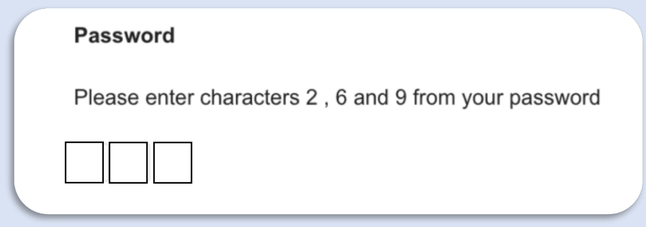
ADVANCECRT

Centre for Research Training

Science Foundation Ireland sfi For what's next

Strategies For Guessing Partial PINs

Ashley Sheil & Dr David Malone



What did want to explore?

- Our aim was to investigate how easy or hard it is to guess a full PIN using partial PIN guessing. Previous work has been done on how quickly you can guess user chosen PINs, if you already know their partial PIN.

Top Ten PINs										
4 Digits	1234	0000	2580	1111	5555	5683	0852	2222	1212	1998
6 Digits	123456	654321	111111	00000	123123	666666	121212	112233	789456	159753

- We wanted to explore these same questions, but with randomly assigned PINs.
- Banks will usually assign you a random PIN, as human chosen PINs tend to be much easier to guess. This is quite clear in the top 4 and 6-digit user chosen PINs above.

How did we go about this?

- We designed four different strategies for guessing PINs.
- For every PIN, a PIN-List is compiled of all possible combinations of the PIN and deletes all guesses as each partial PIN is entered, thus whittling down the list.

  - Max Method
  - Educated Guess
  - Round Robin
  - Random

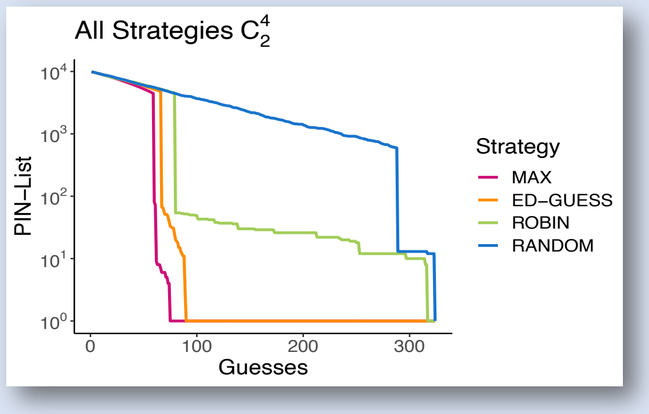
- Max Method and Educated Guess use this PIN-List to make informed guesses, Max using frequency and Educated Guess using distribution of the PIN.
- Round Robin goes trough each digit for each position in order and Random chooses randomly and deletes the guesses from the PIN-List as they go along.

Some Results…

Statistical Summary				
	Max	**EdGuess**	**RRobin**	**Rand**
Min	4.00	5.00	13.00	5.00
1st Qu	42.00	43.75	196.00	201.00
Median	68.00	80.00	299.00	303.50
Mean	74.59	95.93	318.20	326.60
3rd Qu	103.00	134.00	422.20	429.20
Max	171.00	309.00	1098.00	996.00

- The guessing was performed by Python.
- Graphs and statistics were performed using R.
- Above is a statistical summary of 1000 random PIN guesses for a 4-digit PIN with a partial PIN size of 2 digits.

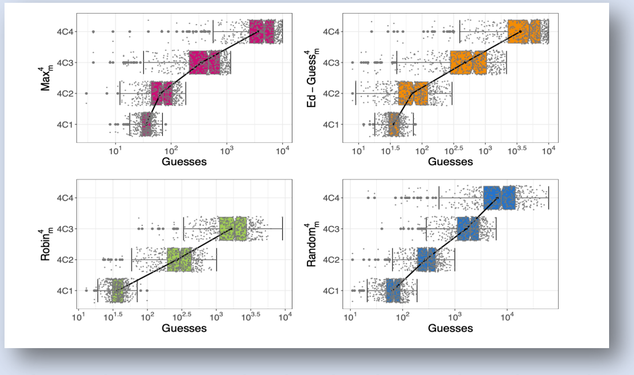
Which is the best Strategy?



- The Max strategy is the clear winner, the graph above shows a 4-digit PIN with a partial PIN of 2 digits.
- The Max method guesses in under 100 guesses as opposed to Random which takes over 300 guesses to guess full PIN.

What does this tell us?

- Partial PINs are starting to be phased out since they have shown to be less secure than originally thought.



- Full passwords and PINs can be hashed in a data base but not partial PINs, this poses a risk.
- The size of the partial PIN and respective full PIN can also make a difference in terms of how easy it is to gain the full PIN.

Also…

- With keylogging software, gaining partial PIN info is an advantage as guessing a full 6-digit PIN is a lot harder!
- In terms of usability, remembering a full PIN is easier than remembering certain digits of the PIN in different order.
- To aid with stronger security other authentication methods have been developed to use with or replace partial PINs, such as Authenticator Apps and Two factor authentication.

What Next?

- We believe we can mathematically analyse some of the situations to understand their behaviour better.
- We are also awaiting results of larger PIN sizes, which further highlights the advantage of having larger passwords and PINs.

Maynooth University
National University of Ireland Maynooth

Host Institution

UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh

CIT Cork Institute of Technology
Institiúid Teicneolaíochta Chorcaí

DUBLIN Ollscoil Teicneolaíochta Bhaile Átha Cliath Technological University Dublin

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin