Password Security

CS463/ECE424

University of Illinois

Background of Password Guessing
Password Strength Evaluation
Password Reuse

Means of Authentication

- Something you know
  - Password or PIN
- Something you have
  - Smart card
  - Private key (of a public-private key pair)
  - Phone (running 2FA)
- Something you are
  - Biometrics (e.g., iris or fingerprint)

Means of Authentication (Cont.)

- Somewhere you are
  - Location-limited channels
- Someone you know (social authentication)
  - Someone vouches for you
  - You can identify people you should know
- Some system vouches for you
  - Single sign-on
  - PKI Certificate Authorities

Password Advantages

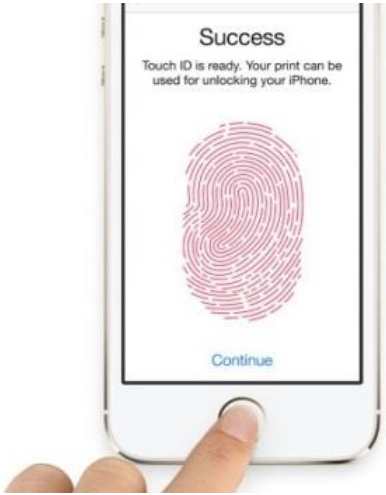
- Familiar to people
- You can have many different ones
- Nothing to carry
- Easy to revoke / replace
- Easy to deploy
- Low cost
- Doesn’t require a trusted third party
- Not linked to an individual*

Disadvantages of Passwords

- Predictability
- Interference between multiple passwords
  - Limits of human memory
  - Password reuse or “trivial” modification
- Requiring a large portfolio of passwords
- Easy to deploy incorrectly / naively
  - System administrators (store in plaintext?)
  - Users

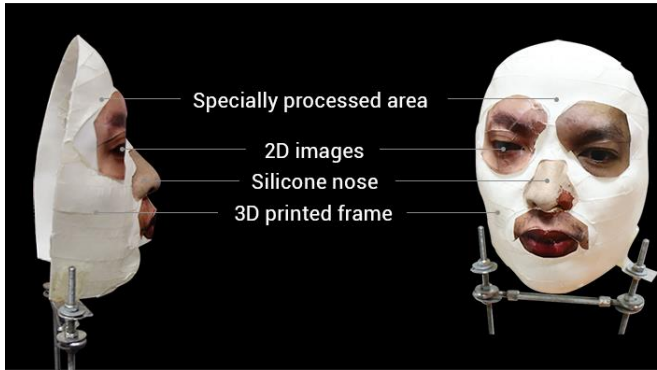
What about Biometrics?

- Fingerprint
- Retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- (Many others)



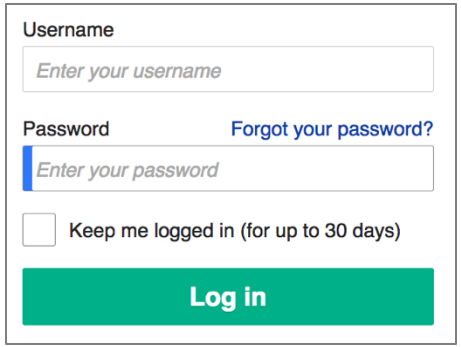
Practical Challenges for Biometrics

- You cannot change them or create a new one (e.g., fingerprint)
- Potentially sensitive data (identifiable information)
- High equipment costs
- Sensitive to changes in the environment
- Biometrics can change over time
- Easy to forge?



Password Guessing: Two Threat Models

- Online guessing
  - Usually has a rate limit
  - Must guess it correctly within a few attempts



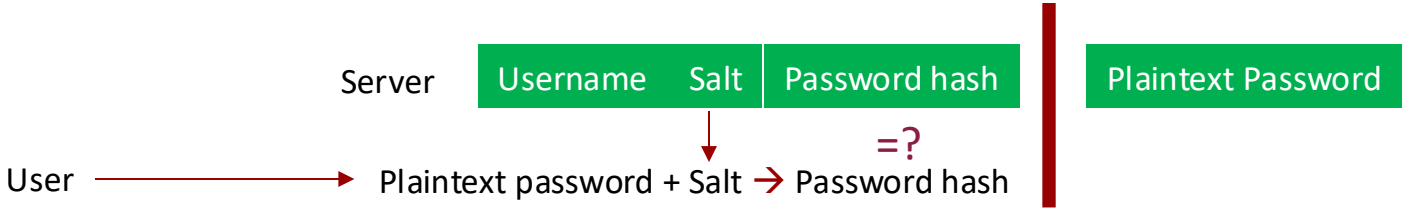
- Offline guessing
  - To crack the password hashes
  - Leaked pwd databases where pwds are stored in a hashed format
  - Inefficient if the password is also “salted”

Passwords, Hashes, Salt

- Password database

Username	Plaintext Password

  - Not a good idea to store plaintext directly
- Login without directly matching plaintext password:
  - HASH(input password + salt) → password hash
  - Plaintext password is stored in other places
  - Password hash and salt is used to authenticate users



Security of Server-side Password Storing

- Worse way: storing password in plaintext
  - Example: username1, password1_plaintext

- Slight better, but still not secure
  - Example: username1, hashed(password1)

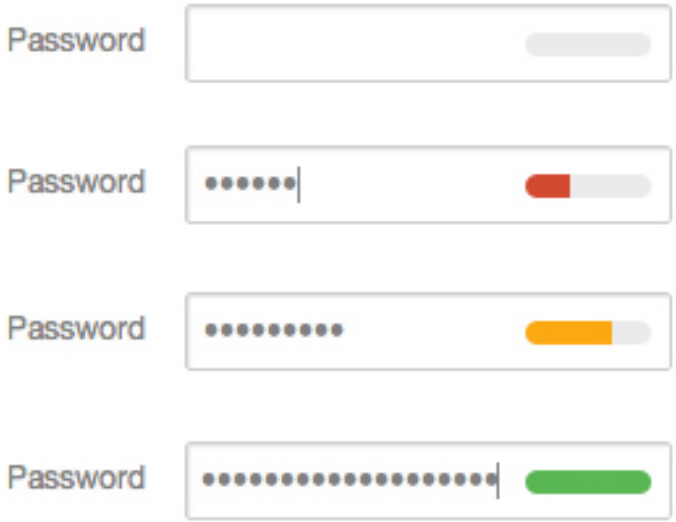
- The right way: adding salt
  - Salt: a fixed length random long string
  - Example: username1, hashed(password1+salt1), salt1

~~Background of Password Guessing~~

Password Strength Evaluation

Password Reuse

How strong is a particular password?



By looking at them?

iloveyou

n(c$JZX!2dfa^dafdIAX^N

j@mesb0nd007

Leet transformation

How to Measure password strength?

- Number of characters, types of characters
- Shannon entropy
- John the Ripper (password cracking software)

- Which one is better?

Old metric: Entropy

- Calculated based on input symbol size (many)
  - Doesn’t account for human patterns
- NIST back-of-envelope estimate (NIST 2006)
  - Vague, not empirical
- Estimated Shannon entropy (Shay 2010)
  - Requires big sample sizes, underestimates

- Average, doesn’t tell you about your weak links

Better Way: Guessability (Offline Guessing)

- How many guesses to reach password?
  - Subject to guessing algorithm, training data
  - Calculate quickly via lookup algorithm
  - Most research focuses on offline guessing model
- Result: guess number or beyond cutoff
  - Model real attacker
  - Per-password estimates

Example:

Password	Guess number
12345678	4
Password178	1.4×10^6
jn%fKXsl!8@Df	Beyond cutoff

Perception vs. Reality

Evaluating Password Pairs

iloveyou88

ieatkale88

4,000,000,000 x more secure!

brooklyn16

brooklynqy

300,000 x more secure!

Ways People Were Wrong

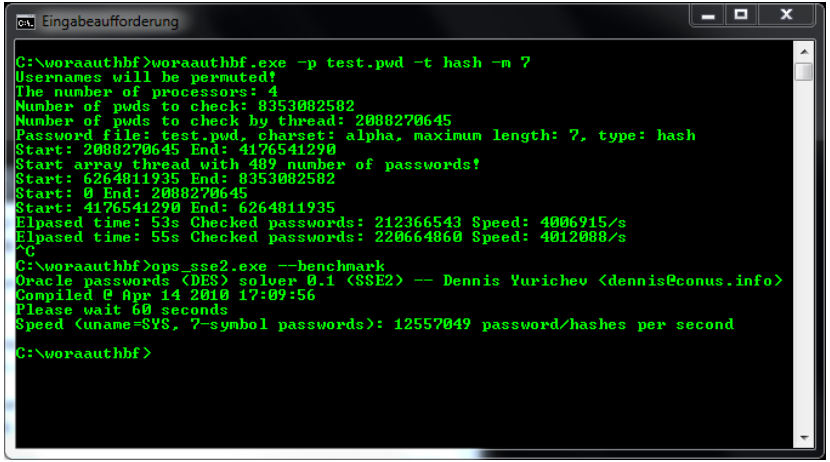
- Overstated security benefits of:
  - Digits
  - Character substitutions (e.g., a→@)
  - Keyboard patterns (e.g., 1qaz2wsx3edc)
- Did not recognize common words/phrases

Many Ways People Were Right

- Capitalize letters other than the first
- Put digits and symbols in middle, not end
- Use symbols rather than digits
- Avoid:
  - Common first names
  - Words related to account
  - Years and sequences

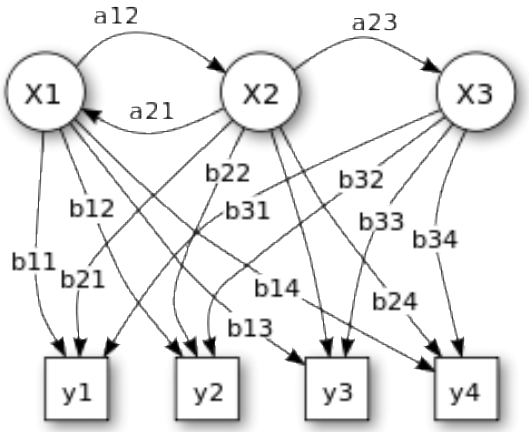
Different Ways to Guess Passwords

- Guessing attacks are data-driven
  - Previously stolen passwords
  - Natural-language corpora
- Array of tools
  - Cracking software
  - Academic algorithms



Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries

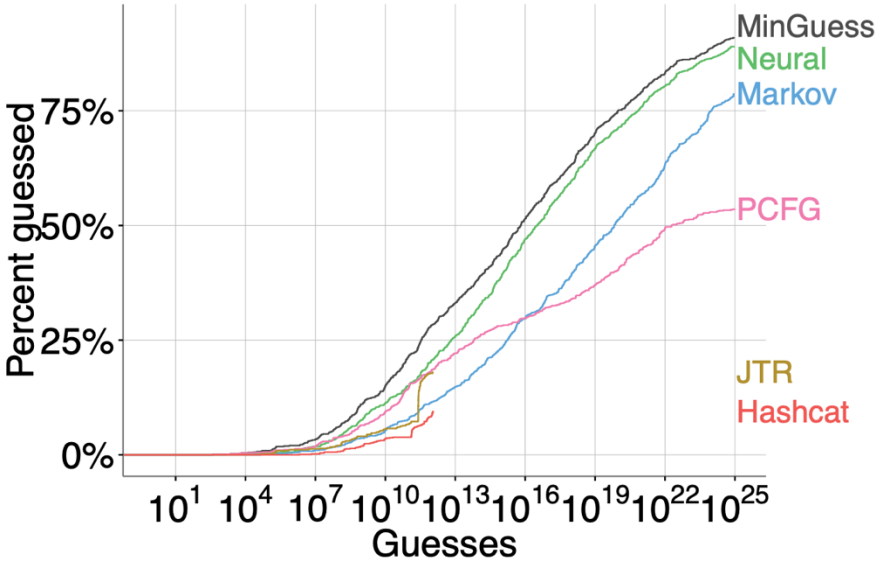


Markov Models: Basic Idea

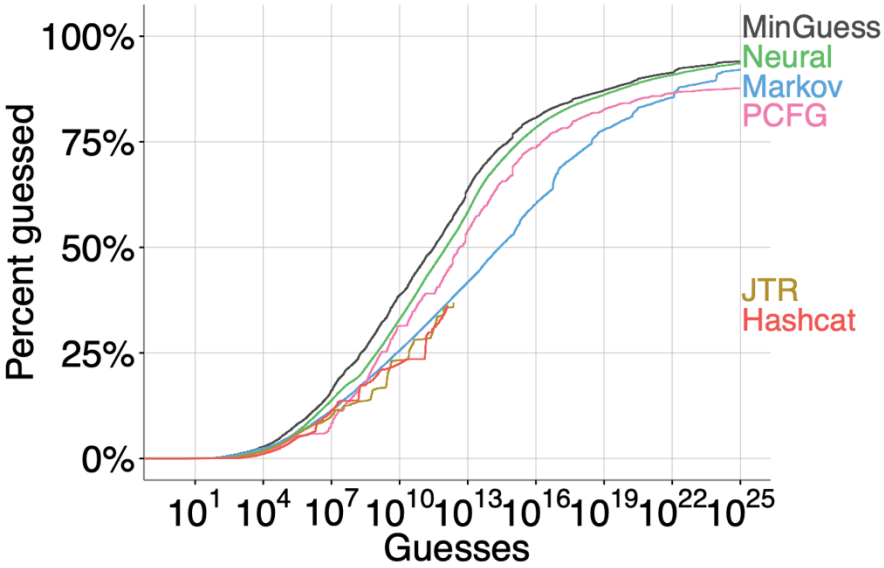
Markov Models: Basic Idea

Deep Learning based Password Guessing

- Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks, USENIX Security 2016



(a) 3class12 passwords



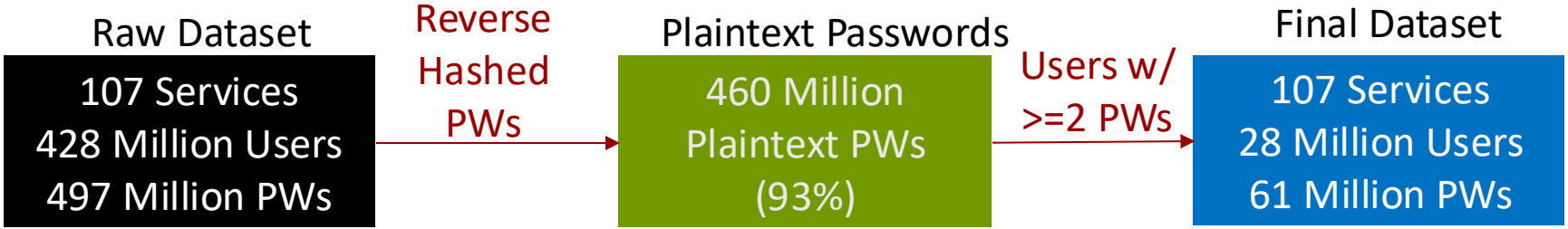
(b) Webhost passwords

~~Background of Password Guessing~~
~~Password Strength Evaluation~~
Password Reuse

Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, Gang Wang. The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services. In Proceedings of The ACM Conference on Data and Applications Security and Privacy (CODASPY), Tempe, AZ, March 2018.

Data-Driven Analysis: Password Reuse & Modification

- Collect massive password datasets with email addresses
  - Link the same users' passwords across services
- Data collection method
  - Searched through online forums, data archives, darknet markets
  - Obtained **107** public password datasets leaked during 2008-2016



Diverse Categories of Online Services

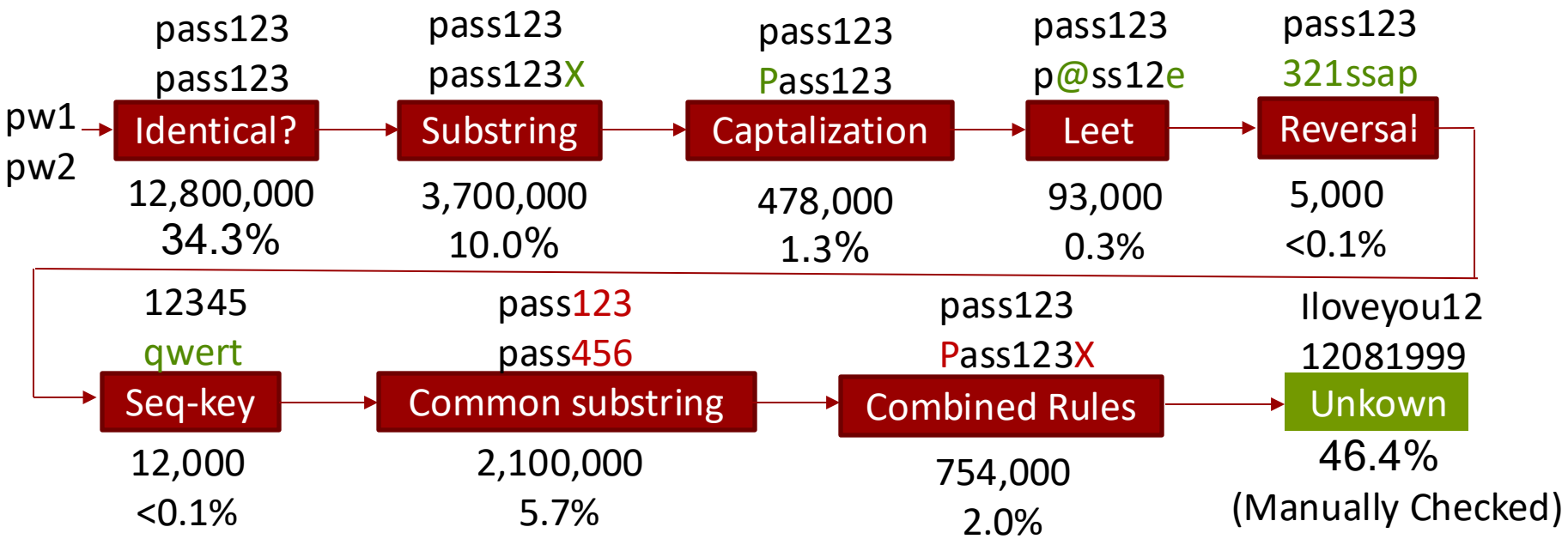
Category	#Plain PWs	# Datasets	Top 3 Largest Datasets
Social	286,000,000	7	Myspace, VK.com, LinkedIn
Adult	75,200,000	9	Zoosk, Mate1, YouPorn
Game	40,800,000	13	Neopets, 7k7k, Lbsg
Entertainment	30,700,000	4	Lastfm, Swingbrasileiro, LATimes
Internet	16,400,000	18	000webhost, Comcast, Yahoo
Email	9,600,000	3	Gmail, Mail.ru, Yandex
Forum	1,100,000	25	CrackingForum, Abusewith.us, Gawker
Shopping	340,000	12	RedBox, 1394store, Myaribags
Others	210,000	7	Data1, Data2, Data3
Business	10,000	9	Movatiathletic, Hrsupporten, 99Fame

Research Questions

- How often do users reuse or modify passwords across services?
- How long does it take for users to update their reused passwords after data breaches?
- How guessable are the modified passwords?

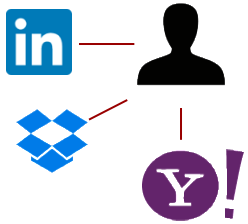
Measuring Password Reuse and Modification

- 37 million password pairs from the same users
- Given a pw pair, determine “reused”, “modified”, or “unknown”



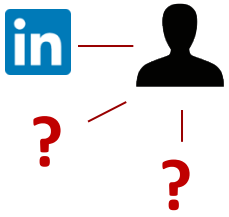
Highlights of Findings

- 53% of the 28.8 million users reused/modified passwords
  - 38% users once reused the same password
  - 21% users once modified an existing password for a new service



- Sensitive services received most reused/modified passwords
  - Ratio = (# reused+modified pws) / (# pws of a service category)
  - Shopping services have the highest ratio (85%)
  - Email services are at the second place (62%)

Password Guessing



Password modification patterns have a low variance

- Given a user's leaked PW→ guess modified PW of un-breached services
- Possible for online guessing

Training-based guessing schemes

- Learn the different rules of transform one password to a new one
- Given a password, learn the optimized orders to apply the transform rules
  - Bayesian inference model

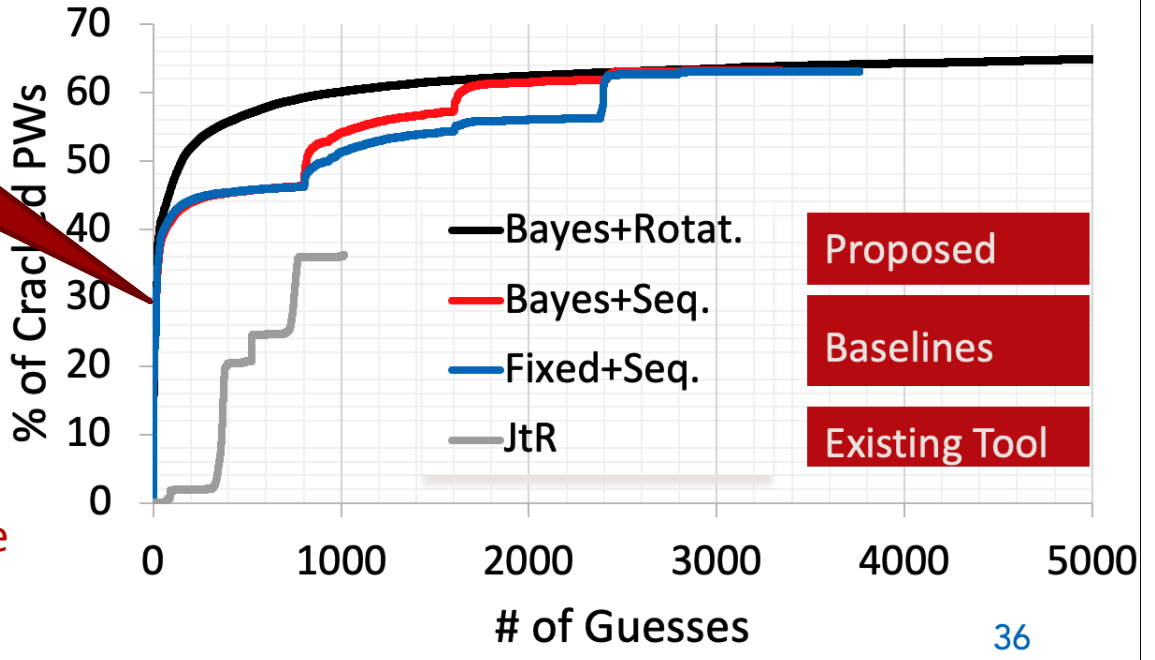
Password Guessing Results

0.1% training data, guess the rest of 99.9% modified passwords

30% of modified PWs guessed in 10 attempts (4.2M out of 14.4M modified PWs)

12.2M reused → 1 guess

Modified passwords highly predicable



Summary

- Offline and online guessing model are very different!
- Password reuse and modification are still common
- Modified passwords are highly predictable
- Password strength meters should consider online guessing models