Leakage-Resilient Password Entry on Head-Mounted Smart Wearable Glass Devices

ABHIJITH K D
S7 CS B

Guided By:
Mrs.Anitha M A
Department of Computer Science and Engineering

22^{nd} October 2020

Overview

INTRODUCTION

- Head-mounted smart wearable glass devices[5] are becoming popular.
  e.g: Google Glass[3], HoloLens[4].
- Services : Email, Social media, maps etc.
- Privacy of Google glasses is a concern.
- Better authentication methods are needed for better security..

Figure 1: Smart Glass

INTRODUCTION (Contd.)

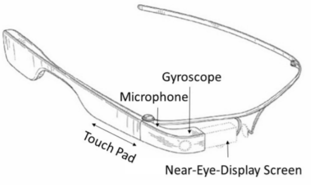


Figure 2: The Design of Google Glass

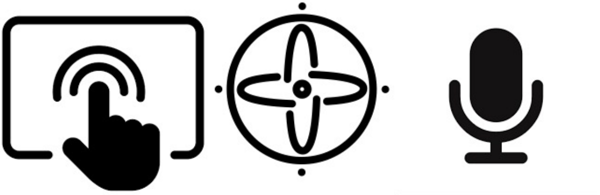
- 4 major parts : Touch Pad, NED Screen, Microphone, Gyroscope[6].
- Rely on additional devices for password entry.
- It will leads to a scope of **Eavesdropping attacks[7]:**
  1. External Eavesdropping attack
     1.1 Vision-based attacks
     1.2 Motion-based attacks
     1.3 Acoustics-based attacks
  2. Internal Eavesdropping attack
     2.1 Privileged attacks
     2.2 Unprivileged attacks

Problems Overview

- The switching between multiple devices for password entry.
- Password entry in outdoors or public area.
- A password enrty scheme within the limited hardware.
- A password entry scheme which cannot be traceable by eavesdropping attackers.

DESIGN OVERVIEW

- To ensure security for smart glasses, three anti-eavesdropping password entry schemes:
  1. gTapper
  2. gRotator
  3. gTalker



- Our **Design goals** are :
  - No additional devices or external hardware to be involved.
  - No password information except password length might be leaked.

gTapper

- Designed based on the small touch-pad.
- The pad accepts user's finger gestures as input signals.
- Tapping, Pressing, and Swiping.
- Forward & Backward, Up & Down.

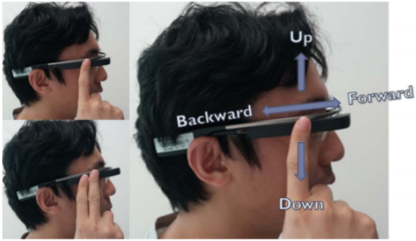


Figure 3: Touch pad Gestures

gTapper

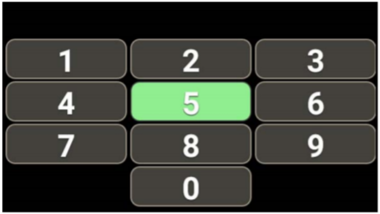


Figure 4: Demonstration of gTapper

- The Password alphabet Ω to be comprised of all single-digit numbers from 0 to 9.
- In each round i, gTapper randomly selects a number $s_i \in \{ 0, 1, 2, \ldots, 9 \}$ and sets the focus on that number.
- Users can use one finger to shift the number focus to $(s_i - 1) \bmod 10$ or $(s_i + 1) \bmod 10$, by swiping forward once or by swiping backward once.

gTapper

- To enter a password element $p_i \epsilon$ 0, 1, 2,..., 9 in round i, a user has to shift the number focus to p_i on the keypad from the initially focused number s_i by swiping forward or backward for op_i times, where $op_i = (s_i - p_i)$ mod 10 or $op_i = (p_i - s_i)$ mod 10 respectively. Then the user can enter the selected number pi with a one-finger tap on the touch pad.
- **Security Analysis of gTapper :**
  - Attackers can know the number and the directions of shifts from the initially focused number to the i^{th} element of the password.
  - But, the hidden keypad is protected
  - It is hard for attackers to know the initially focused number.
  - Therefore cannot infer the i^{th} element of the password.

gRotator

- The design of gRotator relies on a gyroscope[6].
- The password alphabet Ω comprises of single-digit numbers from 0 to 9.
- The hidden keypad is comprised of two number screens: C_s :Small number screen, C_b :Big number screen.

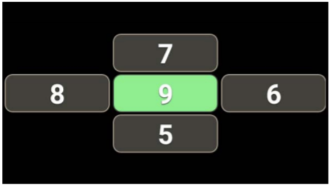
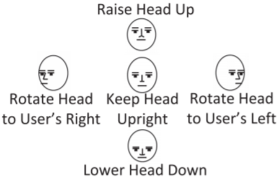


Figure 5: Demonstration of gRotator

- In each round i, five numbers and their positions would be randomly shuffled.
- To change the number screen, users have to swipe forward.

gRotator (Contd.)



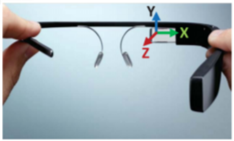


Figure 6: Head movements in gRotator & a typical motion sensor coordinate system on smart glasses.

- Users may need to select a number by rotating head towards up, down, left or right.
- To track users' head movements, we use motion data captured by the gyroscope, including angular speeds on three orthogonal axes (ie. axis X, axis Y & axis Z).

gRotator (Contd.)

- In terms of the angular speed, we can estimate user's head rotation using a dead-reckoning algorithm[8]. Let $R_{t_i} = (r_{x,t_i}, r_{y,t_i}, r_{z,t_i})$ be the angular speed generated by the gyroscope at time t_i.
- The rotation angle along each axis can be calculated by the trapezoidal rule[9] for integral approximation as follows.
  $\theta_{s,t_i} = (r_{s,t_{i-1}} + r_{s,t_i}) \cdot (t_i - t_{i-1})/2$
  Where s ϵ {x,y,z}
- For simplicity, we use angle θ_{x,t_i} and angle θ_{y,t_i} to determine the up/down directions and left/right directions of head movements.
- The initial head pose is calibrated and set at the moment when a user initially launches gRotator.

gRotator (Contd.)

- To avoid the inaccurate control of head poses, we apply thresholds:
  ξ_v : up/down, ξ_h : left/right
- The estimation of head rotation direction H_{t_i} at time t_i can be computed as below.

$$H_{t_i} = \begin{cases} \text{up} & \theta_{x,t_i} \le (-1) \cdot \xi_v \ \text{and} \ |\theta_{y,t_i}| < \xi_h \\ \text{down} & \theta_{x,t_i} \ge \xi_v \ \text{and} \ |\theta_{y,t_i}| < \xi_h \\ \text{left} & \theta_{y,t_i} \ge \xi_h \ \text{and} \ |\theta_{x,t_i}| < \xi_v \\ \text{right} & \theta_{y,t_i} \le (-1) \cdot \xi_h \ \text{and} \ |\theta_{x,t_i}| < \xi_v \\ \text{upright} & |\theta_{x,t_i}| < \xi_v \ \text{and} \ |\theta_{y,t_i}| < \xi_h \end{cases}$$

- **Security Analysis of gRotator:**
  - The keypad, including the two number screens is hidden.
  - In each round i, five numbers and their positions would be randomly shuffled.

gTalker

- The design of gTalker depends on a speech recognition-enabled built-in microphone.
- gTalker adopts the alphabet of password word as $\Omega = \{0, 1, 2, ..., 9\}$.
- Every white number p is followed by an underlined red number s.
- In each round i,
  White numbers(p) :Constant positions
  Red numbers(s): shuffle their positions.

Figure 7: Demonstration of gTalker.

gTalker (Contd.)

- For each white number p_k = k, let s_{ik} denote the corresponding underlined red number in round i, where k ϵ Ω and s_{ik} ϵ Ω. For $\forall j, k \epsilon$ Ω and j $\neq k$, $\mathrm{s}_{ij} \neq \mathrm{s}_{ik}$ holds.
- To enter password element k, users have to firstly identify the position of p_k, and then speak out the underlined red number s_{ik}.
- The mapping between p_k & s_{ik} identify the password element k.
- gTalker uses an offline speech recognition function available in Android API[10], which is developed based on Deep Neural Networks with Hidden Markov Models (DNN-HMM)[11]
- **Security Analysis of gTalker:**
  - The adversary does not know the random mapping between the original keypad and the transformed keypad.

DATA COLLECTION & EVALUATION

- 3 schemes- IRB[12] approved user study:
- **Normal condition:** No time limit, Fixed number of attempt.
- **Timed Condition:** Time limit, Any no.of attempt.
- **No distraction.**
- **Distraction[13].**
- **Heavy distraction[13].**
- **Average Login Time & Login Success Rate.**

Results Analysis

- **Normal Condition.**

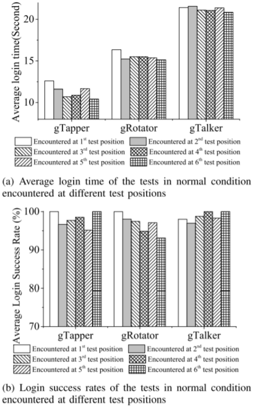


Figure 8: Learning curves for gTapper, gRotator, and gTalker

- Login time decreases as test position increases.
- Change in the test positions would not affect the login success rate.

Results Analysis

- **Normal Condition Vs Timed Condition.**

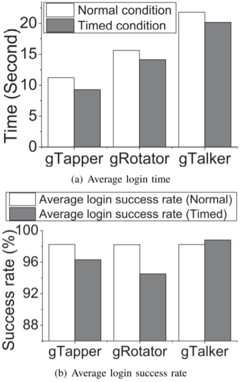


Figure 9: Impact of time pressure

- Login time decreases in Timed condition.
- Timed condition doesn't effect the success rate due to ceiling effect[14].

Results Analysis

- **Impact of Distraction.**

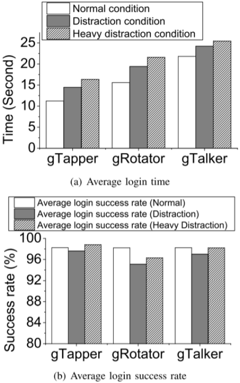


Figure 10: Impact of distraction

- Login time increases with Distractions.
- Distractions doesn't effect the success rate.

Evaluation Results Overview

- Login time decreases as test position increases.
- Login time decreases under timed condition.
- Login time increases with Distractions.
- Login success rate is not effected by test positions, time pressure, distractions.

COMPARISONS

- **gTaper Vs gRotator Vs gTalker.**

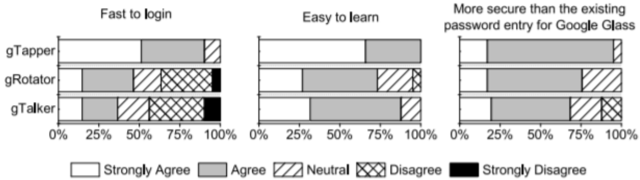


Figure 11: Comparison of 3 schemes

- **gTaper:** Very easy to learn, Very fast login, Secure.
- **gRotator:** Easy to learn, Slow login than gTaper, Secure.
- **gTalker:** Easy to learn, Slow login than gRotator, Secure.

COMPARISONS

- **Proposed scheme Vs Existing schemes.**

Metrics	Our schemes	Existing password entry on smart glasses
Resilient-to-Physical-Observation	▲	
Resilient-to-Targeted-Impersonation	△	△
Resilient-to-Internal-Observation	△	
Resilient-to-Theft	▲	▲
No-Trusted-Third-Party	▲	
Requiring-Explicit-Consent	▲	▲
Unlinkable	▲	▲
Accessible	▲	▲
Negligible-Cost-per-User	▲	△
Mature		▲
Non-Proprietary	▲	▲
Nothing-to-Carry	▲	△
Easy-to-Learn	▲	▲
Efficient-to-Use	△	▲
Infrequent-Errors	△	△
Easy-Recovery-from-Loss	▲	▲

Figure 12: Comparison of 3 schemes

- **Dark Triangle:** Benefit is offered.
- **Bright Triangle:** Benefit is partially offered.
- **Blank Cell:** Benefit is not offered.

ADVANTAGES

- More secure than conventional password entry.
- Can avoid switching between multiple devices.
- Easy to use in outdoors.
- Uses only the available hardware in smart glasses.

DISADVANTAGES

- Don't have a richer password alphabet.
- Password length is less.
- Speech recognition[11].
- Head movement estimation[1].
- Sometimes password entry takes more time.

THINK ABOUT IT

"Richer password alphabet only requires a shorter password length"

SOLUTIONS

- More richer set of alphabet by using AR[15] & VR[16].

Figure 13: Demonstration of AR-VR[15][16] in google glass.

- Bio-metric[17] sensors like fingerprint recognition, iris recognition etc. for password entry.

CONCLUSION

- At present, most existing anti-eavesdropping password entry schemes on smart glasses are heavily depending on additional devices.
- So users neeed to switch between different systems and devices.
- Three anti-eavesdropping password entry schemes for smart glasses: named gTapper, gRotator and gTalker.
- These 3 schemes provides better security for smart glasses from the eavesdropping attacks.
- Don't need to switch between devices.
- These schemes Don't use any extra hardware.
- An an IRB-approved users study conducted.
- Out of 3 schemes, gTapper is easy to use and has a fast login. and these 3 schemes provides more security than other schemes.
- Designed schemes are easy to use in various real-world scenarios.

REFERENCES I

1. Yan Li, Y. Cheng,Weizhi Meng, Yingjiu Li and R. H. Deng "Designing Leakage-Resilient Password Entry on Head-Mounted Smart Wearable Glass Devices", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, Volume: 16, Issue: 5, July 2020.

2. Y. Li, Y. Cheng, Y. Li, and R. H. Deng ""What you see is not what you get: Leakage-resilient password entry schemes for smart glasses," *Computer Community*, in Proc. ACM Asia Conf. Comput. Commun. Secur., April 2017, pp. 327–333

3. "Google. (2017). Google Glass". [Online]. Available: *https://developers.google.com/glass/distribute/glass-at-work* Accessed on: Sept. 28, 2020

4. "Microsoft. (2017). Microsoft Hololens ". [Online]. Available: *https://www.microsoft.com/microsoft-hololens/en-us* Accessed on: Sept. 28, 2020

5. "Smart Wearable Devices ". [Online]. Available: *https://www.gadgetsnow.com/slideshows/8-smart-wearables-you-must-know-about/photolist/51256562.cms* Accessed on: Oct. 12,2020

6. "Wikipedia. Gyroscope ". [Online]. Available: *https://en.wikipedia.org/wiki/Gyroscope* Accessed on: Oct. 12, 2020

7. "Eavesdropping attack ". [Online]. Available: *https://www.sciencedirect.com/topics/computer-science/eavesdropping-attack* Accessed on: Oct. 12, 2020

8. "Wikipedia. Dead Reckoning Algorithm ". [Online]. Available: *https://en.wikipedia.org/wiki/Dead_reckoning* Accessed on: Oct. 12, 2020

REFERENCES II

9. "Wikipedia. Trapezoidal Rule ". [Online]. Available: *https://en.wikipedia.org/wiki/Trapezoidal_rule* Accessed on: Oct. 12, 2020

10. "Wikipedia. API ". [Online]. Available: *https://en.wikipedia.org/wiki/API* Accessed on: Oct. 12, 2020

11. "Wikipedia. DNN-HMM ". [Online]. Available: *https://en.wikipedia.org/wiki/Speech_recognition* Accessed on: Oct. 12, 2020

12. "Wikepedia. IRB ". [Online]. Available: *https://en.wikipedia.org/wiki/IRB_Infrastructure* Accessed on: Oct. 12, 2020

13. P. D. Adamczyk and B. P. Bailey "If not now, when?: The effects of interruption at different moments within task execution," *NDSS*, in Proc. Conf. Hum. Factors Comput. Syst., 2004, pp. 271–278

14. "Wikepedia. Ceiling effect ". [Online]. Available: *https://en.wikipedia.org/wiki/Ceiling_effect_(statistics)* Accessed on: Oct. 12, 2020

15. "Augmented Reality ". [Online]. Available: *https://en.wikipedia.org/wiki/Augmented_reality* Accessed on: Oct. 12, 2020

16. "Virtual Reality ". [Online]. Available: *https://en.wikipedia.org/wiki/Virtual_reality* Accessed on: Oct. 12, 2020

17. "Wikepedia. Biometrics ". [Online]. Available: *https://en.wikipedia.org/wiki/Biometrics* Accessed on: Oct. 12, 2020

18. rQ. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng "Designing leakage resilient password entry on touchscreen mobile devices," *Computer Community*, in Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur., 2013, pp. 37–48

THANK YOU