POSTER: TinPal- An Enhanced Interface for Pattern Locks

Title – TinPal: An Enhanced Interface for Pattern Locks
Authors – Harshal Tupsamudre, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Lodha
Affiliation – TCS Research, Pune, India
Venue – To appear in Workshop on Usable Security (USEC 2018), co-located with NDSS 2018, San Diego, California
Date – 18 February 2018
Link/Doi – To appear in USEC 2018 (Submission Number 21)

Harshal Tupsamudre, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Lodha. TinPal: An Enhanced Interface for Pattern Locks. To appear in Workshop on Usable Security (USEC 2018). Internet Society, San Diego, California, Feb 18, 2018.

Abstract-
Pattern lock scheme in which users connect 4-9 dots in a 3X3 grid is one of the most popular authentication methods on mobile devices. However, numerous research studies show that users choose patterns from a small space which makes them vulnerable to a variety of attacks such as guessing attacks, shoulder-surfing attacks and smudge attacks.
In this work, we enhance the existing 3X3 interface with a visual indicator mechanism and demonstrate how this slight modification can influence users' pattern choices, thereby improving the security of the pattern lock scheme. We refer to this enhanced interface as TinPal. As users draw their pattern, TinPal highlights the next set of unconnected dots that can be reached from the currently connected dot. We gauge the impact of this highlighting mechanism on users' pattern choices by performing a comparative study of two groups, where one group creates pattern using the existing interface while the other group creates pattern using TinPal. The study results show that participants who used the TinPal interface created more secure patterns than participants who used the existing interface.

TinPal: An Enhanced Interface for Pattern Locks

Harshal Tupsamudre, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Lodha

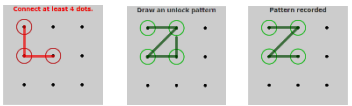
TCS Research, Pune (India)

Contact: harshal.tupsamudre@tcs.com, +91 20 6608 6435

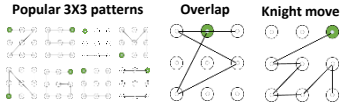
Problem

> **User-selected 3X3 patterns are simple and drawn from a very small space.**

- Pattern Lock Scheme is one of the most popular authentication schemes on mobile devices.
- The rules for creating 3X3 patterns are as follows:
  - Rule 1. At least 4 dots must be chosen
  - Rule 2. No dot can be used twice
  - Rule 3. Only straight lines are allowed
  - Rule 4. Do not jump over dots not visited before
- The total number of possible 3X3 patterns is 389,112.

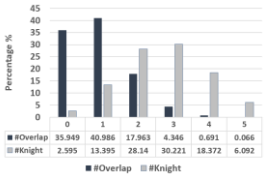


Rules 1,2 and 3 are enforced by existing 3X3 interface. However, this interface does not have any mechanism to inform users about Rule 4.



- Research shows that patterns resembling English letters are very prevalent among users.
- Further, visual features such as overlaps and knight moves which resist shoulder-surfing are rarely used.
- We attribute these insecure behavior to the existing interface which does not inform users about Rule 4.
- The fourth rule, for instance implies that one can connect 1->3 if dot 2 is already connected.
- We conjecture that many users are simply not aware of all possible connection options and hence resort to insecure pattern choices.

Theoretical distribution of overlaps and knight moves in 3X3 patterns

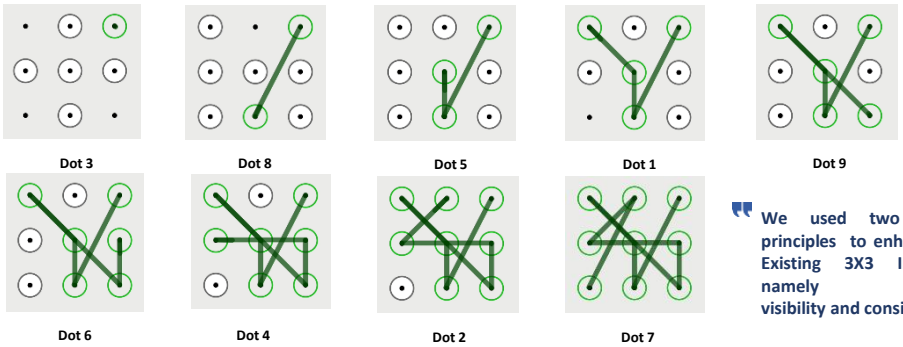


If overlaps are never used in patterns then the theoretical space is reduced from 389,112 to just 139,880 (~1/3rd).

Idea: Highlight dots

> **To help users choose complex patterns, we enhance the existing 3X3 interface with a visual indicator mechanism.**

- As users draw their pattern, the enhanced 3X3 interface highlights the next set of dots that can be reached from the currently connected dot.
- This enhanced interface doesn't force or persuade users to connect any particular dot.
- It simply informs them about the set of choices available to them from the currently connected dot.
- The highlighting of dots happens in real-time during pattern creation as well as during recall.



A step-by-step illustration of creation of pattern 385196427 on the enhanced 3X3 interface.

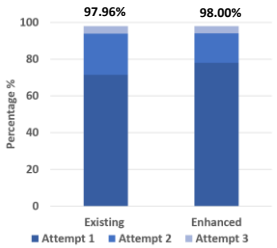
> **We used two design principles to enhance the Existing 3X3 Interface, namely visibility and consistency.**

Usability

Participant demographics

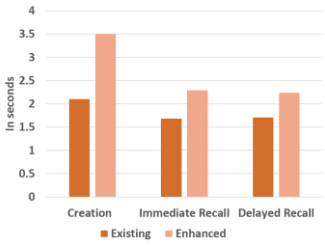
Variable	Values	Existing	Enhanced
Gender	Male	51.02%	56.00%
	Female	48.98%	44.00%
Age Group	20-25	67.35%	80.00%
	>25	32.65%	20.00%
Background	CS/IT	59.18%	54.00%
	Other	40.82%	46.00%
Handedness	Left	4.08%	2.00%
	Right	95.92%	98.00%
Mobile OS	Android	95.92%	92.00%
	Other	4.08%	8.00%
Screen Lock	Pattern	59.18%	58.00%
	PIN	30.61%	38.00%
	Fingerprint	38.78%	42.00%
#Participants		99	49	50

Recall attempts of patterns



Average attempts Existing : 1.31
Average attempts Enhanced : 1.25

Creation and recall time of patterns



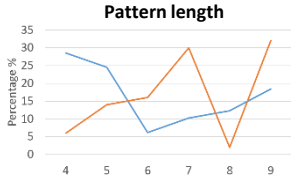
Average creation time Existing: 2.10s
Average creation time Enhanced: 3.50s

Variable	Existing	Enhanced
Stroke Length	6.08	8.39
Immediate Recall	1.68s	2.29s
Normalized (IR)	0.28s	0.27s
Delayed Recall	1.71	2.24
Normalized (DR)	0.28s	0.27s

> **Memorability and efficiency results show that the usability of the Enhanced Interface is comparable to the Existing Interface.**

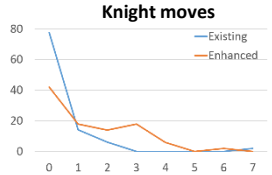
Security

Pattern length



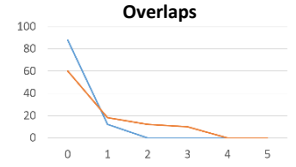
Average pattern length Existing: 6.08
Average pattern length Enhanced: 7.04

Knight moves



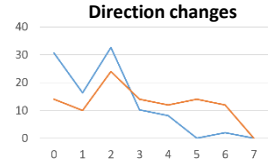
Average knight moves Existing: 0.41
Average knight moves Enhanced: 1.36

Overlaps



Average overlaps Existing: 0.12
Average overlaps Enhanced: 0.72

Direction changes

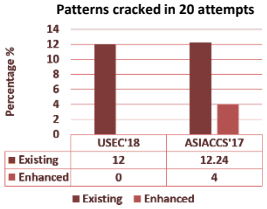


Average direction changes Existing: 1.57
Average direction changes Enhanced: 2.9

Pattern cracking results

- We measure the guessing resistance of patterns using n-gram Markov model.
- We train Markov models on two data sets, one collected in our present study USEC'18 and the other from our ASIACCS'17 paper (69,797 patterns).

Patterns cracked in 20 attempts



> **Pattern characteristics and cracking results show that patterns created on Enhanced Interface are more secure.**

References

- Helen Sharp et al. Interaction Design: Beyond Human-Computer Interaction. In 2011.
- Sebastian Uellenbeck et al. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In CCS '13.
- Panagiotis Andriotis et al. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In WiSec '13.
- Youngbae Song et al. On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks. In CHI '15.
- Adam J. Aviv et al. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In ACSAC'15.
- Marte Loge et al. On User Choice for Android Unlock Patterns. In EuroUSEC'16.
- Harshal Tupsamudre et al. Pass-O: A Proposal to Improve the Security of Pattern Unlock Scheme. In ASIACCS '17.
- Geumhwan Cho et al. SysPal: System-Guided Pattern Locks for Android. In SP'17.