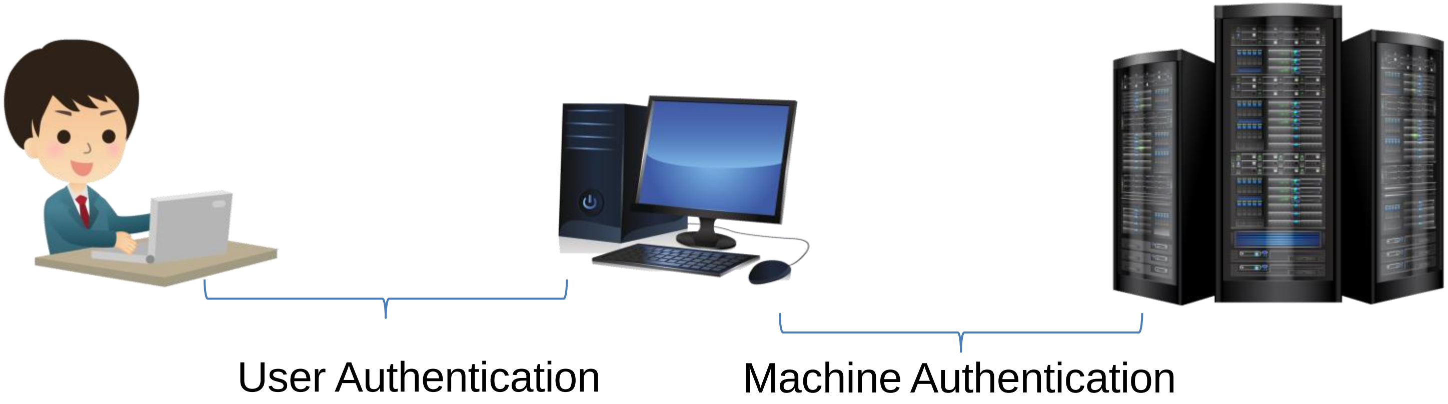


Computer Security

User Authentication

Security is always excessive until it’s not enough.
-Robbie Sinclair

Tamer ABUHMED
Department of Computer Science & Engineering
Sungkyunkwan University

Outline

- Passwords and Password Management
- Attacks on Passwords
- Password Guessing
- Password Selection Guidelines
- Password Spoofing
- Biometric Authentication Approaches
- Two Factor Authentication

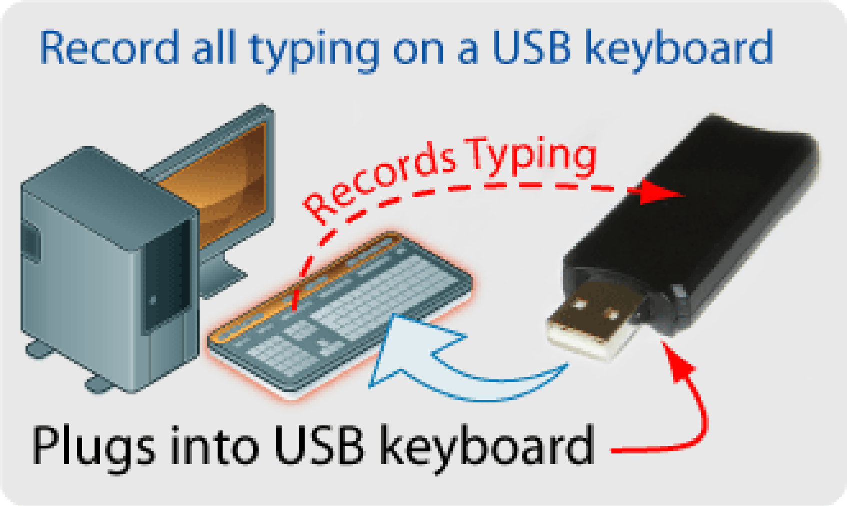
Passwords

- Probably oldest authentication mechanism used in computer systems
- User enters user ID and password, maybe multiple attempts in case of error
- Usability problems
    - Forgotten passwords might not be recoverable
    - Entering passwords is inconvenient
    - If password is disclosed to unauthorized individual, the individual can immediately access protected resource
        - Unless we use multi-factor authentication
    - If password is shared among many people, password updates become difficult

Passwords and Password Management

- A sequence of symbols that only you know and the system that authenticates you can verify
- Not only about Kerberos, but also for all practical systems
  - inevitable mechanism for authentication
- Password related threats
  - Guessing
  - Spoofing
  - Cracking the password file
- Password related rules
  - How to choose
  - How to manage

Attacks on Passwords



Keystroke logging

- Password re-use across sites
- Password guessing

Shoulder surfing

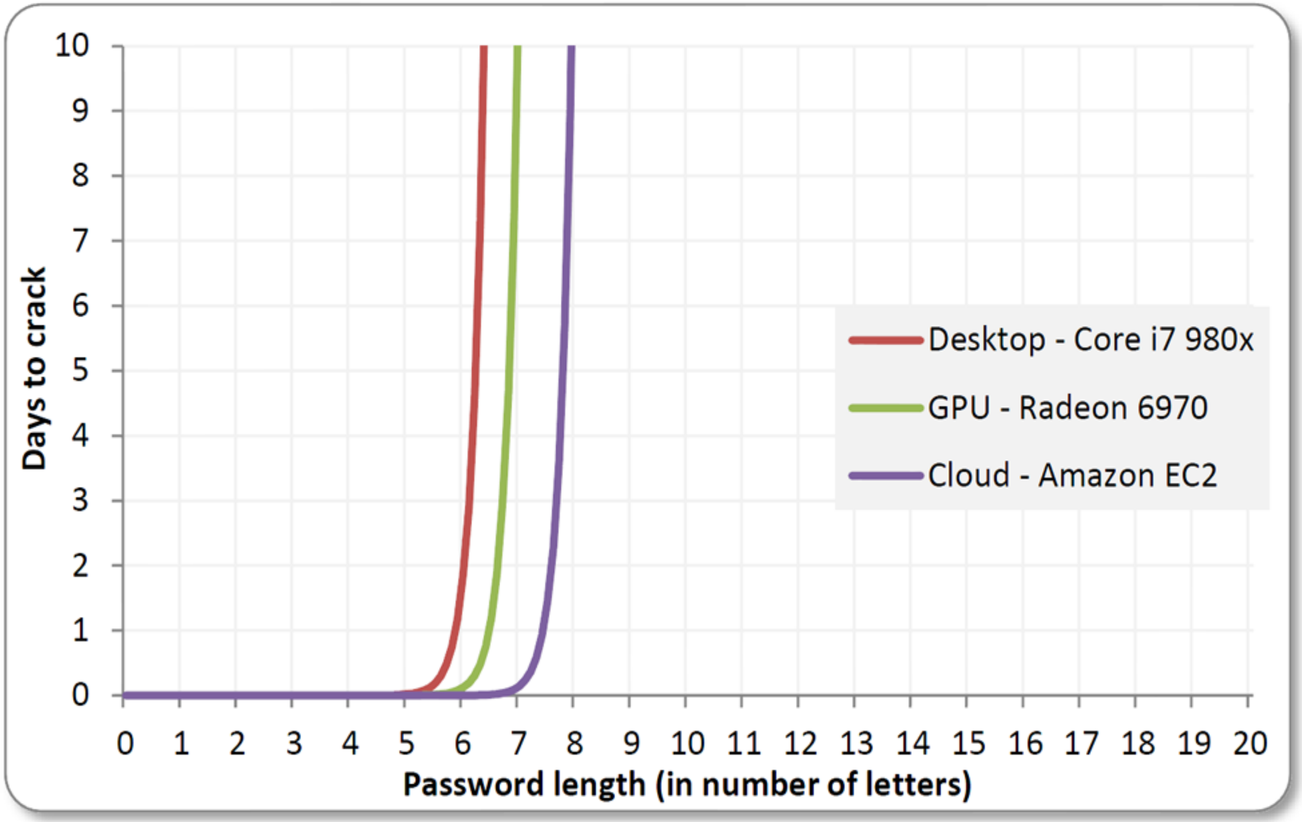
Interface illusions / Phishing

Password Guessing

- Exhaustive Search (Brute Force)
  - try all possible combinations
  - may work if the symbol space and password length are small
- Intelligent Search
  - search possible passwords in a restricted space
    - related to the user: girlfriend/boyfriend name, car brand, phone number, birth date, …
    - generic: meaningful words or phrases, dictionary attack

Brute-forcing passwords is exponential

http://erratasec.blogspot.ca/2012/08/common-misconceptions-of-password.html



Check password crack time: https://howsecureismypassword.net/

Password Selection Guidelines

- “Have” a password and don’t share it
  - do not leave it blank
- Do not use default passwords, change them ASAP
  - like “pass”
- Use mixed symbols
  - upper and lowercase letters, digits, symbols
- use long passwords
- avoid meaningful and obvious words and their derivatives
  - e.g. RoseGarden1, Albert_Levi123
- A useful mechanism: Pick a phrase or sentence and use initials as password
  - e.g. “I hate when system asks me to change password” → Ihwsam2cp
- Evaluate your password here

How the system helps?

- Sysadmin can try to guess a password with known techniques
- Password ageing
  - users are enforced to change their passwords periodically
  - possibly by prohibiting to use old passwords
- Limit login attempts
  - temporarily blocks the account after some login failures
- Use of CAPTCHA

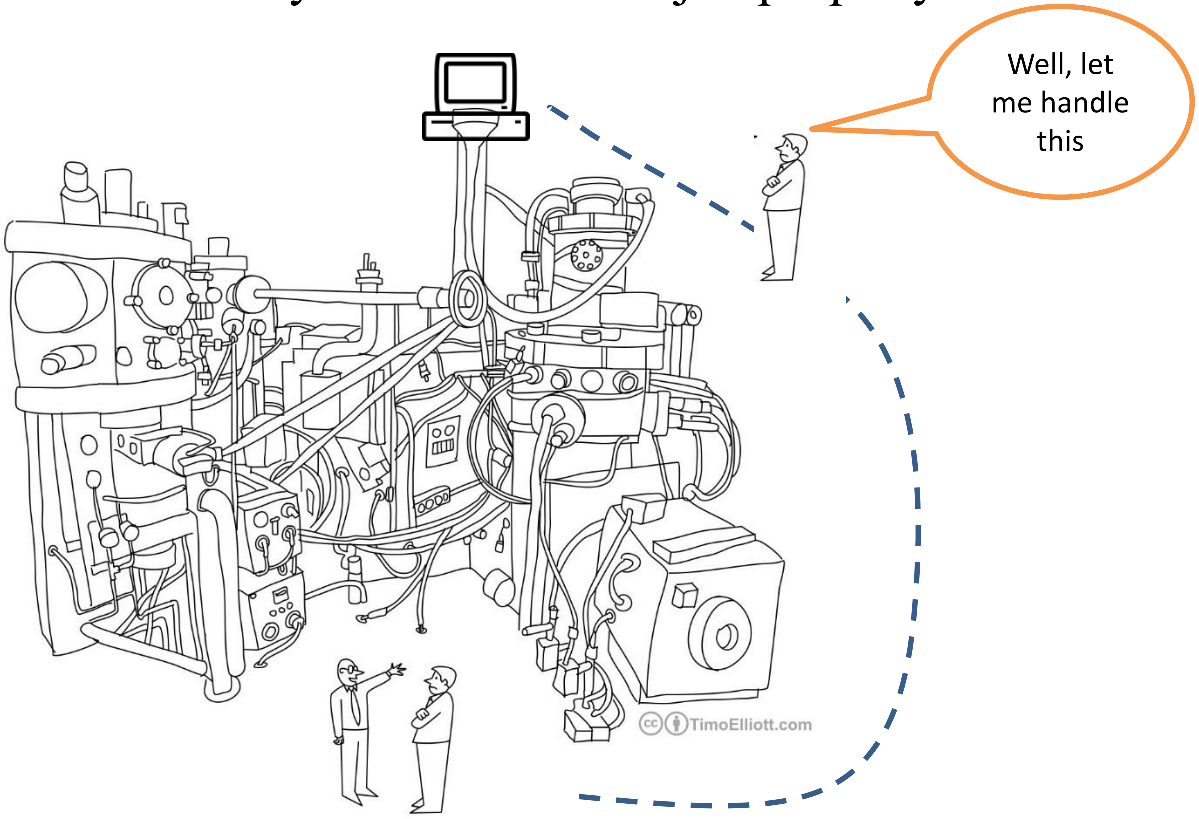
  - To mitigate automated online guessing attempts
- Inform user
  - about last successful login time and number of unsuccessful attempts

Average user behavior

- They do not memorize long and random password
  - instead they prefer to write down passwords
- they tend to derive passwords from the old one
  - e.g. by adding 1, 2, …
  - guessing one makes easier to guess the forthcoming ones
- They prefer not to change or revert back to their original password
  - so it is not a good idea to enforce them to change passwords too often

Rule of thumb

“Enforcing too much security may weaken the system, since the users tend to circumvent security rules to do their job properly”

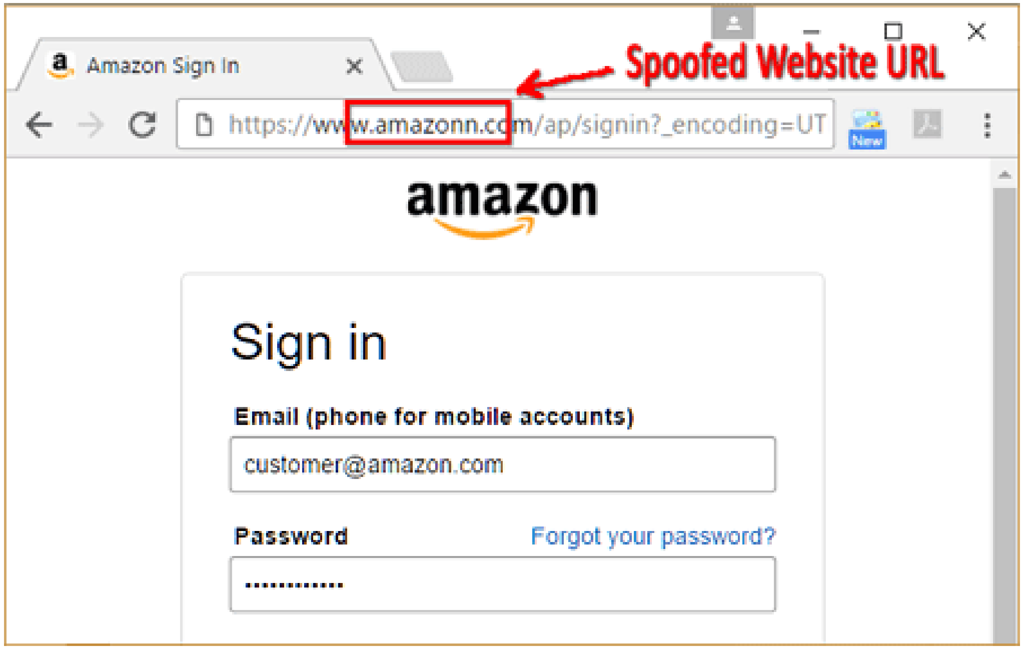


©ⓘ TimoElliott.com

“Well, sure, it looks complicated...”

Password Spoofing

- Are you really talking to the server that you want to talk?
  - fake login prompts
    - when you try to login a shared station
      - previous user may leave a fake login screen
    - how to avoid/detect
      - reboot



Spoofed Website URL

https://www.amazonn.com/ap/signin?_encoding=UT

Sign in

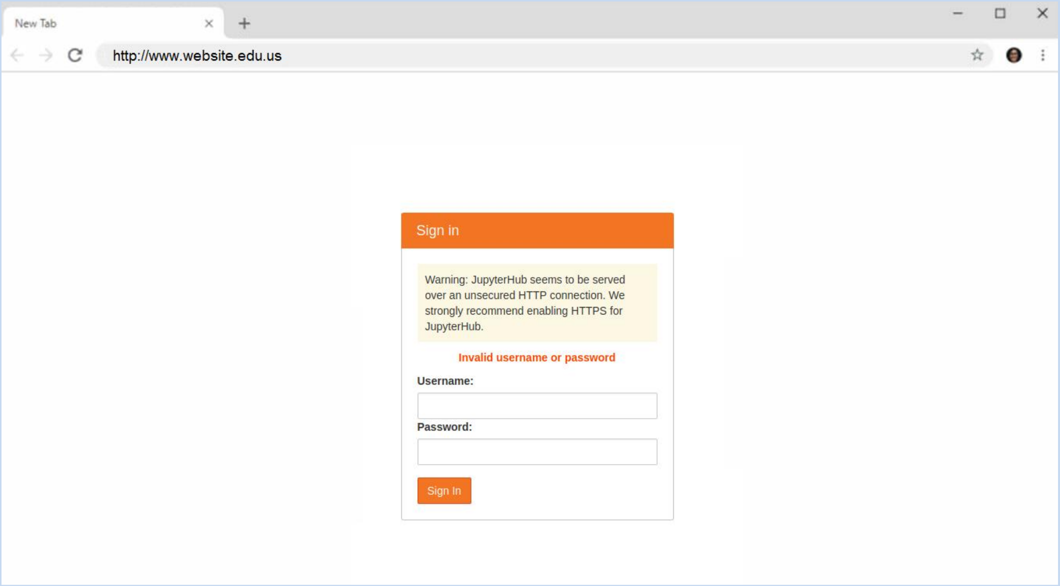
Email (phone for mobile accounts)

customer@amazon.com

Password

·············

Password Spoofing



Sign in

Warning: JupyterHub seems to be served over an unsecured HTTP connection. We strongly recommend enabling HTTPS for JupyterHub.

Invalid username or password

Username:

Password:

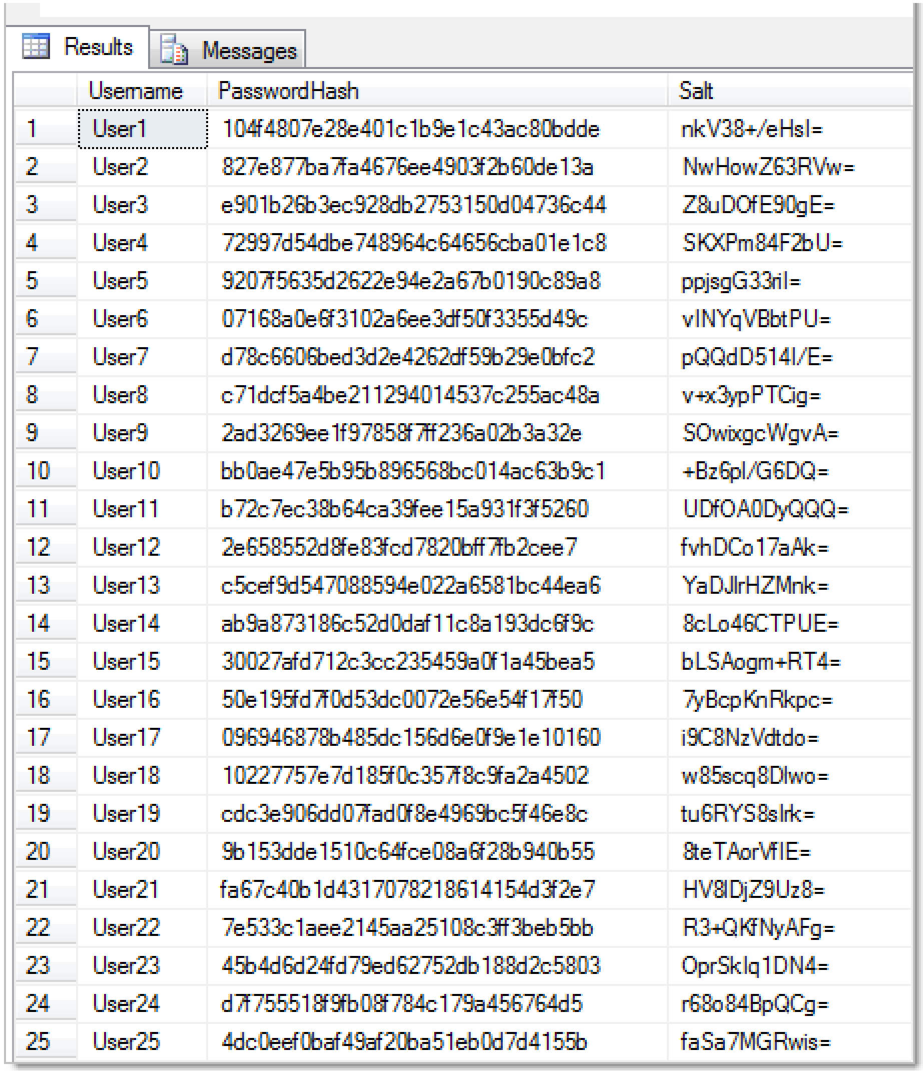
- remote login is even worse,
  - telnet **sends passwords in clear**
  - use SSH (Secure Shell)
- Shoulder surfing
  - Check surroundings in public spaces

Password Storage

- Passwords should be able to be verified by the server
  - so the passwords should be stored, but how?
- Passwords are generally stored in encrypted form
  - using symmetric encryption or one-way hash functions
- Possible *off-line* attack
  - Even if the passwords are stored in encrypted form, dictionary attacks are possible when the file contains the encrypted passwords is obtained by the attacker
  - this is a passive off-line attack
    - unsuccessful attempt limits do not help

Passwords are generally stored hashed

- Hash password with salt
- Choose random salt s and compute Y= H(password, s)
- Store (s,Y) in the password file
- Note: The salt s is not secret



	Username	PasswordHash	Salt
1	User1	104f4807e28e401c1b9e1c43ac80bdde	nkV38+/eHsI=
2	User2	827e877ba7fa4676ee4903f2b60de13a	NwHowZ63RVw=
3	User3	e901b26b3ec928db2753150d04736c44	Z8uDOfE90gE=
4	User4	72997d54dbe748964c64656cba01e1c8	SKXPm84F2bU=
5	User5	9207f5635d2622e94e2a67b0190c89a8	ppjsgG33riI=
6	User6	07168a0e6f3102a6ee3df50f3355d49c	vINYqVBbtPU=
7	User7	d78c6606bed3d2e4262df59b29e0bfc2	pQQdD514I/E=
8	User8	c71dcf5a4be211294014537c255ac48a	v+x3ypPTCig=
9	User9	2ad3269ee1f97858f7ff236a02b3a32e	SOwixgcWgvA=
10	User10	bb0ae47e5b95b896568bc014ac63b9c1	+Bz6pI/G6DQ=
11	User11	b72c7ec38b64ca39fee15a931f3f5260	UDfOA0DyQQQ=
12	User12	2e658552d8fe83fcd7820bff7fb2cee7	fvhDCo17aAk=
13	User13	c5cef9d547088594e022a6581bc44ea6	YaDJIrHZMnk=
14	User14	ab9a873186c52d0daf11c8a193dc6f9c	8cLo46CTPUE=
15	User15	30027afd712c3cc235459a0f1a45bea5	bLSAogm+RT4=
16	User16	50e195fd7f0d53dc0072e56e54f17f50	7yBcpKnRkpc=
17	User17	096946878b485dc156d6e0f9e1e10160	i9C8NzVdtdo=
18	User18	10227757e7d185f0c357f8c9fa2a4502	w85scq8DIwo=
19	User19	cdc3e906dd07fad0f8e4969bc5f46e8c	tu6RYS8sIrk=
20	User20	9b153dde1510c64fce08a6f28b940b55	8teTAorVfIE=
21	User21	fa67c40b1d4317078218614154d3f2e7	HV8IDjZ9Uz8=
22	User22	7e533c1aee2145aa25108c3ff3beb5bb	R3+QKfNyAFg=
23	User23	45b4d6d24fd79ed62752db188d2c5803	OprSkIq1DN4=
24	User24	d7f755518f9fb08f784c179a456764d5	r68o84BpQCg=
25	User25	4dc0eef0baf49af20ba51eb0d7d4155b	faSa7MGRwis=

How to prevent dictionary attacks on password files – 1

- Slow down password encryption
  - UNIX crypt function
    - repeats a modified version of DES 25 times
    - on all-zero block data and using the password as the key
- Do not make the password file publicly readable
  - shadow passwd file in UNIX systems

How to prevent dictionary attacks on password files - 2

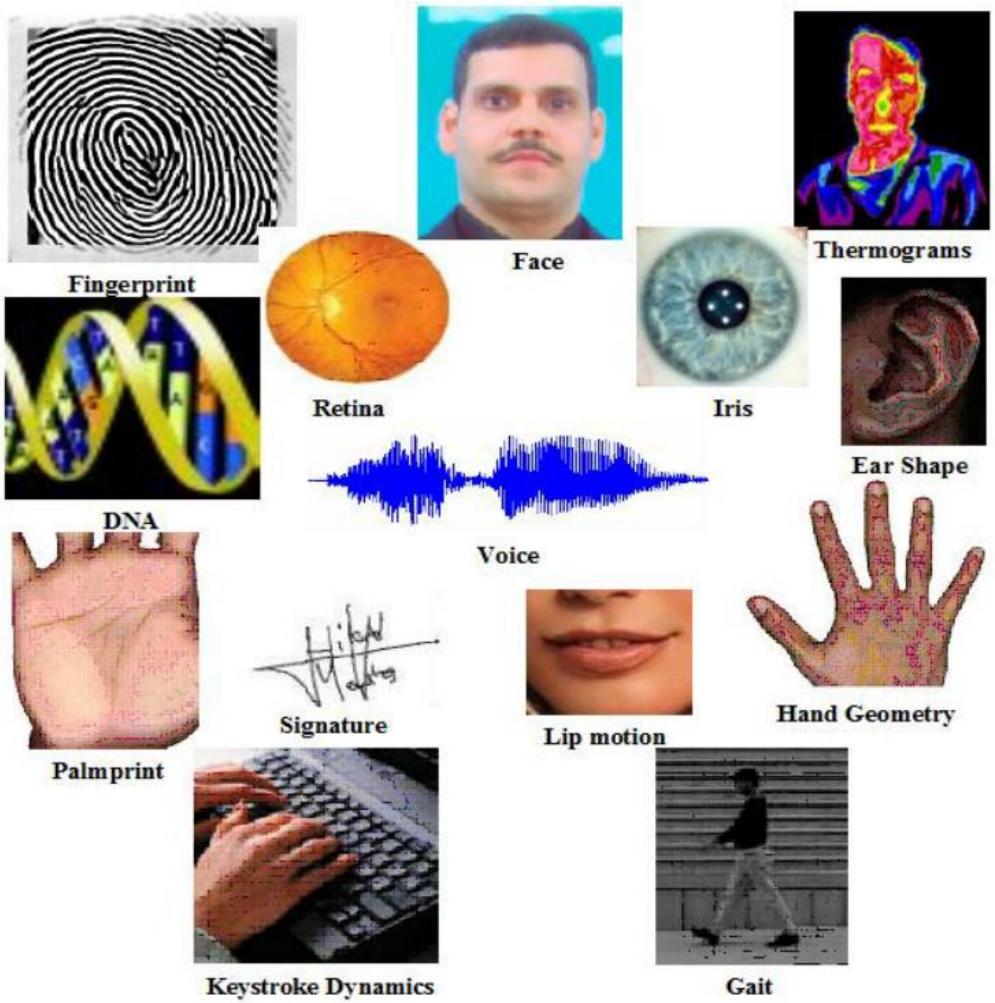
- Password Salting
  - Encrypt passwords with additional random value (salt)
  - salt is not a secret value
  - store the encrypted password with salt
  - Salting slows down dictionary attack
    - since the attacker should run a brand new dictionary search for each user
  - Another advantage
    - if two users have the same password, their encrypted passwords will not be same (of course if the salt values are not accidentally the same)

Other Authentication Approaches

- Password is example of “what you know” type of authentication
  - it is a piece of information
  - may be guessed or obtained by the attacker
- Other authentication instruments also exist
  - What you have (smartcards, tokens, …)
  - Who you are (biometrics)
  - What you do (dynamic handwritten signature, key strokes, gait)
  - Where you are (on the network or physically using GPS)

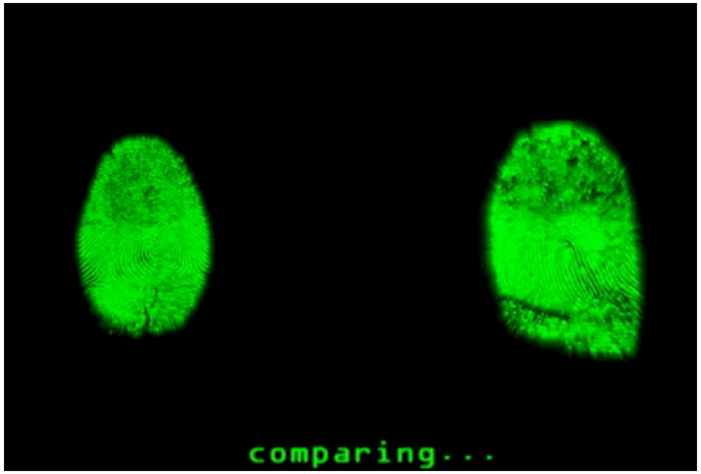
Other Authentication Approaches

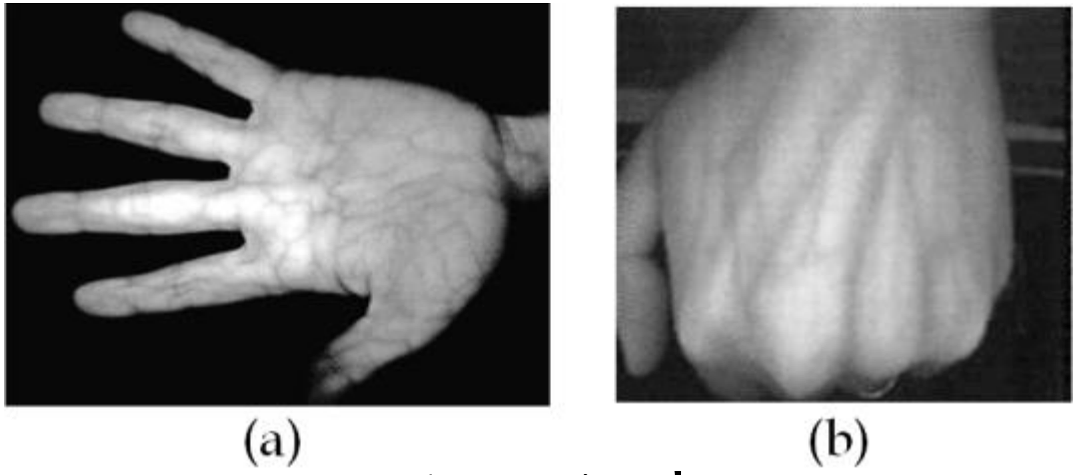
- Who you are (Biometrics)
  - uses unique biological properties



Biometrics Authentication Approaches

- Who you are (Biometrics)
  - uses unique biological properties like



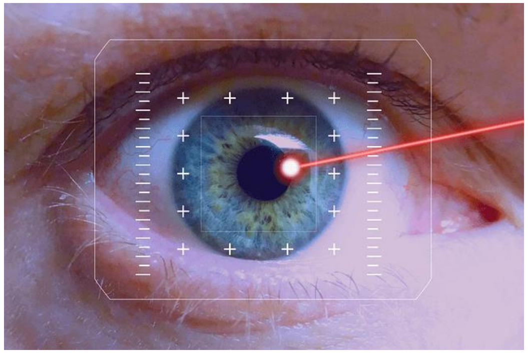

(a)
(b)

vein geometry

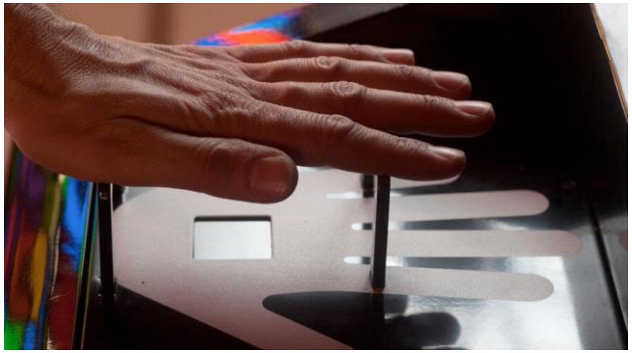
fingerprint

Biometrics Authentication Approaches

- Who you are (Biometrics)
  - – uses unique biological properties like

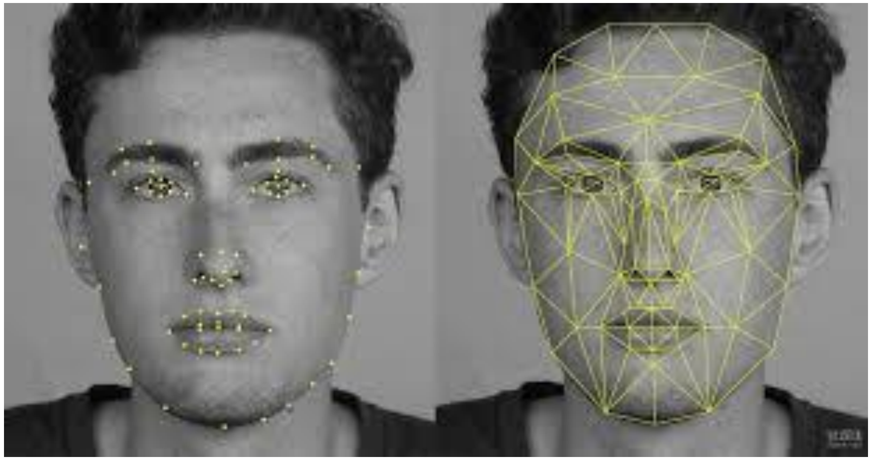


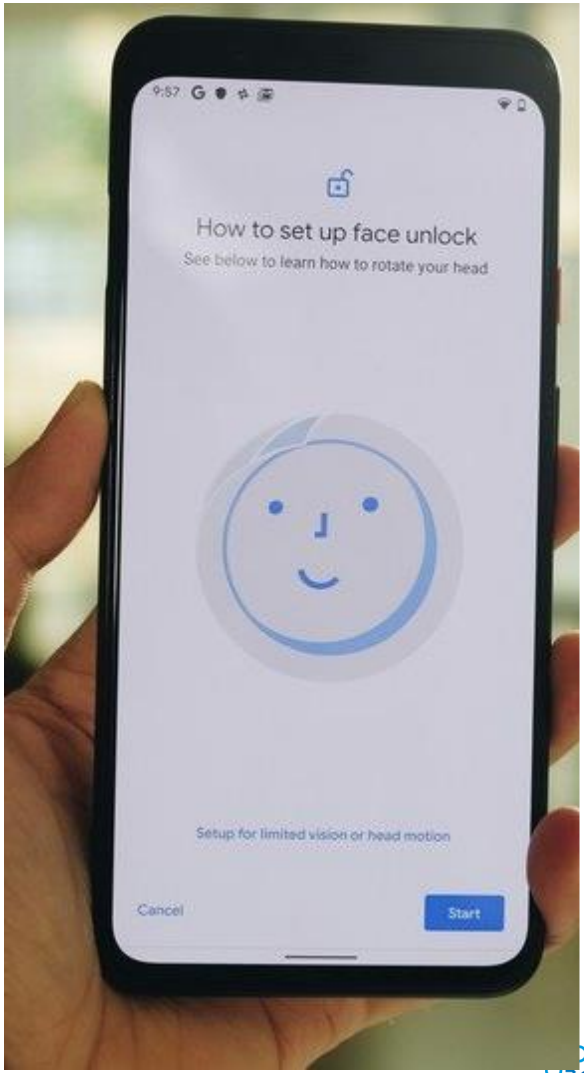
retina pattern



palm print

Biometrics authentication- Face





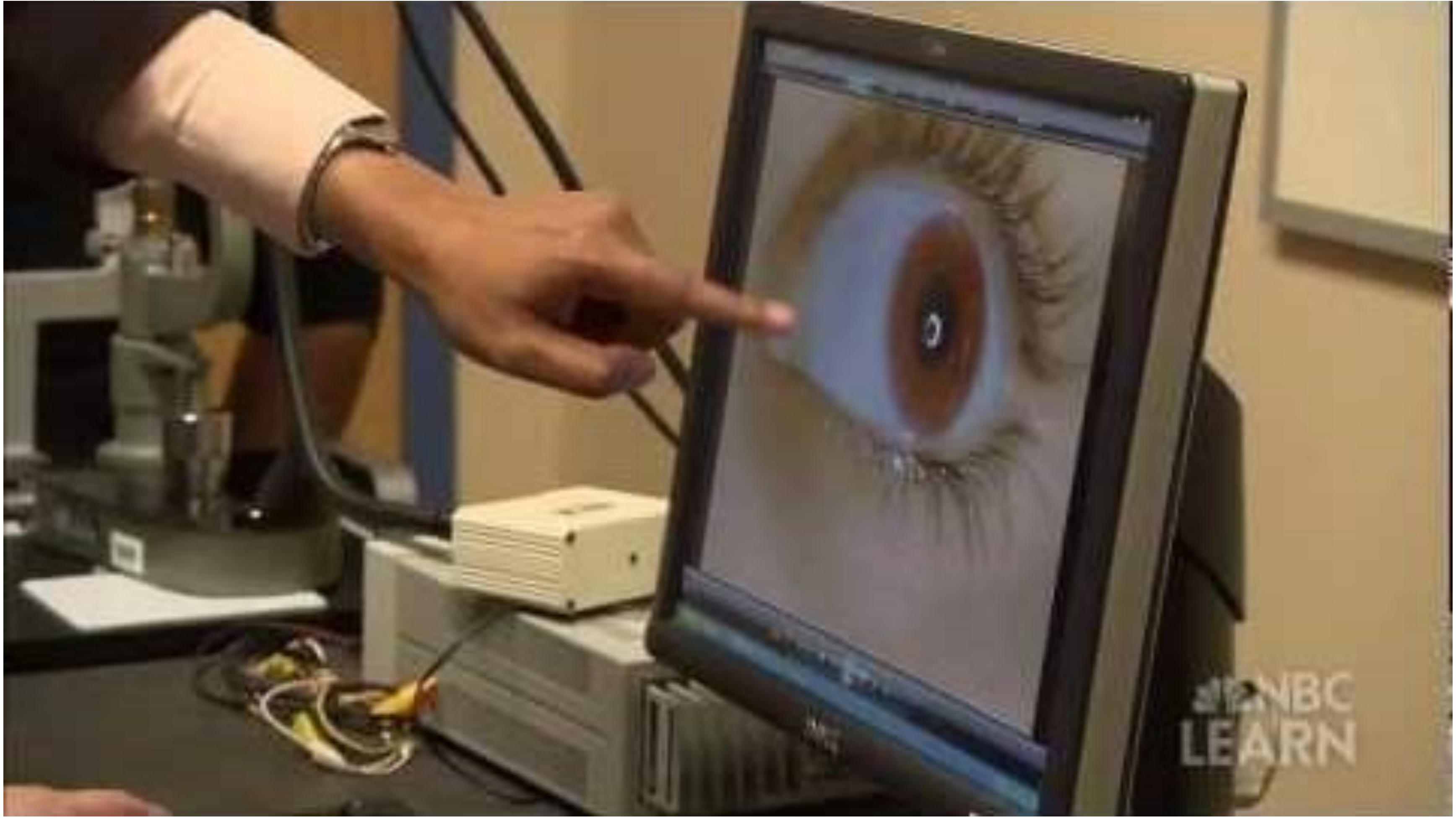
How to set up face unlock

See below to learn how to rotate your head

Setup for limited vision or head motion

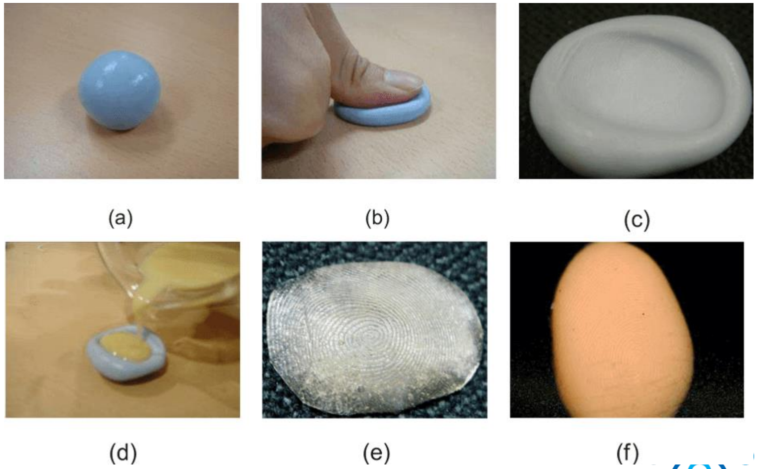
Biometrics Authentication

Play video



Authentication Approaches

- does not have 100% accuracy
  - false accept
    - should reject, but accepts - very bad
  - false reject
    - should accept, but rejects
    - not so bad but may create lots of false alarms and user-unfriendliness that make the system inefficient
    - trade-off between false accept and false reject
- two controversies
  - if copied or broken, you cannot change it
  - people may not like their fingerprints are taken as criminals or beams in their eyes



Other Authentication Approaches

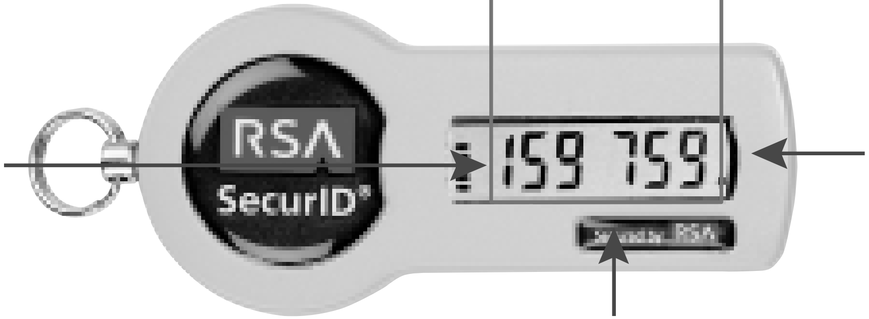
- What you have
  - a physical device that you hold
  - smartcards and smart tokens are the best examples
    - Mostly to generate one-time passwords
  - can be stolen or lost
    - should be used together with a PIN or password
- What you do
  - mechanical tasks that have specific properties that only you can do
  - dynamic signatures
    - pressure, speed, orientation are properties as well as the shape
  - Keyboard typing
    - speed, intervals between keystrokes
  - false accept, false reject problems exist here too

Tokens: Something You Have

Time-Based Token Authentication

Login: mcollings
Passcode: 2468159759

PASSCODE = PIN + TOKENCODE



Token code: Changes every 60 seconds

Clock synchronized to UCT

Unique seed

An RSA SecurID with a code that changes every 60 seconds.
Physical possession of the token should be necessary for successful authentication.

Token: Two Factor Authentication

- First factor: **what user *knows***
- Second factor: **what user *has***
- Without the second factor, user cannot log in

RSA SecurID SD600

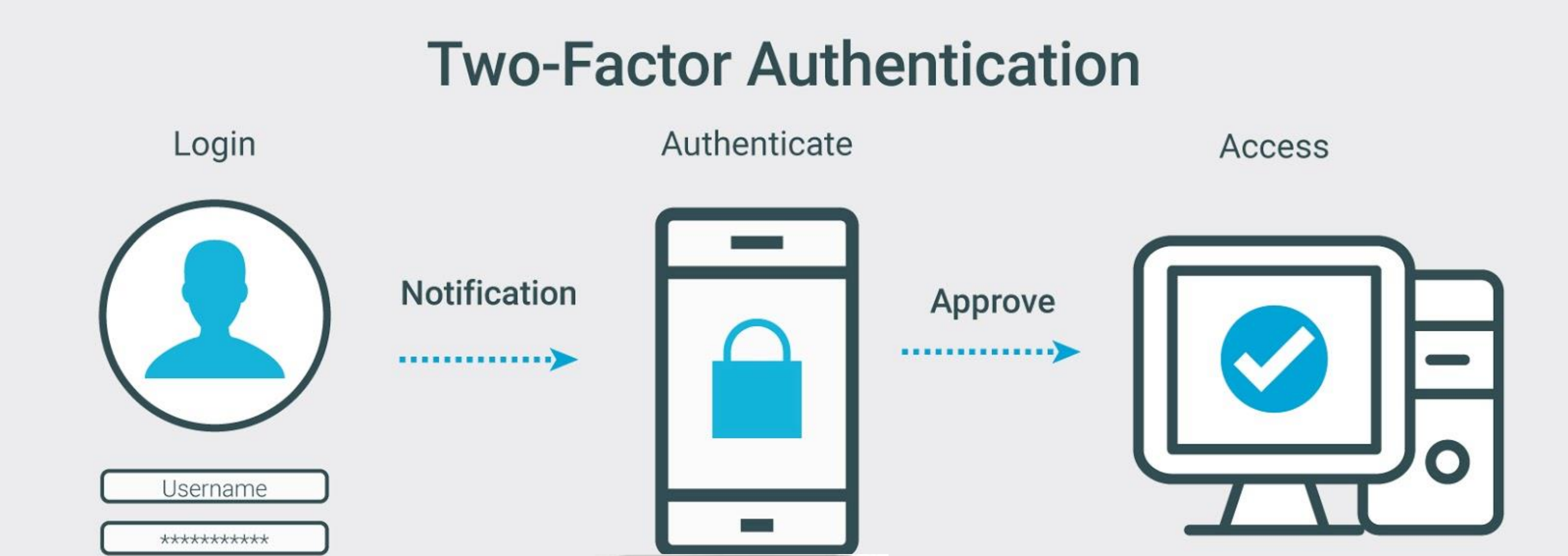
RSA SecurID SID700

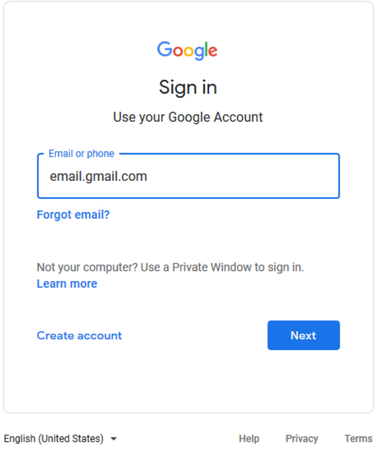
RSA SecurID SD200

RSA SecurID SID800

RSA SecurID SD520

Token: Two Factor Authentication




Google

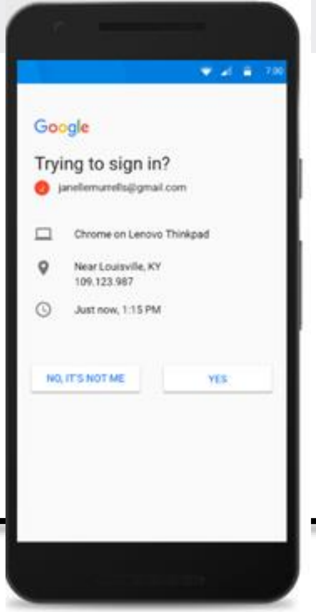
Sign in

Use your Google Account

Email or phone: email.gmail.com

Forgot email?

Not your computer? Use a Private Window to sign in. Learn more


Google

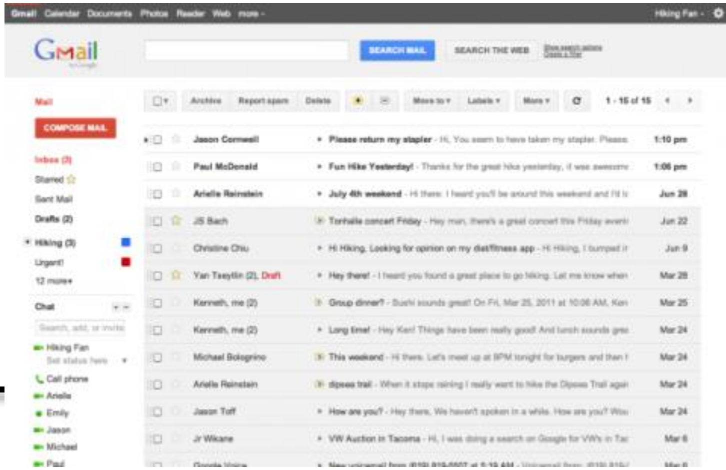
Trying to sign in?

janellemurrells@gmail.com

Chrome on Lenovo Thinkpad

Near Louisville, KY
109.123.987

Just now, 1:15 PM



Jason Cornwell	Please return my stapler - Hi, You seem to have taken my stapler. Please	1:10 pm
Paul McDonald	Fun Hike Yesterday! - Thanks for the great hike yesterday, it was awesome	1:06 pm
Arielle Reinstein	July 4th weekend - Hi there. I heard you'll be around this weekend and I'd li	Jun 28
JS Bach	Tonhalle concert Friday - Hey man, there's a great concert this Friday eveni	Jun 22
Christine Chiu	Hi Hiking, Looking for opinion on my diet/fitness app - Hi Hiking, I bumped i	Jun 9
Yan Tseytlin (2), Draft	Hey there! - I heard you found a great place to go hiking. Let me know when	Mar 28
Kenneth, me (2)	Group dinner? - Sushi sounds great! On Fri, Mar 25, 2011 at 10:06 AM, Ken	Mar 25
Kenneth, me (2)	Long time! - Hey Ken! Things have been really good! And lunch sounds grea	Mar 24
Michael Bolognino	This weekend - Hi there. Let's meet up at 8PM tonight for burgers and then I	Mar 24
Arielle Reinstein	dipsea trail - When it stops raining I really want to hike the Dipsea Trail agai	Mar 24
Jason Toff	How are you? - Hey there, We haven't spoken in a while. How are you? Wou	Mar 24
Jr Wikane	VW Auction in Tacoma - Hi, I was doing a search on Google for VW's in Tac	Mar 6
Google Voice	New voicemail from (819) 819-8807 at 5:19 AM - Voicemail from: (819) 819-	Mar 6

Summary

- Passwords and Password Management
- Attacks on Passwords
- Password Guessing
- Password Selection Guidelines
- Password Spoofing
- Biometric Authentication Approaches
- Two Factor Authentication