# Compound Password System for Mobile

Zachary Hills, David Arppe, Dr. Amin Ibrahim, Dr. Khalil El-Khatib

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

# Outline

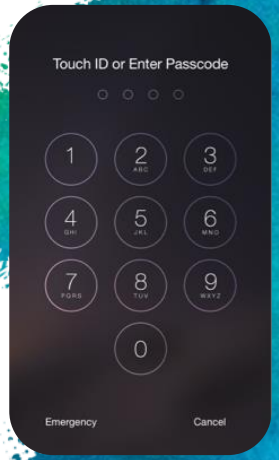
1. Traditional Mobile Authentication Schemes
2. PIN Passwords
3. Pattern Passwords
4. Issues with Traditional Mobile Authentication Schemes
5. Proposed Approach
6. Proposed Approach cont.
7. Theoretical Security
8. Conclusion
9. Future Work

# Traditional Mobile Authentication

- Pattern Passwords
- PIN Passwords (Personal Identification Number)

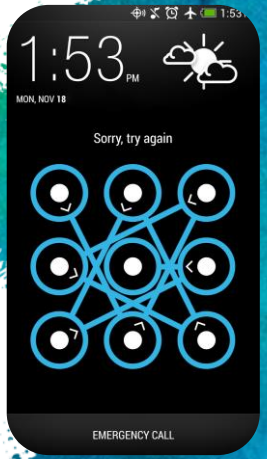

# PIN Passwords

- User enters a combination of digits ranging from 0-9
- The number of digits entered in this case is 4
- Number of combinations can be represented by $10^N$ where N is the number of digits.
- The example image represents a scheme where the number of possibilities is $10^4$



# Pattern Passwords

- User draws a pattern on a 3x3 grid
- The pattern must follow certain criteria:
  - The pattern has to have a minimum of 4 swipes
  - No node can be activated twice
- The number of combinations a 3x3 grid can have is 389,112



# Pattern Passwords Issues

- Susceptible to Smudge attacks and Video Tracking algorithms
- Smudge attacks are simplistic in nature. Users typically use their fingers to input their password.
- Their fingers leave an oily residue on the surface of the phone which can define the pattern password.
- Video tracking algorithm takes advantage of the linear behaviour of pattern passwords
- The video tracking algorithm is able to decipher the password from a distance by tracking the user's motion of their hand

# Our Proposed Approach

- Combining the traditional authentication schemes into one Compound Password System (CPS)
- The CPS inherits properties from PIN and pattern passwords.

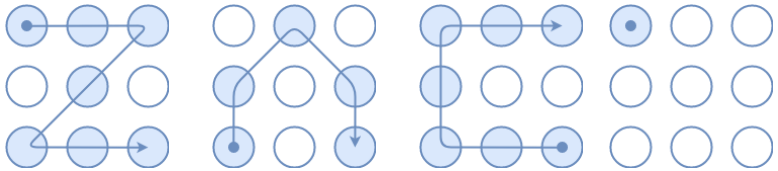
# Our Proposed Approach

Proposed Feature:

- Dots are labeled 1 through 9, for memorability if a PIN is used
- The option to use a pattern in-place-of or in-conjunction-with a PIN is given

Proposed Rules:

- Four minimum entries are required for a valid password
- Each dot will only appear once in the sequence



*The password 'ZAC1'*

# Number Of Combinations

| Length | Combinations | Length | Combinations |
|---|---|---|---|
| 1 | 9 | 6 | 26,016 |
| 2 | 40 | 7 | 72,912 |
| 3 | 168 | 8 | 140,704 |
| 4 | 1624 | 9 | 140,704 |
| 5 | 7152 | Total | 389.329 |

# Theoretical Security*

Brute-force algorithm: A trial-and-error method of obtaining a password

We can mathematically compute the strength of PIN passwords, and use an algorithm to compute the base strength of Pattern and CPS passwords

| | Combinations Possible |
|---|---|
| PIN | 10,000 ($10^4$) |
| Pattern | 389,112 |
| CPS | $389{,}329^N$ |

** Not taking into consideration attacks like over-the-shoulder, or smudge attacks*

# Conclusion

We have presented a compound password system that combines two existing methods of unlocking a mobile device. This increases the security greatly, while remaining relatively simple.

# Future Work

- We would like to gather user analytics to establish the usability of the proposed scheme
- The data we would like to collect consists of length of passwords, number of times password is incorrectly entered over time, frequency of authentication and a small survey so the user can dictate their experience with the password scheme
- From the data we hope to outline the learning curve, the average length of passwords and the overall convenience of the proposed scheme.

# Compound Password System for Mobile

Zachary Hills, David Arppe, Dr. Amin Ibrahim, Dr. Khalil El-Khatib

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY