟他人的声音、面孔、表情、动作等细节，让受害者难以分辨真假，从而降低警惕。

难以追踪: 随时更换伪造的身份、号码、地址等信息，犯罪分子隐匿在网络的阴暗角落，给警方侦破带来困难。

针对性强: 根据受害者的个人信息、社交关系、消费习惯等进行精准定位，制定出最合适的骗局方案，提高成功率。

手段多样: 结合各种诈骗手段，如冒充亲友、领导、客服等要求转账汇款；冒充明星、网红、富豪等诱导交友恋爱；冒充公检法、银行、保险等威胁恐吓等。

https://www.thepaper.cn/newsDetail_forward_23193760

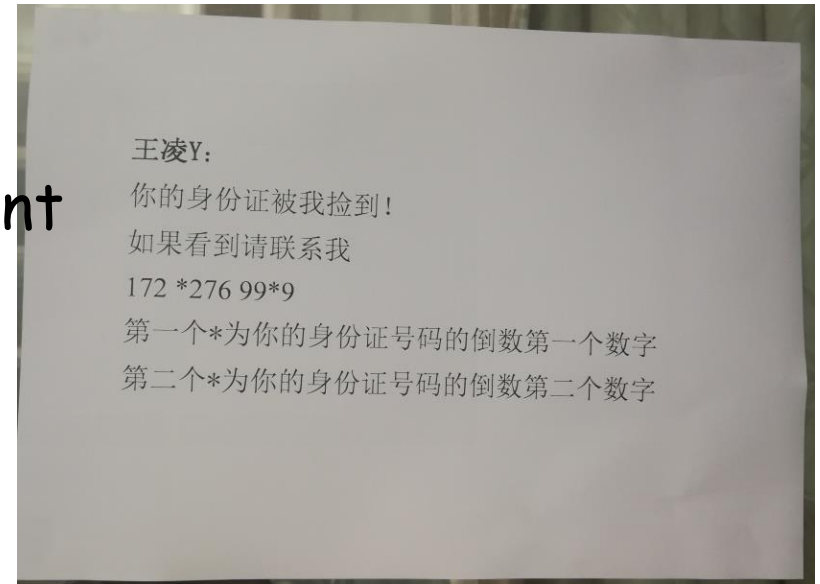
《生成式人工智能服务管理办法（征求意见稿）》 国家互联网信息办公室 2023年4月11日

Access Control

- Two parts to access control…
- **Authentication:** Are you who you say you are?
  - Determine whether access is allowed or not
  - Authenticate human to machine
  - Or, possibly, machine to machine
- **Authorization:** Are you allowed to do that?
  - Once you have access, what can you do?
  - Enforces limits on actions
- Note: "access control" often used as synonym for authorization

Are You Who You Say You Are?

- Authenticate a human to a machine?
- Can be based on…
  - Something you **know**
    - For example, a password
  - Something you **have**
    - For example, a smartcard
  - Something you **are**
    - For example, your fingerprint



Something You Know

- Passwords
- Lots of things act as passwords!
  - PIN
  - Social security number
  - Mother's maiden name
  - Date of birth
  - Name of your pet, etc.

Trouble with Passwords

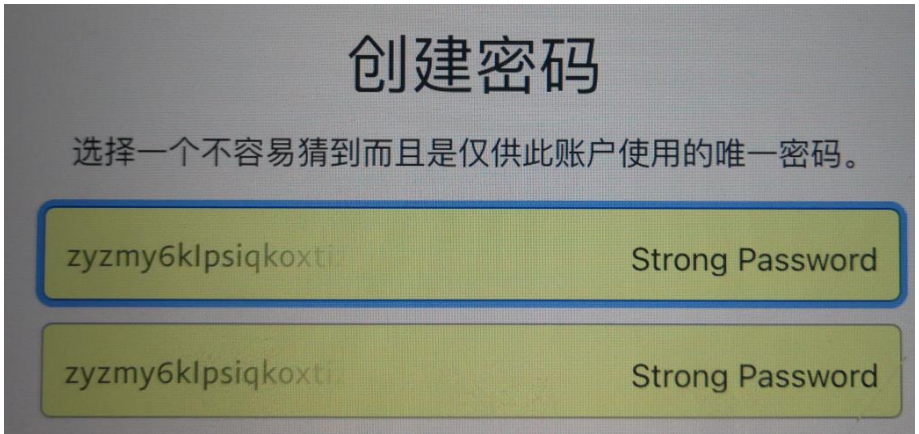
- "Passwords are one of the biggest practical problems facing security engineers today."
- "Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed.)"

Why Passwords?

- Why is "something you know" more popular than "something you have" and "something you are"?
- **Cost**: passwords are free
- **Convenience**: easier for sysadmin to reset pwd than to issue a new thumb

Keys vs Passwords

- **Crypto keys**
- Spse key is 64 bits
- Then 2^{64} keys
- Choose key at random…
- …then attacker must try about 2^{63} keys



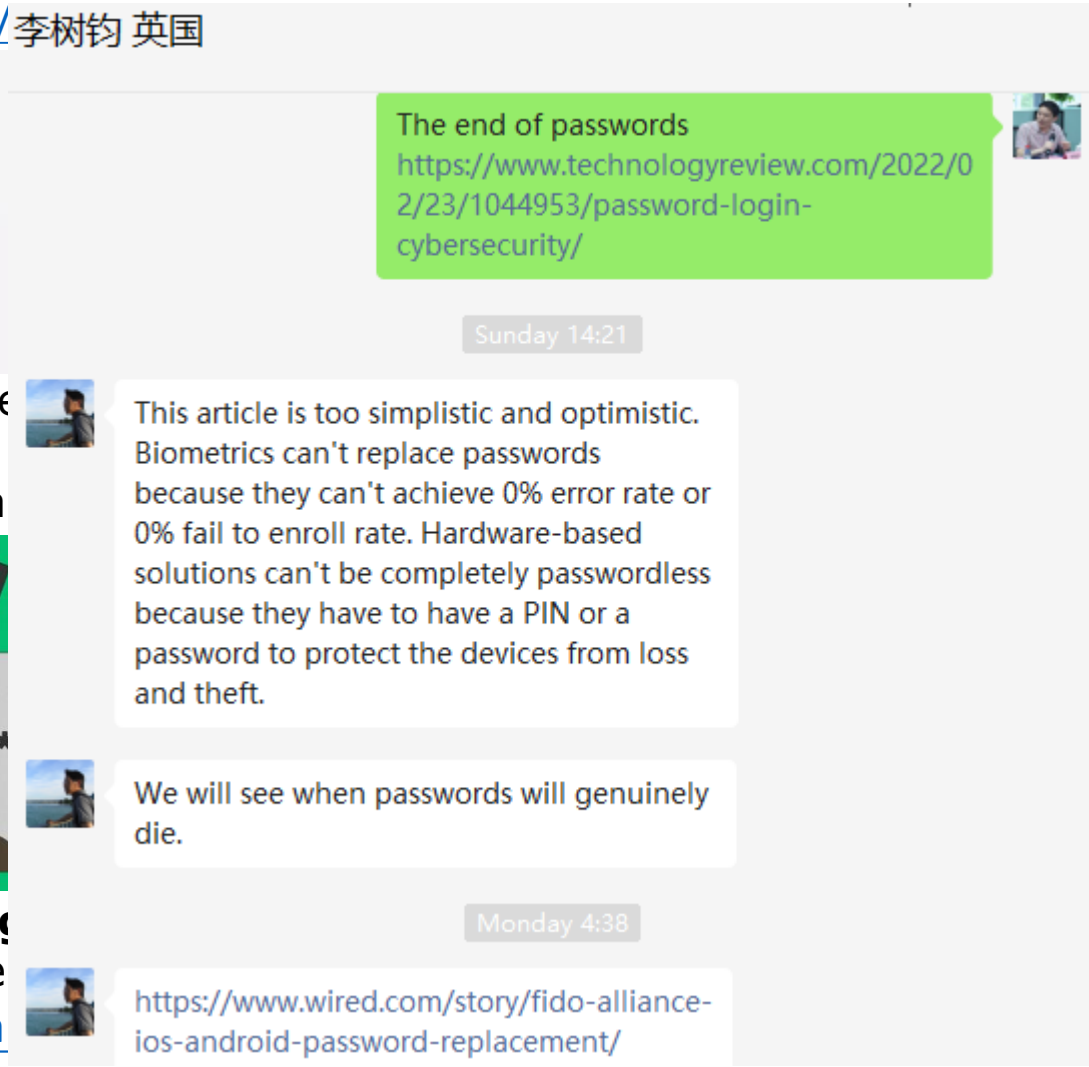
- **Passwords**
- Spse passwords are 8 characters, and 256 different characters
- Then $256^8 = 2^{64}$ pwds
- Users do not select passwords at random
- Attacker has far less than 2^{63} pwds to try (dictionary attack)

Password (口令)

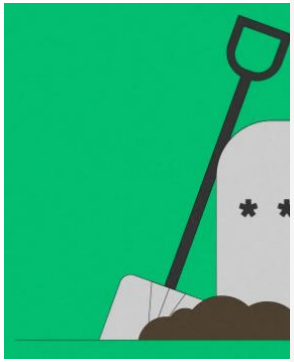
The end of passwords

Companies are finally shifting away from notoriously insecure alphanumerics to other methods of authentication

www.technologyreview.com/2022/02/



Biometrics can't replace passwords be
fail to enroll rate. Hardware-based
because they have to have a PIN or a
theft.



A big bet to kill the password for g

Not using a password should be easie

www.wired.com/story/fido-alliance-ios-a

Password (口令)

请选择安全认证方式

* 选择认证方式

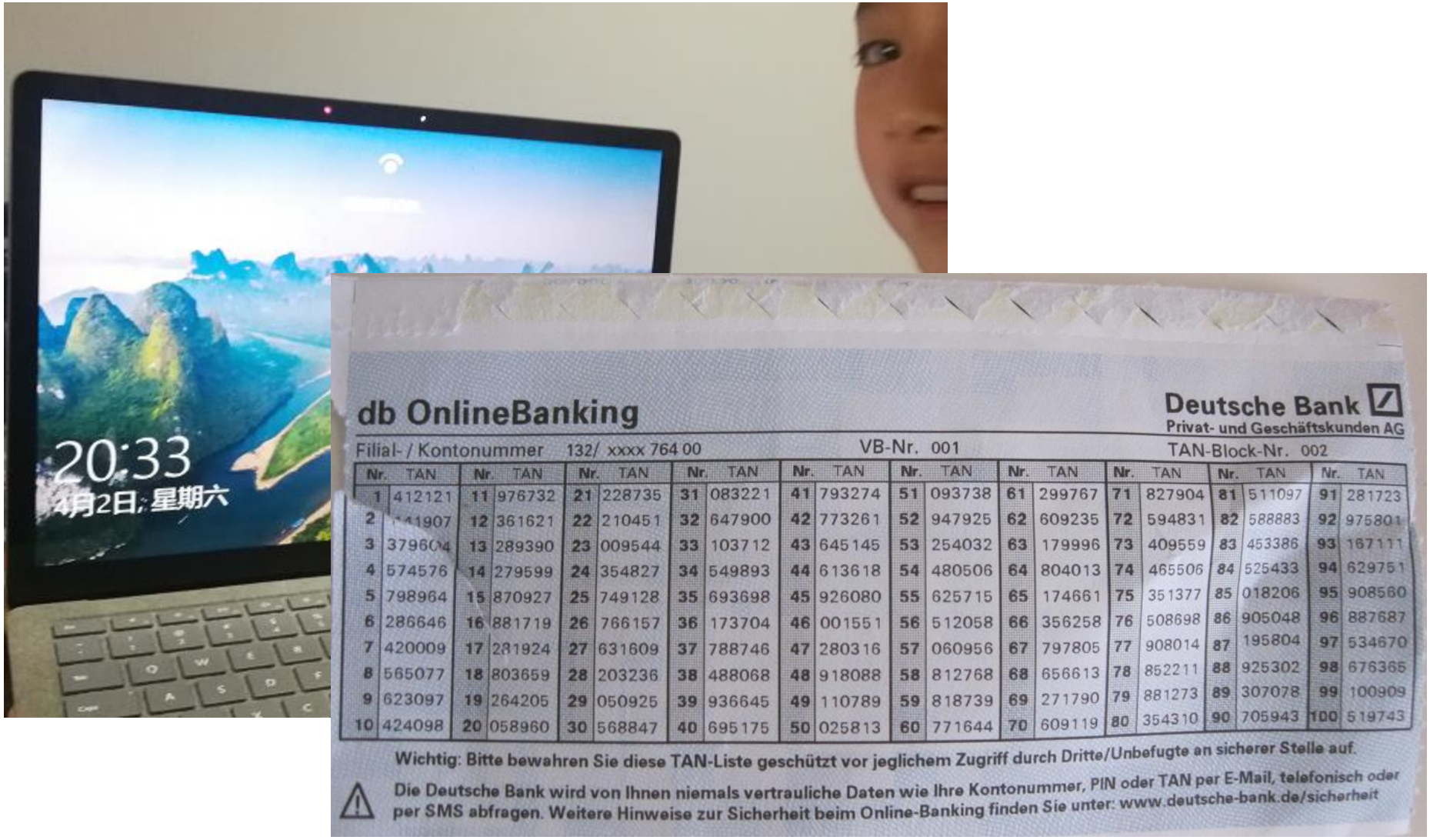
请用手机银行扫描二维码验证，日累计交易限额50,000元。
调整限额

* 请扫描二维码

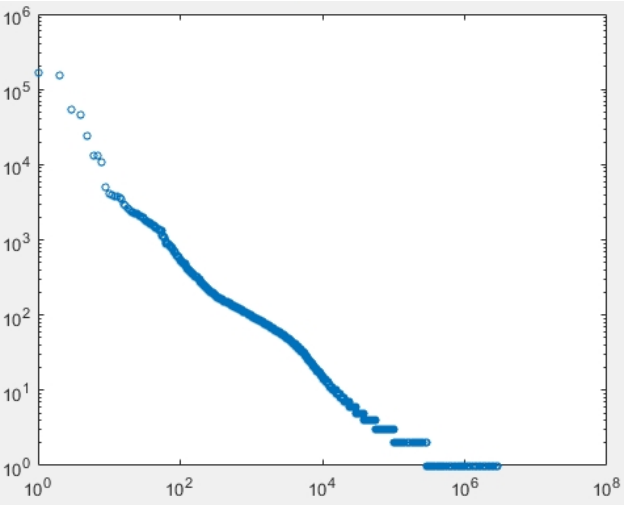
请使用我行手机银行客户端（4.0及以上版本）扫描二维码。

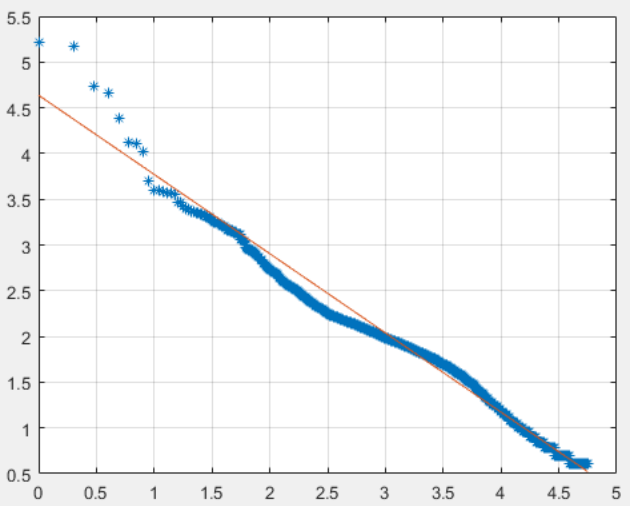
The Best Password Managers to Secure Your Digital Life
www.wired.com/story/best-password-managers

Password (口令)


20:33
4月2日, 星期六
db OnlineBanking
Deutsche Bank
Privat- und Geschäftskunden AG
Filial- / Kontonummer 132/ xxxx 764 00
VB-Nr. 001
TAN-Block-Nr. 002
Nr. TAN
1 412121
2 [illegible]907
3 379604
4 574576
5 798964
6 286646
7 420009
8 565077
9 623097
10 424098
11 976732
12 361621
13 289390
14 279599
15 870927
16 881719
17 281924
18 803659
19 264205
20 058960
21 228735
22 210451
23 009544
24 354827
25 749128
26 766157
27 631609
28 203236
29 050925
30 568847
31 083221
32 647900
33 103712
34 549893
35 693698
36 173704
37 788746
38 488068
39 936645
40 695175
41 793274
42 773261
43 645145
44 613618
45 926080
46 001551
47 280316
48 918088
49 110789
50 025813
51 093738
52 947925
53 254032
54 480506
55 625715
56 512058
57 060956
58 812768
59 818739
60 771644
61 299767
62 609235
63 179996
64 804013
65 174661
66 356258
67 797805
68 656613
69 271790
70 609119
71 827904
72 594831
73 409559
74 465506
75 351377
76 508698
77 908014
78 852211
79 881273
80 354310
81 511097
82 588883
83 453386
84 525433
85 018206
86 905048
87 195804
88 925302
89 307078
90 705943
91 281723
92 975801
93 167111
94 629751
95 908560
96 887687
97 534670
98 676365
99 100909
100 519743
Wichtig: Bitte bewahren Sie diese TAN-Liste geschützt vor jeglichem Zugriff durch Dritte/Unbefugte an sicherer Stelle auf.
Die Deutsche Bank wird von Ihnen niemals vertrauliche Daten wie Ihre Kontonummer, PIN oder TAN per E-Mail, telefonisch oder per SMS abfragen. Weitere Hinweise zur Sicherheit beim Online-Banking finden Sie unter: www.deutsche-bank.de/sicherheit

Password





1、常用口令排名（前20名）

passwd | count
123456789 | 235029
12345678 | 212766
11111111 | 76348
dearbook | 46052
00000000 | 34953
123123123 | 20010
1234567890 | 17794
88888888 | 15033
111111111 | 6995
147258369 | 5966
aaaaaaaa | 5890
987654321 | 5555
1111111111 | 5145
66666666 | 5026
a123456789 | 4686
11223344 | 4096
1qaz2wsx | 3969
password | 3654
xiazhili | 3649
789456123 | 3611
ilove*** | 12031

2、大学统计

根据邮箱后缀来统计各大学注册人数

mail.ustc.edu.cn 2035 中科大
sjtu.edu.cn 1876 上海交大
bjtu.edu.cn 1341 北京交大
fudan.edu.cn 981 复旦
stu.xjtu.edu.cn 930 西安交大
zju.edu.cn 876 浙大
mails.tsinghua.edu.cn 716 清华
bit.edu.cn 691 北京理工
mail.nankai.edu.cn 640 南开
stu.edu.cn 559 汕头大学
emails.bjut.edu.cn 487 北京工大
swu.edu.cn 450 西南大学
nenu.edu.cn 413 东北师范
ustc.edu 345 中科大
mail.dhu.edu.cn 327 东华大学
cqu.edu.cn 311 重庆大学
pku.edu.cn 309 北大
mail.sdu.edu.cn 309 山东大学
stu.snnu.edu.cn 299 陕西师范大学
cqut.edu.cn 260 重庆理工

640万csdn口令数据分析
https://blog.csdn.net/wzkyy/article/details/84121058

On the Implications of Zipf's Law in Passwords
https://doi.org/10.1007/978-3-319-45744-4_6

Password

3、80后统计
把密码设为日期的应该就是自己的出生日期了吧
来统计一下80后
birth count
1980 15374
1981 21923
1982 34535
1983 35144
1984 39849
1985 41709
1986 50940
1987 59569
1988 53519
1989 45269
----- ------
397831

4、注册邮箱排名（前20）
qq.com 1972584
163.com 1763310
126.com 806199
sina.com 350870
yahoo.com.cn 205110
hotmail.com 202361
gmail.com 186086
sohu.com 104554
yahoo.cn 86797
tom.com 72231
yeah.net 53114
21cn.com 50597
vip.qq.com 35055
139.com 29105
263.net 24756
sina.com.cn 19103
live.cn 18860
sina.cn 18574
yahoo.com 18338
foxmail.com 16382

5、没有重复的密码：
!(*!!
!()!!!^
!((%)*)(QWtxd
!((%!((%
!(($)
!((!)*)
!((!)()%
!((
!(&^)^!(
!(&^!!@&
!()!!@
!()!@)(cloud
!()!@)6125dou
!()jian20
!((^)^@@12312
3
!((@0709yxw
!((*03230225tia
n
!()HB1990128
!()0803
!())@)@@

6、两个段子
CSDN杯我最喜欢的口令大决选总冠军

ppnn13%dkstFeb.1st
中文解析：
娉娉袅袅十三余，豆蔻梢头二月初

经查，没有这个密码

CSDN杯我最喜欢的口令大决选季军

FLZX3000cY4yhx9day
飞流直下三千尺，疑似银河下九天

hanshansi.location()!∈[gusucity]
姑苏城外寒山寺）

hold?fish:palm
鱼和熊掌不可兼得

经查，只有FLZX3000C这个存在

Password

CSDN-中文IT社区-600万

Name	Date modified	Type	Size
www.csdn.net.sql	2012/1/12 11:04	SQL File	197,285 KB

www.csdn.net.sql - Notepad

File Edit Format View Help

```
laozhuang # laozhuang # fj9lihu@sina.com
hyzhou # zhy1997 # hyzhou@whu.edu.cn
johnchow # 314000 # jx_zzq@telekbird.com.cn
crazeblue # bluesky # crazebluesky@163.com
stone_xu # 10220712 # xuzsssh@263.net
cxw # 9758 # tianfei@371.net
hxn # 781207 # hxnnj@263.net
Only1You1 # 89313e # getwindow@163.net___csdn_1
nill0705 # nill0705 # nill@kietou.com
wfm # 123 # wfmwfm@263.net
hjf # 04614 # zeybow@hotmail.com
ldmark # 771206 # hlwd@netease.com
miss # miss # wen-xin@126.com
onedolph # 541788 # onedolph@163.com
bgying # dtnet # bgying168@sina.com
microfeng # fengboy # fengboy@371.net
youpeng99 # yp781012 # youpeng99@sina.com
stephenwoo # 19750519 # stevewood_cn@yahoo.com
bluesea # randy0 # hu_rong@263.net
WalkAlone # 942608 # WalkAlone@990.net
wangjue28 # 99603696 # s99online@netease.com
justtouch # 851997 # justtouch@263.net
lwd12345 # lwd12345 # jfyjgs@public2.lyptt.ha.cn
zzhu # zzhu09 # zzhumail@263.net
wjj # 3028 # 1111wjj@sohu.com
dinodino # 511511920920 # only_ahua@163.com
echenz # citier # chenz@soim.com
xawind # 9104122 # wu.derong@mail.zhongxing.com
caojunjie # 41818 # jjcao@hotmail.com
gnt_xxy # gallant # gnt_xxy@371.net
XieZhenMin # mrgmrg # xiezhenmin@cmmail.com
vbo # 6998 # vbo@sina.com
profl # ljf111 # soft_ljf@sina.com
enmy # asd # jh@uyuy.jkjk
```

New password should not match previous 4 passwords

New password

•••

Must be 8 or more characters and contain:
- at least 1 numeral: 0 - 9
- at least 1 alpha character, case-sensitive
- at least 1 symbol: ! @ # $ % ^ * ( ) ~ ' { } [ ] | & _

Confirm new password

Show password

Update password

Problems resetting your password?

用户注册

为了您的账号安全，请输入8位以上、由大小写字母+数字或特殊字符组成的密码，不包含特殊字符的情况下，大小写字母必须同时存在（示例：Hn612331、621233$##、hn2324&#、Hn1233#$），请勿使用该示例密码，以防账号泄露。

South Africa Cyber Incident in 2022

Top 200 most common passwords of the year 2020

Here are the worst 200 passwords of 2020. The list details how many times a password has been exposed, used, and how much time it would take to crack it. We also compare the worst passwords of 2019 and 2020, highlighting how their positions have changed. The green arrows indicate a rise in the position while the red ones - a fall off. Check if your password is on the list and strengthen it if it is.

Position	Password	Time to crack it	Number of users
1 ▲ (2)	123456	< 1 sec	2,543,285
2 ▲ (3)	123456789	< 1 sec	961,435
3 ● (New)	picture1	3 hrs	371,612
4 ▲ (5)	password	< 1 sec	360,467
5 ▲ (6)	12345678	< 1 sec	322,187
6 ▲ (17)	111111	< 1 sec	230,507
7 ▲ (18)	123123	< 1 sec	189,327
8 ▼ (1)	12345	< 1 sec	188,268
9 ▲ (11)	1234567890	< 1 sec	171,724
10 ● (New)	senha	10 sec	167,728
11 ▲ (12)	1234567	< 1 sec	165,909
12 ▼ (10)	qwerty	< 1 sec	156,765

https://nordpass.com/json-data/top-worst-passwords/pdfs/worst-passwords-2020.pdf

South Africa Cyber Incident

The "N4ughtysecTu" threat actor also told us they didn't steal any user credentials but performed a brute force attack on the SFTP server. The account they ultimately breached was allegedly using the password "Password", so it was quick and straightforward to brute-force.
www.bleepingcomputer.com/news/security/hackers-claim-to-breach-transunion-south-africa-with-password-password
https://newsroom.transunion.co.za/update-south-africa-cyber-incident

Just this week password allegedly allowed hackers to break in to a server, steal data and issue a $15 million ransom demand to the victim.
https://www.forbes.com/sites/leemathews/2022/03/20/a-password-set-to-password-leads-to-a-15-million-ransom-demand/?sh=19b0d6ffcaba

Good and bad Passwords

- Bad passwords
  - frank
  - Fido
  - Password
  - incorrect
  - Pikachu
  - 102560
  - AustinStamp

- Good Passwords?
  - jfIej,43j-EmmL+y
  - 0986437653726 3
  - POkemON
  - FSa7Yago
  - OnceuPOnAt1m8
  - PokeGCTall150

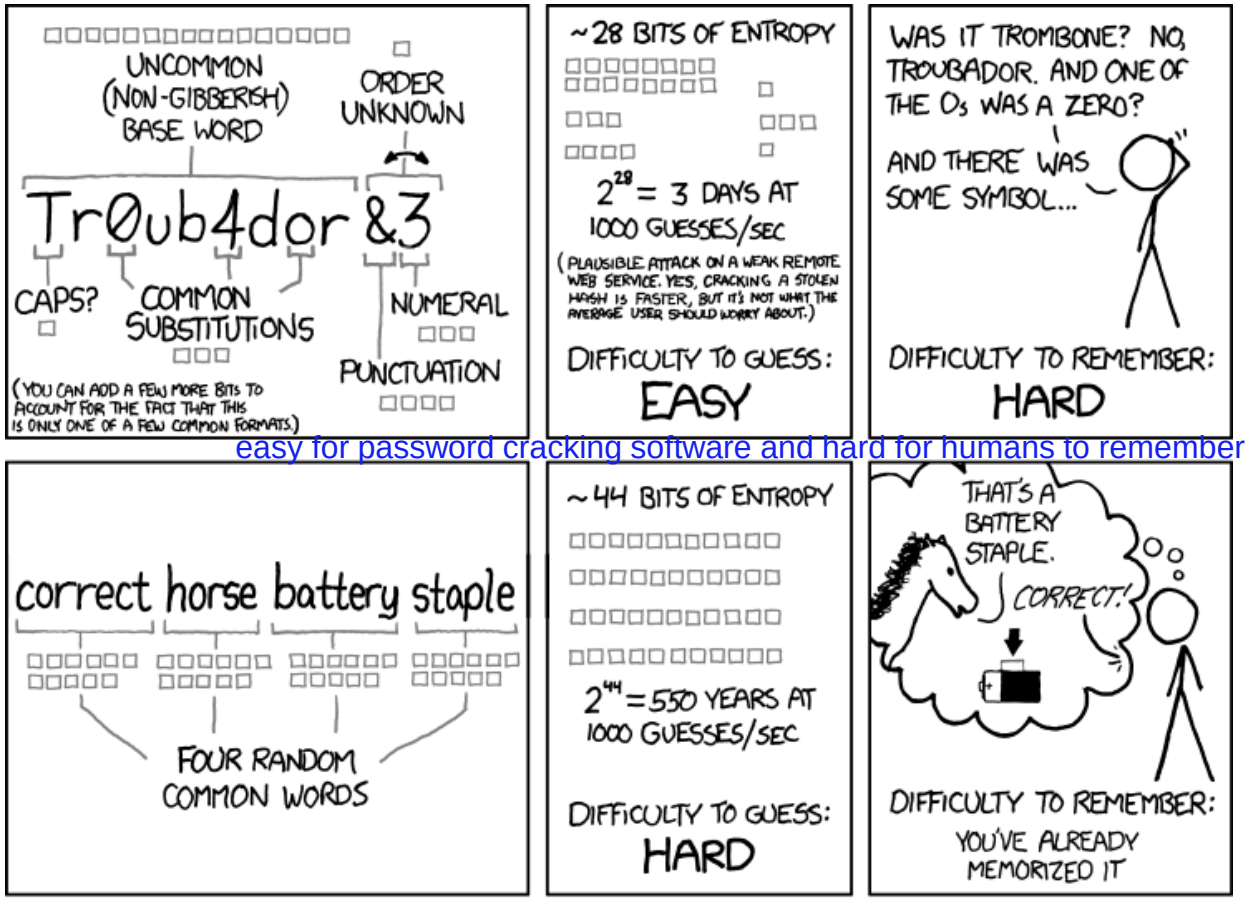
Passphrase: derived from the phrase "**f**our **s**core **a**nd **seven** **y**ears **ago**"

Good and bad Passwords

When people choose their own keys, they generally choose poor ones. They'1e far more likely to choose "Barney" than "*9lhH/A." This is not always due to poor security practices; "Barney" is easier to remember than "*9lhH/A."
The world’s most secure algorithm won't help much if the users habitually choose their spouse’s names for keys or write their keys on little pieces of paper in their wallets.
A smart brute-force attack doesn't try all possible keys in numerical order; it tries the obvious keys first.

Passwords are difficult to use and manage, which drives people to take shortcuts like reusing them across accounts and creates security issues at every turn.

Password strength



trombone

Troubador

"Tr0ub4dor&3"

Caps: the written abbreviation of capital letters

easy for password cracking software and hard for humans to remember

xkcd Password Generator

https://preshing.com/20110811/xkcd-password-generator

www.explainxkcd.com/wiki/index.php/936:_Password_Strength

Password Experiment

- Three groups of users — each group advised to select passwords as follows
  - **Group A:** At least 6 chars, 1 non-letter
  - **Group B:** Password based on passphrase
  - **Group C:** 8 random characters
- Results
  - **Group A:** About 30% of pwds easy to crack
  - **Group B:** About 10% cracked
    - Passwords easy to remember
  - **Group C:** About 10% cracked
    - Passwords hard to remember

Password Experiment

- User compliance hard to achieve
- In each case, 1/3rd did not comply
  - And about 1/3rd of those easy to crack!
- Assigned passwords sometimes best
- If passwords not assigned, best advice is…
  - Choose passwords based on passphrase
  - Use pwd cracking tool to test for weak pwds
- Require periodic password changes?

Password Retry

- Suppose system locks after 3 bad passwords. How long should it lock?
  - 5 seconds
  - 5 minutes
  - Until SA restores service
- What are +'s and -'s of each?

Password File?

- Bad idea to store passwords in a file
- But we need to verify passwords
- Solution? **Hash** passwords
  - Store $y = h(\text{password})$
  - Can verify entered password by hashing
  - If Trudy obtains the password file, she does not (directly) obtain passwords
- But Trudy can try a *forward search*
  - Guess x and check whether $y = h(x)$

Dictionary Attack?

- Trudy pre-computes $h(x)$ for all x in a **dictionary** of common passwords
- Suppose Trudy gets access to password file containing hashed passwords
  - She only needs to compare hashes to her pre-computed dictionary
  - After one-time work of computing hashes in dictionary, actual attack is trivial
- Can we prevent this forward search attack? Or at least make it more difficult?

Salt (Random Value)

- Hash password with **salt**
- Choose random salt s and compute

$$y = h(\text{password}, s)$$

  and store (s,y) in the password file
- Note that the salt s is not secret
  - Analogous to IV
- Still easy to verify salted password
- But lots more work for Trudy
  - Why?

Password Cracking: Do the Math

- Assumptions:
- Pwds are 8 chars, 128 choices per character
  - Then $128^8 = 2^{56}$ possible passwords
- There is a **password file** with 2^{10} pwds
- Attacker has **dictionary** of 2^{20} common pwds
- **Probability** 1/4 that password is in dictionary
- **Work** is measured by number of hashes

Password Cracking: Case I

- Attack 1 specific password ***without*** using a dictionary
  - E.g., administrator's password
  - Must try $2^{56}/2 = 2^{55}$ on average
  - Like exhaustive key search
- Does **salt** help in this case?

Password Cracking: Case II

- Attack 1 specific password ***with*** dictionary
- With **salt**
  - Expected work: $1/4\ (2^{19}) + 3/4\ (2^{55}) \approx 2^{54.6}$
  - In practice, try all pwds in dictionary…
  - …then work is at most 2^{20} and probability of success is $1/4$
- What if **no salt** is used?
  - One-time work to compute dictionary: 2^{20}
  - Expected work is of same order as above
  - But with precomputed dictionary hashes, the "in practice" attack is essentially free…

Password Cracking: Case III

- Any of 1024 pwds in file, ***without*** dictionary
  - Assume all 2^{10} passwords are distinct
  - Need 2^{55} **comparisons** before expect to find pwd
- If **no salt** is used
  - Each computed hash yields 2^{10} comparisons
  - So expected work (hashes) is $2^{55}/2^{10} = 2^{45}$
- If **salt** is used
  - Expected work is 2^{55}
  - Each comparison requires a hash computation

Password Cracking: Case IV

- Any of 1024 pwds in file, ***with*** dictionary
  - Prob. one or more pwd in dict.: $1-(3/4)^{1024} \approx 1$
  - So, we ignore case where no pwd is in dictionary
- If **salt** is used, expected work less than 2^{22}
  - See book, or slide notes for details
  - Work $\approx$ size of dictionary / P(pwd in dictionary)
- What if **no salt** is used?
  - If dictionary hashes not precomputed, work is about $2^{19}/2^{10} = 2^9$

Other password Issues

- Too many passwords to remember
  - Results in password reuse
  - Why is this a problem?
- Who suffers from bad password?
  - Login password vs ATM PIN
- Failure to change default passwords
- Social engineering
- Error logs may contain "almost" passwords
- Bugs, keystroke logging, spyware, etc.

Passwords

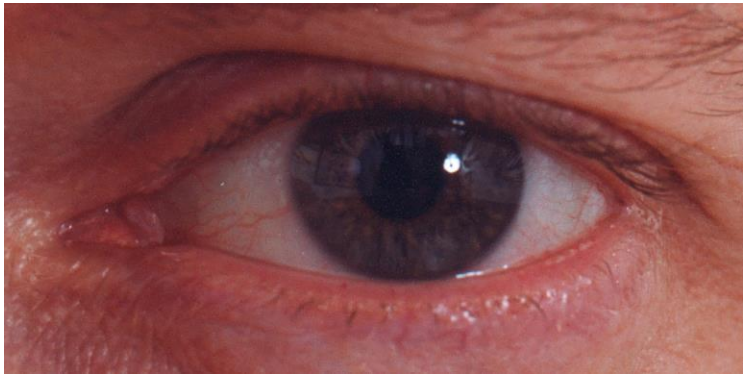
- The bottom line…
- **Password attacks are too easy**
  - Often, one weak password will break security
  - Users choose bad passwords
  - Social engineering attacks, etc.
- Trudy has (almost) all of the advantages
- All of the math favors bad guys
- Passwords are a **BIG** security problem
  - And will continue to be a problem

Passwords Crack Tools

- Popular password cracking tools
  - Password Crackers
  - Password Portal
  - L0phtCrack and LC4 (Windows)
  - John the Ripper (Unix)
- Passper for ZIP https://passper.imyfone.com/zip-password-unlocker

  VeryPDF PDF Password Remover https://www.verypdf.com
- Admins should use these tools to test for weak passwords since attackers will use them.
- Good articles on password cracking
  - Passwords - Conerstone of Computer Security
  - Passwords revealed by sweet deal

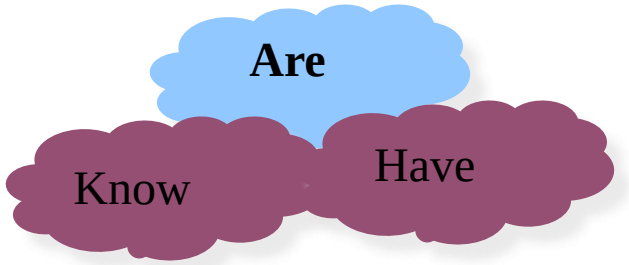
Biometrics



Something you are

- Biometric
  - "You are your key" — Schneier

- Examples
  - Fingerprint
  - Handwritten signature
  - Facial recognition
  - Speech recognition
  - Gait (walking) recognition
  - "Digital doggie" (odor recognition)
  - Many more!



Why Biometrics?

- May be better than passwords
- But, cheap and reliable biometrics needed
  - Today, an active area of research
- Biometrics **are** used in security today
  - Thumbprint mouse
  - Palm print for secure entry
  - Fingerprint to unlock car door, etc.
- But biometrics not really that popular
  - Has not lived up to its promise/hype (yet?)

Idea Biometrics

- **Universal** — applies to (almost) everyone
  - In reality, no biometric applies to everyone
- **Distinguishing** — distinguish with certainty
  - In reality, cannot hope for 100% certainty
- **Permanent** — physical characteristic being measured never changes
  - In reality, OK if it to remains valid for long time
- **Collectable** — easy to collect required data
  - Depends on whether subjects are cooperative
- Also, safe, user-friendly, and ???

Biometrics Modes

- **Identification** — Who goes there?
  - Compare **one-to-many**
  - Example: FBI fingerprint database
- **Authentication** — Are you who you say you are?
  - Compare **one-to-one**
  - Example: Thumbprint mouse
- Identification problem is more difficult
  - More "random" matches since more comparisons
- We are (mostly) interested in authentication

Enrollment vs Recognition

- Enrollment phase
  - Subject's biometric info put into database
  - Must carefully measure the required info
  - OK if slow and repeated measurement needed
  - Must be very precise
  - May be a weak point in real-world use
- Recognition phase
  - Biometric detection, when used in practice
  - Must be quick and simple
  - But must be reasonably accurate

Cooperative Subjects?

- Authentication — cooperative subjects
- Identification — uncooperative subjects
- For example, facial recognition
  - Used in Las Vegas casinos to detect known cheaters (also, terrorists in airports, etc.)
  - Often, less than ideal enrollment conditions
  - Subject will try to confuse recognition phase
- Cooperative subject makes it much easier
  - We are focused on authentication
  - So, we can assume subjects are cooperative

Biometrics Errors

- **Fraud rate** versus **insult rate**
  - Fraud — Trudy mis-authenticated as Alice
  - Insult — Alice not authenticated as Alice
- For any biometric, can decrease fraud or insult, but other one will increase
- For example
  - 99% voiceprint match ⇒ low fraud, high insult
  - 30% voiceprint match ⇒ high fraud, low insult
- **Equal error rate:** rate where fraud == insult
  - A way to ***compare*** different biometrics

Fingerprint History

- 1823 — Professor Johannes Evangelist Purkinje discussed 9 fingerprint patterns
- 1856 — Sir William Hershel used fingerprint (in India) on contracts
- 1880 — Dr. Henry Faulds article in *Nature* about fingerprints for ID
- 1883 — Mark Twain's *Life on the Mississippi* (murderer ID'ed by fingerprint)

Fingerprint History

- 1888 — Sir Francis Galton developed classification system
  - His system of "minutia" can be used today
  - Also verified that fingerprints do not change
- Some countries require fixed number of "points" (minutia) to match in criminal cases
  - In Britain, at least 15 points
  - In US, no fixed number of points

¥799.00

小米 智能门锁 E10 C级锁芯 指纹锁电子锁家用门锁 防盗门锁NFC密码锁

50万+条评价

小米京东自营旗舰店

¥1299.00

小米 智能门锁 1S标准门锁 碳素黑 指纹锁电子锁密码锁防盗门锁

20万+条评价

小米京东自营旗舰店

¥499.00

京东超市 海尔 (Haier) 智能门锁 T15 指纹锁 C级锁芯 入户门 防盗门锁 门卡密码

2万+条评价

海尔智能设备京东自...

¥498.00

京东超市 指纹锁3D人脸识别密码锁智能锁 电子锁 全自动 入户门标准锁体霸王锁

2万+条评价

五星店铺 米系旗舰店

¥1099.00

英典（YINGDIAN）R10智能门锁指纹锁 3D人脸识别智能锁全自动密码锁入户门电

2万+条评价

英典智能锁京东自营...

Fingerprint Comparison

- Examples of **loops（环型）**, **whorls（螺旋型）**, and **arches（弓形）**
- Minutia extracted from these features（提取细节特征）

Loop (double)

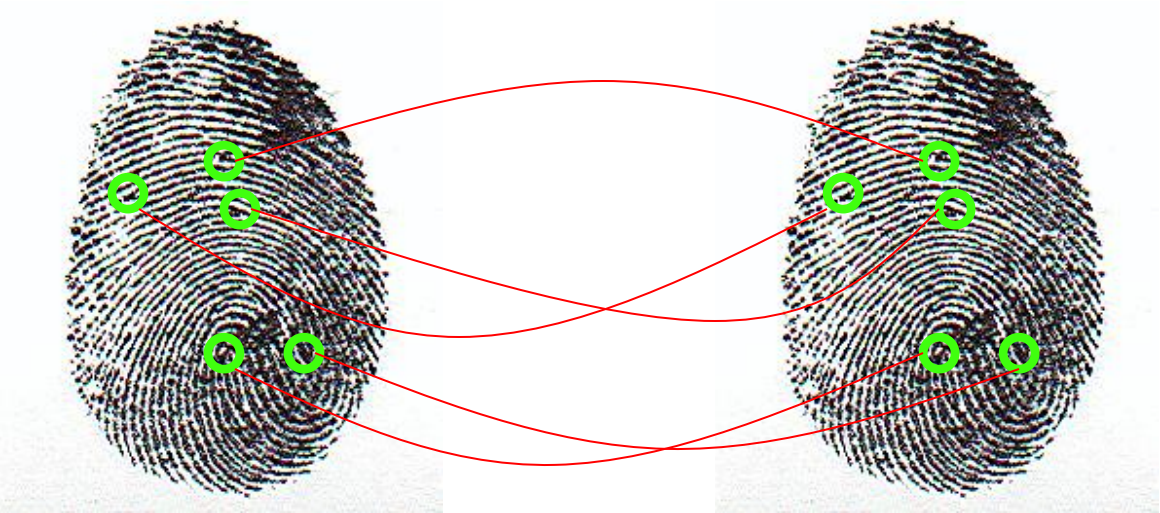
Whorl

Arch

Fingerprint Enrollment

- Capture image of fingerprint
- Enhance image
- Identify "points"

Fingerprint Recognition



- Extracted points are compared with information stored in a database
- Is it a statistical match?
- Aside: Do identical twins' fingerprints differ?

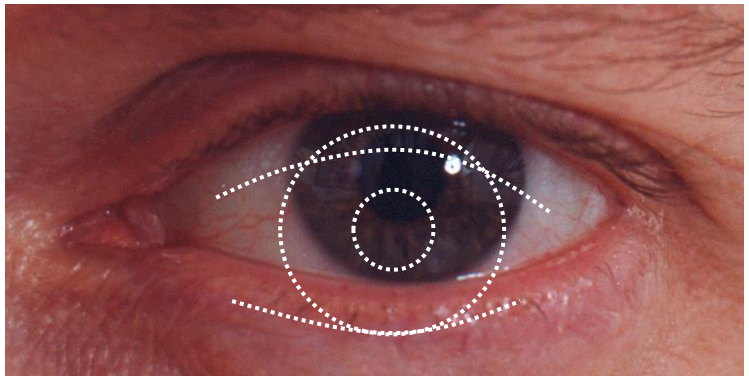
Hand Geometry

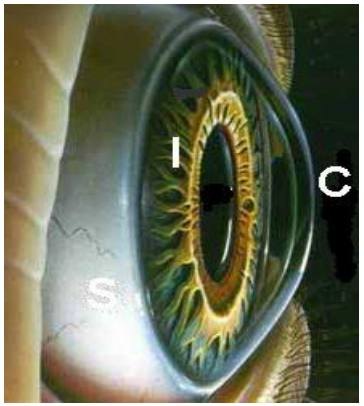
- A popular biometric
- Measures shape of hand
  - Width of hand, fingers
  - Length of fingers, etc.
- Human hands not so unique
- Hand geometry sufficient for many situations
- OK for authentication
- Not useful for ID problem

Hand Geometry

- Advantages
  - Quick — 1 minute for enrollment, 5 seconds for recognition
  - Hands are symmetric — so what?
- Disadvantages
  - Cannot use on very young or very old
  - Relatively high equal error rate

Iris Patterns





- Iris pattern development is "chaotic"
- Little or no genetic influence
- Even for identical twins, uncorrelated
- Pattern is stable through lifetime

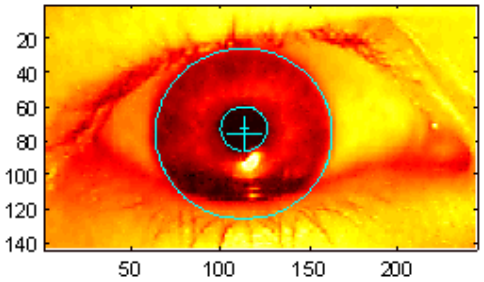
F. Hao, R. Anderson, J. Daugman,
"Combining crypto with biometrics effectively,"
IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088, 2006
http://dx.doi.org/10.1109/TC.2006.138

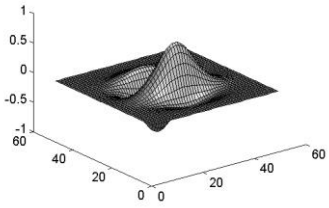
Iris Recognition: History

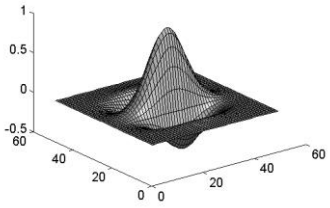
- 1936 — suggested by ophthalmologist
- 1980s — James Bond film(s)
- 1986 — first patent appeared
- 1994 — John Daugman patents new-and-improved technique
  - Patents owned by Iridian Technologies

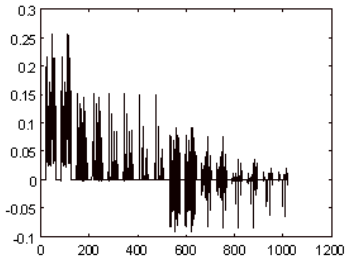
Iris Scan

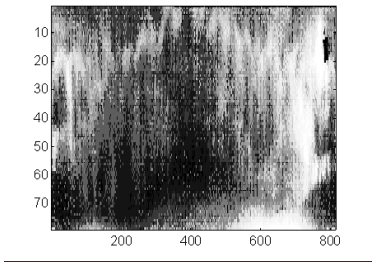
- Scanner locates iris
- Take b/w photo
- Use polar coordinates…
- 2-D wavelet transform
- Get 256 byte iris code











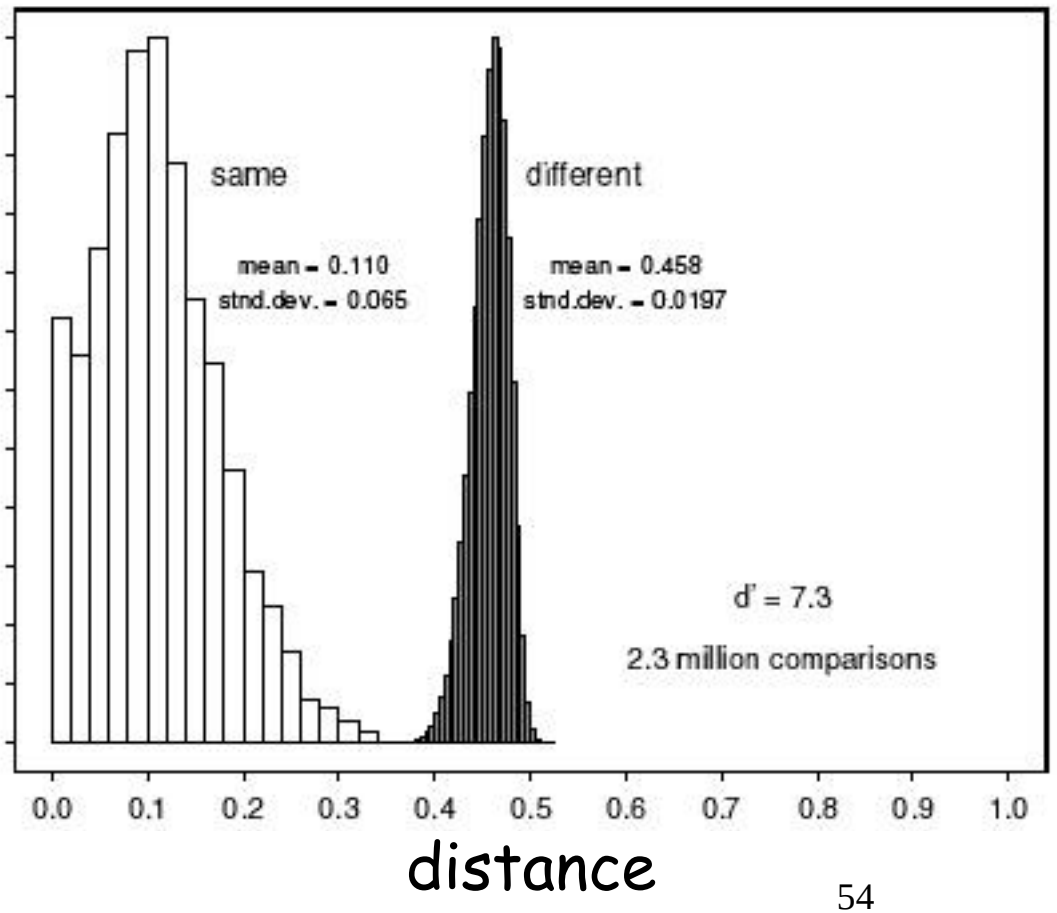
Measuring Iris Similarity

- Based on Hamming distance
- Define $d(x,y)$ to be
  - # of non-match bits / # of bits compared
  - $d(0010,0101) = 3/4$ and $d(101111,101001) = 1/3$
- Compute $d(x,y)$ on 2048-bit iris code
  - Perfect match is $d(x,y) = 0$
  - For same iris, expected distance is 0.08
  - At random, expect distance of 0.50
  - Accept iris scan as match if distance < 0.32

Iris Scan Error Rate

distance	Fraud rate
0.29	1 in $1.3*10^{10}$
0.30	1 in $1.5*10^{9}$
0.31	1 in $1.8*10^{8}$
0.32	1 in $2.6*10^{7}$
0.33	1 in $4.0*10^{6}$
0.34	1 in $6.9*10^{5}$
0.35	1 in $1.3*10^{5}$

== equal error rate



Attack on Iris Scan

- Good **photo** of eye can be scanned
  - Attacker could use photo of eye
- Afghan woman was authenticated by iris scan of old photo
  - Story can be found here
- To prevent attack, scanner could use light to be sure it is a "live" iris

Equal Error Rate Comparison

- Equal error rate (EER): fraud == insult rate
- **Fingerprint** biometrics used in practice have EER ranging from about 10^{-3} to as high as 5%
- **Hand geometry** has EER of about 10^{-3}
- In theory, **iris scan** has EER of about 10^{-6}
  - Enrollment phase may be critical to accuracy
- Most biometrics much worse than fingerprint!
- Biometrics useful for authentication…
  - …but for identification, not so impressive today

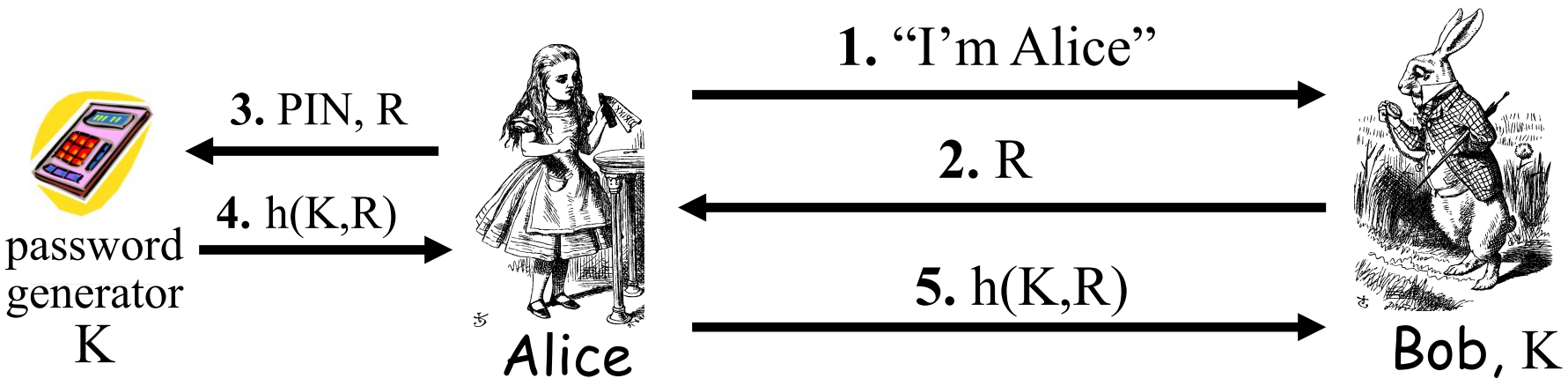
Biometrics: The Bottom Line

- Biometrics are hard to forge
- But attacker could
  - Steal Alice's thumb
  - Photocopy Bob's fingerprint, eye, etc.
  - Subvert software, database, "trusted path" …
- And how to revoke a "broken" biometric?
- **Biometrics are not foolproof**
- Biometric use is relatively limited today
- That should change in the (near?) future

Something you have

- Something in your possession
- Examples include following…
  - Car key
  - Laptop computer (or MAC address)
  - Password generator (next)
  - ATM card, smartcard, etc.

Password Generator



- Alice receives random "challenge" R from Bob
- Alice enters PIN and R in password generator
- Password generator hashes symmetric key K with R
- Alice sends "response" h(K,R) back to Bob
- Bob verifies response
- Note: Alice **has** pwd generator and **knows** PIN

2-factor authorization

- Requires any 2 out of 3 of
  - Something you **know**
  - Something you **have**
  - Something you **are**
- Examples
  - ATM: Card and PIN
  - Credit card: Card and signature
  - Password generator: Device and PIN
  - Smartcard with password/PIN

Single Sign-on

- A hassle to enter password(s) repeatedly
  - Alice would like to authenticate only once
  - "Credentials" stay with Alice wherever she goes
  - Subsequent authentications transparent to Alice
- Kerberos — a single sign-on protocol
- Single sign-on for the Internet?
  - Microsoft: **Passport**
  - Everybody else: **Liberty Alliance**
  - Security Assertion Markup Language (**SAML**)

Web Cookies

- Cookie is provided by a Website and stored on user's machine
- Cookie indexes a database at Website
- Cookies **maintain state** across sessions
  - Web uses a stateless protocol: HTTP
  - Cookies also maintain state within a session
- Sorta like a single sign-on for a website
  - But, very, very weak form of authentication
- Cookies also create privacy concerns

Homework

- 使用Oracle对CSDN口令数据库进行读取和数据挖掘，并计算其口令分布的拟合参数

  New Observations on Zipf'sLaw in Passwords https://doi.org/10.1109/TIFS.2022.3176185

- 找几个生活中感兴趣的认证实例，阐述可用性与安全性的矛盾
- 编程实现基于虹膜生物特征的安全有效认证算法

  Combining crypto with biometrics effectively http://dx.doi.org/10.1109/TC.2006.138