Securing Systems

Programming and Data Systems

secure

passwords

1. 123456

1. 123456
2. 123456789

1. 123456
2. 123456789
3. qwerty

1. 123456
2. 123456789
3. qwerty
4. password

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567

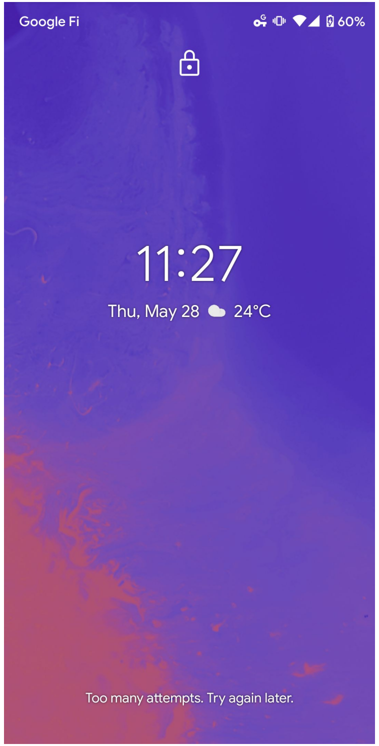
1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. iloveyou

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. iloveyou
9. 111111

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. iloveyou
9. 111111
10. 123123



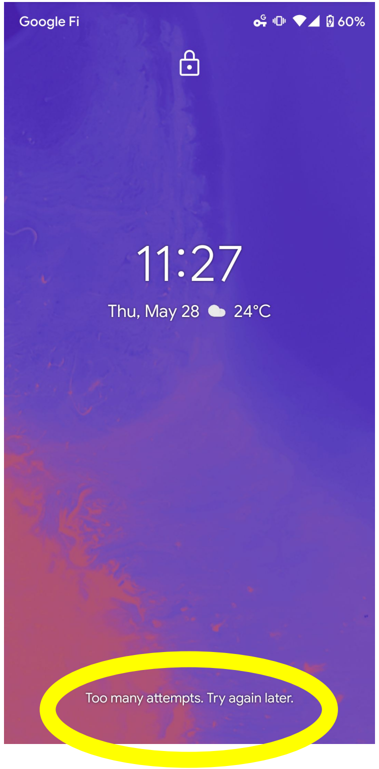
Google Fi

60%

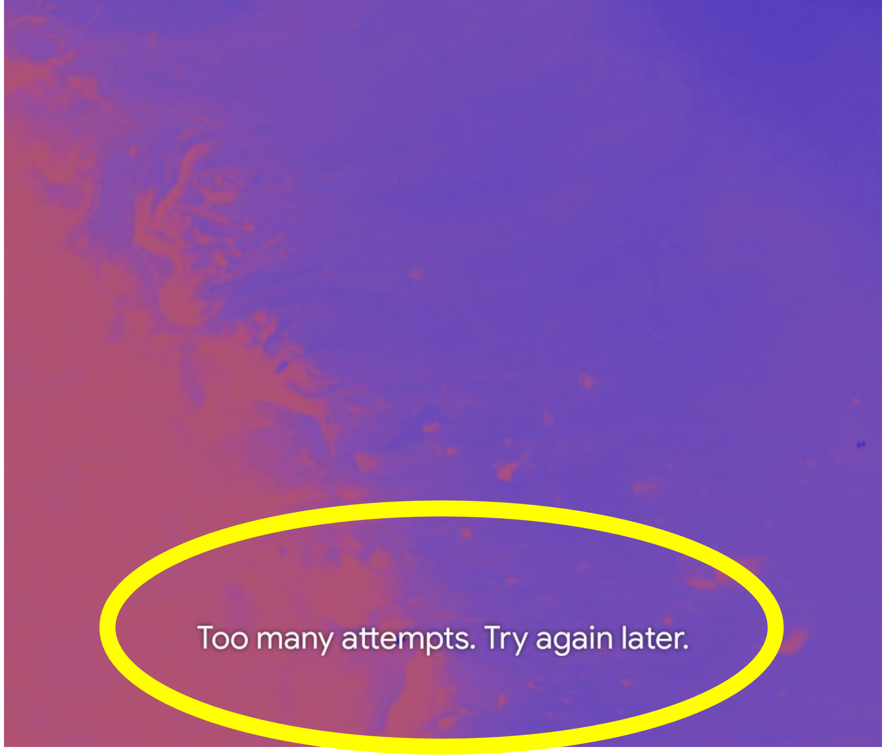
11:27

Thu, May 28 24°C

Too many attempts. Try again later.



Too many attempts. Try again later.



Too many attempts. Try again later.

two-factor authentication

private

NETFLIX

Netflix Prize

User ID, Movie Title, Date, Rating

100M ratings, 500K users, 18K movie titles, rating scale of 1–5

3M ratings withheld

Doe v. Netflix

Robust De-anonymization of Large Datasets

(How to Break Anonymity of the Netflix Prize Dataset)

National Institute of Standards and Technology (NIST)

https://pages.nist.gov/800-63-3/sp800-63b.html

"Memorized secrets SHALL be at least **8 characters** in length…"

"Verifiers SHOULD permit subscriber-chosen memorized secrets at least **64 characters** in length. All printing ASCII characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode characters SHOULD be accepted as well."

"… verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised…

- "Passwords obtained from previous breach corpuses.
- "Dictionary words.
- "Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').
- "Context-specific words, such as the name of the service, the username, and derivatives thereof."

"Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets."

"Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)."

"Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account…"

password managers

passkeys

best practices

Target

encryption

https://

end-to-end encryption

full-disk encryption

automatic updates

Wrapping Up

Programming and Data Systems

Lessons Learned

Modules

1. Thinking about Data
2. Data at Scale
3. Introduction to Programming in Python
4. Data Structures in Python
5. Monte-Carlo Simulation, Machine Learning, and Time-Space Tradeoffs
6. Artificial Intelligence
7. Computation at Scale
8. Securing Systems & Wrapping Up

Lessons Learned?

1. What are the right questions to ask?
2. How to pick the “right” tool for the job?
3. When to prevent versus detect?
4. ...

Souvenir Photo

The End