# Preventing Shoulder Surfing using Randomized Augmented Reality Keyboards

Anindya Maiti, Murtuza Jadliwala, and Chase Weber

March 13, 2017

SPriTE Lab
Wichita State University

## Table of Contents

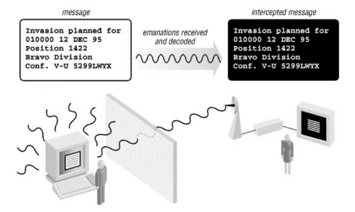
1. Introduction
2. Related Work
3. Adversary Model
4. Proposed Defense Model
5. Evaluation
6. Discussion
7. Conclusion

# Introduction

# Keystroke Inference Attacks - Visual Shoulder Surfing

Visual Shoulder Surfing: Direct observation techniques, such as looking over someone's shoulder, to obtain typed information (such as passwords, PINs, credit card details, emails, etc.).

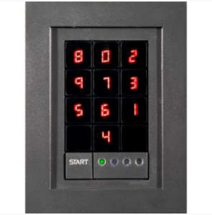
# Keystroke Inference Attacks - Side-Channel Shoulder Surfing

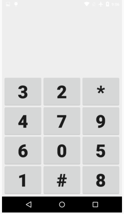


Side-Channel Shoulder Surfing: Indirect observation techniques, such as analysis of keystroke emanations or wrist movements, to infer typed information.

# How to Protect Keystroke Privacy?

Randomizing the keyboard layout from the default to something different.





**Limitations:** Works only against side-channel shoulder surfing, and requires dynamically changeable keypad.

**Our Solution:**

Key Randomization + Augmented Reality = Keystroke Privacy

# Related Work

# Keystroke Privacy

Kumar et al. [11] proposed EyePassword, where orientation of the user's pupils were used for password entry.

Graphical password is also proposed as an alternative, where users select a predetermined image or set of images in a particular order [12] [13].

Recently, Yan et al. [17] proposed CoverPad where a user covers the screen (by hand) to securely read a hidden message that contains information on removing the correlation between the actual password (or PIN) and the one entered by the user.

# Limitations of Previous Works

Focus on preventing shoulder surfing attacks only for authentication information such as passwords or PINs.

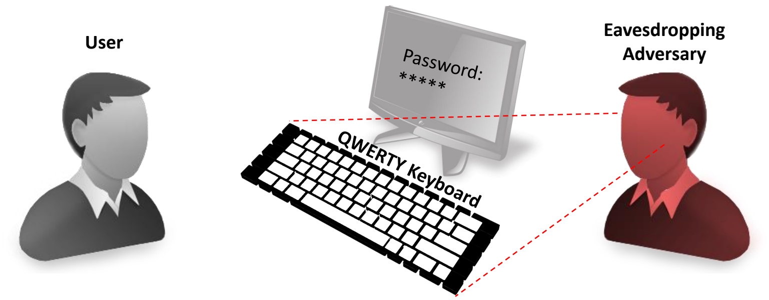
Graphical passwords are not completely secure against visual shoulder-surfing attacks [15] [16].

Usability factors.

Our model protects all kinds of textual inputs, against both visual and side-channel shoulder surfing attacks.

# Adversary Model

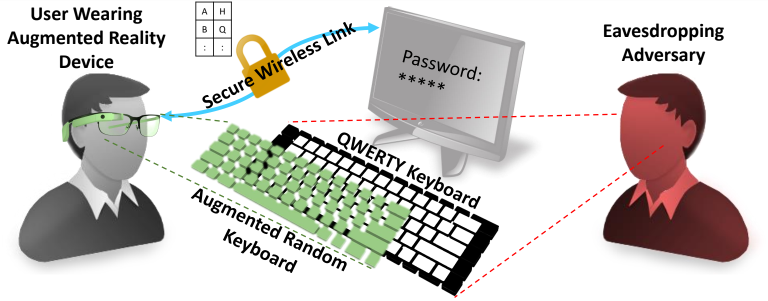
# Eavesdropping Adversary



The adversary may attempt to accomplish the keystroke inference attack directly using visual channel, or using other forms of side-channels.

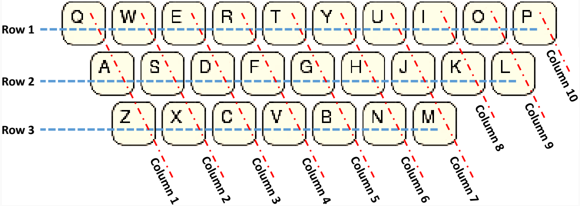
# Proposed Defense Model

# Key Randomization + Augmented Reality



To obscure keystrokes from the eavesdropping adversary, we propose the use of randomized keyboard layouts in cohort with an augmented reality device.

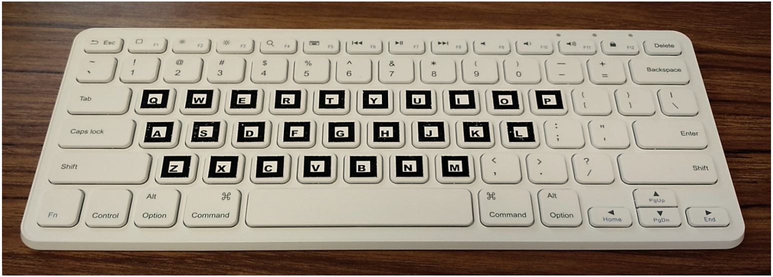
# Randomization Strategies



Individual Key Randomization (IKR), Row Shifting (RS), and Column Shifting (CS).

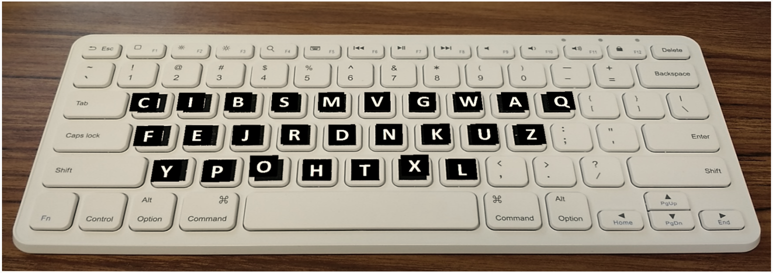
Security Analysis (Based on Possible Number of Unique Layouts):
IKR $>$ CS $>$ RS

# Proof-of-Concept



A QWERTY keyboard with alphabetic Hiro markers glued on top of the corresponding alphabet keys.

# Proof-of-Concept



An instance of augmented keyboard with IKR strategy as observed by a typer wearing a EPSON Moverio BT-200.

Custom implementation of ARToolKit library [19] in Android 4.0.

# Evaluation

# Experimental Setup

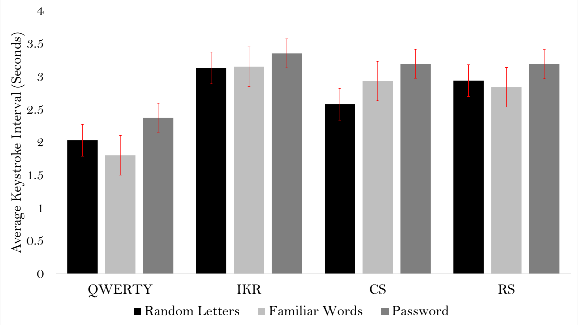
Study Design:

- Anker A7726121 Bluetooth keyboard (with Hiro markers).
- EPSON BT-200 with 640x480 resolution front camera.
- 13 participants.

Task:

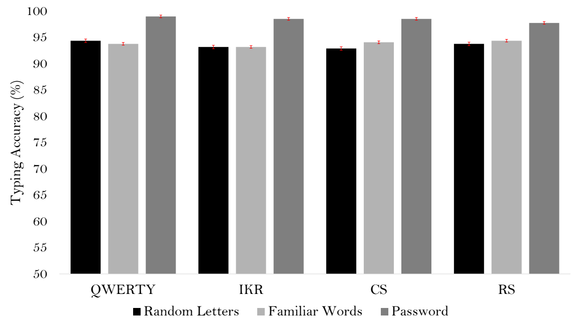
- Audio-visual instructions on what to type on the keyboard.
- 26 alphabets of English language in random order.
- 5 familiar words: first name, last name, hometown, address street, and area of work.
- An experimental password of choice.

# Results - Typing Speed



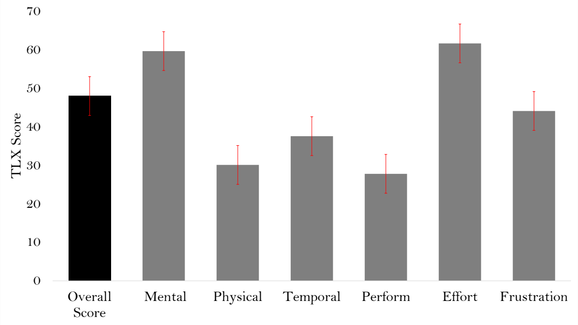
Results suggest that there is an increase in task completion time. However, it may decrease with prolonged usage and habituation.

# Results - Typing Accuracy



Typing accuracies are comparable to typing on QWERTY keyboards.

# Results - Perceived Task Load (NASA-TLX)



**Low:** Physical demand, Temporal demand and Performance Issues. However, few participants complained about lag in rendering of the keys, noticeable when the user moves his/her head.

**High:** Mental demand and Effort.

# Discussion

# Limitations and Future Work

**Hardware Limitations:** Camera resolution of EPSON BT-200 is extremely low (640x480 pixels), which makes marker recognition error-prone and difficult, especially at a distance from the keyboard. These limitations can be resolved with advances in augmented reality device technology.

**Usability:** We plan to conduct a comprehensive usability study with the help of a significant number of participants, prolonged natural typing experiments, and standard usability metrics.

# Generalization to Other Keyboards

Proposed design can be easily generalized and deployed across different types of keyboards/keypads.

Character recognition, instead of the exemplary marker recognition used in our prototype, can enable such a generalized design.

# Conclusion

# Conclusion

We proposed a novel technique to overcome various forms of shoulder surfing attacks on physical keyboards.

Preliminary evaluation showed that keyboard randomization strategies and augmentation does increase the time required by users to complete their typing tasks.

Requires further investigation on usability and prolonged usage.