Countdown

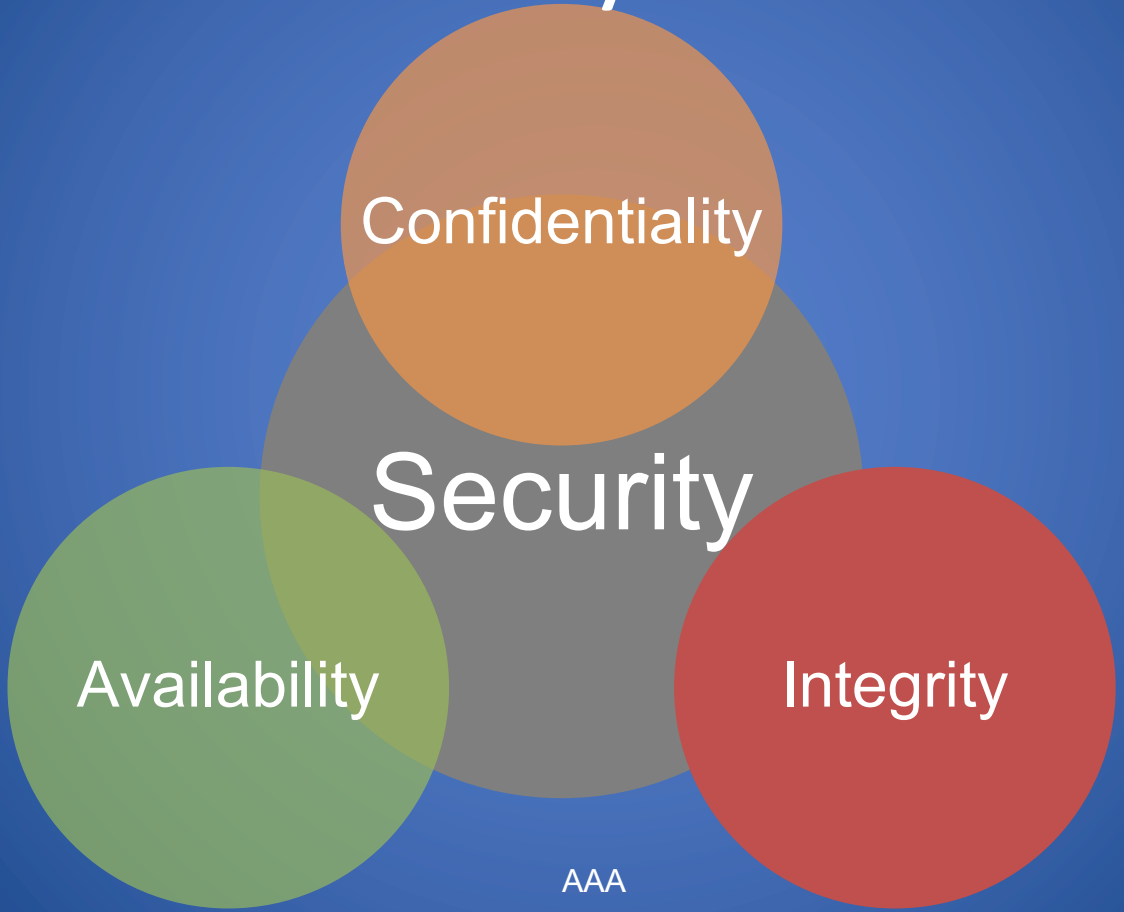
Class is starting now!

AAA
Authentication, Authorization, and Accounting

CS 1660/1620/2660: Introduction to Computer Systems Security

Authentication, Authorization, and Accounting (AAA)

Security Goals



Beyond CIA…

Identification

Authentication

Authorization

Identification

- Humans are generally indistinguishable in front of a computer
- A subject should provide a identifier (e.g. email has to be unique)
- The system will verify if you have the proof to claim an identity
  - This process is called Authentication

Authentication

- Authentication is the act of confirming the truth of an attribute of a datum or entity
- There are three authentication factors:
  - Knowledge: Something you know
  - Ownership: Something you have
  - Inherence: Something you are

Knowledge

- Something the user knows (e.g., a password, or PIN, challenge/response (the user must answer a question), pattern)

Strengths

- Easy to transport
- Can be changed
- Easily transferrable/easy to duplicate

Weaknesses

- Can be forgotten
- Easy to duplicate
- Verifier often learns the secret

Ownership

- Something the user has (e.g., phone number, ID card, security token, etc.)

Strengths

- Easily transferable
- More difficult to clone that what you know

Weaknesses

- Can be lost or stolen
- Can be forged
  - e.g. a key can be made from photos

Inherence

- Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, voice, etc.).

Strengths

- Non-transferable
- Usually identifies individual

Weaknesses

- Forgeable (ie, fingerprint from picture or from a glass)
- Can be lost (ie, loss or degradation)
- Can’t be changed

Authentication Devices

Time-Varying Codes

(One Time Password)

- Physical/Tamper proof
- Precise clock
- Hash chain inside

Biometric

- physiological or behavioral characteristic
- Irises, fingerprints, etc.
- If it does not work usually you use a password

More authentication factors?

- Location factor
  - Where you are (ie. Gps, Mobile Cell, etc.)
- Ability factor
  - What you can do (ie. Keystroke Dynamics, mouse tracking, etc.)
- …
- Usually they are classified in the inherence factor, It is an open problem
  - NIST SP 800-63-1

If you need more security?

- Could you use more authentication factor to verify the identity of a user?
  - **Multi Factor Authentication** is born
    - To increase the level of security, many systems will require a user to provide different types of authentication factor

2-factor authentication

- ATM card + PIN
- Credit card + signature
- Passport + fingerprint
- …

Clicker Question 1

Which multi factor schema is more secure?

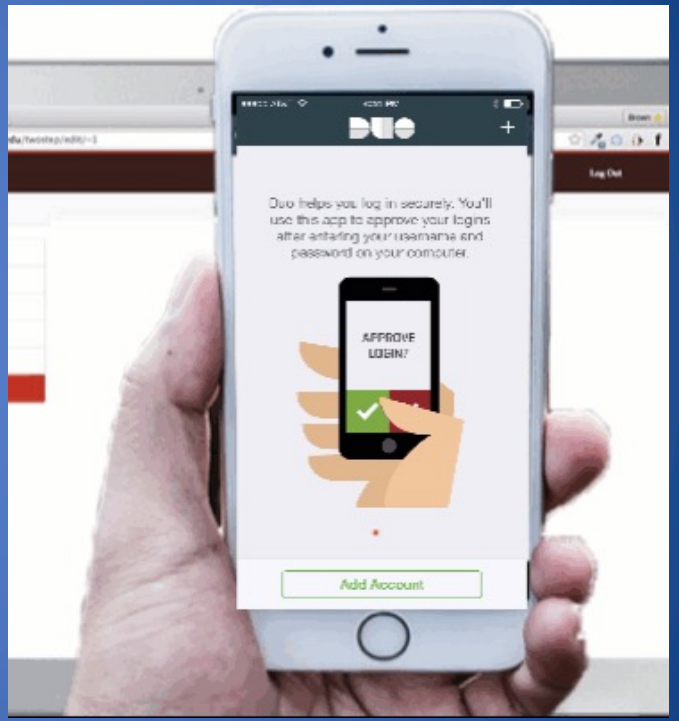
A. ATM Card + Pin + Fingerprint
B. Passport + fingerprint + face
C. Same level of security
D. It is not possible to establish

Clicker Question 1 - Answer

- Answer: A
  - It is the only three-factor authentication schema
  - B fingerprint and face
  - they belong both to the ownership authentication factor
  - C, D are not true

Multi-step Authentication

- User submits two or more authentication tokens
- ATM bank card (Two Factor)
  - –Physical card (something you have)
  - –PIN (something you know)
- Password + code sent to the phone (Two Step) Brown Authentication
  - –Enter password (something you know)
  - –Enter code (something you know)



Security Questions (aka Personal Questions)

- Questions about the user like city of birth, high school, first car, favorite color, etc.

- Used as supplementary authentication factor
  - When user logs in from new device
  - For password reset

- Answer selection strategies
  - Truthful answers
  - Untruthful but plausible answers
  - Randomly generated answers

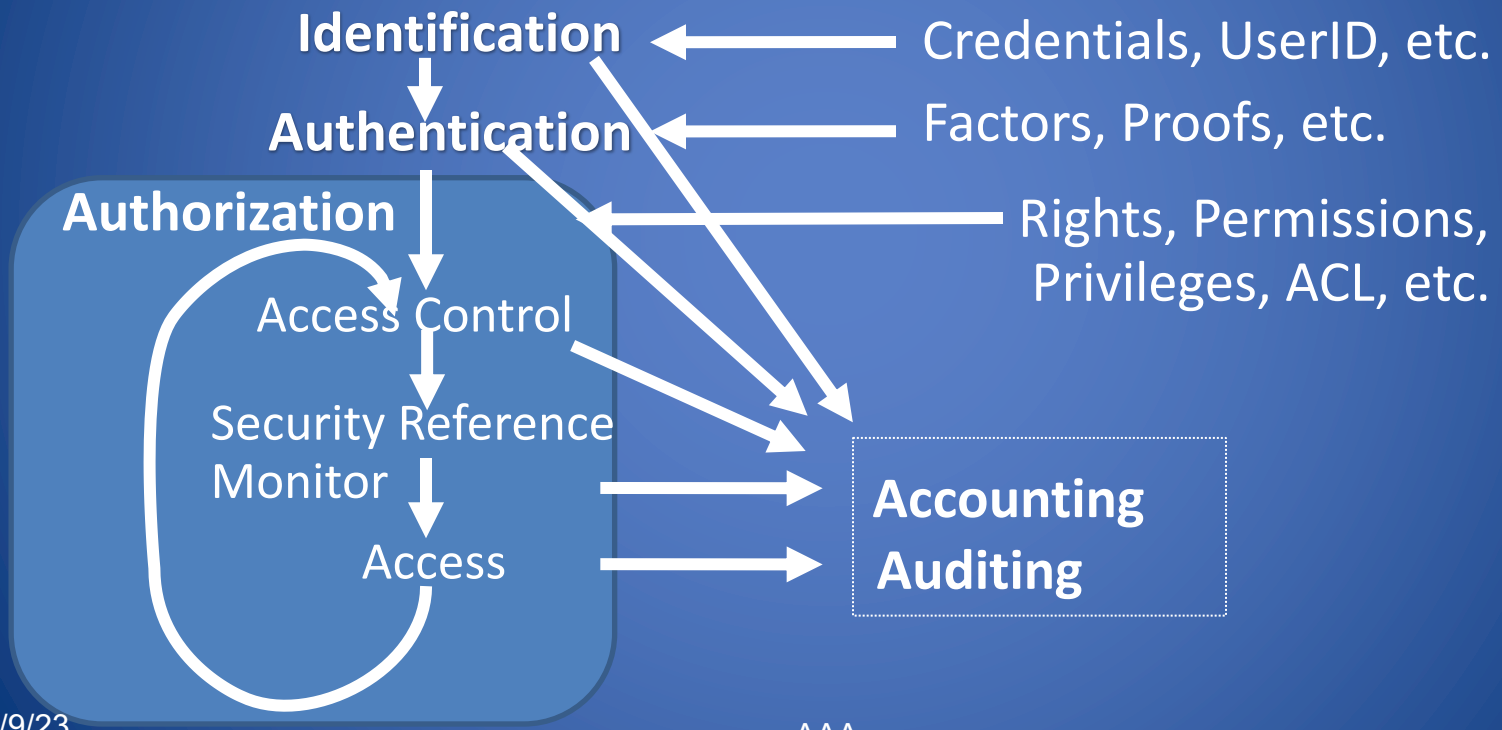
Authorization

- Once a subject is Authenticated, access should be authorized
- Authorization is the function of specifying access rights to resources (access control)
- More formally, "to authorize" is to define access policy: permissions, rights, etc.

AAA and more…

Identification, **Authentication**, **Authorization**, **Accounting**, Auditing

- AAA Working Group, IETF



AAA Summary

- Often broken into three steps
  - Identification, Authentication, and Authorization
- Three ways to prove authentication
  - Something you have/are/know
- Multifactor authentication is generally more secure

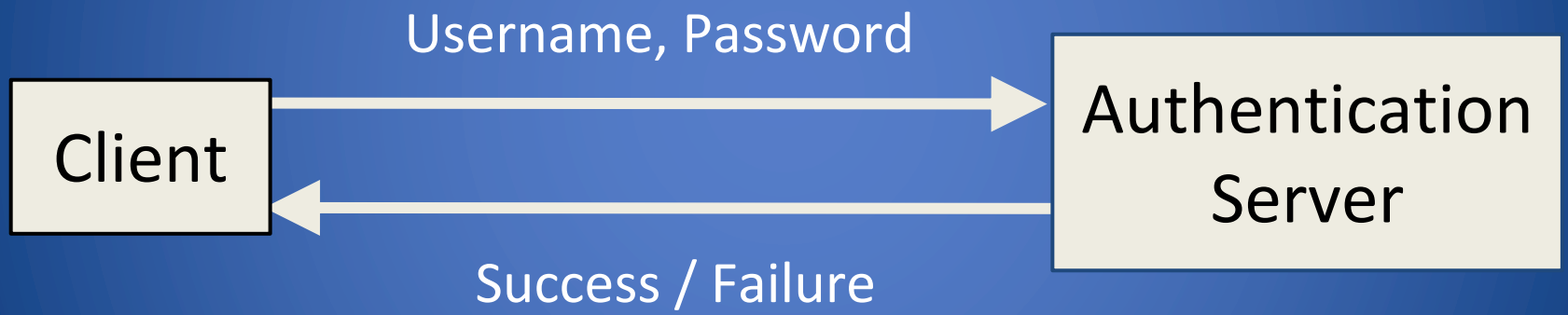
Password Authentication

What Do These Passwords Have in Common?

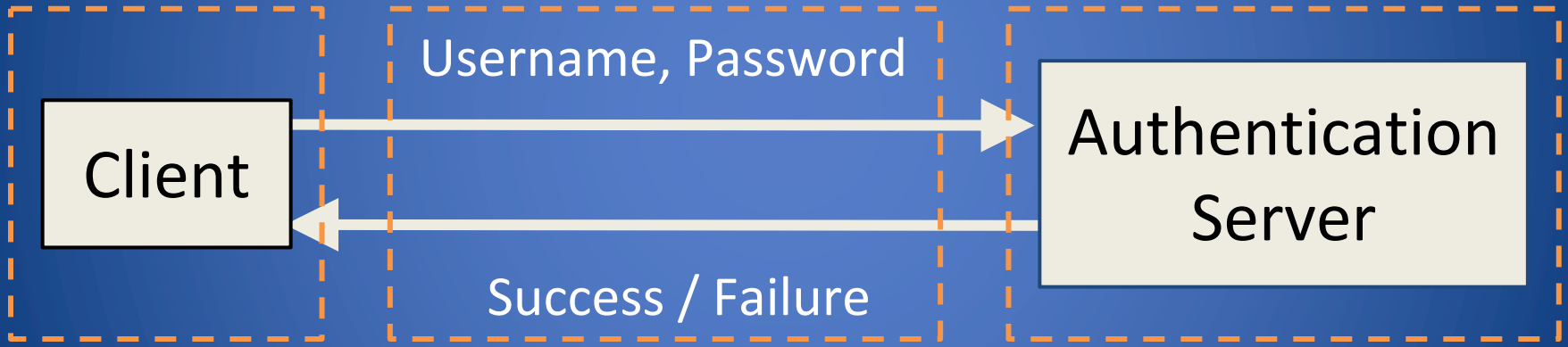
- 123456
- password
- 123456789
- 12345678
- 12345
- 111111
- 1234567q
- sunshine
- qwerty
- iloveyou
- princess
- admin
- welcome
- 666666
- abc123
- football
- 123123
- monkey
- 654321
- !@#$%^&*
- charlie
- aa123456
- donald
- Password1
- qwerty123

Top 25 passwords used in 2018 according to SplashData

Password Authentication



Attacks on Passwords



Information States (MC CUMBER CUBE):

Storage,Transmission, Processing

Password Complexity

Characters in Passwords

- Consider a standard US English keyboard
- Lower case characters: 26
- UPPER and lower case: 52
- Digits: 10
- Special characters: 32
- Standard keyboard characters: 94
- All 7-bit ASCII characters: 128

Size of Password Space

- 6-character password
- Only lower case letters, no numbers or symbols

Char	*	*	*	*	*	*

Size of Password Space

- 6-character password
- Only lower case letters, no numbers or symbols
- There are 26 x 26 … x 26 or 26^6 (≈ 309M) possible passwords
- Easy to try all of them

Char	*	*	*	*	*	*
Choices	26	26	26	26	26	26

Other Password Schemes

- How many possible 6-character passwords?
  - Digits (10): 10^6
  - UPPER and lower case (52): 52^6
  - Special characters: &, %, $, @, “, |, ^, <, … (32): 32^6
  - Standard keyboard characters (94): 94^6
  - All 7-bit ASCII characters (128): 128^6

Number of Possible Passwords

Assume a standard keyboard with 94 characters

Password length	Number of passwords
5	$94^5 = 7{,}339{,}040{,}224$
6	$94^6 = 689{,}869{,}781{,}056$
7	$94^7 = 64{,}847{,}759{,}419{,}264$
8	$94^8 = 6{,}095{,}689{,}385{,}410{,}816$
9	$94^9 = 572{,}994{,}802{,}228{,}616{,}704$

Brown University Password Policy

- Cannot contain your first name, last name, or username
- Cannot match your last three passwords
- Must be at least 10 characters in length
- Must contain at least one lowercase character
- Must contain at least one number
- Must contain at least one special character
- Must contain at least one uppercase character

Source: https://it.brown.edu/information-security/guard-your-privacy/strong-passwords

Strong Passwords

- Long passwords preferred
- Use all available characters
  - UPPER/lower case characters
  - Digits
  - Special characters: &, %, $, £, “, |, ^, §, …
- Which of the following passwords are strong?
  - Seattle1
  - M1ke03
  - P@$$w0rd
  - TD2k5s@}ecV87^R:@DKlksj298RLO<j;-*h

Clicker Question 2

Which password policy is more secure?

Policy A	Policy B
8 characters total: • 1 lowercase • 1 uppercase • 1 digit • 1 symbol • 4 of any keyboard characters	8 of any keyboard characters

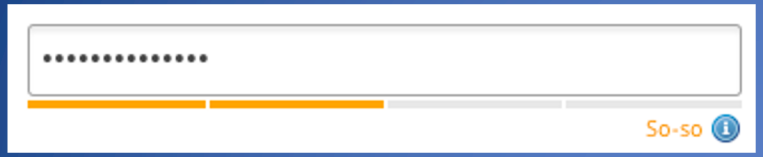
A. Policy A
B. Policy B
C. Both are equally secure
D. It is not possible to evaluate the security

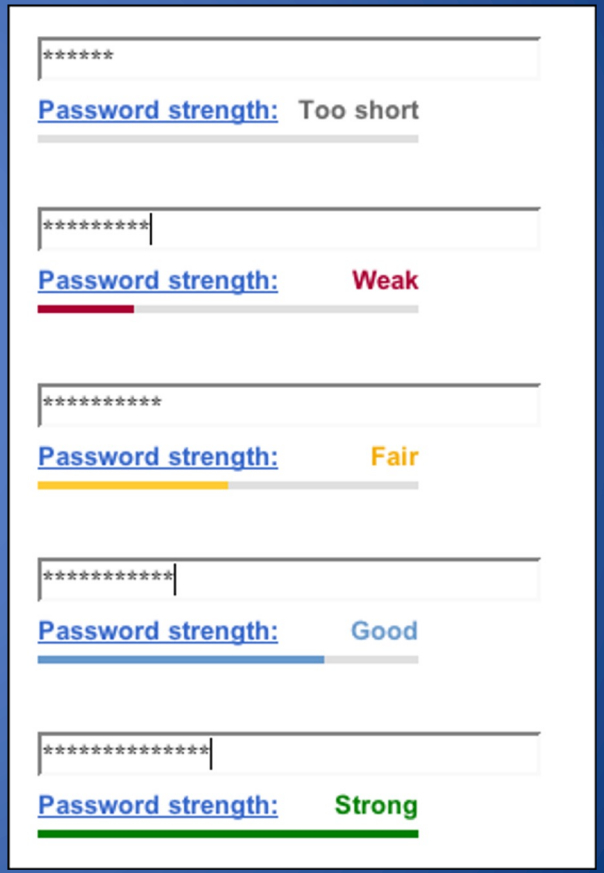
Clicker Question 2 - Answer

- Answer: A, B, or C
  - Depends on the assumptions you make
    - Policy B has bigger password space, though users can pick bad passwords (i.e. `password, 12345678`)
    - What if both policies prevented users from picking common passwords?

Password Complexity In Practice

Password Strength Meter





History of LUDS

- **L**ower- and **U**ppercase letters, **D**igits and **S**ymbols
- Became standard ~ 1985
- US Defense Department - *Password Management Guideline(Green Book)*
  - **Guessing space**
- NIST - *Password Usage of the Federal Information Processing Standards*
  - Take English words(dictionary) into consideration

LUDS in Practice

passwordmeter.com

Test Your Password		Minimum Requirements
Password:		• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	0%	
Complexity:	Too Short	

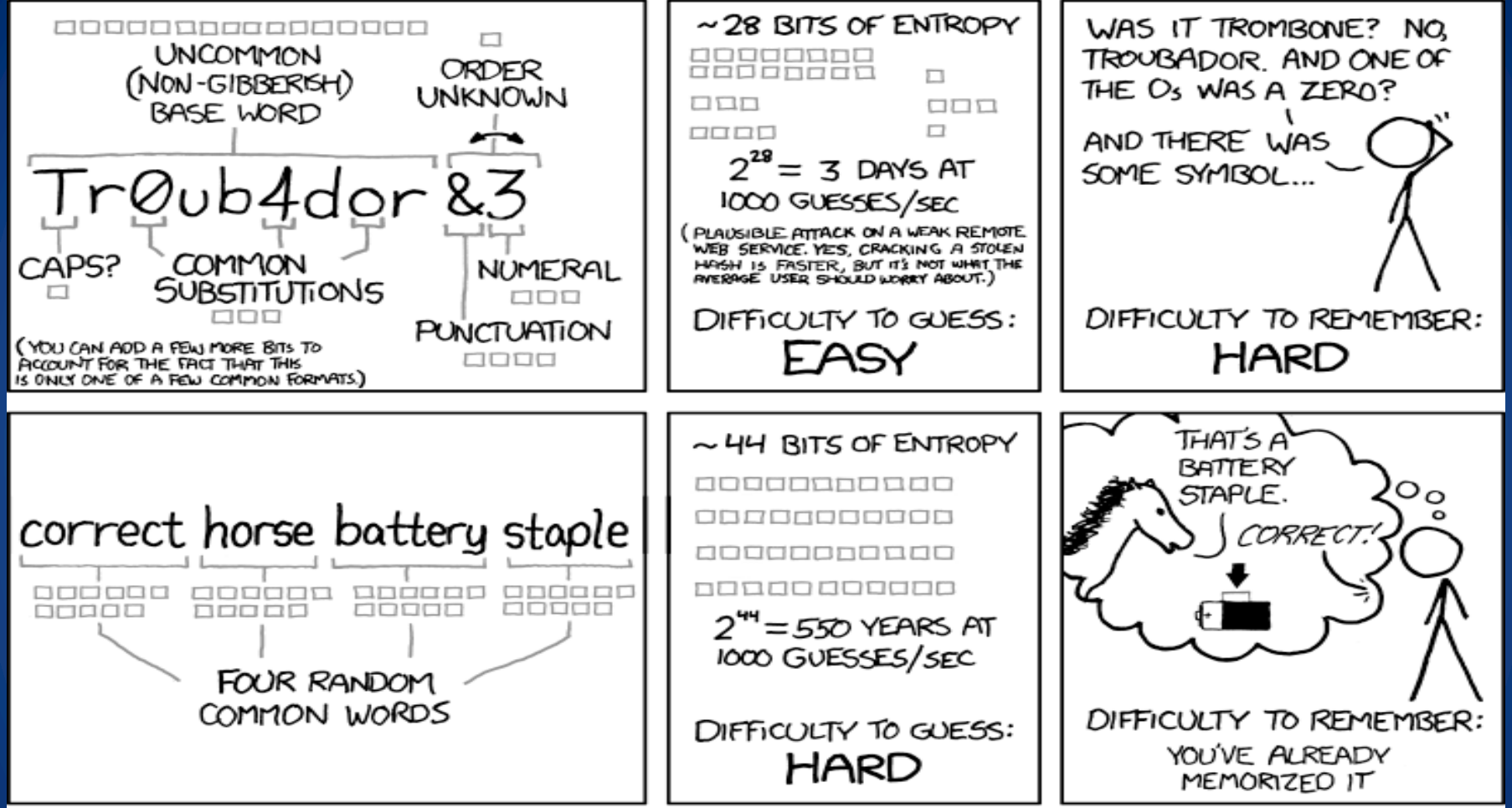
Additions		Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	0	0
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Numbers	Cond	+(n*4)	0	0
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	0	0
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0

Problems with LUDS

- Characters frequency is not random
- Frequently used words (password, name)
- Special Dates (Birthday of a relative)
- Keyboard Patterns
- Wrong password strength estimation
  - P@$$w0rd1

zxcvbn: realistic password strength estimation

- A model developed by Dropbox
- Easy to adopt
- A rigorous estimation
  - Estimating guess attack directly
- Non-probabilistic
  - Assume attackers know the patterns that make up a password


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Practicing in class

- You can practice in class with something similar to your real password:
  - **passwordmeter.com** (LUDS)
  - zxcvbn alternatives to bit.ly/2dp7BD3
    (no more public on dropbox from 9/1/2017):
    - **goo.gl/DUSwys** (Cygnius)
    - **goo.gl/epu13n**(Takecontrolbooks)

Break!!!!!

60 60 60 60 60

Class is starting now!

One-time Password Generators

Overview of OTPs

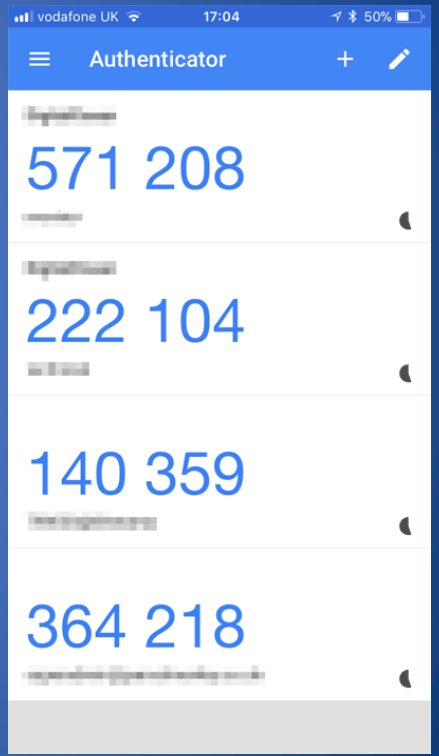
- An OTP is an authentication token valid for only one login session
- Generally used as a second factor to a long-term password
- Time-based or counter-based
  - Both can be generated offline by an app after initialization
  - List of counter-based OTPs can be printed on a sheet of paper or stored in a file

OTP Generation Algorithm

- OTPs can be derived from a message authentication code (MAC), a cryptographic hash function h(s, t) with two inputs
  - s: secret key shared by the client and server
  - t: current time (e.g., 30 seconds resolution) or counter value
- We have OTP(t) = h(s, t)
- The security of the OTP relies on the one-way property of the hash function and the attacker not knowing the secret key s
- One can derive a secure MAC from a standard single-input cryptographic hash function (e.g., HMAC construction)

OTP Apps

- OTPs can be generated by a phone app, e.g., Google Authenticator
  - Secret key provided by server needs to be securely transmitted to app, e.g., scan QR code from server or receive key by mail
  - User needs to protect access to phone (e.g., complex PIN or biometric authentication)
  - For time-based OTPs, phone needs to keep accurate clock



OTP Devices

- OTPs can be generated by dedicated tamper-proof device
  - Integrated display (e.g., RSA SecurID) or USB interface
  - Secret key safely stored in device
    - Expensive to provision due to cost of acquisition of device and shipment to users
    - User may lose or forget to carry device

Source: public domain image by Ochro, Wikimedia Commons

Attacks on OTP MFA

- App OTP generator
  - Exploit app/data synchronization across devices and compromise a vulnerable device
- App and display device OTP generator
  - Intercept transmission of secret key
  - Intercept transmission of OTP
- USB device OTP generator
  - Capture key from USB interface
- Display and USB device OTP generator
  - Steal device (e.g., from user or from mailbox)

Final Considerations on OTP MFA

- OTPs are easy to use
- They require modern phones, dedicated devices, or cumbersome crib sheets
- Smaller attack surface than SMS codes implies simpler risk mitigation
- OTP authentication is effective
- OTP authentication usually not mandated by regulators

What We Have Learned

- AAA
  - Authentication Factors
  - Knowledge, Ownership, Inherence
- Password authentication
  - Principles and attack vectors
- Password Complexity
  - LUDS
  - zxcvbn
- Password cracking
  - Brute-force
  - Dictionary precomputation
  - Intelligent guessing

Exceptional Access to Encrypted Data

So what can we do with crypto?

- Confidentiality: can communicate secretly
- Authenticity: can verify identity, integrity of messages from another party

These are very powerful concepts!

Before computers…

Before modern computing, access to cryptography was mainly limited to governments

Vigenère cipher (1866)

Enigma Machine (1940s)

ROMULUS (1960s)

Now..

Cryptography is open—anyone can use it.

What does that mean?

“Crypto Wars”

In US, cryptography was subject to ”export controls” until 1996-1997

- Categorized similarly to weapons, military technology
- Limited sharing outside US, often required using weaker systems

Example: TLS cipher suites

- TLS is the main protocol that secures web traffic
- Early cipher modes for TLS had weaker “export” versions (eg. DES key size reduced 56 => 40 bits!)

0x00,0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Y	N
0x00,0x0B	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	Y	N
0x00,0x0C	TLS_DH_DSS_WITH_DES_CBC_SHA	Y	N
0x00,0x0D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Y	N
0x00,0x0E	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	Y	N
0x00,0x0F	TLS_DH_RSA_WITH_DES_CBC_SHA	Y	N
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	Y	N
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	Y	N

- This can still affect badly-configured TLS versions!

For Law Enforcement

Exceptional access: should a government be able to access encrypted data if they have a warrant?

- Can law enforcement compel someone to disclose your password?
- Should cryptosystems have builtin exceptions?

Key Escrow

Idea: Build exceptional access into algorithm, or how it's deployed

- Off-device: government keeps a copy of key
- On-device: store key in such a way government can obtain it

Problems?

Clipper Chip (~1993)

- Device proposed for encrypting landline telephone communications, promoted by NSA
- Used then-undisclosed algorithm that designed for using key escrow

- Never actually adopted
- Vulnerabilities discovered in key escrow mechanism

FBI vs. Apple (2015)

The New York Times

F.B.I. Asks Apple to Help Unlock Two iPhones

The request could reignite a fight between the Silicon Valley giant and law enforcement over access to encrypted technology.


By Jack Nicas and Katie Benner

Jan. 7, 2020

SAN FRANCISCO — The encryption debate between Apple and the F.B.I. might have found its new test case.

If we allow exceptional access…

What risks does this create?

- Could a malicious actor use the system?
- Can we trust the government/company/etc to use the system properly?
- Does it add complexity?
  - More complexity => more that can go wrong
- Will users just switch to other, more secure systems?

Millions Flock to Telegram and Signal as Fears Grow Over Big Tech

The encrypted messaging services have become the world's hottest apps over the last week, driven by growing anxiety over the power of the biggest tech companies and privacy concerns.

KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS

Wednesday, January 27, 2016 - 9:00am–9:30am

Ron Rivest, Massachusetts Institute of Technology

Abstract:

Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels “going dark,” these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today we are again hearing calls for regulation to mandate the provision of exceptional access mechanisms. In this report, a group of computer scientists and security experts, many of whom