REU Project Overview: Informing Guessing Attacks on Publicly Performed Secrets

Laura South
Research Mentors: Dr. Janne Lindqvist and Gradeigh Clark
Mobile Authentication

- Mobile authentication differs from traditional authentication
  - Performed frequently
  - Triggered by external stimuli
  - Often conducted in public

- Opportunity for information leakage
  - Smudge attacks
  - Thermal camera-based attacks
  - Shoulder surfing attacks
Password cracking

- In a traditional system, guessing attacks are most effective offline
  - No restrictions on number of attempts

- But mobile authentication systems often have this restriction, so offline attacks are impossible
  - Different strategy is necessary

- Information leakage
  - Use information gained from publicly performed secrets to improve guessing strategy
• Can enough information be obtained from shoulder surfing to significantly improve the guessing attack?

• If so, can an automated version of the shoulder surfing attack be created and utilized by attackers?
Process

1. Determine if correlation exists
2. Create training set of movements
3. Consider experimental setup
4. Build and test classifier to determine effectiveness
Acknowledgements

- Work supported by NSF grant CCF-1559855