BITART PASSWORDS

CPSC 530

Bret Shilliday
Md Mushfiqur Rahman
Oscar Campos
Zach Brown

Information to look out for:

- Examples of weakness of graphical passwords over alphanumeric passwords

- Tradeoffs to achieve more secure bitart passwords

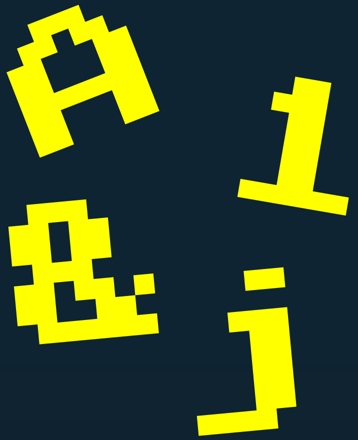
- Bit art attack types and protection techniques

INTRODUCTION

Can bitart be used as a viable alternative to text based passphrases?

TRADITIONAL PASSPHRASES

- Capital Letters (A-Z): 26
- Lowercase Letters (a-z): 26
- Numbers (0-9): 10
- Special Characters: 33
  - @#$%^&*-_!+=[]{}|\:’,.?/`~”();<>
- Total 95 Characters

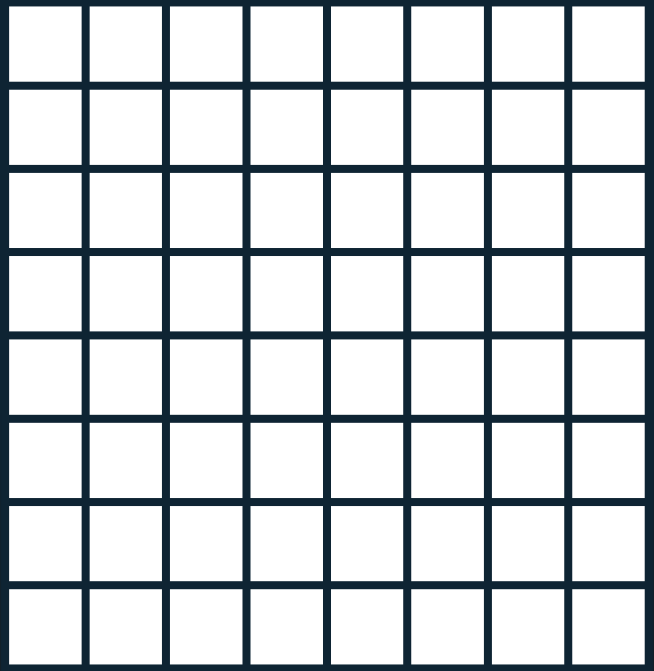


TRADITIONAL PASSPHRASES

01000001

- Could be represented using 7 bits
  - $2^7 = 128 > 95$
- However 8 bits is what is used for ASCII encoding

PROPOSED BITART DESIGN



- Grid that represents a graphical “bit art” password
- User can toggle each cell to create an image

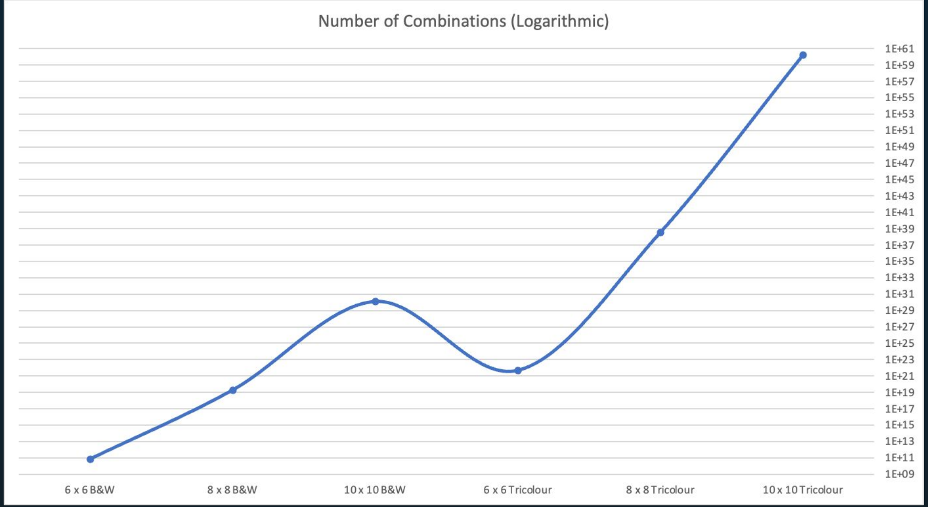
VARIATIONS

- 6 Variations
  - Size
    - 6 x 6
    - 8 x 8
    - 10 x 10
  - Colour
    - Black and White
    - Tricolour

- Black and White
  - Each cell represents 1 bit:
    - 1/0
- Tricolour
  - Each cell represents 2 bits:
    - White - 00
    - Red - 01
    - Green - 10
    - Blue - 11

COMBINATIONS

- 6 x 6 B&W - 2^{36}
- 8 x 8 B&W - 2^{64}
- 10 x 10 B&W - 2^{100}
- 6 x 6 Tricolour - 4^{36}
- 8 x 8 Tricolour - 4^{64}
- 10 x 10 Tricolour - 4^{100}



COMPARISON TO PASSPHRASE

Determine how many characters a password would need to contain to be equivalent to each bitart password:

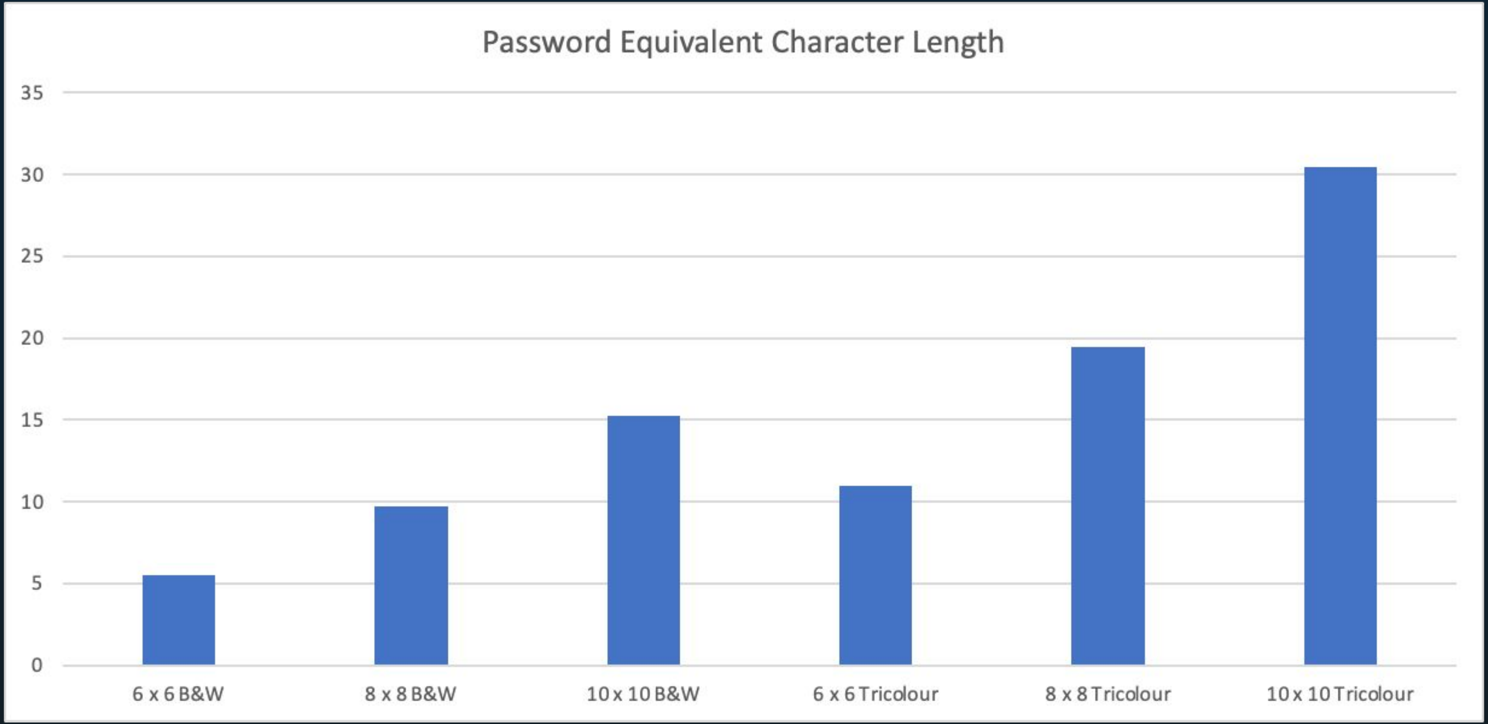
$$\text{Possible Bit Colors}^{\text{Number of Bits}} = \text{Possible Text Characters}^{x}$$

Example for 6 x 6 B&W:

$$2^{36} \approx 95^{5.5}$$

Thus, a 6 x 6 B&W bitart password is roughly equivalent to a 5.5 character passphrase.

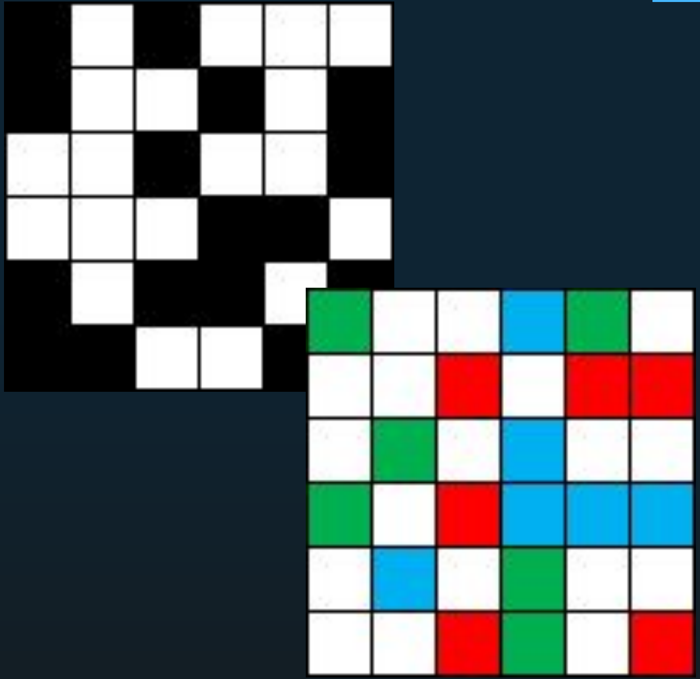
COMPARISON TO PASSPHRASE



LIMITED ENTROPY

6x6 B&W and Colour

- B&W = 36 bits of entropy
  - 6x6 grid contains 2^{36} combinations
- Colour = 72 bits of entropy
  - 6x6 grid contains 4^{36} combinations



8 Character Alphanumeric

- 52.4 bits of entropy
  - 95^{8} possible combinations

OUR EXPERIMENT

DESIGN

Each group member will create one of each type of password. They will then attempt to recreate these passwords after 1 day, 1 week and 1 month.

SECURITY

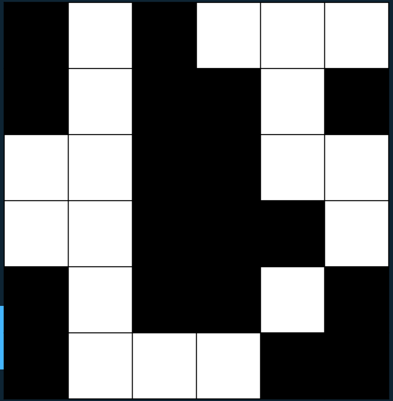
Security of Grid Size

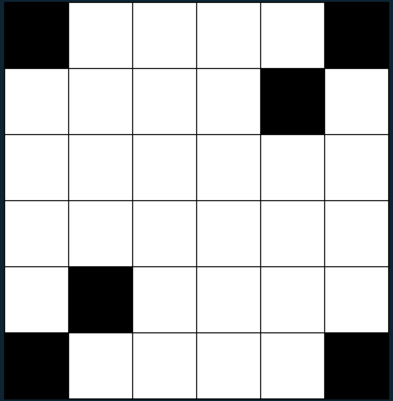
MEMORABILITY

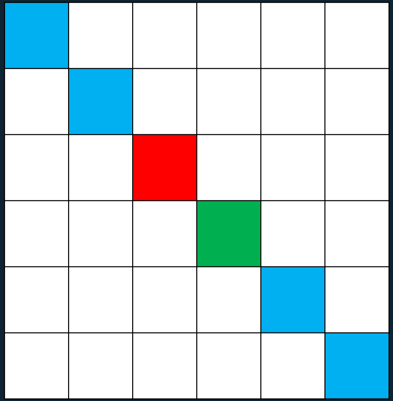
How easily/accurately the password can be reproduced

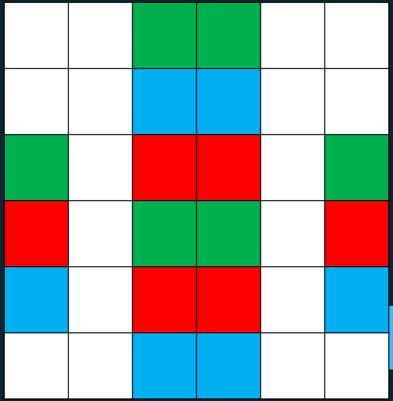
OUR
BITART
PASSWORDS

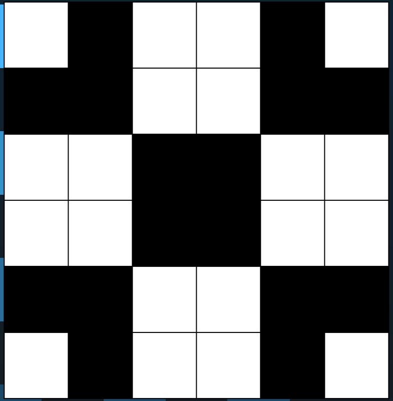
6x6

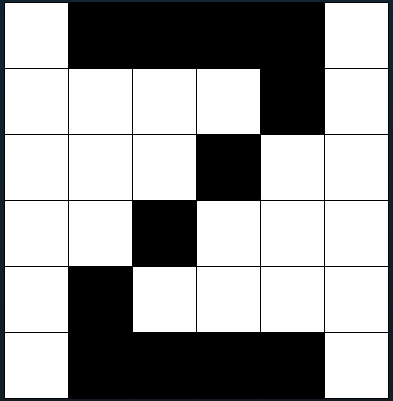


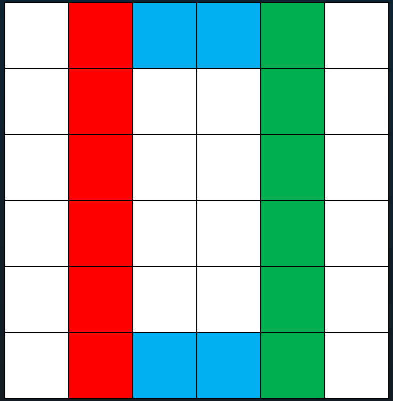


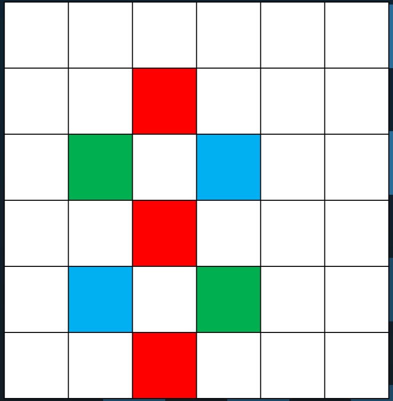




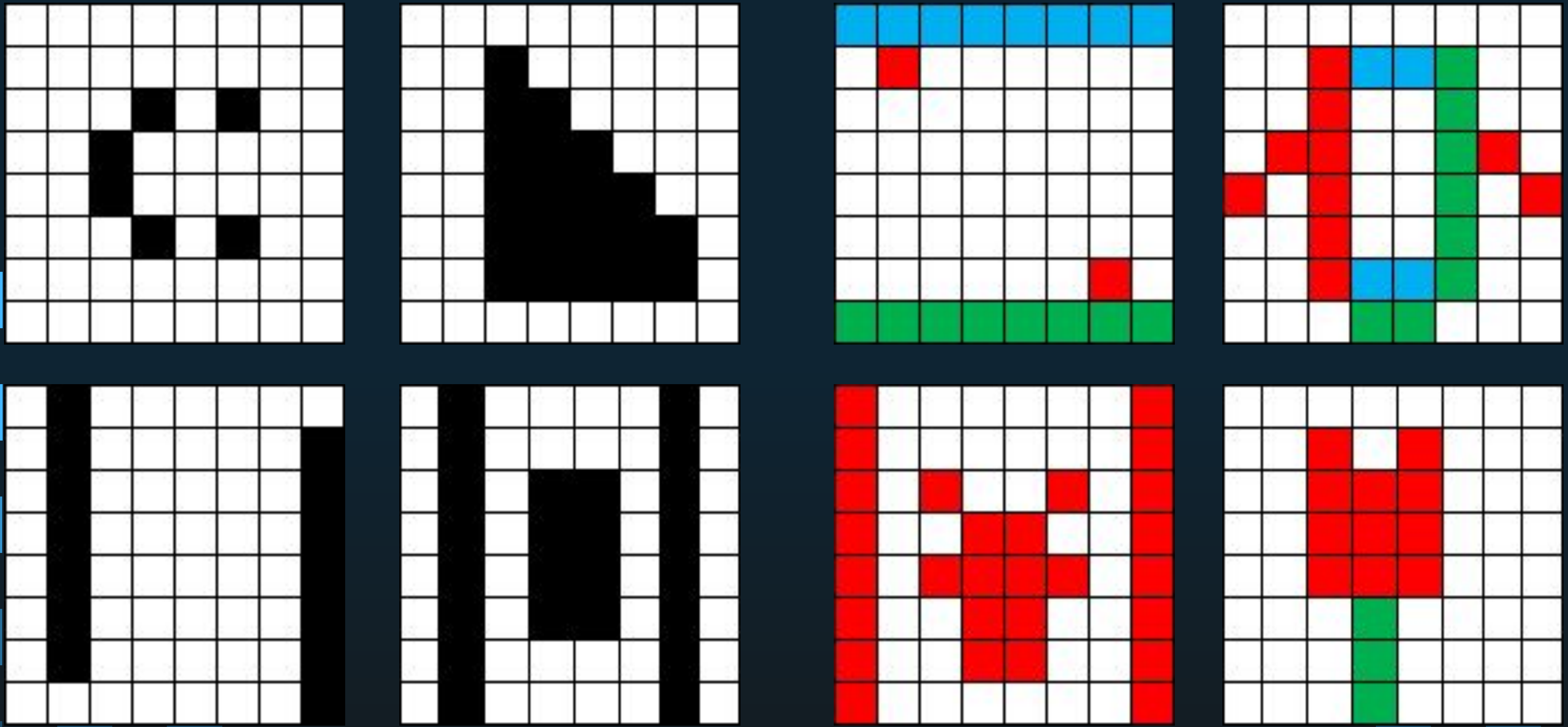




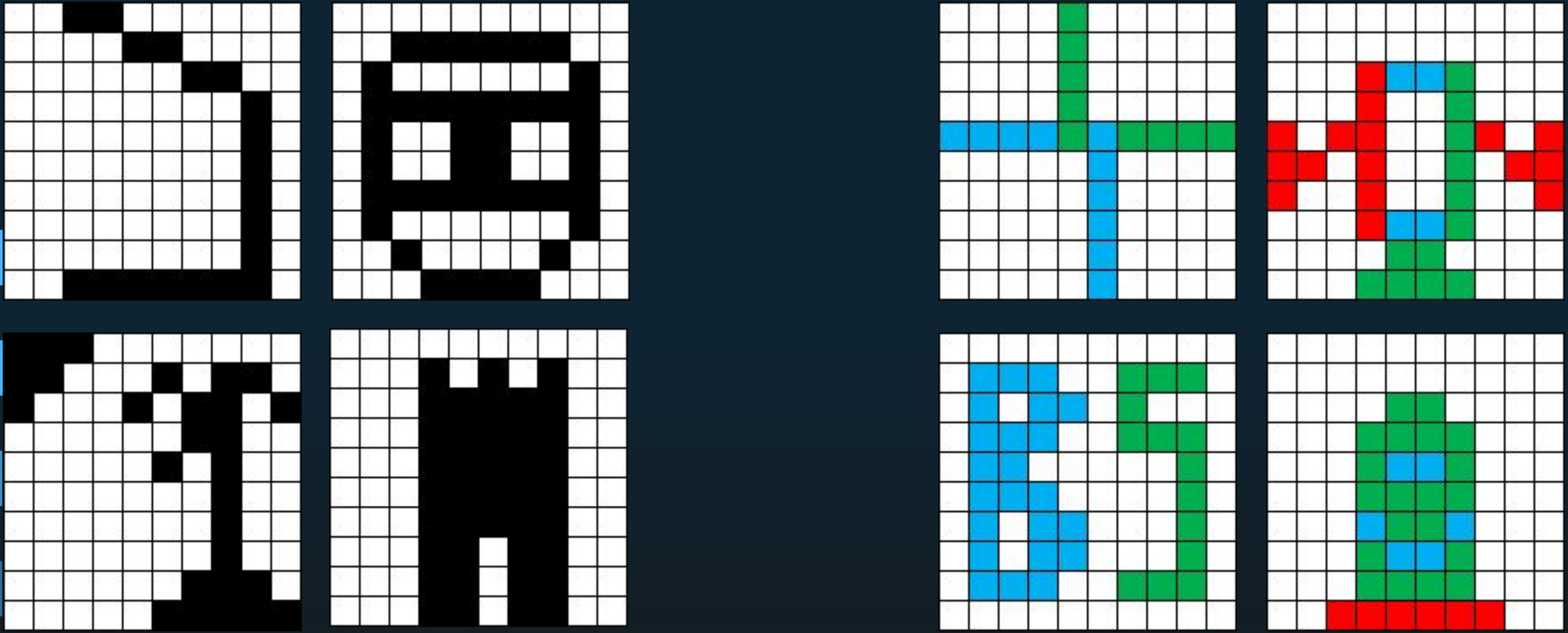




8x8



10x10



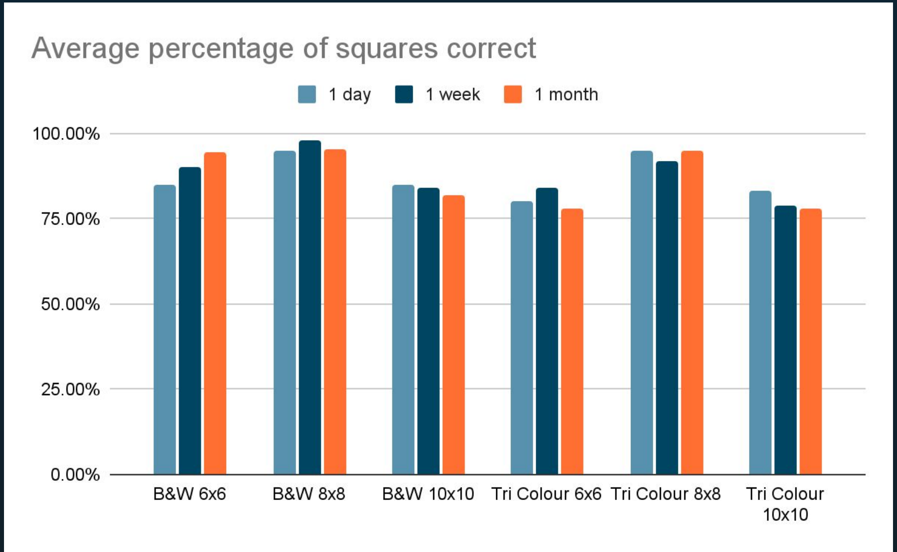
RESULTS

MEMORIZATION

- Tricolour did not have much effect on memorization

- 10x10 grids were the hardest to remember

- 8x8 grids were the easiest to remember (may be due to certain biases in password creation)



ANALYSIS

- 10x10 grid is the most secure but was also the hardest to remember

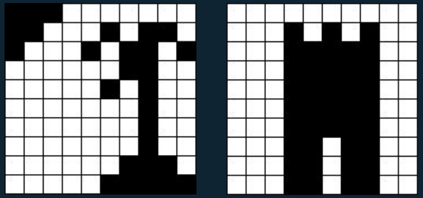
- 6x6 is much easier to remember however the entropy is much lower

- Big trade-off between security and memorization

- To make the passwords easier to remember, we implemented certain biases

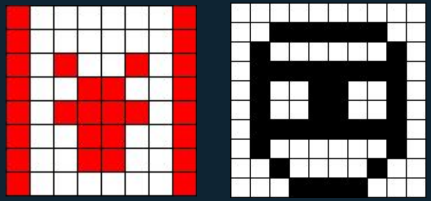
- These biases come at a cost of security

BIASES IN OUR PASSWORD CREATION



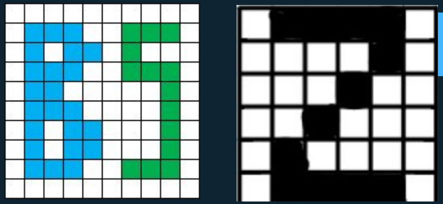
Drawings

- Many of our passwords consisted of drawings which contain clusters of certain colours in an area
- Very predictable compared to a random assortment of squares



Symmetry

- Many of our passwords consisted of symmetrical objects or patterns
- Knowing half of the password could be enough to crack it

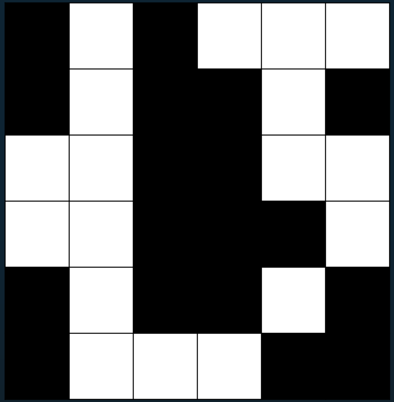


Personal Symbols

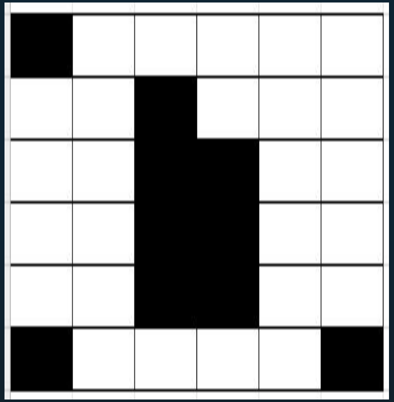
- Some of our passwords contained personal symbols such as letters of our first or last name
- Can be easily guessed if attacker knows user

BIASES IN OUR PASSWORD CREATION

- There was one password generated by Oscar using a coin flip for each square
- Less predictable pattern
- Came at the cost of memorization
- Only password not consistently recreated of the 6x6 B&W
  - 40% of the password was remembered after 1 day
  - Memorization improved over time to 95% after one month

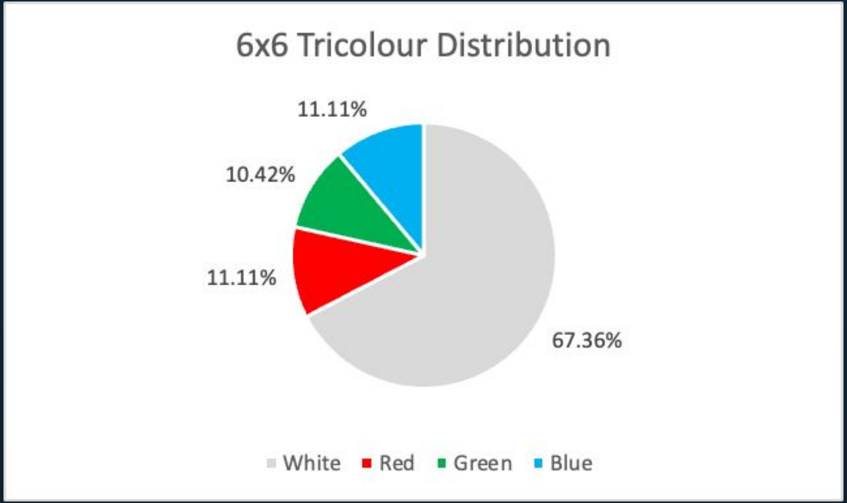


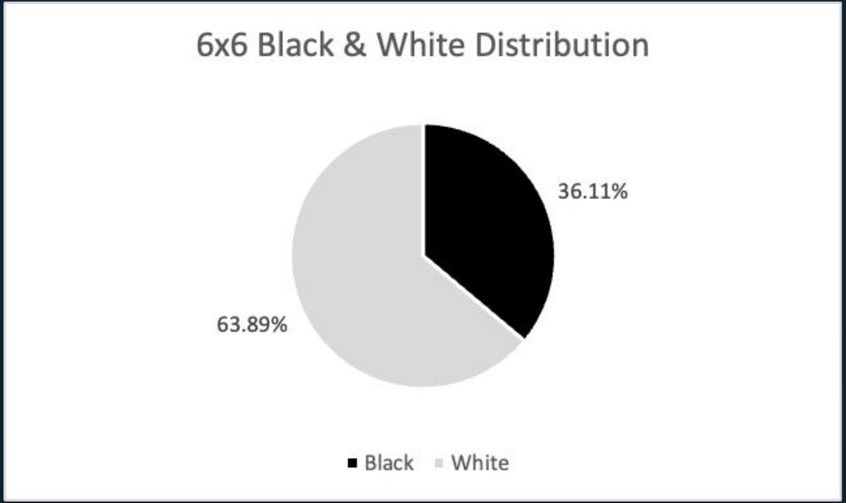
Original



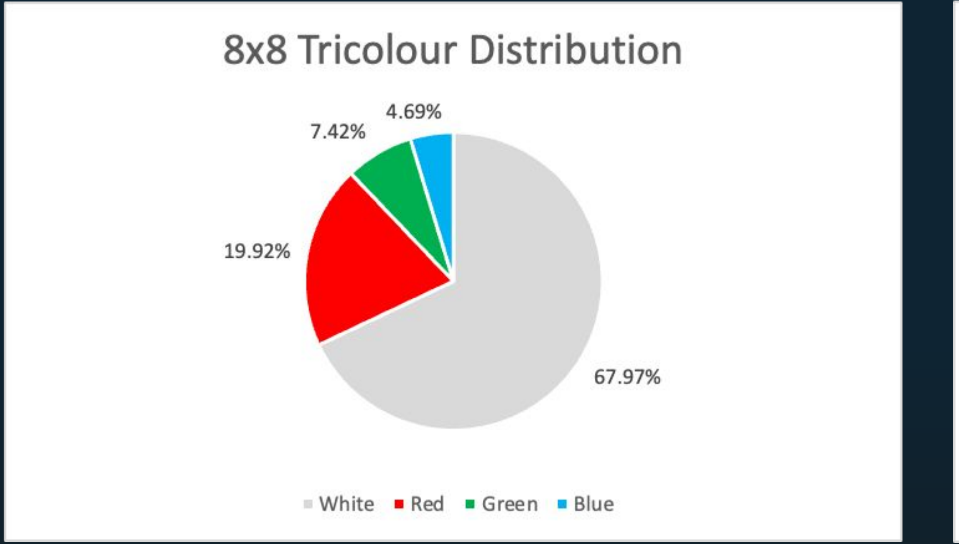
1 Week Attempt

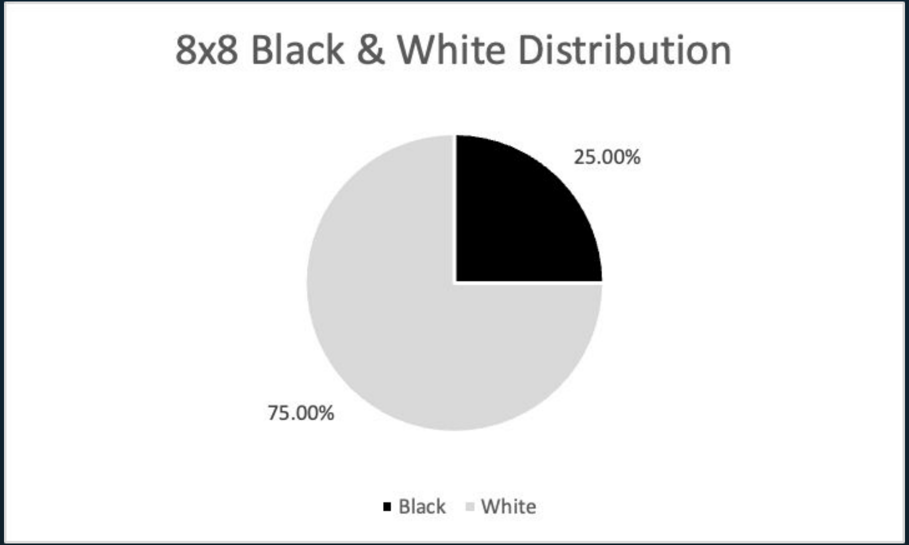
CHOSEN PASSWORD DISTRIBUTIONS 6x6



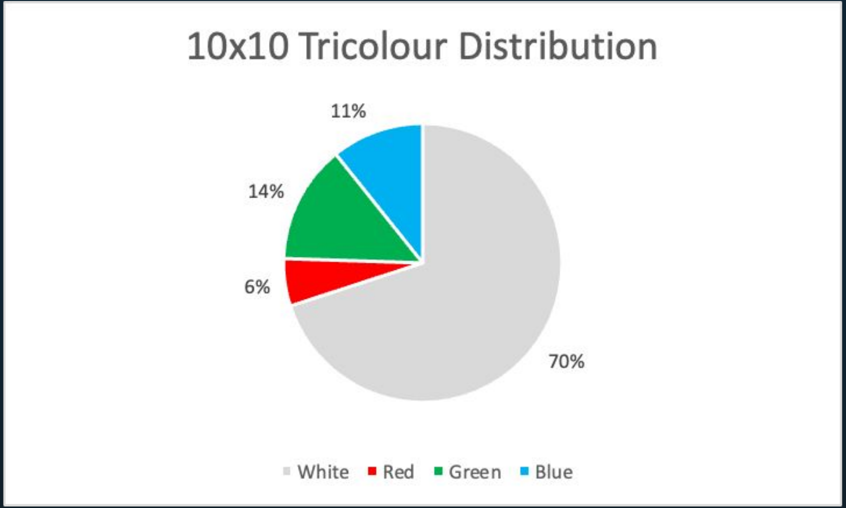


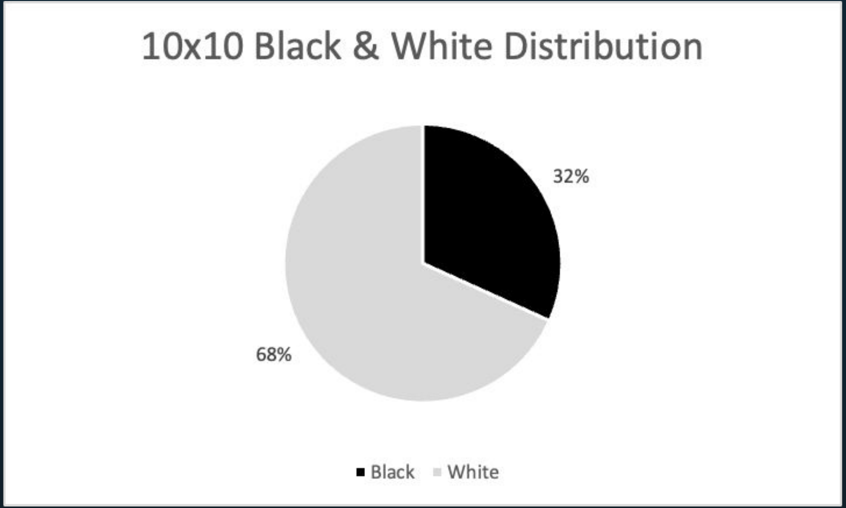
CHOSEN PASSWORD DISTRIBUTIONS
8x8





CHOSEN PASSWORD DISTRIBUTIONS 10x10





CONSIDERATIONS

LARGER + MULTICOLOUR TRADOFFS

Time Consuming to Enter

More Difficult to Memorize

Vulnerable to Minor Errors

Accessibility

GRAPHICAL ATTACKS

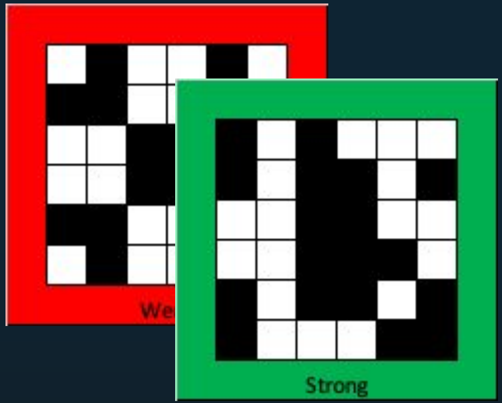
- OVER THE SHOULDER

- "SMUDGE"

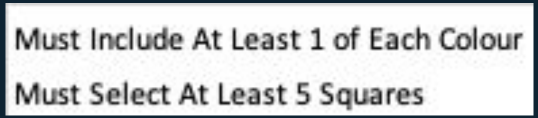
- BRUTE FORCE

USABILITY VS COMPLEXITY

How can we encourage complex patterns?

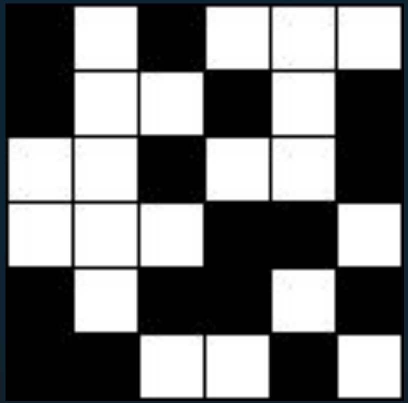


Strength Meter


Must Include At Least 1 of Each Colour

Must Select At Least 5 Squares

Minimum Requirements



Random Starting Grid

RECOMMENDATION

Advantages

Alternative Memorization Method
Resilience Against Keylogging
Initial Resistance to Dictionary Attacks

Disadvantages

Longer Authentication Time
Limited Research and Standardization
Ease of Attacks

MFA

Should be used with MFA as over the shoulder and smudge attacks are easier to conduct

Storage

Should still be stored using a hashing method to prevent leaking of plaintext grids and building of dictionaries

RECOMMENDATION

A good option for specific use cases such as alternative authentication method for people with difficulty using passphrases however the advantages are not compelling enough to replace passphrases completely.

Thank You