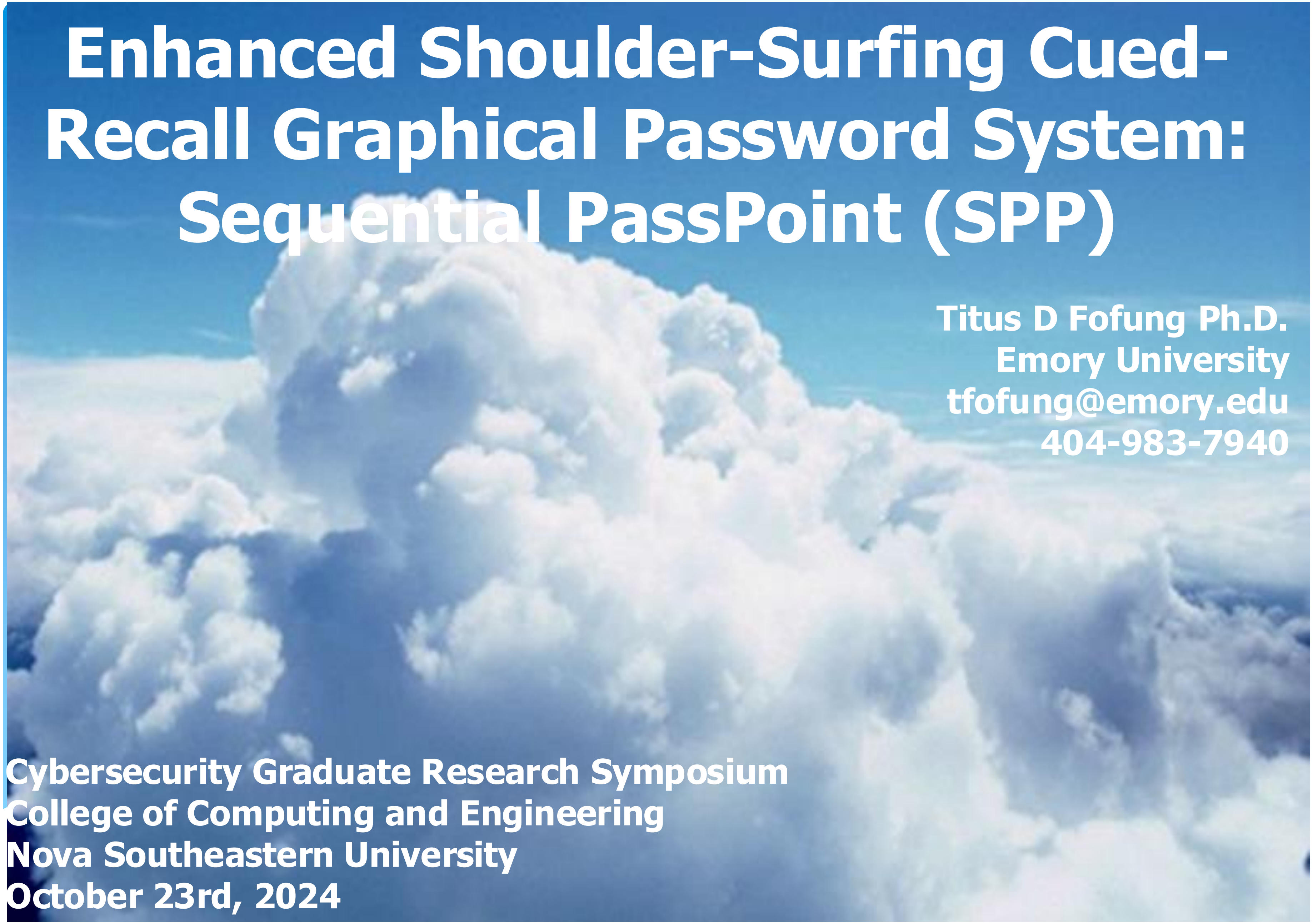
Enhanced Shoulder-Surfing Cued-Recall Graphical Password System: Sequential PassPoint (SPP)



Titus D Fofung Ph.D.
Emory University
tfofung@emory.edu
404-983-7940

Cybersecurity Graduate Research Symposium
College of Computing and Engineering
Nova Southeastern University
October 23rd, 2024

Password Systems

- Token-based authentication
- Biometric-based
- Text-Based
- Graphical Password
- Mixed authentication

Graphical Passwords Techniques

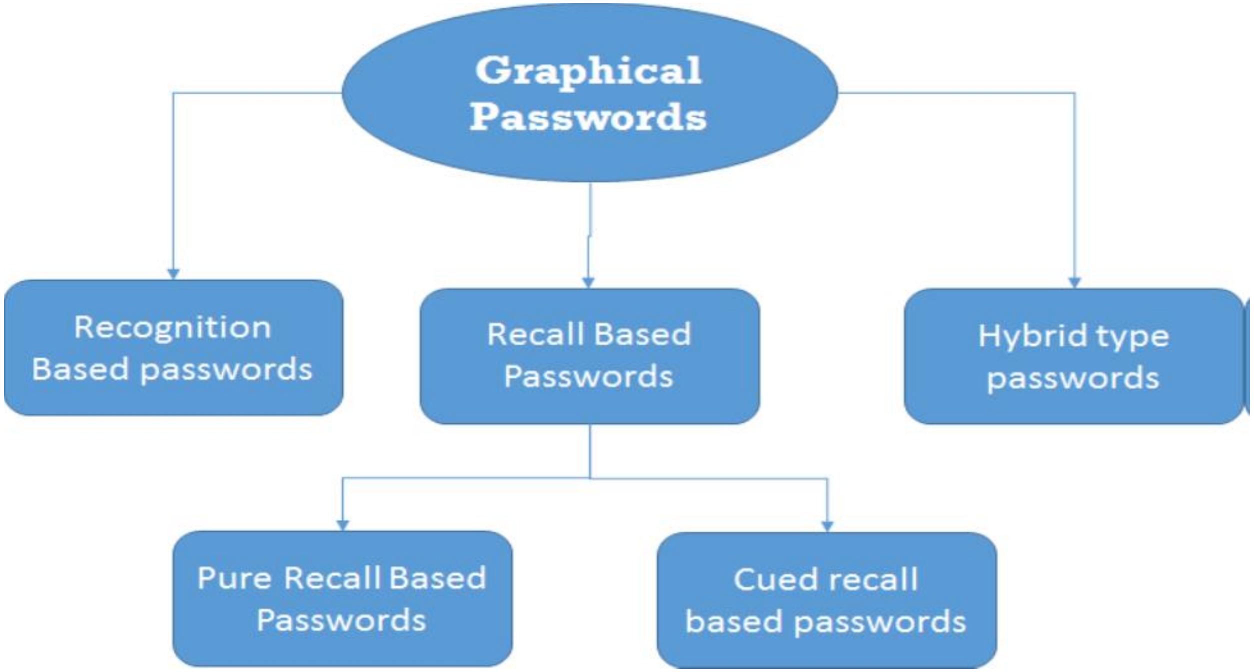

Graphical Passwords
Recognition Based passwords
Recall Based Passwords
Hybrid type passwords
Pure Recall Based Passwords
Cued recall based passwords

Figure 1: Graphical Password categories (Sonawane et al., 2016)

Motivation

- Employs images as a basis for creating and recalling passwords.
- Based on the **Picture Superiority Effect Theory**
  - images are more memorable than words (Gao et et al, 2010)
- Image-space
  - **generous surface** for solid passwords
  - resistant to **guessing** (Seelos et et al, 2011)
- more secure and usable against **shoulder surfing** (Wiedenbeck et al., 2005)
- Cheaper to implement (Bhand et al., 2015)
- Simplicity and dependability (Bilgi & Tugrul, 2018)

Pass-Point scheme

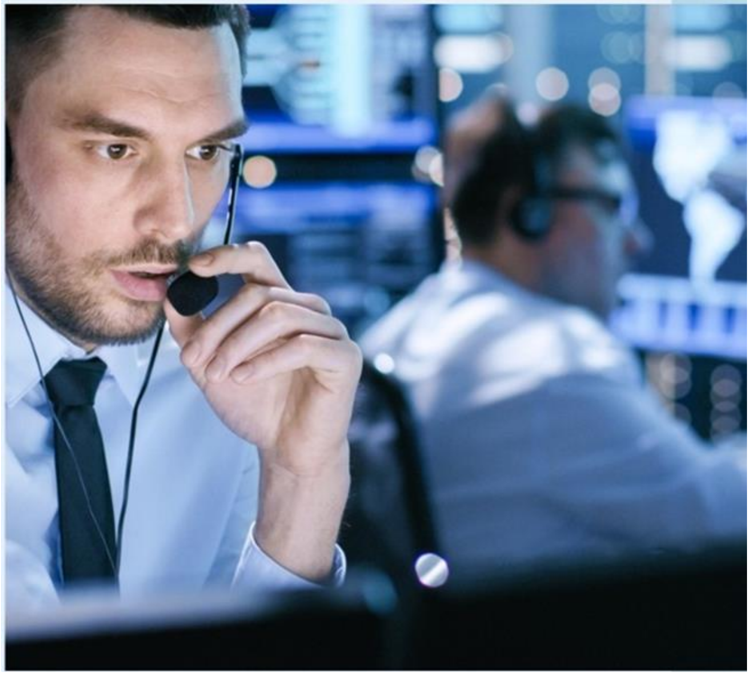
- Registration
  - select a point on an image.
  - tolerance is computed
- Authentication
  - point must be within the tolerance
  - in the correct order (Birget et al, 2006).
- password points **not precise** enough
  - decreasing the password's **robustness**
    - 'brute force attacks (Devlin et al, 2015)
- “**hotspots**” problem
  - many users select similar password points (Schneegass et al, 2015)
- allows **ten trials**

Cued Click Points (CCP).

- one click-point on five Sequenced images (Ambade & Dixit, 2013)
- restart the password entry
  - wrong order
- problems
  - **memorability**
  - 70% - 80% of click spots compare to PassPoints (Al-Ameen et al, 2015)
  - takes more **time**
- Limitations
  - plagued with **predictability** (Al-Ameen et al, 2015)
  - does not challenge **Spyware attacks** (Bhanushali et al, 2005)

Shoulder Surfing

- **Spying on a proximate target** to acquire the information they are exposing or entering (Bhanushali & Shahade, 2013)
- Shoulder surfing is a growing concern
- malicious individuals
  - can overhear passwords or sensitive information
  - **direct observation**
- Over the past decade
  - significant security vulnerability in public logins (Gaikwad, 2017)



Reducing Shoulder Surfing Incidents

- measures to curb shoulder surfing
  - visual shields
  - using decoy images
  - Users’ awareness

User Memory and Usability Concerns

- **complexity** of graphical password systems
  - impair user **memory** and **usability**
  - longer authentication times
- recall may not be as efficient
  - integrating cues and reminders
    - minimize frustration during login

Sequential PassPoint (SPP) - Registration

- user enters the username
- user is passed images
- user chooses two images they like

- user selects three locations in order
- on each of the two images
- user affirms the clicked locations

- images are added to the user's profile
- username and other research information

- user selects any two additional images
- these are decoys

- **must note the order of the password images**
- **must recognize the first image**

SPP Flowchart

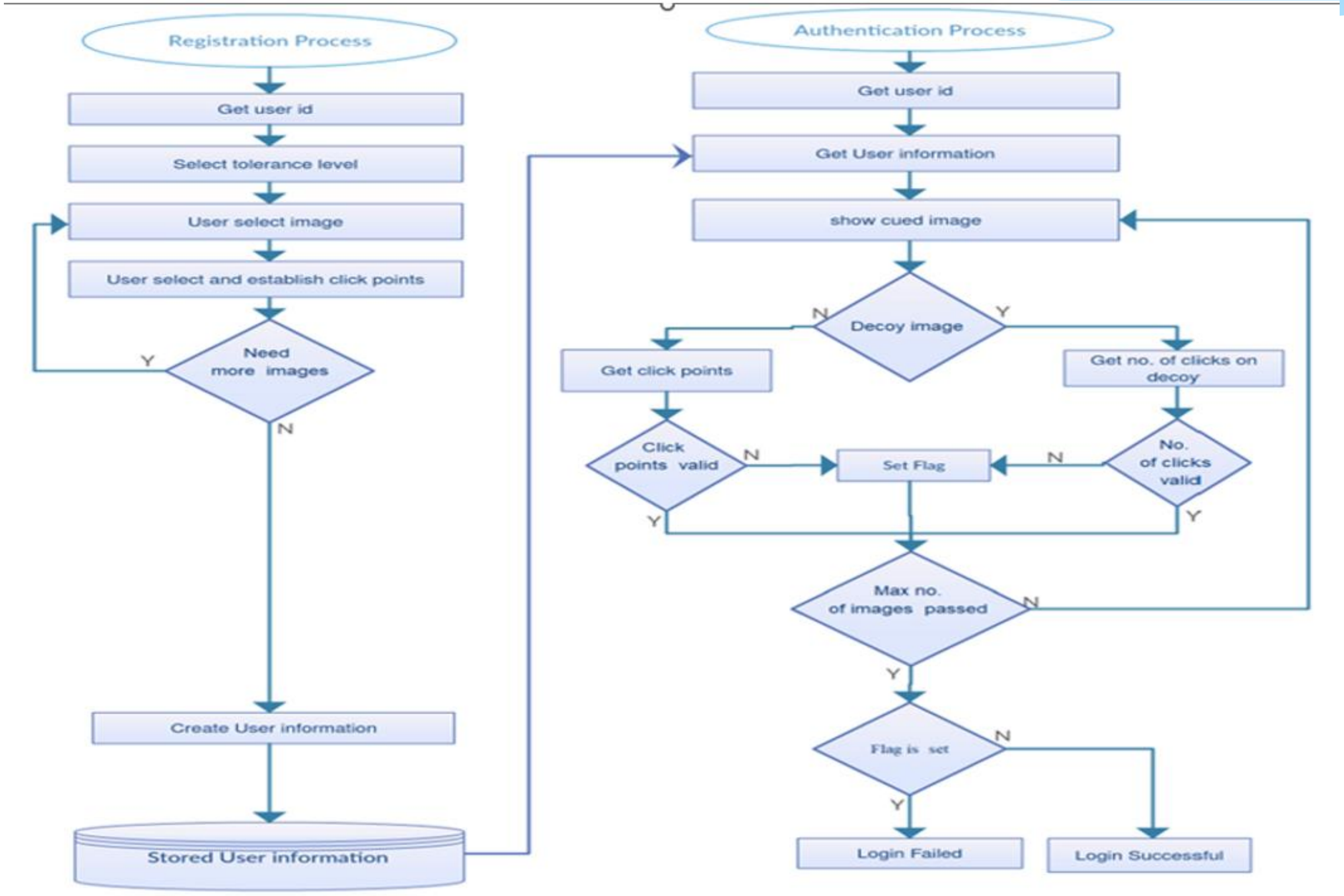


Figure 2: Flowchart for proposed model sequenced PassPoint

SPP Authentication Phase

- authentication phase consists of the following steps.
  - User type in a username
  - user is passed four images in random order.
  - user makes three phony clicks on all the decoy images on consistent
  -
- passed image is the one the user selected during registration
  - user selects the registered ordered click points
- real (password) image in the registration order
  - click the three password points in order
- real (password) image is not in the registration order
  - click the three password points in **reverse order**
- decoy image
  - click any three points in a reasonably consistent manner or order.

SPP Features

- images are **constantly shuffled**
- three ordered click points on the two images
- three random click points on the two decoy
- images in random order
  - **robustness** of SPP
  - increases **memorability**
  - reduces **shoulder-surfing**
  - attacker with a **video recorder** readily
  - **Spyware hindered**
    - Dynamic nature

Size of Password Space

Text-based passwords

- Length six using the 64-character alphabet
- lowercase are considered
- each 6 could be any of the 64 characters
- $(64)^6$ = 6.9 x 10^{10} passwords

SPP

- image size of 500 x 500
- grid is discretized into a square size of 50 x 50 pixels
- approximates to about (500 x 500) / (50 x 50) = **100 grid squares**
- six clicks on two images
- P (n, r) = P (**100**,3) = (100!)/ (100−6)! = **1.6 x 10^5** passwords one image
- (P (**100**,3))^4 = **2.6 x 10^{20}** passwords four images
- 2((P (**100**,3))^4) = **1.3 x 10^{21}** passwords four images for reverse order

Comparing Possible Passwords

Table I. Comparison of the Number of Possible Passwords

System	N = 5	**N = 6**	N = 7	N = 8
Text-based password	9.1×10^{8}	5.4×10^{10}	3.1×10^{12}	1.8×10^{14}
Graphical password (PassPoint)	9.0×10^{9}	8.6×10^{11}	8.1×10^{13}	7.5×10^{15}
Graphical password (CCP)	1.0×10^{10}	1.0×10^{12}	1.0×10^{14}	1.0×10^{16}
Proposed SPP system (perceived by hacker)	2.1×10^{19}	1.3×10^{21}	1.8×10^{24}	1.8×10^{24}

Ethical issues

- no identifiable information collected
- all results were reported as an aggregate
- ensured data security for the integrity of the research
  - only the researcher had access to this data
- participants
  - voluntarily participated
  - withdraw from the research at any time
  - aware of the ultimate purpose of the research
- carried out
  - in a comfortable environment
  - in a professional manner

Validity and reliability

- using two pictures for different graphical passwords
  - similar pictures employed for two sets of the PassPoints
- issues about content of the images
  - content of two related images
  - relevant or not similar
    - user may get confused

Usability

- time spent on the authentication process was measured
  - from the beginning of the first click on the first image to the last click on the last image
  - first training login with the first login
- experimental results
  - all participants could operate the login process

Registration Phase

Table IV. Training/Authentication Phase

	SPP			PassPoint			CCP		
	Training (Trial 1)	Login (Trial 1)	Login (Trial 2)	Training (Trial 1)	Login (Trial 1)	Login (Trial 2)	Training (Trial 1)	Login (Trial 1)	Login (Trial 2)
Accounts	**Time(s)**	**Time(s)**	**Time(s)**	**Time(s)**	**Time(s)**	**Time(s)**	**Time(s)**	**Time(s)**	**Time(s)**
1	40.00	27.00	26.00	30.00	24.00	23.00	37.00	24.00	24.00
2	35.00	26.00	25.00	26.00	23.00	24.00	31.00	26.00	24.00
3	34.00	24.00	25.00	26.00	22.00	23.00	29.00	27.00	28.00
4	37.00	26.00	26.00	29.00	25.00	24.00	28.00	26.00	26.00
5	39.00	27.00	24.00	30.00	26.00	26.00	30.00	28.00	27.00
6	37.00	23.00	23.00	27.00	24.00	24.00	27.00	24.00	24.00
Mean	**37.00**	**25.50**	**24.83**	**28.00**	**24.00**	**24.00**	**30.33**	**25.83**	**25.50**
Median	37.00	26.00	25.00	28.00	24.00	24.00	29.50	26.00	25.00
Standard Deviation	2.28	1.64	1.17	1.90	1.41	1.10	3.56	1.60	1.76

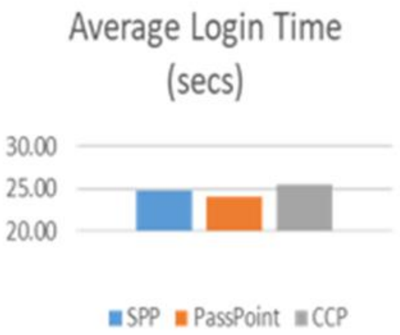
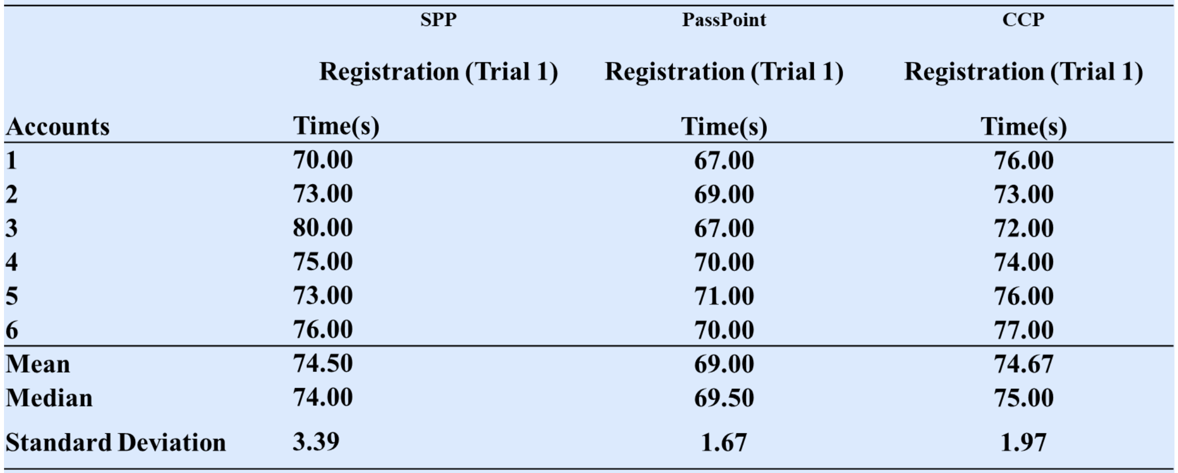


Figure 4: Comparing login time

Registration Phase

Table III. Registration Phase Times(SECS).



	SPP	PassPoint	CCP
	Registration (Trial 1)	Registration (Trial 1)	Registration (Trial 1)
Accounts	**Time(s)**	**Time(s)**	**Time(s)**
1	70.00	67.00	76.00
2	73.00	69.00	73.00
3	80.00	67.00	72.00
4	75.00	70.00	74.00
5	73.00	71.00	76.00
6	76.00	70.00	77.00
Mean	74.50	69.00	74.67
Median	74.00	69.50	75.00
Standard Deviation	3.39	1.67	1.97

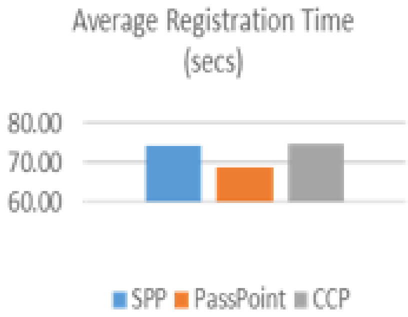


Figure 3: Comparing average registration time

Results and Conclusion

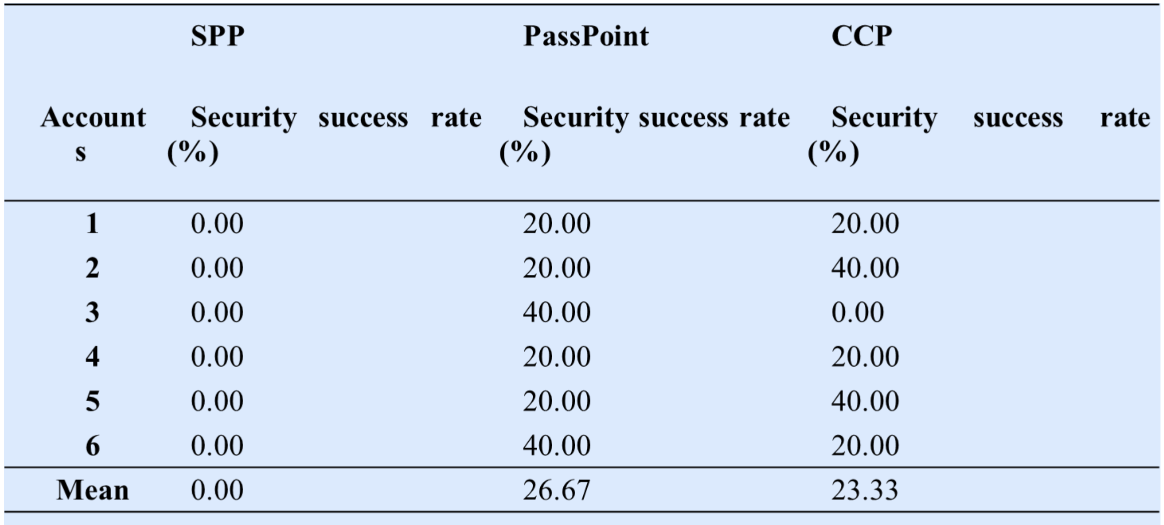
- SPP password scheme had more password space in Table I
  - multiple images were involved
- **complexity** of the theory of password creation
  - ordered sequences
  - reverse click orders are challenging
- CCP and PassPoint schemes
  - **more vulnerable**
  - more **shoulder surfing attacks**

Results and Conclusion

- SPP behaved as anticipated since shoulder-surfing attacks
  - **12 perceived points** to recall on the four images
    - less susceptible to shoulder surfing
- SPP scheme most robust
  - less than 30% break-in via shoulder-surfing see Fig. 3.
  - not susceptible to **brute force attacks**
- SPP and CCP
  - similar in their success rates when they were asked to log in four consecutive times (Fig. 2)
- system's **usability** was realized in Table III and Table IV

Comparing Shoulder Surfing Attacks

Table II. Shoulder Surfing % Success in 4 Trials



	SPP	PassPoint	CCP
Accounts	Security success rate (%)	Security success rate (%)	Security success rate (%)
1	0.00	20.00	20.00
2	0.00	20.00	40.00
3	0.00	40.00	0.00
4	0.00	20.00	20.00
5	0.00	20.00	40.00
6	0.00	40.00	20.00
Mean	0.00	26.67	23.33

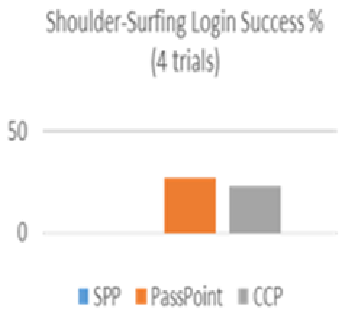


Figure 3: Comparing shoulder surfing success

Discussion and Conclusion

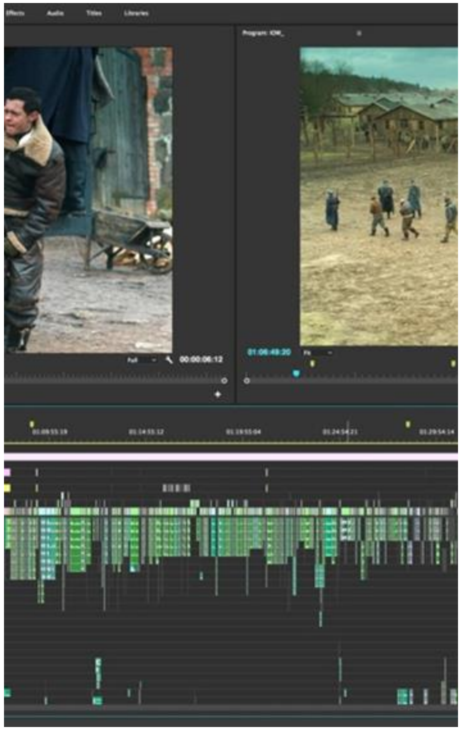
- analysis presented
  - theoretical
  - empirical
- three essential password factors
  - **memorability**
  - **usability**
  - **security** (Xiaoyuan et et al, 2005)
  - SPP
    - has met all these aspects at different levels
  - SPP
    - increase the usability of graphical password systems

Discussion and Conclusion

- susceptibility to attacks
  - someone who has learned the scheme thoroughly
    - Watch the same user log in several times
- problems
  - computational overhead
  - user acceptability should also be evaluated
  - more user participants

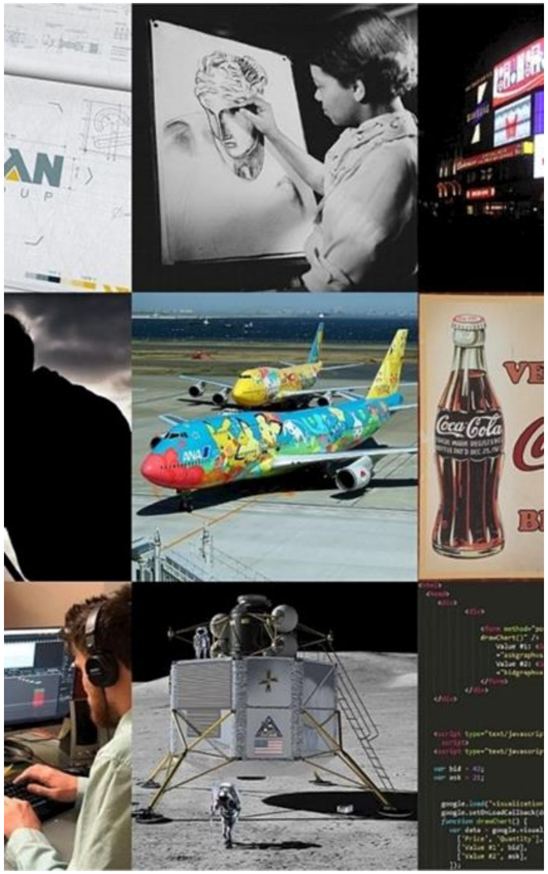
Discussion and Conclusion

- SPP password scheme
  - **more password space**
  - **complexity** of the theory of password creation
    - less susceptible to **shoulder surfing**
    - ordered sequences and reverse click orders
      - challenging to determine
  - **brute force attack**
    - not vulnerable
  - Issues
    - Image **storage**
    - **login duration**
    - **registration**



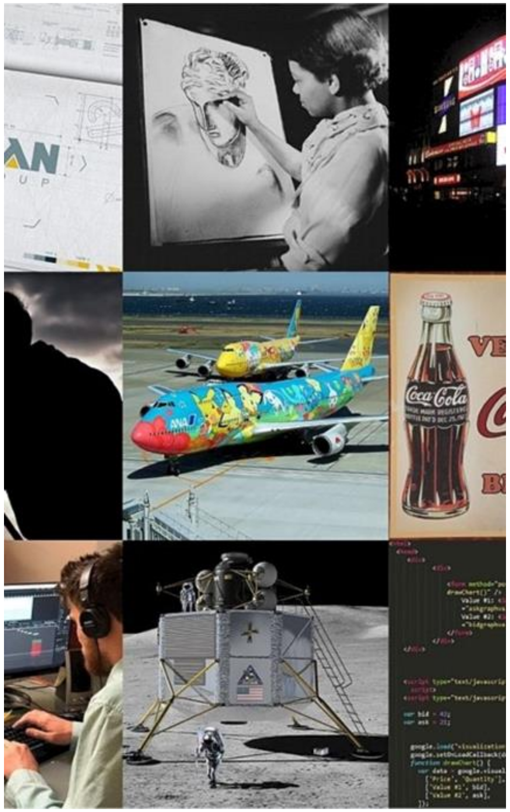
Future Work

- SPP will increase the usability
  - graphical password systems across different domains
  - system login and logout processes
    - banking
    - web locking systems
    - folder locking systems
  - More evaluation
    - computational overhead
    - user acceptability
    - user participation



Future Work

- future studies should investigate
  - user adaptation to SPP over time
  - effectiveness in diverse real-world scenarios
  - combining SPP with emerging technologies
    - biometric interfaces
      - enhanced security solutions.
- SPP can be validated with a varied number
  - registration images
  - decoy images
  - click points



References

- Al-Ameen, M. N., Fatema, K., Wright, M., & Scielzo, S. (2015, July). The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In Symposium on Usable Privacy and Security (SOUPS) (pp. 22-24).

- Alt, F., Schneegass, S., Shirazi, A. S., Hassib, M., & Bulling, A. (2015, August). Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes. In Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (pp. 316-322). ACM.

- Birget, J.C., Hong, D., and Memon, N. (2006). Graphical Passwords Based on Robust Discretization. IEEE Transactions on Information Forensics and Security 1(3), pp. 395-399, 200.

- Devlin, M., Nurse, J. R., Hodges, D., Goldsmith, M., & Creese, S. (2015, August). Predicting graphical passwords. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 23-35). Springer, Cham.

- Seelos, F. P., Murchie, S. L., Humm, D. C., Barnouin, O. S., Morgan, F., Taylor, H. W., ... & CRISM Team. (2011, March). CRISM Data Processing and Analysis Products Update--Calibration, Correction, and Visualization. In Lunar and Planetary Science Conference (Vol. 42, p. 1438).

- Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12). ACM.

- Xiaoyuan, S., Ying, Z., & Owen, G. S. (2005, December). Graphical passwords: a survey. In 21st Annual Computer Security Applications Conference, IEEE Computer Society Washington, DC, USA (pp. 463-472).

- Bhanushali A, Mange B, Vyas H, Bhanushali H, Bhogle P, Comparison of graphical password authentication techniques, International Journal of Computer Applications, vol. 116, no. 1, 2005.

- Bhong V, and Shahade V, “Authentication using graphical passwords: effects of tolerance and image choice,” International Journal for Engineering Applications and Technology, vol. 5., pp. 239-245, 2013.

- Ambade N. T., and Dixit A, Graphical Passwords Authentication: A Survey. IJCSMC, vol. 4, no. 2, pp. 247-254, 2015
- Wiedenbeck S., Waters J., Birget J. C. , Brodskiy A, and Memon, Authentication using graphical passwords: Effects of tolerance and image choice, ACM Proceedings of the 2005 symposium on Usable privacy and security, pp. 1-12, July 2005.

END

Thanks!!!

END

Questions