

Is Bigger Better?

*Comparing User-Generated
Passwords on 3x3 vs. 4x4 Grids Sizes
for Android's Pattern Unlock*

Adam J. Aviv



Devon Budzitowski



Ravi Kuber



Android's Pattern Unlock



Android pattern unlock is an authentication method to lock (and unlock) Android phones

Rules of the Game

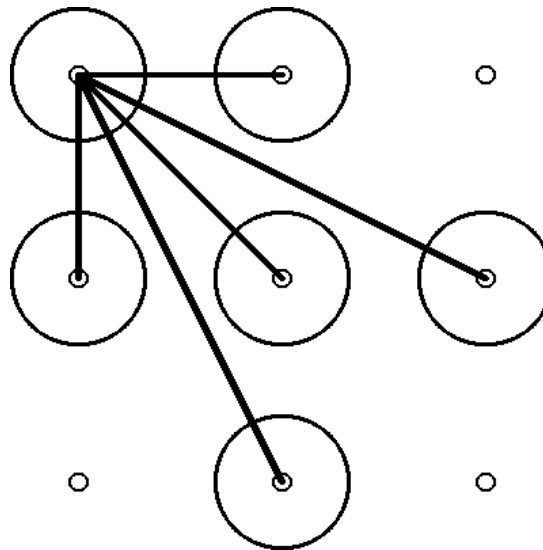
(1)

Maintain contact with the screen and connect 4 points without repetition



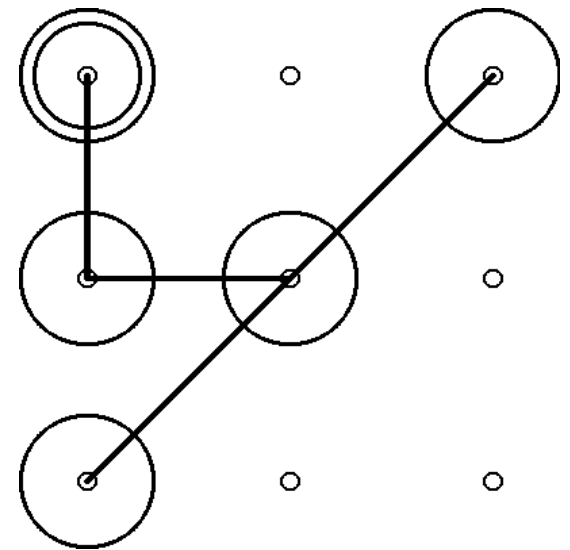
(2)

Can only connect adjacent contact points



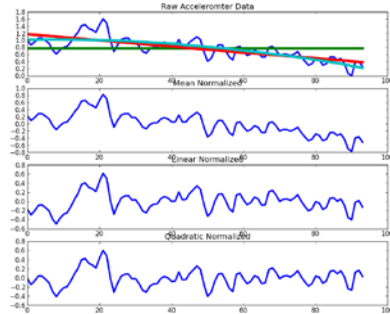
(3)

Can trace over previously contacted points



Recent Work on Android Unlock Patterns

Attacks



[_GMBS:WOOT'10] [_SMS:ACASC'12]

Measurement

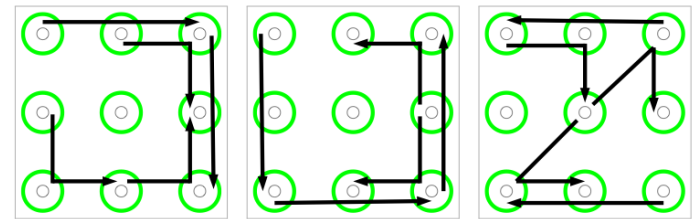
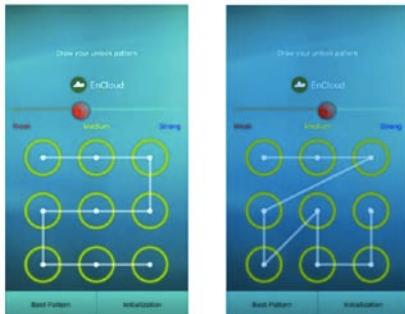


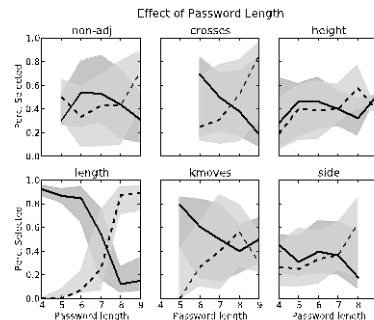
Figure 8: The most frequent 3-grams, from most frequent (left) to less frequent (right).

Meters

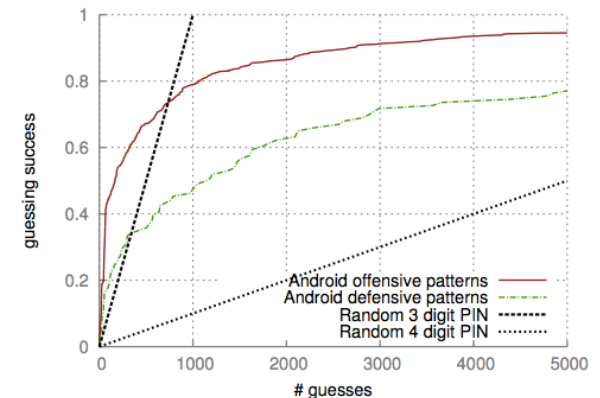


[SCOKH:CHI'15]

Perceptions



[_D:ACASC'14]



[UDWH:CCS'13]

How strong are patterns?

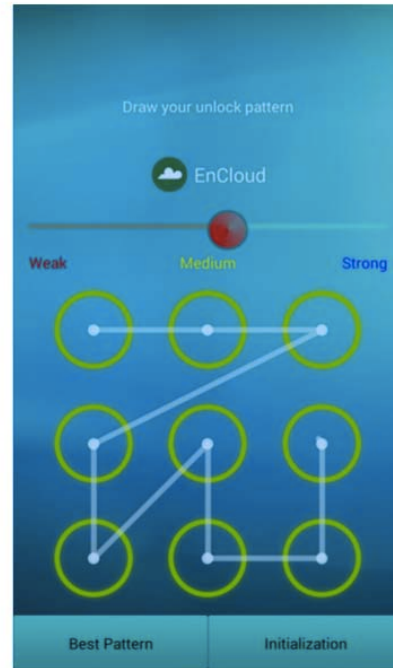
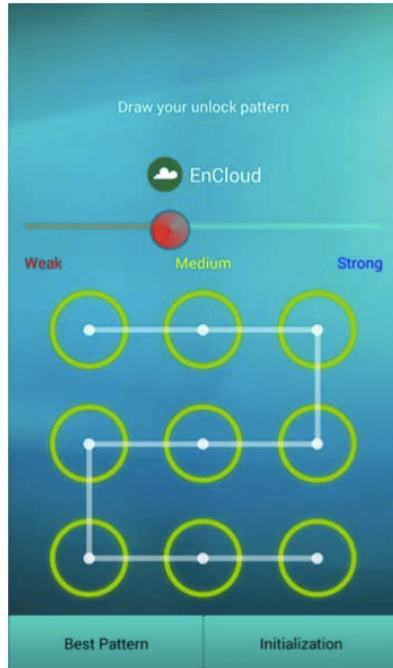
- There are 389,112 total 3x3 patterns
 - Users do not select uniformly from the set of total available patterns

“ *Consequently, **the entropy of patterns is rather low**, and our results indicate that the security offered by the scheme **is less than the security of only three digit randomly-assigned PINs** for guessing 20% of all passwords (i. e., we estimate a partial guessing entropy $G_{0.2}$ of 9.10 bit).* ”

Uellenbeck et. al at CCS'13

How to increase the security?

Password Meters?

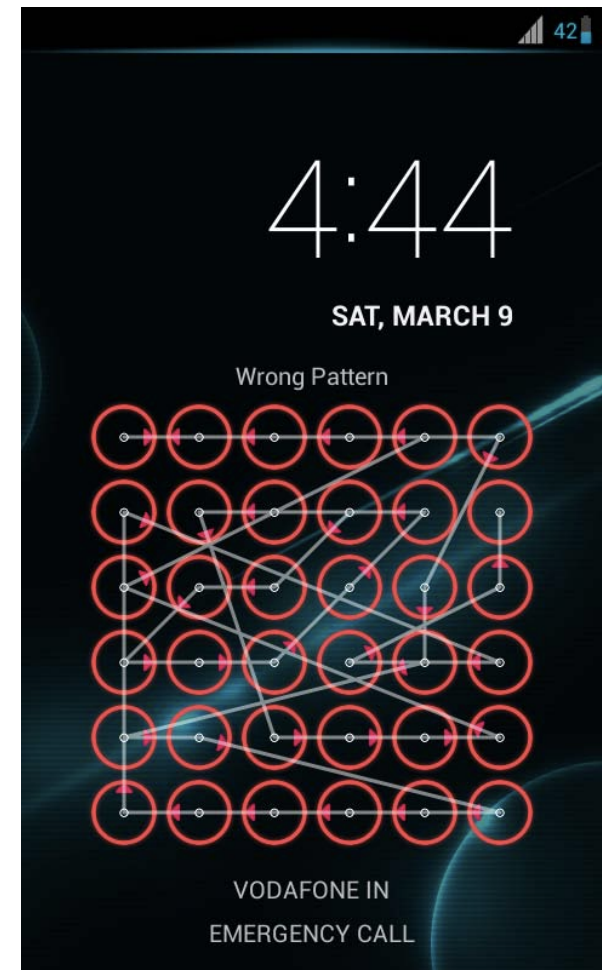
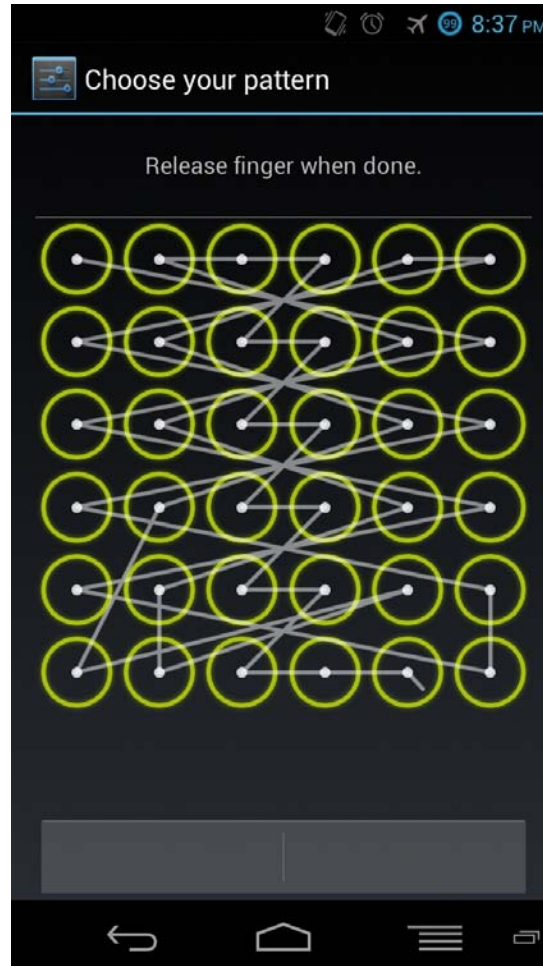
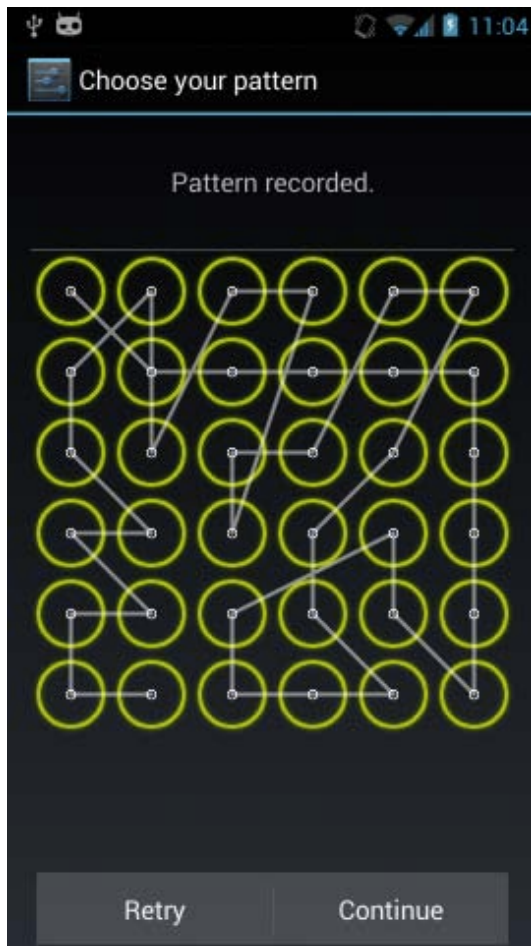


[SCOKH:CHI'15]

[SWZ:JISA'15]

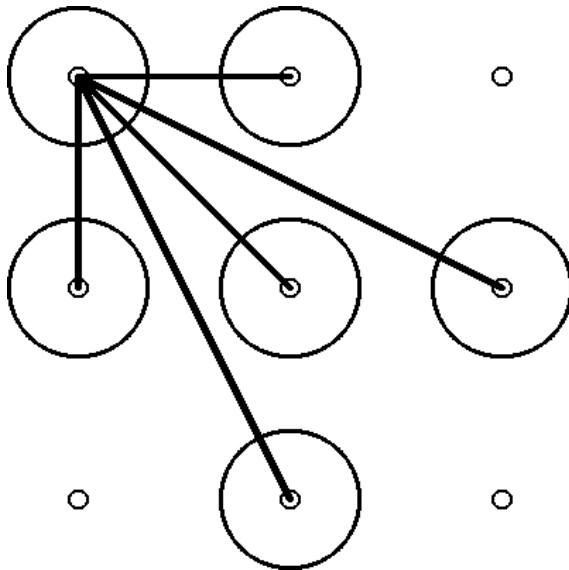
Increasing the Grid Size

Cyanogen Mod

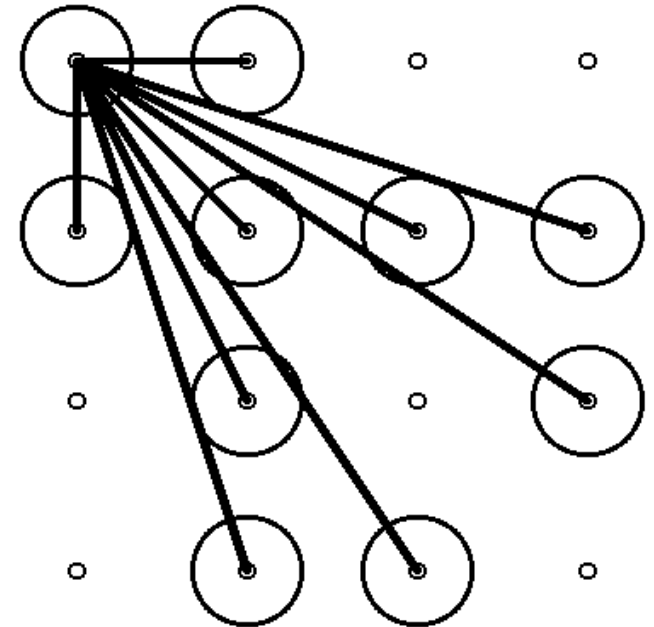


Research Question

Does increasing the grid size increase the security of human generated patterns?



3x3 vs. 4x4



389,112

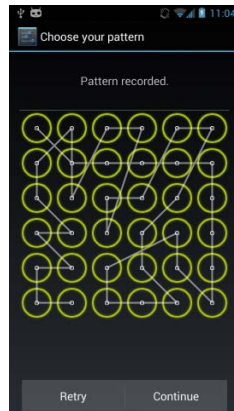
possible patterns

4,350,069,823,024

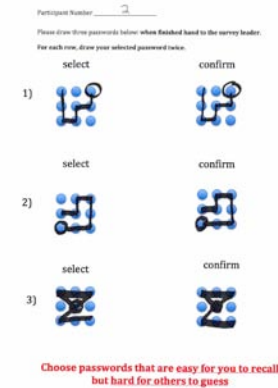
possible patterns

Talk Outline

Motivation



Methodology



Data Analysis

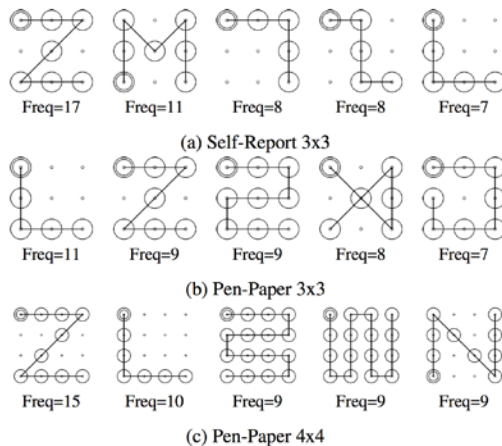


Figure 6: Top 5 Most Frequently Occurring Patterns

Security Analysis

	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.5$	Perc. Guessed Total	Perc. Guessed with 20 attempts
Self-Reported 3x3	6.62	6.95	9.49	95.9%	15.0%
Pen-Paper 3x3 (all)	6.59	6.99	8.93	97.2%	16.7%
Pen-Paper 3x3 (Off.)	6.98	7.69	9.31	95.3%	12.5%
Pen-Paper 3x3 (Def.)	9.43	9.79	10.98	90.2%	4.0%
Pen-Paper 4x4 (all)	6.23	6.64	11.61	66.7%	19.9%
Pen-Paper 4x4 (Off.)	6.46	7.57	10.40	67.7%	16.7%
Pen-Paper 4x4 (Def.)	6.23	6.64	11.61	37.4%	3.2%
Uellenbeck et. al 3x3 (Off.) [23]	7.56	7.74	8.19		
Uellenbeck et. al 3x3 (Def.) [23]	8.72	9.10	10.90		
Song et. al 3x3 (w/ Meter) [18]	8.96	10.33	12.29		
Song et. al 3x3 (w/o Meter) [18]	7.38	9.56	10.83		
Random 3x3 Pattern ($U_{389,112}$)	18.57	18.57	18.57		
Random 4x4 Pattern ($U_{4,350,069,825,024}$)	41.98	41.98	41.98		
Random 6-dit PIN ($U_{1,000,000}$)	19.93	19.93	19.93		
Random 5-dit PIN ($U_{100,000}$)	16.60	16.60	16.60		
Random 4-dit PIN ($U_{10,000}$)	13.29	13.29	13.29		
Random 3-dit PIN ($U_{1,000}$)	9.97	9.97	9.97		
Random 2-dit PIN (U_{100})	6.64	6.64	6.64		
Real Users' 4-Digit PINs [18, 15]	5.19	7.04	10.08		

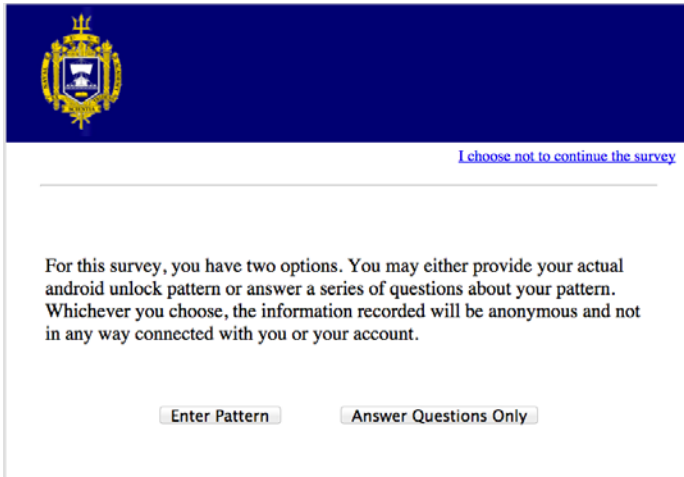
Table 3: Partial Guessing Entropy Comparisons

METHODOLOGY

Methodology Challenges

No good datasets of 3x3 graphical passwords

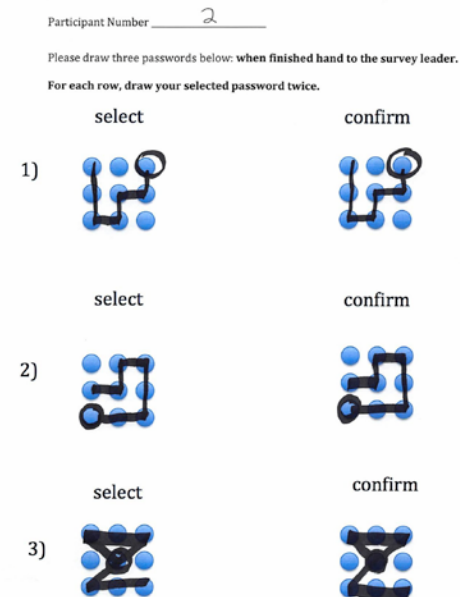
How to collect real 3x3 patterns?



The screenshot shows a survey interface with a blue header containing a crest. Below the header, there is a link that says "I choose not to continue the survey". The main text reads: "For this survey, you have two options. You may either provide your actual android unlock pattern or answer a series of questions about your pattern. Whichever you choose, the information recorded will be anonymous and not in any way connected with you or your account." At the bottom, there are two buttons: "Enter Pattern" and "Answer Questions Only".

4x4 patterns are not widely used

How to collect realistic 4x4 patterns?



The screenshot shows a survey interface for collecting 4x4 graphical passwords. It includes a "Participant Number" field with the number "2" entered. Below this, it says "Please draw three passwords below: when finished hand to the survey leader. For each row, draw your selected password twice." There are three rows, each with a "select" and a "confirm" column. Each row shows a 4x4 grid of dots with a pattern drawn through them. The patterns are: 1) a path starting at (1,1), going down to (4,1), then right to (4,2), then up to (3,2), then right to (3,3), then down to (4,3), then left to (4,4), then up to (3,4), then left to (2,4), then up to (2,3), then left to (2,2), then up to (1,2), then left to (1,1). 2) a path starting at (1,1), going down to (4,1), then right to (4,2), then up to (3,2), then right to (3,3), then down to (4,3), then left to (4,4), then up to (3,4), then left to (2,4), then up to (2,3), then left to (2,2), then up to (1,2), then left to (1,1). 3) a path starting at (1,1), going down to (4,1), then right to (4,2), then up to (3,2), then right to (3,3), then down to (4,3), then left to (4,4), then up to (3,4), then left to (2,4), then up to (2,3), then left to (2,2), then up to (1,2), then left to (1,1).

**Choose passwords that are easy for you to recall
but hard for others to guess**

All protocols were reviewed by the USNA and UMBC Institutional Review Board

Online Self-Report Survey

- *Pay people to self-report their pattern* or provide statistics about their pattern
- Amazon Mechanical Turk
 - Paid participants \$0.50 or \$0.75 (two runs)
 - 750 respondents data was included
- Must complete the survey on their mobile devices

Not for Everyone

Turk Opticom

**USNA Comp. Sci.
Research**
A2W8K2STMNJFHJ
[Averages »](#)
[HIT Group »](#)
[Review Requester »](#)

FAIR: NO DATA
FAST: NO DATA
PAY: NO DATA
COMM: NO DATA

Self-Reporting of Android Pattern Unlock --- requires an Android device 3/21/15

"You will be asked to (optionally) self-report what your Android unlock pattern is, or report statistics about your pattern. If you do not use the Android unlock pattern, please do not complete the HIT. This is an institution approved survey, and your participation is protected. You must complete the survey portion of this HIT on an Android device; however, you do not need to log onto Mturk on your Android device to submit work."

NO.

Mar 22 2015 |
[comments »](#)

| [flag](#) | [comment](#) | [flags,](#)

NO.

Procedure



[I choose not to continue the survey](#)

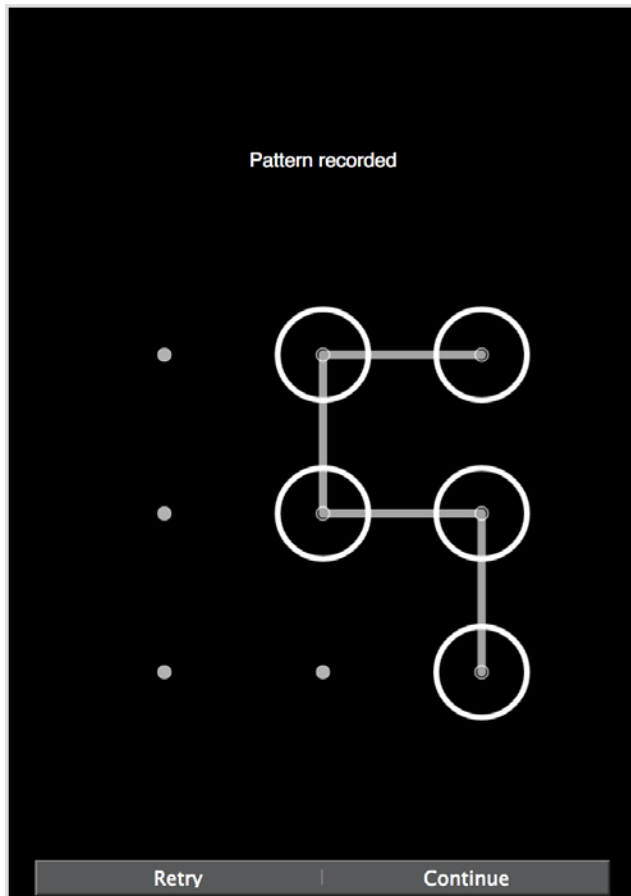
For this survey, you have two options. You may either provide your actual android unlock pattern or answer a series of questions about your pattern. Whichever you choose, the information recorded will be anonymous and not in any way connected with you or your account.

Enter Pattern

Answer Questions Only

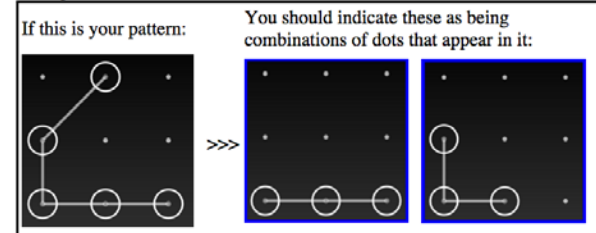
Report Pattern or Stats

Pattern Entry on Device

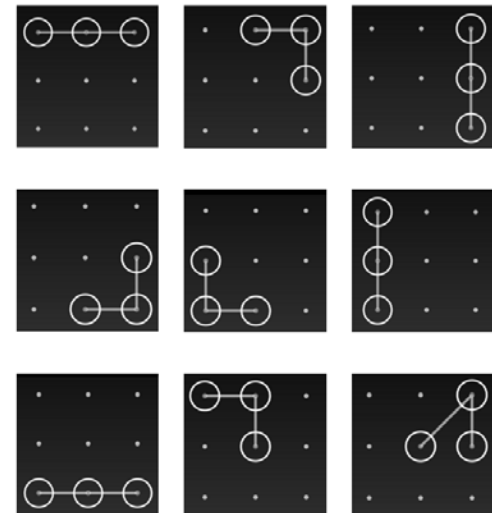


Select Features of Pattern

Example:



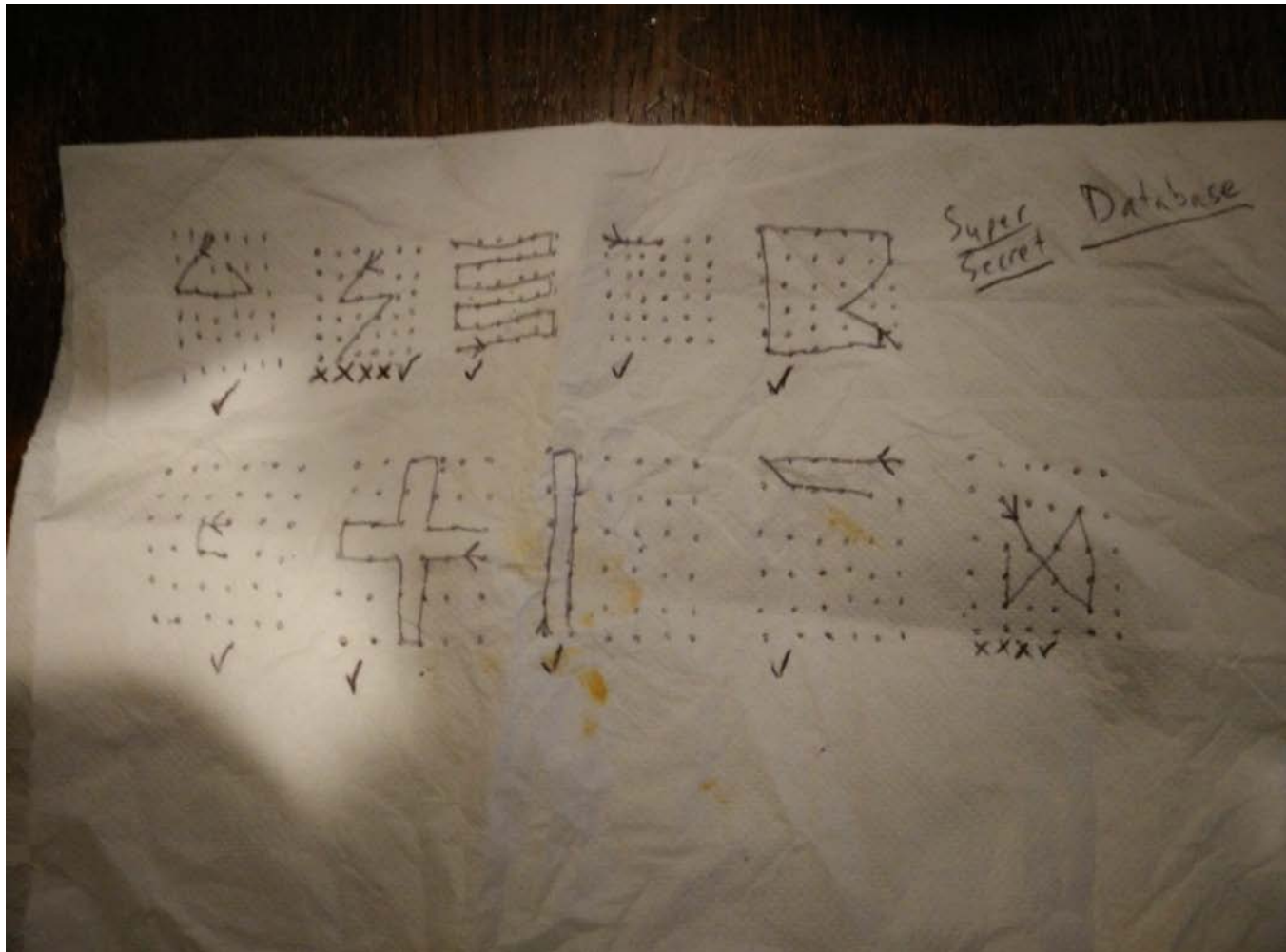
Select all that might apply:



Attention Tests

- Device Completion
 - Elaborate code/token system
 - Check user agents (*yes, I know that can be forged*)
- Must enter in results twice
 - Report pattern, then survey, then report again
 - If results don't match, throw data out
- Rejections
 - We do not reject people within Mturk
 - Just don't include their data

Pen and Paper Survey



Adversarial Model

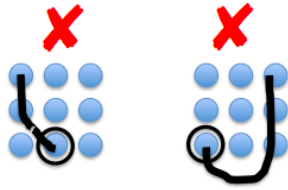
Participant Number _____

Directions: You will be required to select three graphical passwords of your own and also guess others passwords.

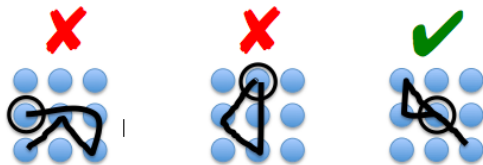
1. Passwords are selected by drawing connections between dots in the grid without lifting your pen from the paper, circling the initial dot. Like below.



2. Passwords must select at least 4 dots using straight lines, and you may not avoid unselected dots along a straight line between points.



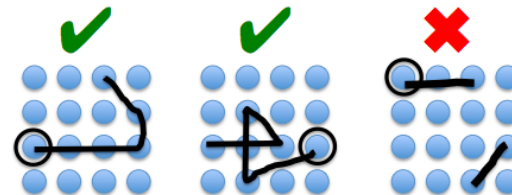
3. You may not select a dot more than once; however, you may cross over previously selected dots.



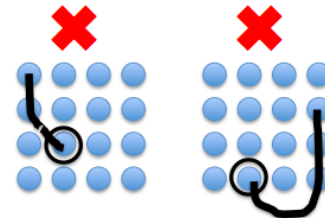
Participant Number _____

Directions: You will be required to select three graphical passwords of your own and also guess others passwords.

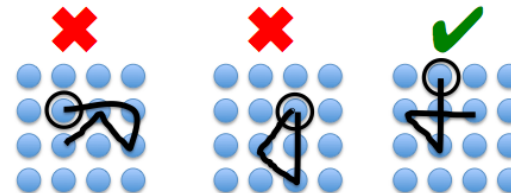
1. Passwords are selected by drawing connections between dots in the grid without lifting your pen from the paper, circling the initial dot. Like below.



2. Passwords must select at least 4 dots using straight lines, and you may not avoid unselected dots along a straight line between points.



3. You may not select a dot more than once; however, you may cross over previously selected dots.

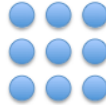
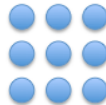


Defensive Selection

Participant Number _____

Please draw three passwords below: **when finished hand to the survey leader.**

For each row, draw your selected password twice.

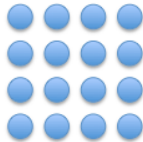
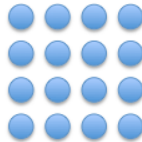
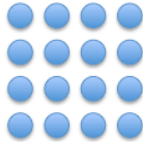
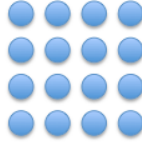
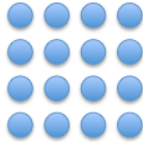
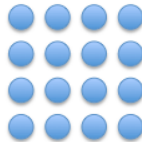
	<u>select</u>	<u>confirm</u>
1)		
2)		
3)		

**Choose passwords that are easy for you to recall
but hard for others to guess**

Participant Number _____

Please draw three passwords below: **when finished hand to the survey leader.**

For each row, draw your selected password twice.

	<u>select</u>	<u>confirm</u>
1)		
2)		
3)		

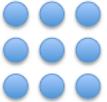
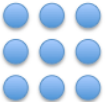
**Choose passwords that are easy for you to recall
but hard for others to guess**

Offensive Selection

Participant Number _____

Guess 10 passwords that you believe other participants might have selected. For each password you guess right, you will earn an additional treat.

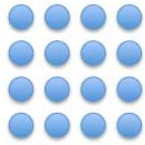
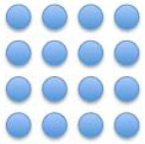
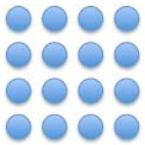
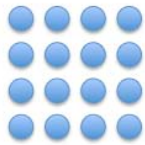
When finished hand to survey leader.

- 1)   (6
- 2)   (7
- 3)   (8
- 4)   (9
- 5)   (10

Participant Number _____

Guess 10 passwords that you believe other participants might have selected. For each password you guess right, you will earn an additional treat.

When finished hand to survey leader.

- 1)   (6
- 2)   (7
- 3)   (8
- 4)   (9
- 5)   (10

Recall

Participant Number _____

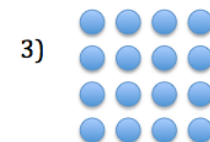
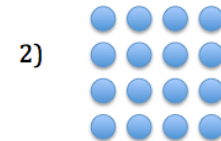
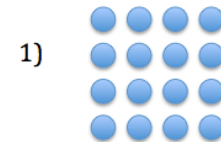
Please recall the three passwords you initial selected. For each password you can recall **that was not guessed** by another participant, you will earn an additional treat.



When finished, please hand to survey leader to tally the results.

Participant Number _____

Please recall the three passwords you initial selected. For each password you can recall **that was not guessed** by another participant, you will earn an additional treat.



When finished, please hand to survey leader to tally the results.

Sample Data

Participant Number 2

Please draw three passwords below: **when finished hand to the survey leader.**

For each row, draw your selected password twice.

select

confirm

1)



select

confirm

2)



select

confirm

3)

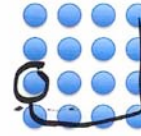


**Choose passwords that are easy for you to recall
but hard for others to guess**

Participant Number 20

Guess 10 passwords that you believe other participants might have selected. For each password you guess right, you will earn an additional treat.
When finished hand to survey leader.

1)



(6

2)



(7

3)



(8

4)



(9

5)



(10

Demographics and Collection

Self Report

- 750 Respondents
- 440 Self-Reported their password, remaining provided statistics
- 251 Males, 189 Females
- Age range: 18 – 55+
- Location: USA

Pen and Paper

- 80 Participants
 - 10 Focus Groups over 6 weeks
 - 8 to 20 members per group
- 494 3x3 Patterns
 - 380 offensive
 - 114 defensive
- 504 4x4 Patterns
 - 385 Offensive
 - 114 Defensive
- 48 males, 24 Females
- Age range: 18-40
- Location: @USNA and @UMBC

Limitations

- **Drawing patterns with Pen and Paper**
 - Comparison between 3x3 pen and paper and 3x3 self reported patterns
- **Veracity of Self Reported Data**
 - Similar features as other reported publications
 - Provide on their own mobile devices
 - Not required to report, can provide stats, which seem to match those that are reported
- **Cannot cross reference 4x4 patterns**
 - Comparison between 3x3 suggest consistency
- **Priming: Knowing that others will guess**
 - Trend patterns towards strong patterns for defensive
 - Have offensive and defensive in analysis
- **Entry Exhaustion: Entering too many patterns**
 - Entering too many patterns in a row can reduce creativity and result in less realistic patterns
 - Impact appears small when comparison between pen and paper and self reported

DATA ANALYSIS

Characterizing Data

- What are the most common patterns?
 - Symmetries and Embeddings
 - Common tri- and quad- grams
- Other Data Features
 - Length/stroke-length, start and end

Most Common Patterns

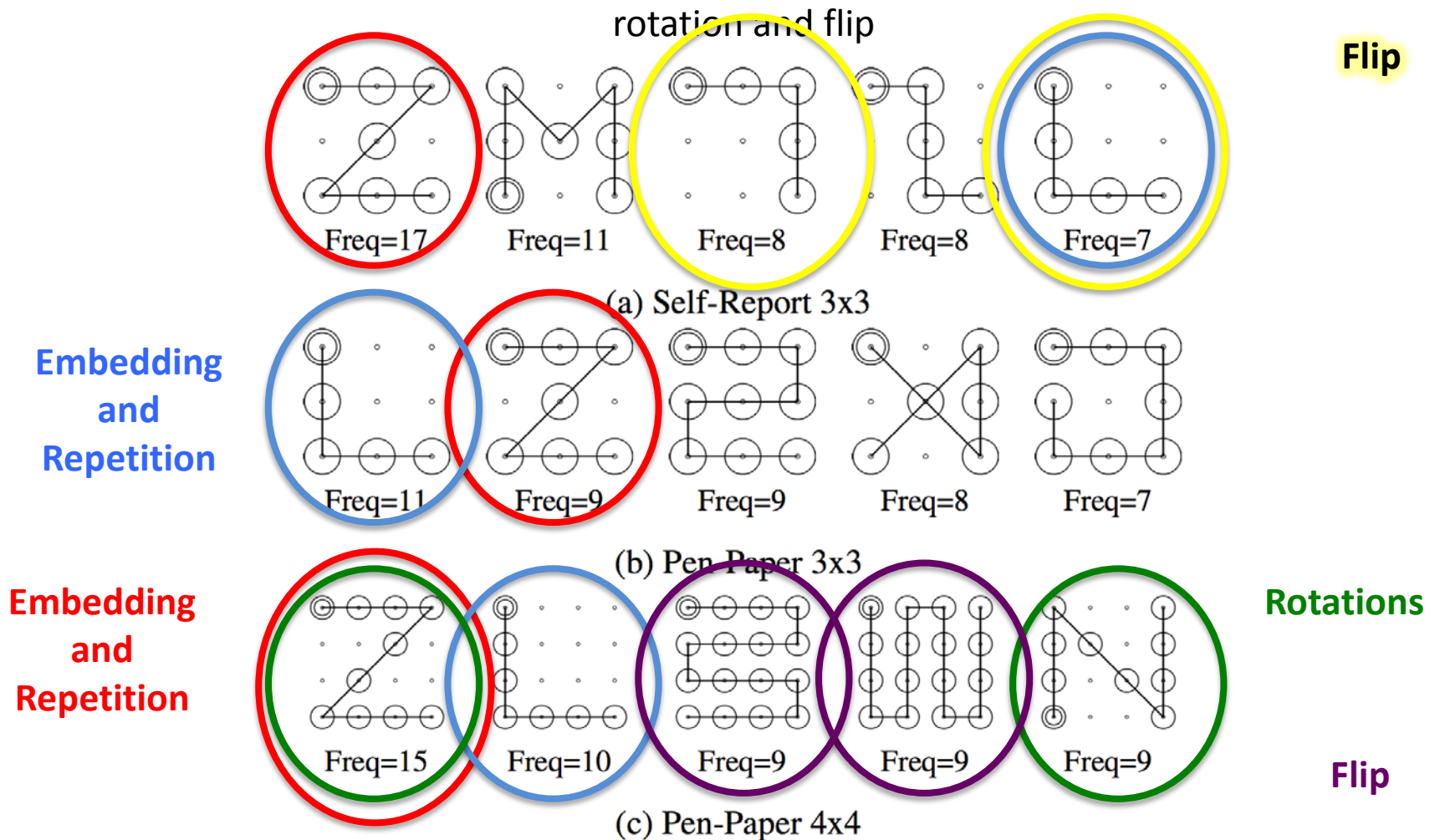


Figure 6: Top 5 Most Frequently Occurring Patterns

Symmetries and Embeddings

	Size	Repetitions	Symmetries	Embedding
Self-Report 3x3	440	203 (46.1%)	336 (76.36%)	n/a
Pen-Paper 3x3 (All)	491	245 (49.9%)	398 (81.1%)	n/a
Pen-Paper 3x3 (Off.)	378	187 (48.3%)	309 (79.8%)	n/a
Pen-Paper 3x3 (Def.)	113	16 (14%)	54 (47%)	n/a
Pen-Paper 4x4 (All)	501	179 (35.7%)	204 (40.7%)	166 (33.1%)
Pen-Paper 4x4 (Off.)	382	156 (40.8%)	177 (46.3%)	142 (37.1%)
Pen-Paper 4x4 (Def.)	119	10 (8.4%)	10 (8.4%)	24 (20.1%)

Symmetries: Two patterns that can be converted into the other through a series of flips or rotations

Embedding: A 3x3 pattern that can be drawn into a 4x4 space by the addition of a row or column

GOAL

*Use all this information to build a
guesser for patterns to measure the
security using guessability*

STRENGTH METRICS

Guessability

- *How many guesses does it take for an attacker to guess a given password?*
- **PARTIAL GUESSABILITY** (alpha-guesswork)
 - *How many guesses does it take to guess a fraction of the dataset?*
 - Measured in bits of information
- **Offline Attack:**
 - Assumes attack can crack passwords without having to engage the authentication method (e.g., cracking hashes)
 - No lockouts (traditionally, 20 guesses on Android)

Guessing Algorithm

- Input: Training Set, Guessing Set
- Train Likelihood Measure (Markov model)
 - Use training set and symmetries of training set with different weights
- Guess Order
 1. All patterns in training set order based on frequency with ties broken by likelihood measure
 2. All rotations/symmetries of training set ordered based on likelihood measure (added embeds of 3x3 patterns for 4x4 guessing)
 3. Set of generated patterns using the Markov Model ordered by likelihood measure

Experimental Design

- **Testing and Training**

- Trained on the pen-and-paper 3x3 and 4x4 data using a cross-fold validation
- Used 3x3 pen-and-paper as additional embedding training for the 4x4 data.
- Tested on self-reported 3x3 data using the pen and paper data as the training set.

- **Data Sets**

- Pen and Paper:
3x3,4x4, 3x3-off, 3x3-def, 4x4-off,4x4-def
- Self Reported: 3x3

Entropy

	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.5$	Perc. Guessed Total	Perc. Guessed with 20 attempts
Self-Reported 3x3	6.62	6.95	9.49	95.9%	15.0%
Pen-Paper 3x3 (all)	6.59	6.99	8.93	97.2%	16.7%
Pen-Paper 3x3 (Off.)	6.98	7.69	9.31	95.3%	12.5%
Pen-Paper 3x3 (Def.)	9.43	9.79	10.98	90.2%	4.0%
Pen-Paper 4x4 (all)	6.23	6.64	11.61	66.7%	19.9%
Pen-Paper 4x4 (Off.)	6.46	7.57	10.40	67.7%	16.7%
Pen-Paper 4x4 (Def.)	6.23	6.64	11.61	37.4%	3.2%
Uellenbeck et. al 3x3 (Off.) [23]	7.56	7.74	8.19		
Uellenbeck et. al 3x3 (Def.) [23]	8.72	9.10	10.90		
Song et. al 3x3 (w/ Meter) [18]	8.96	10.33	12.29		
Song et. al 3x3 (w/o Meter) [18]	7.38	9.56	10.83		
Random 3x3 Pattern ($U_{389,112}$)	18.57	18.57	18.57		
Random 4x4 Pattern ($U_{4,350,069,823,024}$)	41.98	41.98	41.98		
Random 6-dit PIN ($U_{1,000,000}$)	19.93	19.93	19.93		
Random 5-dit PIN ($U_{100,000}$)	16.60	16.60	16.60		
Random 4-dit PIN ($U_{10,000}$)	13.29	13.29	13.29		
Random 3-dit PIN ($U_{1,000}$)	9.97	9.97	9.97		
Random 2-dit PIN (U_{100})	6.64	6.64	6.64		
Real Users' 4-Digit PINs [18, 15]	5.19	7.04	10.08		

Table 3: Partial Guessing Entropy Comparisons

CONCLUSIONS

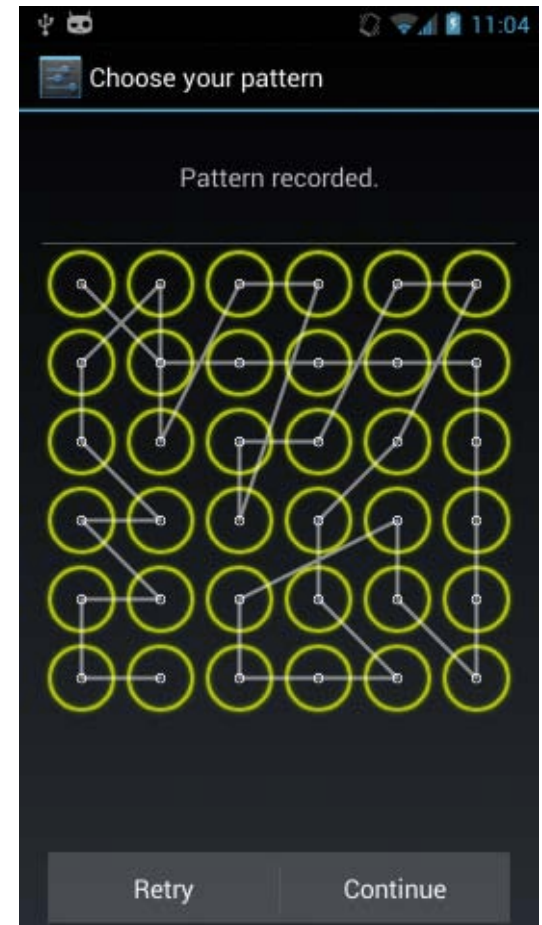
Conclusions:

Is 4x4 really better than 3x3?

- **NO:** The strength of *most* of the 4x4 patterns are similar to that of 3x3 patterns
- **YES:** The fraction of total guessed is less for 4x4 patterns
- **NO:** The fraction of most common 4x4 patterns are *more* guessable than the most common 3x3
- **YES:** User recall rates for 4x4 are the same for 3x3 but 4x4 patterns are less easily naïvely guessed

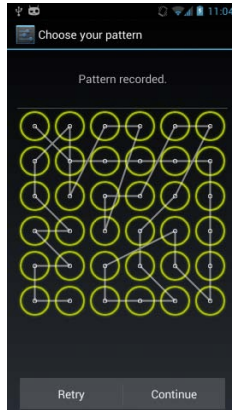
Would bigger grid sizes help?

- **Probably not**
 - More complex patterns become harder to enter and remember
 - May revert more common forms even more so than 4x4 patterns
- **Maybe yes**
 - Even less naively guessed more starting contact points
 - SO MANY MORE PATTERNS
- Open question: Future work.

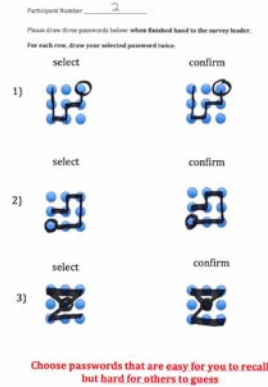


Summary

Motivation



Methodology



Data Analysis

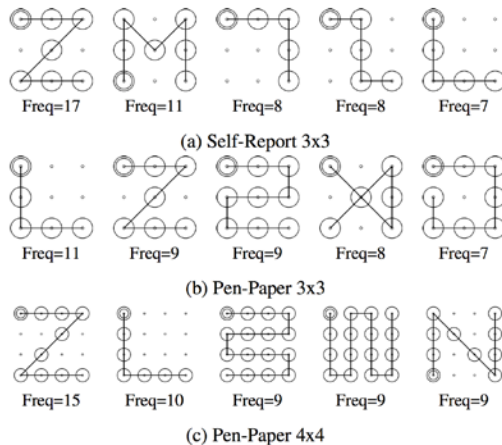


Figure 6: Top 5 Most Frequently Occurring Patterns

Security Analysis

	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.5$	Perc. Guessed Total	Perc. Guessed with 20 attempts
Self-Reported 3x3	6.62	6.95	9.49	95.9%	15.0%
Pen-Paper 3x3 (all)	6.59	6.99	8.93	97.2%	16.7%
Pen-Paper 3x3 (Off.)	6.98	7.69	9.31	95.3%	12.5%
Pen-Paper 3x3 (Def.)	9.43	9.79	10.98	90.2%	4.0%
Pen-Paper 4x4 (all)	6.23	6.64	11.61	66.7%	19.9%
Pen-Paper 4x4 (Off.)	6.46	7.57	10.40	67.7%	16.7%
Pen-Paper 4x4 (Def.)	6.23	6.64	11.61	37.4%	3.2%
Uellenbeck et. al 3x3 (Off.) [23]	7.56	7.74	8.19		
Uellenbeck et. al 3x3 (Def.) [23]	8.72	9.10	10.90		
Song et. al 3x3 (w/ Meter) [18]	8.96	10.33	12.29		
Song et. al 3x3 (w/o Meter) [18]	7.38	9.56	10.83		
Random 3x3 Pattern ($U_{389,112}$)	18.57	18.57	18.57		
Random 4x4 Pattern ($U_{4,350,069,825,024}$)	41.98	41.98	41.98		
Random 6-dit PIN ($U_{1,000,000}$)	19.93	19.93	19.93		
Random 5-dit PIN ($U_{100,000}$)	16.60	16.60	16.60		
Random 4-dit PIN ($U_{10,000}$)	13.29	13.29	13.29		
Random 3-dit PIN ($U_{1,000}$)	9.97	9.97	9.97		
Random 2-dit PIN (U_{100})	6.64	6.64	6.64		
Real Users' 4-Digit PINs [18, 15]	5.19	7.04	10.08		

Table 3: Partial Guessing Entropy Comparisons

Adam J. Aviv

Devon Budzitowski

Ravi Kuber

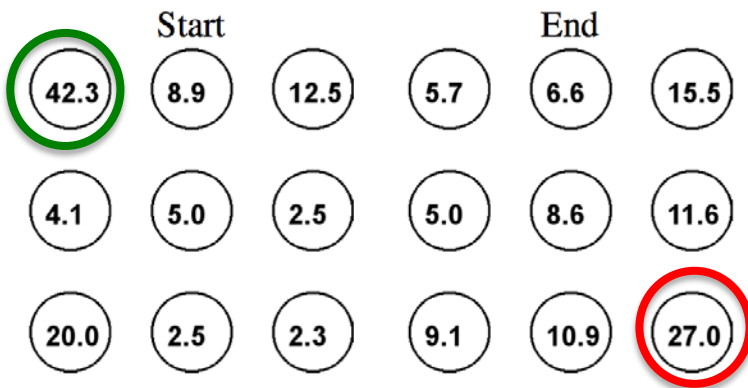


Is bigger better? Comparing User-Generated Passwords on 3x3 vs 4x4 Grid Sizes for Android's Pattern Unlock

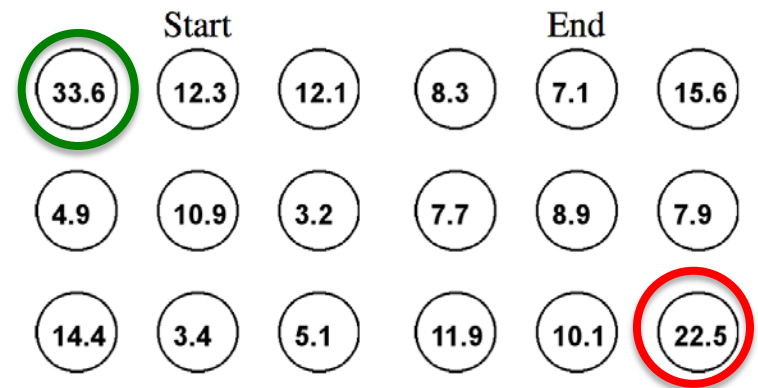
THANKS AND QUESTIONS?

BACKUP

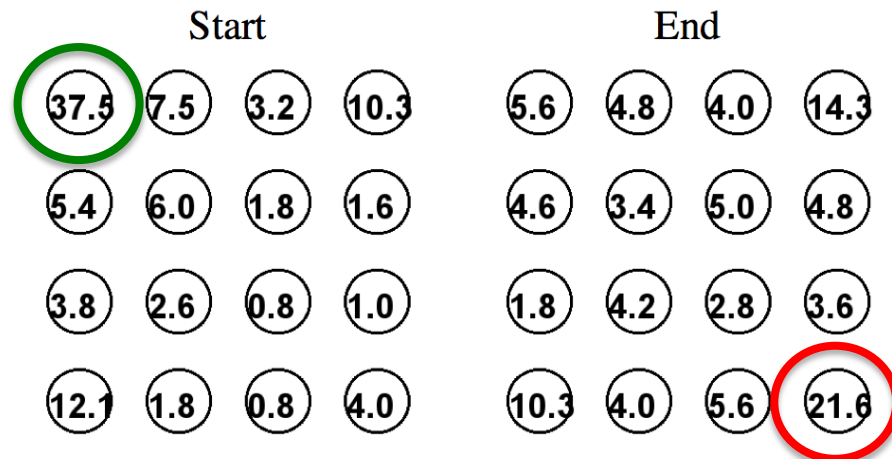
Start and End Conditions



(a) Self-Report 3x3

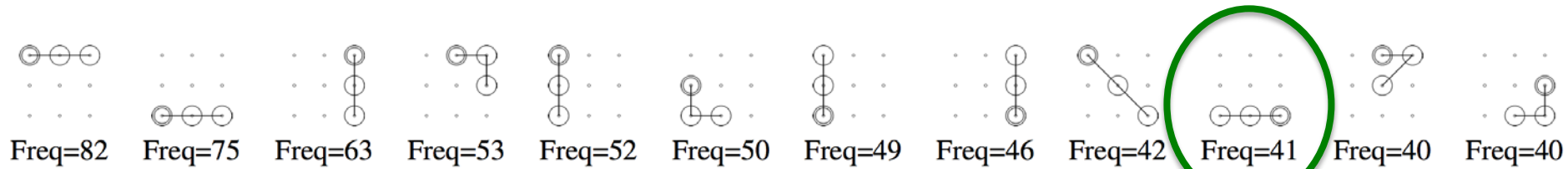


(b) Pen-Paper 3x3

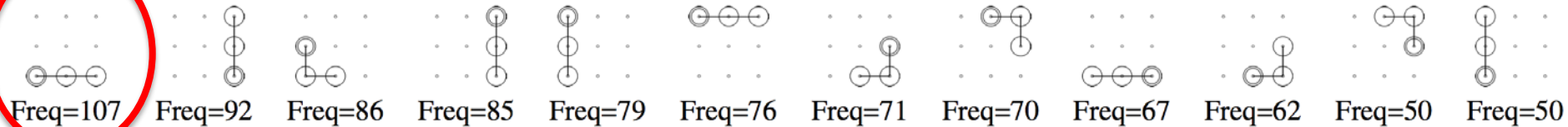


(c) Pen-Paper 4x4

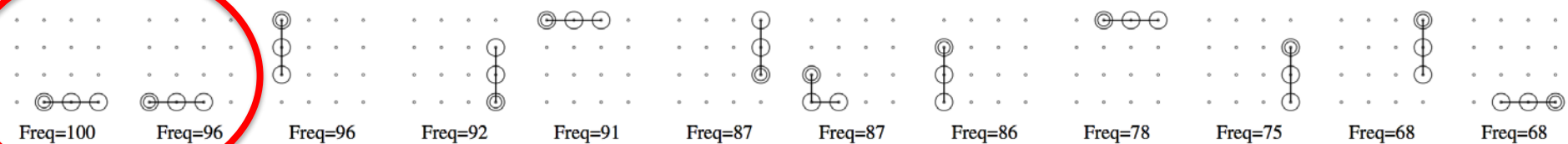
Sub-Sequences



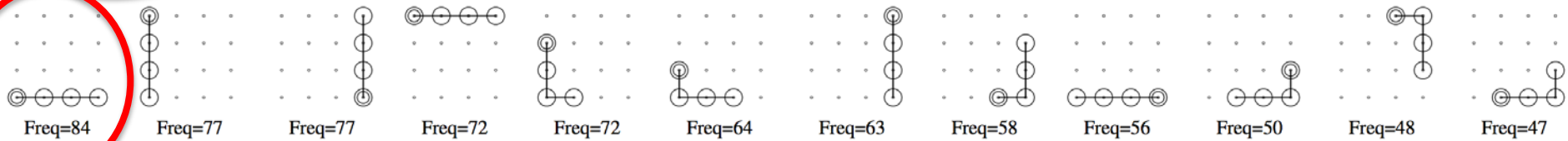
(a) Self-Report 3x3



(b) Pen-Paper 3x3



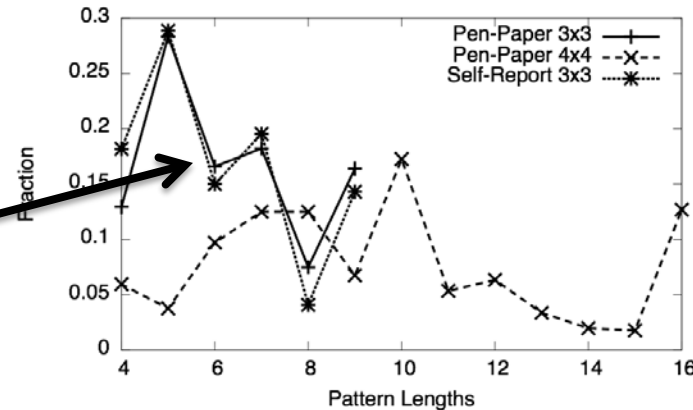
(c) Pen-Paper 4x4 (tri-grams)



(d) Pen-Paper 4x4 (quad-grams)

Length and Stroke Length

**Similar
Distribution**



*Suggests that
the pen-and-
paper and self-
report survey
have similarly
shaped
patterns*

Figure 2: The distribution of length in the data sets.

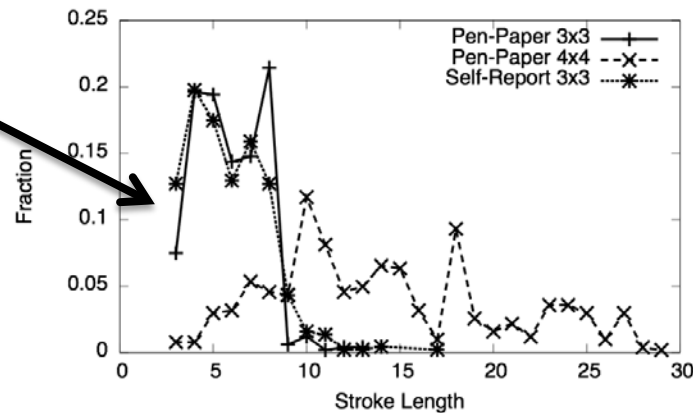
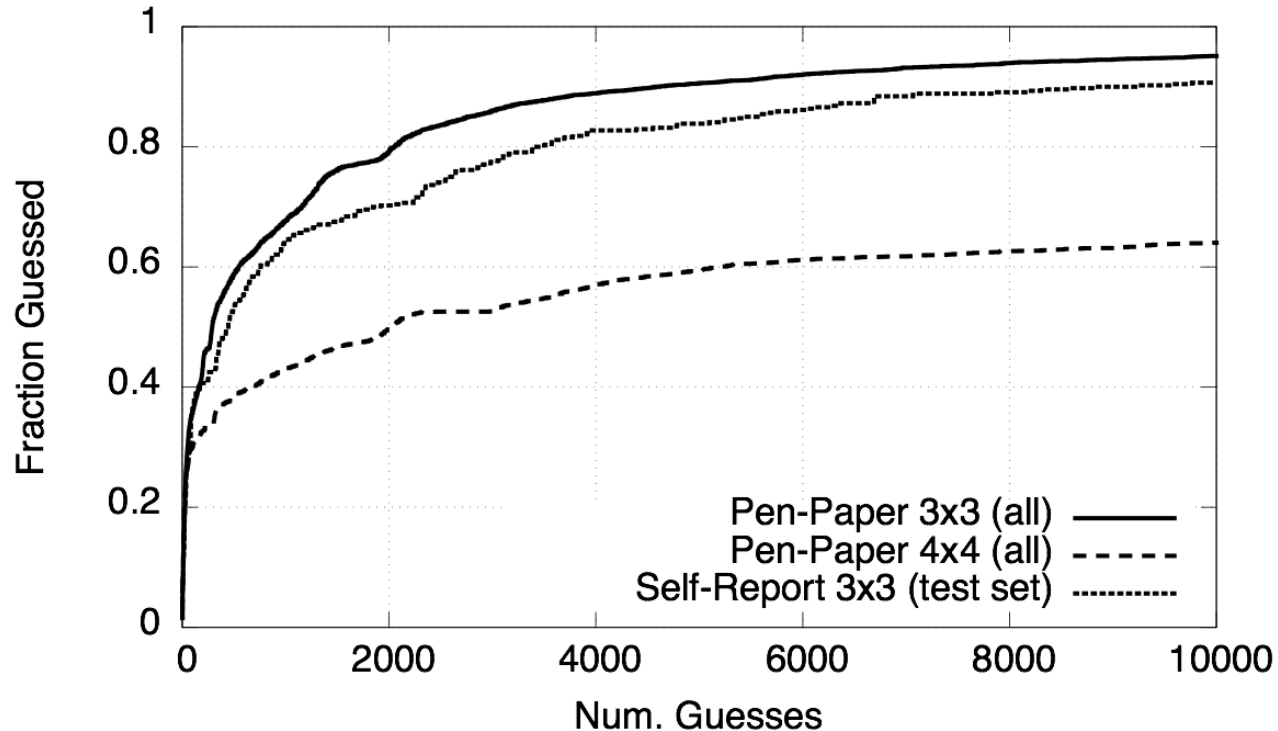


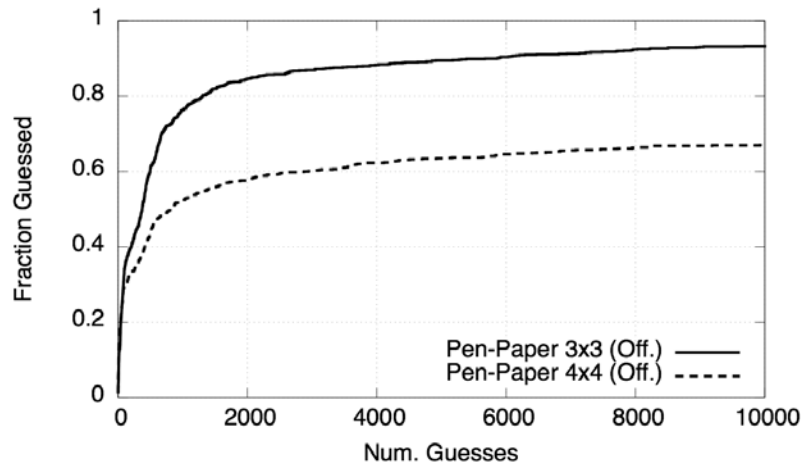
Figure 3: The distribution of stroke-lengths in the data set

Guessing Rates

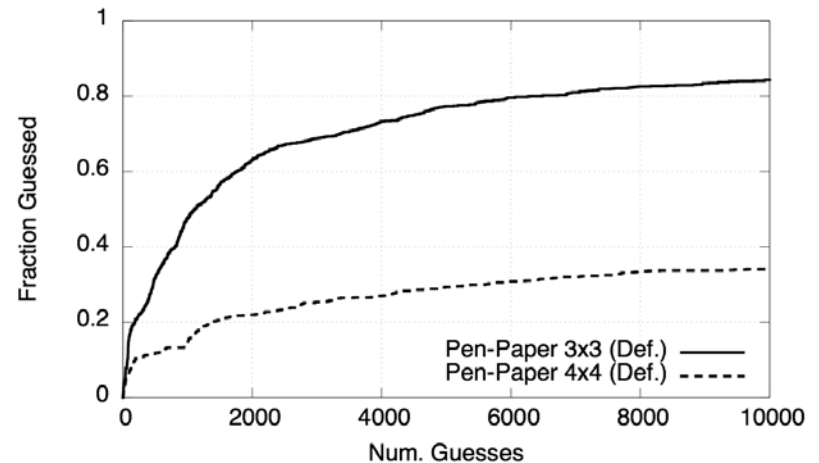


(a) *All* patterns using the average of 10 runs of a 5-fold cross-validation with 500 randomly selected patterns and self-reported 3x3 patterns

Offensive vs. Defensive



(b) *Offensive* patterns using the average of 10 runs of a 5-fold cross-validation with 100 randomly selected patterns



(c) *Defensive* patterns using the average of 10 runs of a 5-fold cross-validation with 100 patterns

Repeats and Symmetries

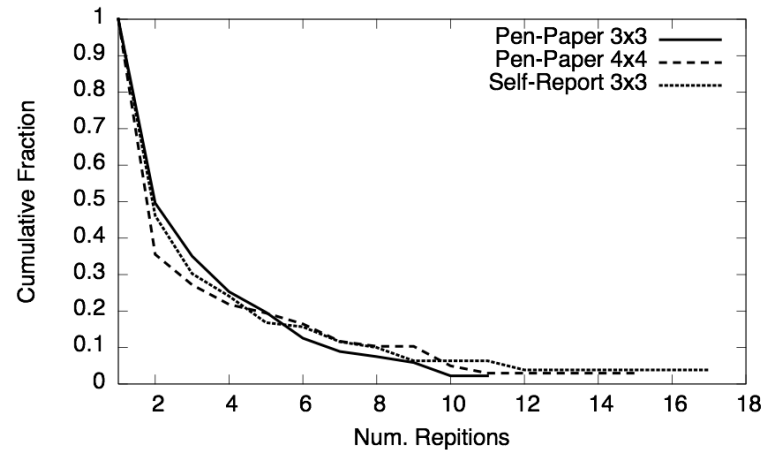


Figure 7: Cumulative fraction of patterns that repeat

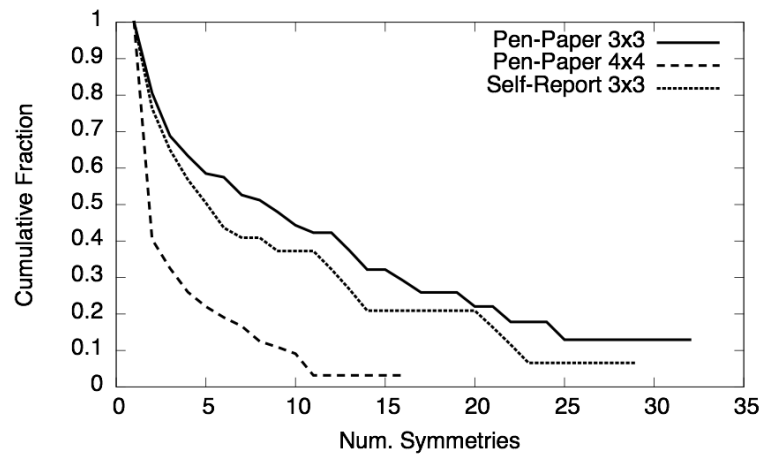


Figure 8: Cumulative fraction of patterns that have symmetries