RandomPad: Usability of Randomized Mobile Keypads for Defeating Inference Attacks

Saturday 29th April, 2017. IMPS 2017, Paris, France.

Anindya Maiti[†], Kirsten Crager[†], Murtuza Jadliwala[†], Jibo He[†], Kevin Kwiat[◇] *and* Charles Kamhoua[◇]

[†]Wichita State University, Wichita, KS, USA
[◇]Air Force Research Laboratory, Rome, NY, US

Table of Contents

Introduction

Side-Channel Inference Attacks on Mobile Device Keypads

Indirect observation techniques used by ‘attackers’ to obtain victim’s personal information (such as passwords, credit card details, SSN/NIR, etc.) from their typing actions.

Types of Keystroke Inference Attacks 1/2

Based on time delays between audio feedback of keystrokes [8].

Sun et al. [29] used video recordings of the backside of a tablet to infer typed keystrokes.

Simon et al. [24] used microphone to detect touch events, while the camera is used to estimate the smartphone's orientation, and correlate it to the position of the digit tapped by user.

Zhang et al. [33] analyzed finger smudges left on the touch screen surface to infer touch patterns, with remarkable success.

Types of Keystroke Inference Attacks 2/2

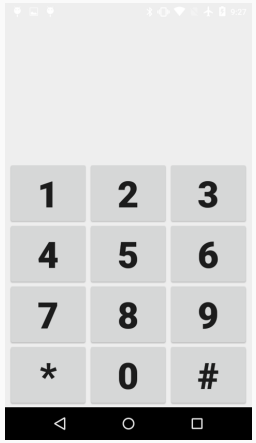
Motion sensor-based attacks on mobile keypads:

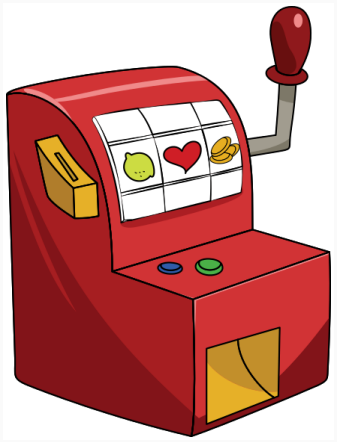
- On-Device: Cai et al. [4] and Owusu et al. [18] used accelerometer and gyroscope for keystroke inference.
- Off-Device: Maiti et al. [17] used user's smartwatch motion sensors for keystroke inference.

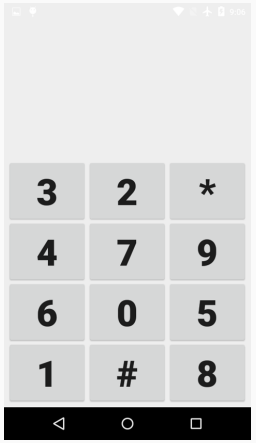
How to Protect Smartphone Keystroke Privacy?

Interestingly, all these attacks share one common assumption: *the numeric keypad employed by the target user has a standardized key layout known to the adversary*.

Solution: Randomizing the keyboard layout from the default to something different.







Randomization Strategies

Randomization Strategies

We propose five representative strategies spanning from purely-random to partially-random keypad layouts.

The latter preserves some characteristics of the default layout, to achieve a favorable security-usability trade-off.

For stronger security, keypad randomization can be performed either at the beginning of every keystroke or at the beginning of each typing session.

Randomization Strategies - Sequence Randomization

(a) (b) (c)

Figure 1: Examples of (a) Row Randomization (RR), (b) Column Randomization (CR), and (c) Individual Key Randomization (IKR)

Randomization Strategies - Size and Location Randomization

(a) (b) (c)

Figure 2: Examples of (a) Key Size Randomization (KSR) and (b) Key Location Randomization (KLR), and (c) The hidden 7×6 grid layout used in KSR and KLR.

Security Analysis of the Randomization Strategies

Table 1: Security assurance of the five proposed randomization strategies. Lower rank is better security.

Randomization Strategy	Correct Entire Keypad Guessing Probability	Security Assurance Rank
IKR	$\frac{1}{12!} = 2.08 \times 10^{-9}$	1
RR	$\frac{1}{4!} = 0.04167$	2
KLR	$\frac{1}{16} = 0.0625$	3
KSR	$\frac{1}{12} = 0.08333$	4
CR	$\frac{1}{3!} = 0.16667$	5

Human Factors

Design Principles Against Side-Channel Attacks

Cai et al. [5] pointed out the following desirable properties in any defense solution:

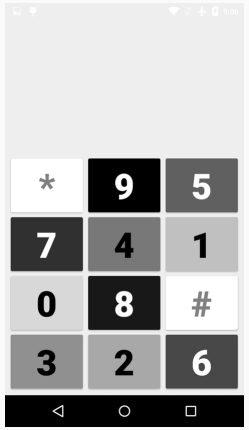
- **Security:** solution must protect against side-channel attacks,
- **Usability:** ideally, solution should require no extra effort from users and if extra effort is unavoidable, it should not disrupt the users' work flow,
- **Backward and Forward Compatibility:** no or minimal modification to existing applications and operating systems,
- **Performance:** no or minimal overhead, and
- **Versatility:** should be deployable on various types of mobile hardware, software, and user interfaces.

Evaluation Goals

Time required for completing a typing task and the number of errors made during the task, while using RandomPad.

User-provided subjective workload and usability measures using NASA-TLX [10] and SUS [3].

Effect of additional visual cues in form of contrasting shades of gray [13][30] to represent each of the keys.



Study

Study - Participants

Table 2: Demographics and preferences of 100 participants.

Gender	56% Female 44% Male
Occupation	33% Employed 67% Student
Smartphone Ownership Duration	26% Less than 5 Years 74% More than 5 Years
Current Smartphone	59% iOS (iPhone) 41% Android
Willingness to Use Random Keypad (Before Study)	22% In Favor 78% Not in Favor

Study - Task

Dictated Typing

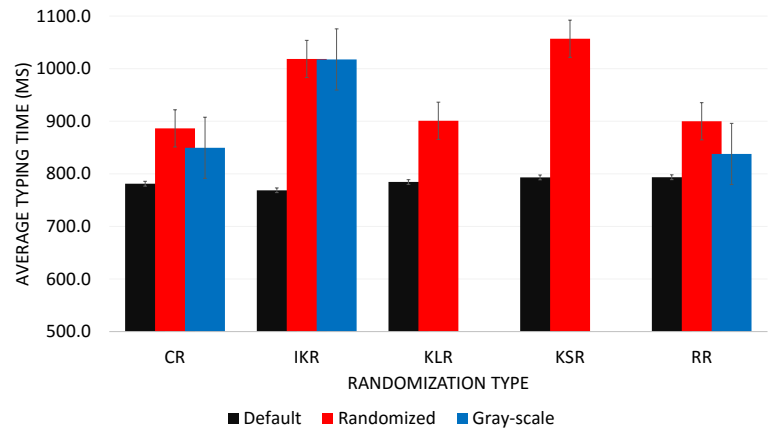
- Visually and acoustically dictated sequences of pseudo-random single digit numbers.
- Repeated for default, randomized and gray-scale keypads.

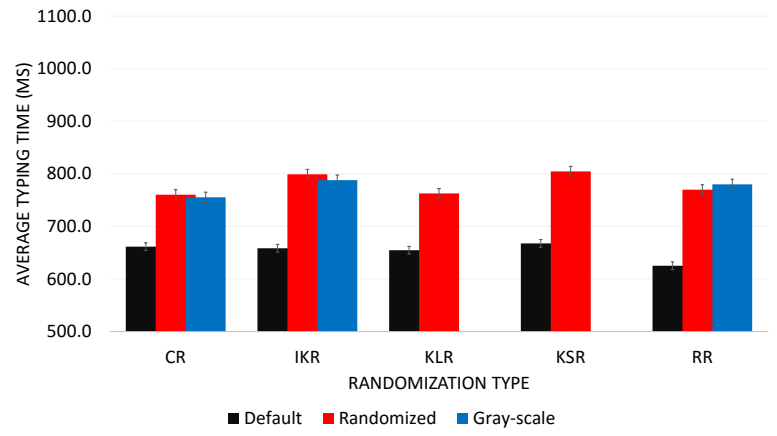
Natural Typing

- Participants were instructed to type information already known to them such as zip code (5 digits), phone number without area code (7 digits), birth date (8 digits), etc.
- Repeated for default, randomized and gray-scale keypads.

Evaluation

Results - Typing Speed

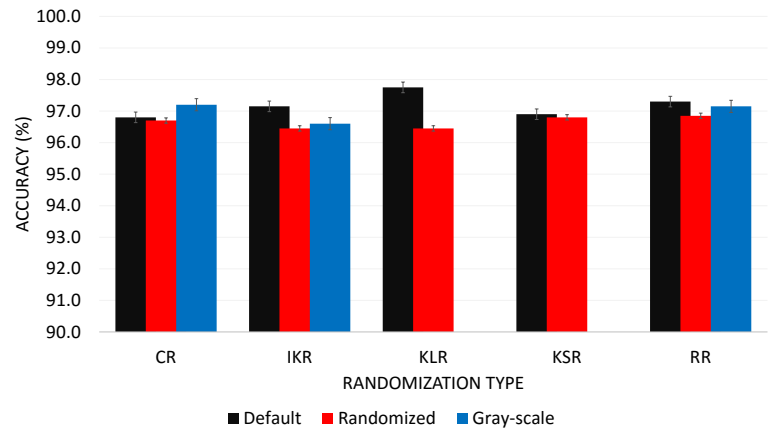


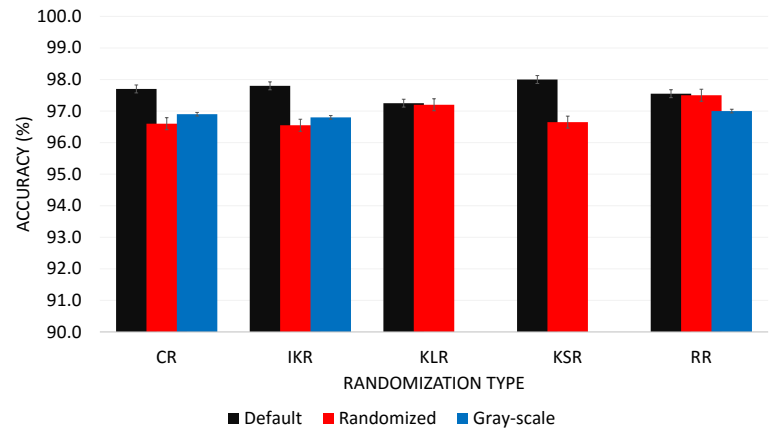


Randomized keypads do increase task completion times, by approximately 21% for dictated and 16% for natural typing.

$$CR < KLR < RR < IKR < KSR$$

Results - Typing Accuracy





It may be concluded that the task completion time was traded-off for higher accuracy by the participants.

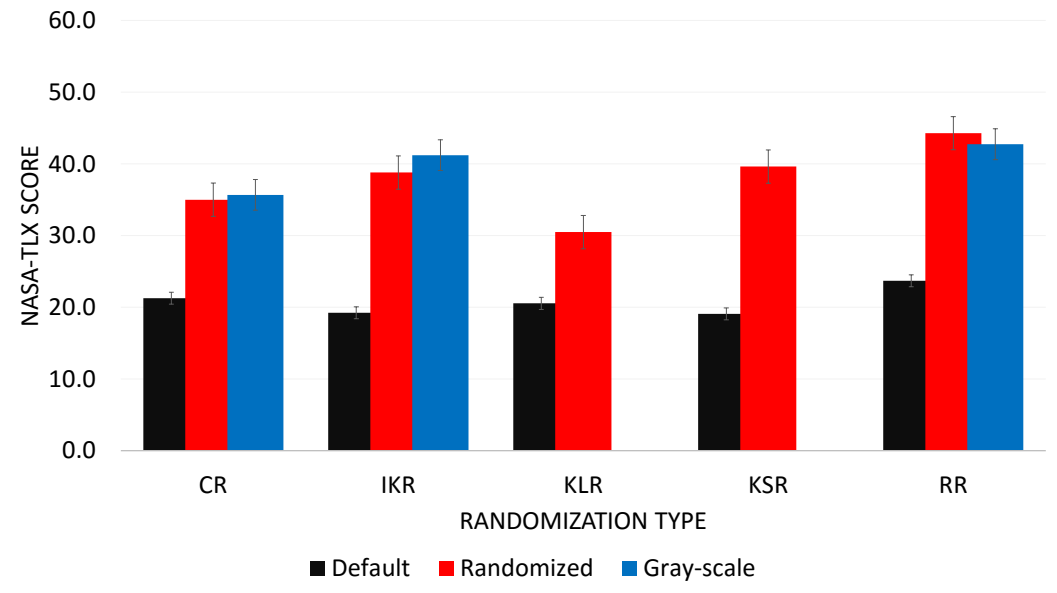
Results - Learning Curve

In order to analyze if the typing performance (speed and accuracy) improves with more usage of the randomized keypad, we compare the average per key typing time for the first and last ten numbers typed with RandomPad, in the natural typing session.

The overall mean drop in per key typing time is recorded as -163.09 ms, with $p < 0.001$.

However, we did not observe any significant improvement in accuracy.

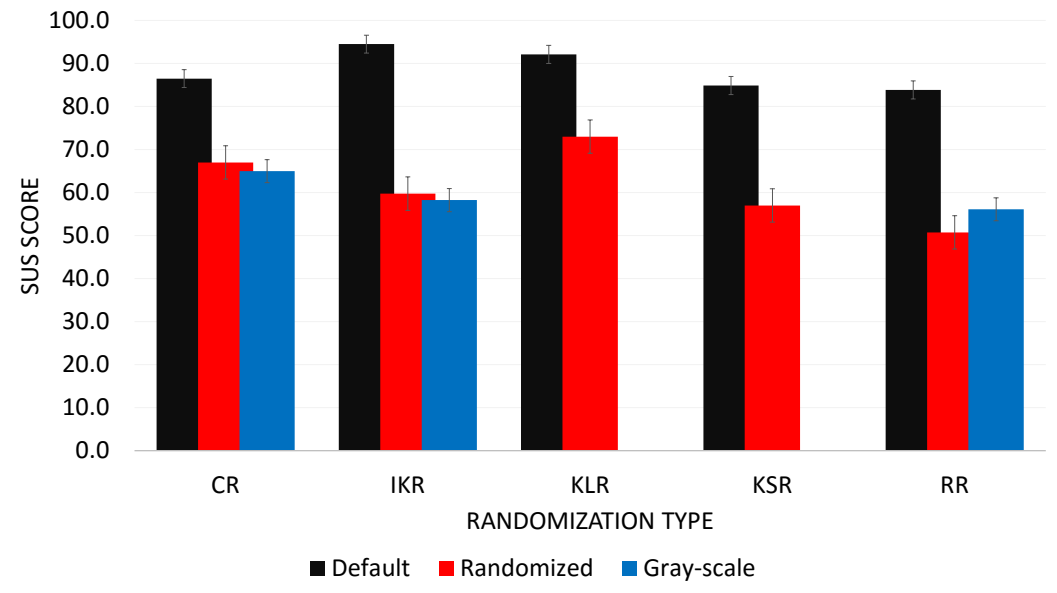
Results - Perceived Workload



KLR is reported to take the least effort compared to the other four randomization strategies on the NASA-TLX.

$$KLR < CR < IKR < KSR < RR$$

Results - Perceived Usability



KLR is again reported to be the most usable compared to the other four randomization strategies on the SUS.

$$KLR > CR > IKR > KSR > RR$$

Results - Gray-Scale

On the NASA-TLX and SUS scores, there are no significant differences between the randomized keypads without gray-scale shading versus randomized keypads with gray-scale shading

Thus, contrasting gray-scale shades on the keypad does not lower the perceived workload or improve the perceived usability of RandomPad.

However, gray-scale keypads could be potentially improved by adjusting and optimizing this contrast between the different shades [34].

Results - Are Users Going to Use it?

In the initial pre-survey recorded before the participants were introduced to side-channel keystroke inference attacks, only 22% of the participants reported that they would be willing to use a randomized version of the keypad.

After completing the experimental trials, as many as 80% of the participants reported in the post-survey that they would be willing to use a randomized keypad in order to protect their privacy.

Discussions and Conclusion

Privacy-Usability Trade-Off 1/2

Table 3: Usability rankings of the five randomization strategies calculated using average typing speed, workload (lower better) and perceived usability (higher better). Lower least rank is better usability.

Randomization Strategy	Typing Speed Rank	Workload Rank	Perceived Usability Rank	Summed Usability Rank (Least Rank)
KLR	2	1	1	4 (1)
CR	1	2	2	5 (2)
IKR	4	3	3	10 (3)
KSR	5	4	4	13 (4)
RR	3	5	5	13 (4)

Privacy-Usability Trade-Off 2/2

Comparing Table 1 (Security Analysis) and 3 (Usability Analysis), we see that KLR ranks relatively highest on both ($3 + 1 = 4$) tied with IKR ($1 + 3 = 4$), followed by RR ($2 + 4 = 6$), CR ($5 + 2 = 7$), and KSR ($4 + 4 = 8$), respectively.

In other words, KLR and IKR provides the best balance between security and usability, while KSR provides the least.

Future Work

Prevent visual channel attacks using randomized augmented reality keyboards (PerCom'17 Workshop).

Publicly available RandomPad plug-in for Android smartphones.

Conclusion

We proposed the use of randomized keypads for typing sensitive information on mobile device keypads.

Increased task completion time. Perceived to be less usable and more work.

However, the learning curve associated with randomized keypads can improve user performance and usability with prolonged use.

Interestingly, even with the degraded usability of randomized keypads, participants were willing to use it for improved privacy.

Appendix

Challenges in Protection Against Side-Channel Attacks

Zero-permission sensors. Adding all-sensor access control imposes high security-usability trade-off. Also, requires significant OS and app modifications.

Biometric sensors (which require specialized hardware), works only for authentication.

No universal defense mechanism against off-device inference attacks.

Protection by Randomization

ScrambleKeypad [26] for electronic door access control systems.

Limited flexibility in terms of available set of randomization strategies. Fixed security-usability trade-off.

We propose, implement, and comprehensively evaluate different randomized keypads (or *RandomPad*) for mobile devices.

How to Protect Smartphone Keystroke Privacy? 2/2

Two new challenges:

- Users may be uncomfortable typing on a keypad different from the one they are habituated to, and
- As the keypad changes randomly, users will always face an unfamiliar keypad.

Our Research: We comprehensively assess the *usability* and *perceived workload* of typing on keypads generated by different randomization strategies with the help of actual typing experiments involving a diverse set of 100 human subjects.