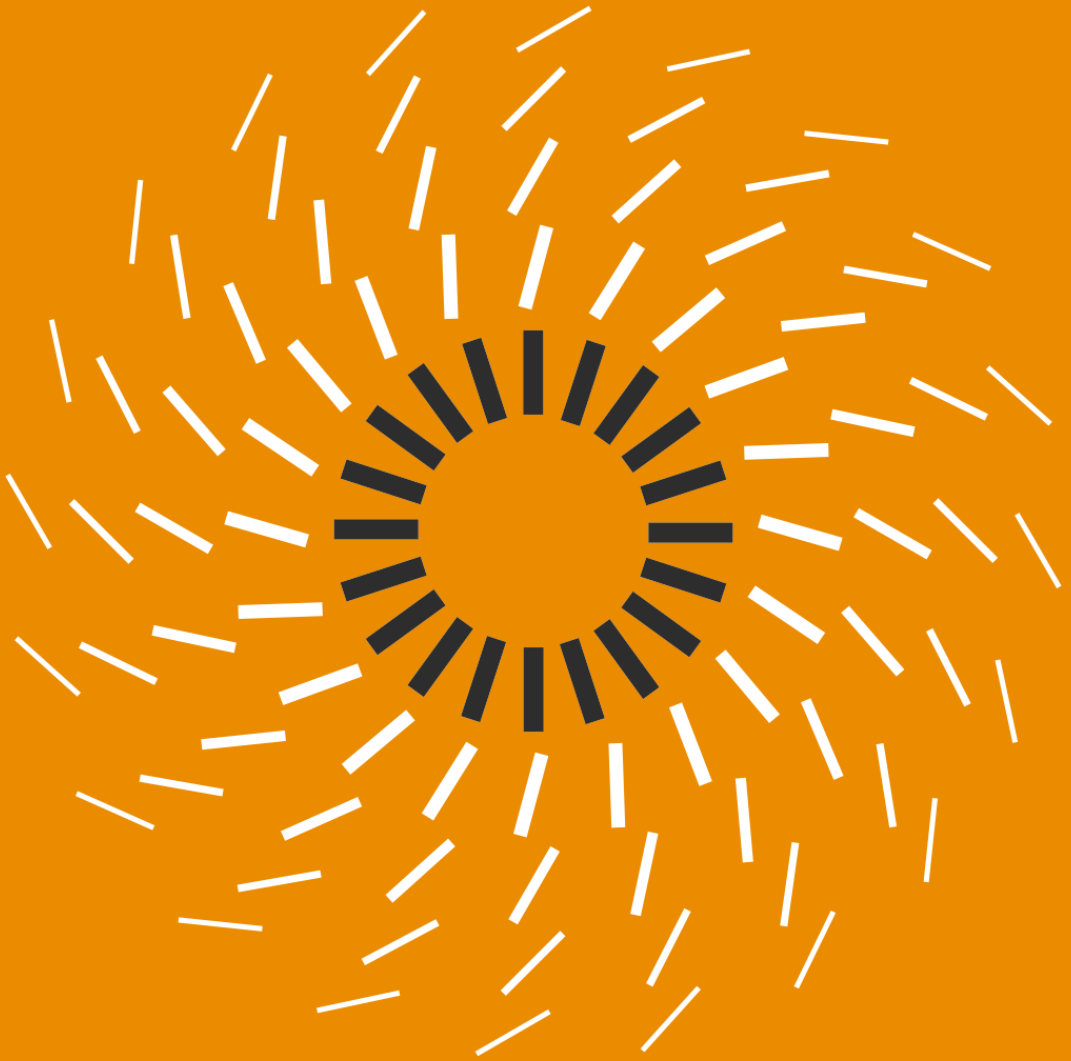
Breaking brains, solving problems

Lessons learnt from two years of setting puzzles and riddles for infosec professionals

Matt Wixey

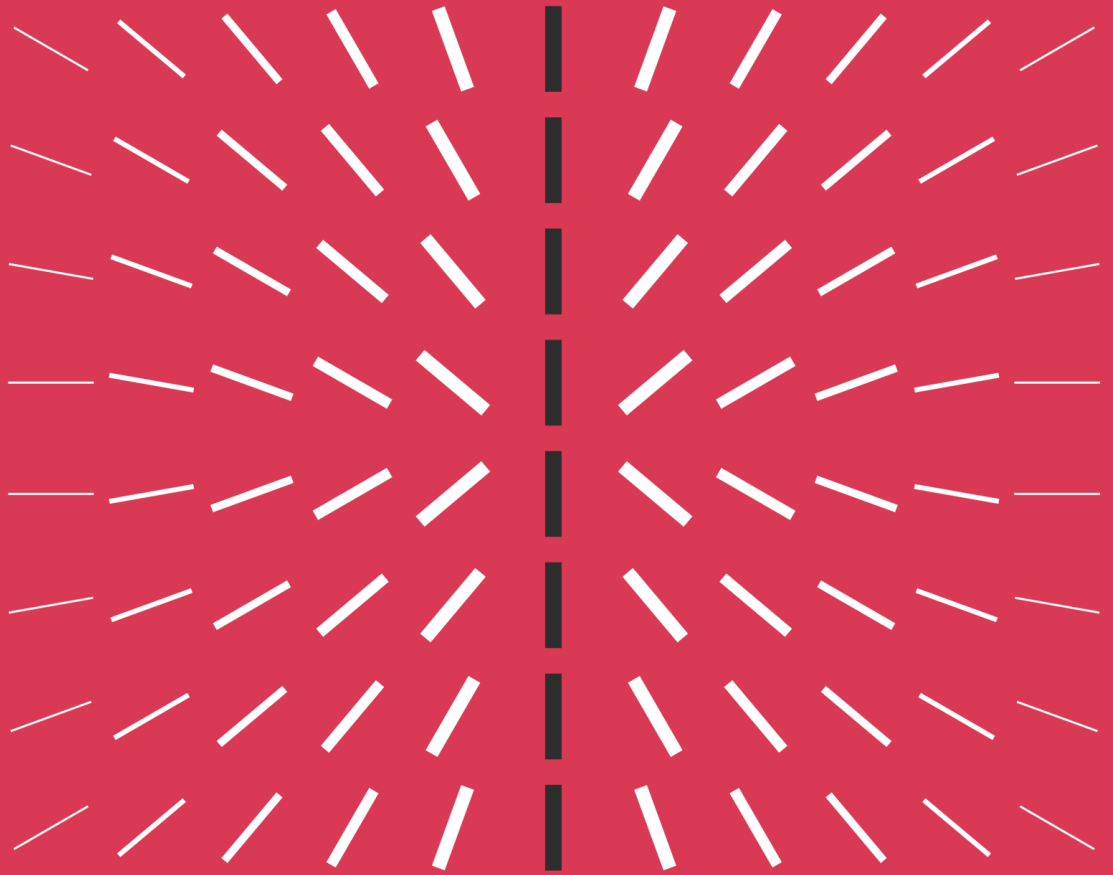
August 2020



pwc

1

Introduction



Matt Wixey

- Cyber Research Lead, PwC UK
- Part-time PhD at UCL
- Previously worked in law enforcement doing cyber R&D
- Love puzzles!

Puzzle competition

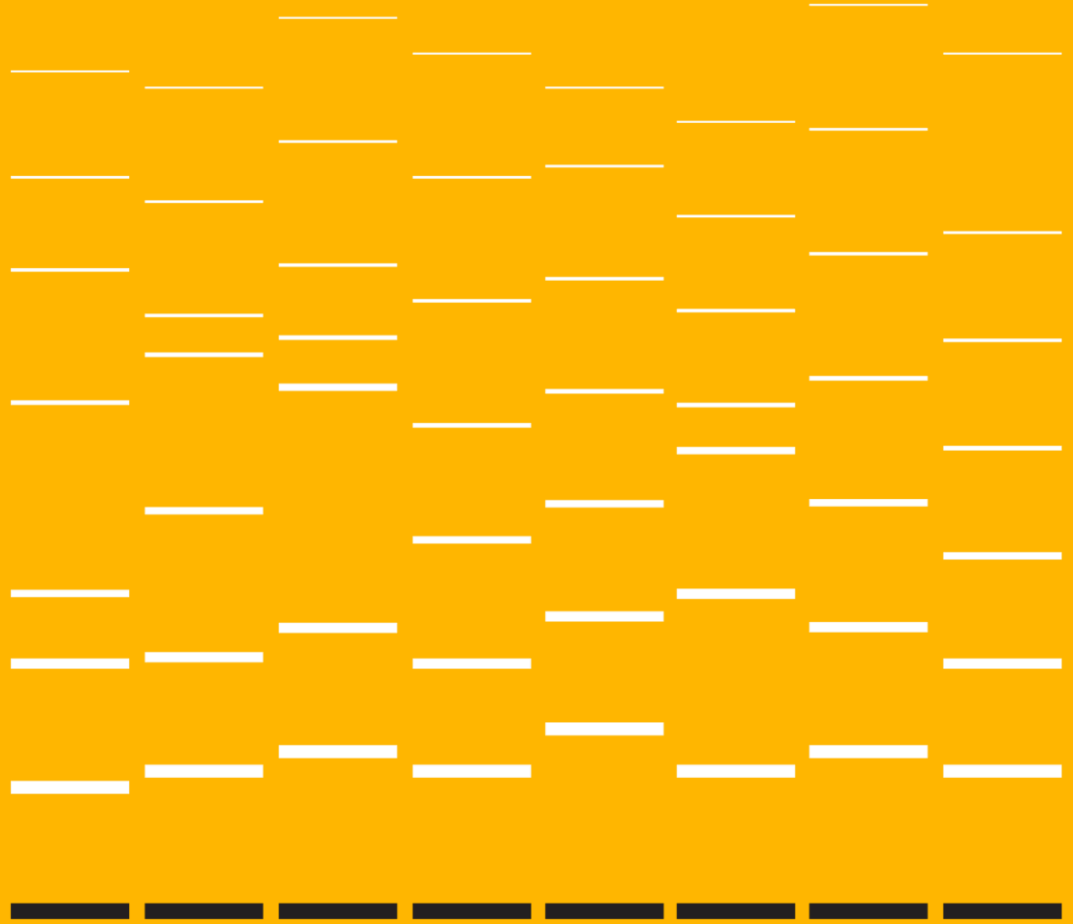
- At **thedarkartlab.com/crossword20**, you'll find a security-themed cryptic crossword
- Whoever sends me the most correct answers by 13th Aug 1300 PST wins a prize (TBC, puzzle-related)
- Feel free to start during the talk if your mind wanders (good approach to problem-solving!)
- https://www.theguardian.com/lifeandstyle/2010/may/03/how-to-solve-cryptic-crossword

Aims

- Look at some processes underpinning problem-solving
- The roles of expertise and bias
- Improvement strategies
- Problem-solving in infosec
- Our puzzle programme
- Tips and resources to create your own

2

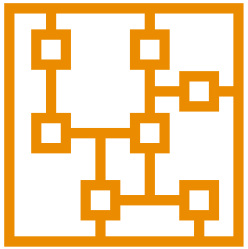
How problem-solving works



Background

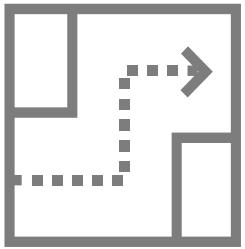
- All higher-level cognition is problem-solving
- Activation of concepts in the brain to access further concepts
- Various regions - mostly PFC, also middle temporal gyrus and frontal gyrus
- Hippocampus and amygdala activate afterwards - the “ah ha!” moment
- Some form of abstract representation, but mechanisms unclear

Understanding and searching



Understanding

- Assimilating stimulus
- Forming structures to represent the problem
- Variety of perceptual processes



Searching

- Finding or calculating a solution
- Usually a blend of the two, may be circular

Problem spaces and strategies

Proceed strategies
Choose operator, test, repeat

Backward chaining
Start at end state, if known

Subgoaling
Choose operator; if n/a, make operator fit

Means-end analysis
Calculating/reducing difference between current state and goal

Insight
Change in problem space
Example: boat and river problem

1 Initial problem state

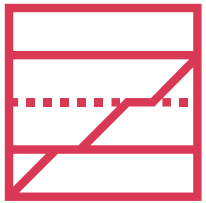
2 Operators change state

3 Test if new state = solution

Testing and measuring problem-solving ability

- Often considered an innate, fixed ability which can't be taught
- Not true – latent power, everyone has it
- Measure by time, approach, comfort

Survey of statements
Identifies people who may avoid/ignore/distort new info (Cacioppo & Petty, 1982)



Tolerance for ambiguity
Measuring comfort with uncertainty and multiple demands on attention (Butler, 2010)

Embedded figures tests
Ability to deal with unstructured tasks (Witkins et al, 1971)

The role of expertise in problem-solving

- Experts know a larger variety of problem schemas
- Triggering happens early (can cause assumptions, e.g. knights and knaves)
- May not play a huge role in some problems – algebra example

Sort problems into categories based on solutions
Novices rely on categories based on the problem

Perform faster (‘chunking’), but often don’t

Self-monitor and estimate difficulties better

The role of bias in problem-solving

Experience bias relying on past experience to make decisions

Self-serving bias believing we're making logical decisions

Hindsight bias putting higher probabilities on known outcomes

Anchoring avoiding cognitive dissonance

Confirmation bias prioritising evidence that reinforces beliefs

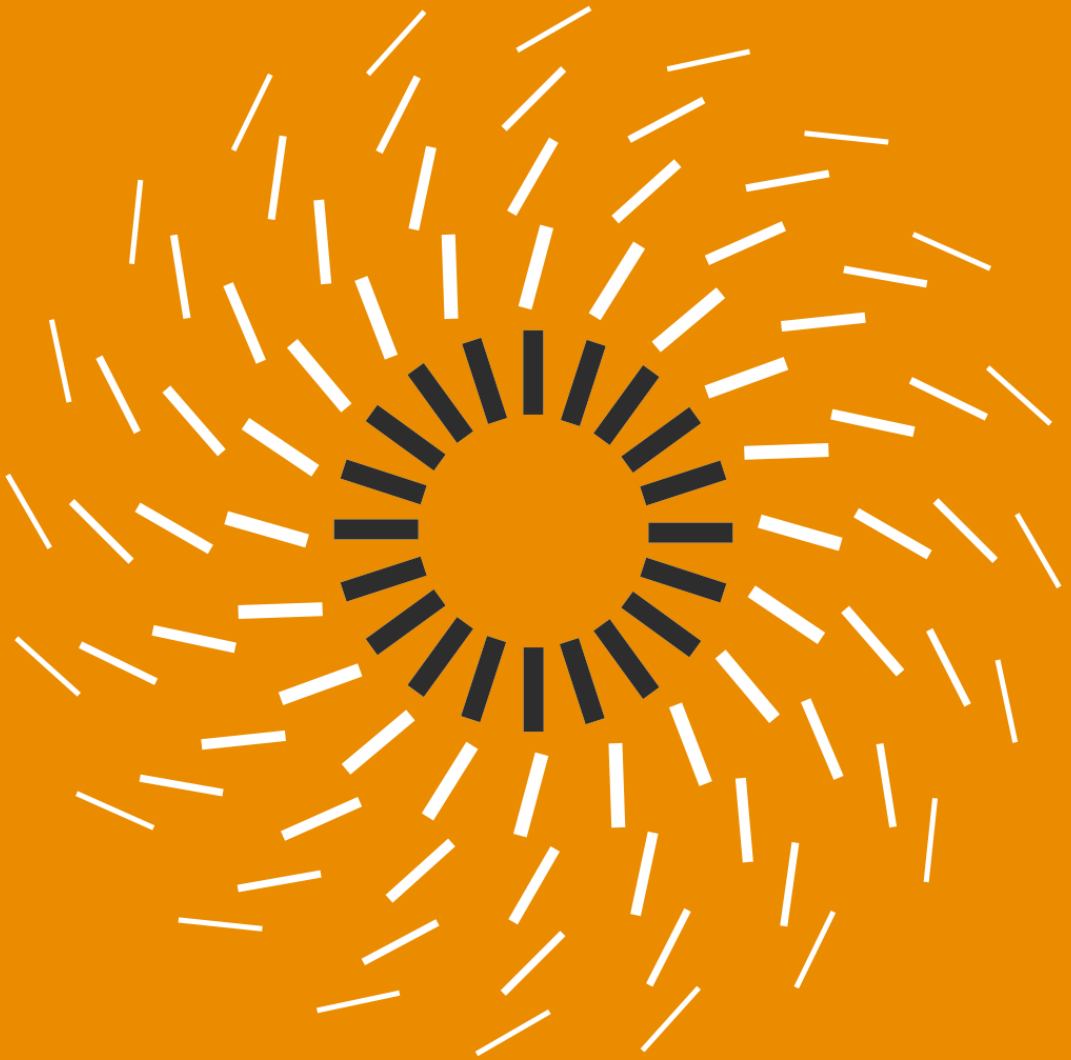
Sunk costs fallacy "Oh well, we've come this far"

Improvement strategies

- Do more!
- Compounding – deductive leaps by compounding operators
- Test assumptions, change beliefs
- Top-down refinement - starting small/big (Monty Hall/Blue eyes)
- Avoiding rabbitholes
- Self-explanation (rubber ducky debugging!), spontaneous thought
- Awareness of various biases – dominant vs alternate construals

3

Problem-solving in infosec



What do we mean by infosec problem-solving?

- Often knowledge-rich and ill-defined
- Undertaken by experts, novices, pre-novices
- Many schemas
- Example – Offensive Security exploit (https://www.youtube.com/watch?v=gHISpAZiAm0)
- Same strategies apply for improvement

Problem isomorphs

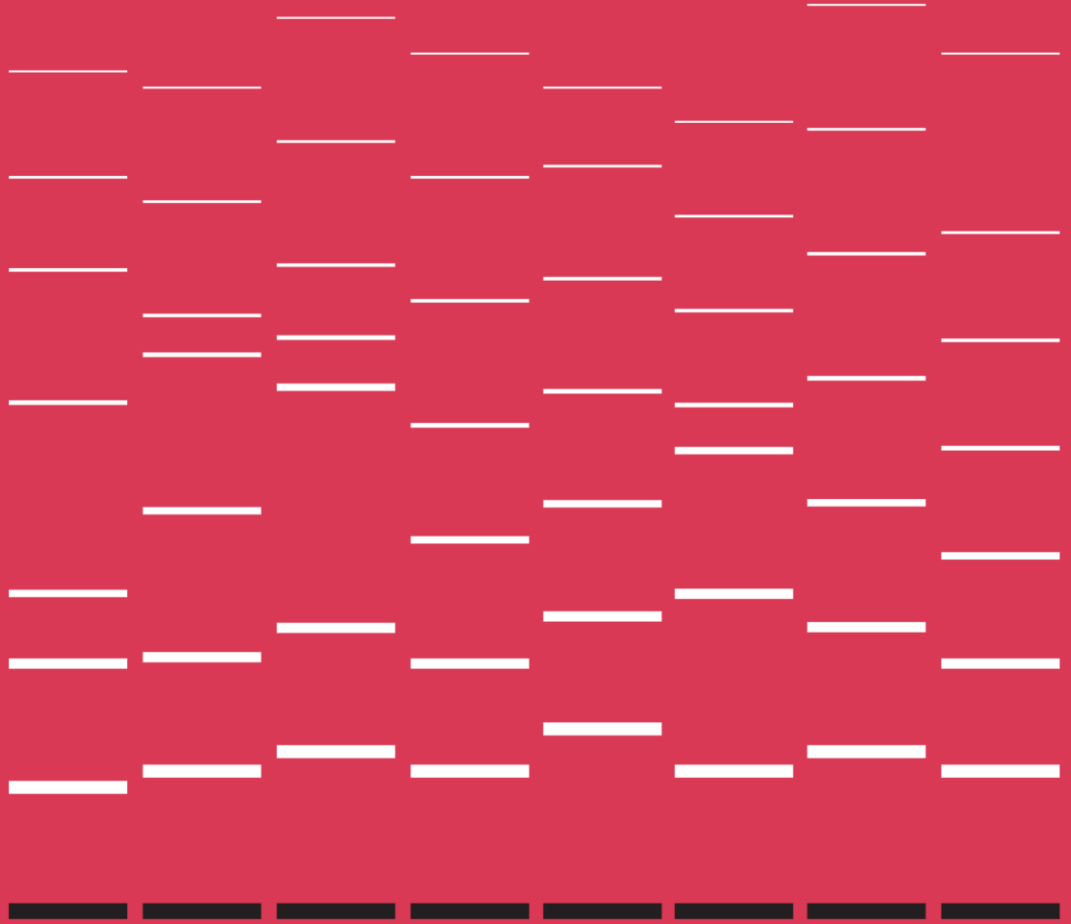
- Can change ‘cover story’ – problem space remains the same
- Incomplete knowledge transfer may be useful
- Diversity in background and expertise
- Useful for applying puzzles to real-world situations

Problem-solving by analogy

- Can help, but solvers might need to be explicitly told of the analogy
- May not be obvious how it relates to a current problem
- Unless it’s exactly, or almost exactly, the same situation
- So other than CTFs etc, how can we measure/improve problem-solving?

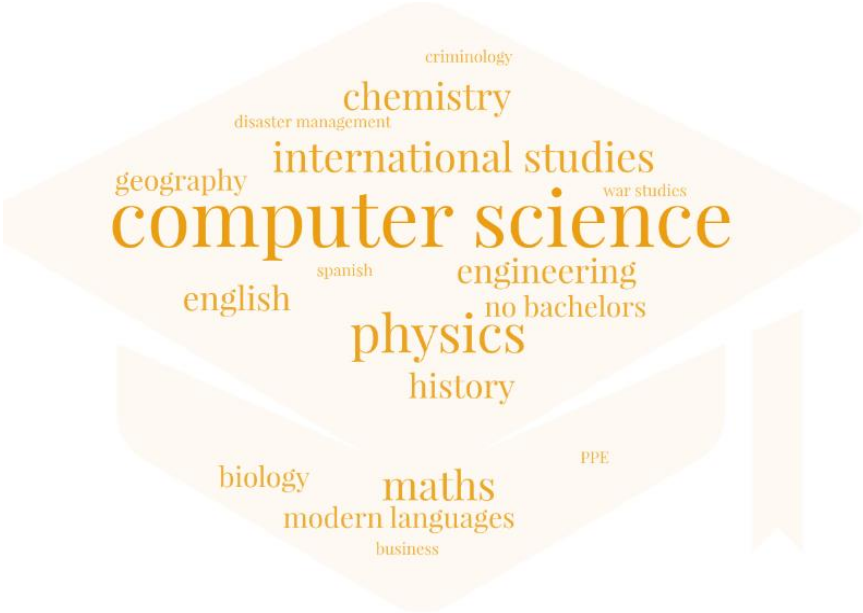
4

The puzzle programme



Background and origin story

- Around 300 staff, comprising deep technical disciplines, architecture, core, sector-specific, consultancy, support, policy, leadership, etc
- Varied mix of backgrounds and technical knowledge



The first puzzle

- Began with me trolling a colleague with this puzzle:
- https://xkcd.com/blue_eyes.html
- Since then, ~40 puzzles, most designed from scratch
- Wordplay/cryptic; logic; maths/probability; technical
- Some themed, others abstract/standalone
- Most independent, some multi-stage
- Most designed to be solved within 2-3 days, others weeks

The perfect puzzle

- Interesting story/premise
- Little exposition/explanation
- Hidden ‘trapdoor’ function (optional)
- Red herrings and Easter Eggs (optional)
- May ask something completely unconnected to premise
- But also an internal logic – answer obtainable from question
- No specialist knowledge needed beyond a quick search

Example 1: The birthday (2019)

Last week, I was at a bar having a beer with an old school friend, and I realised I didn't know when her birthday was. She said "I can't tell you, but the way I describe it is: the day has at least 2 prime factors, 1 of which is also the month. Subtract the month from the day to get the age I'll be at my next birthday. Or to put it another way, square eight to get the month and day. Add another square to that, and it's obvious.

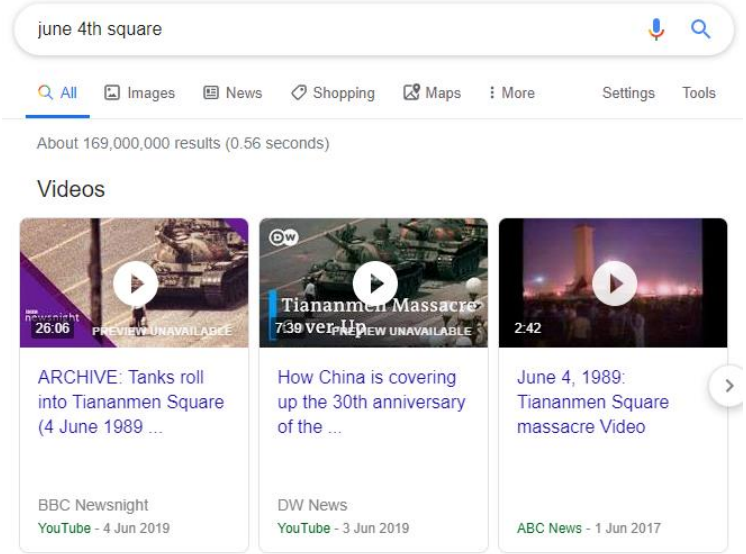
What is my friend's birthday, and where does she live?

Assumptions and clues

- Normal dates (max 31 for days, max 12 for months)
- Having a beer at a bar (at least 18 in UK)
- Square eight to get the month and day = 64 = either 6th April or 4th June
- Add another square?

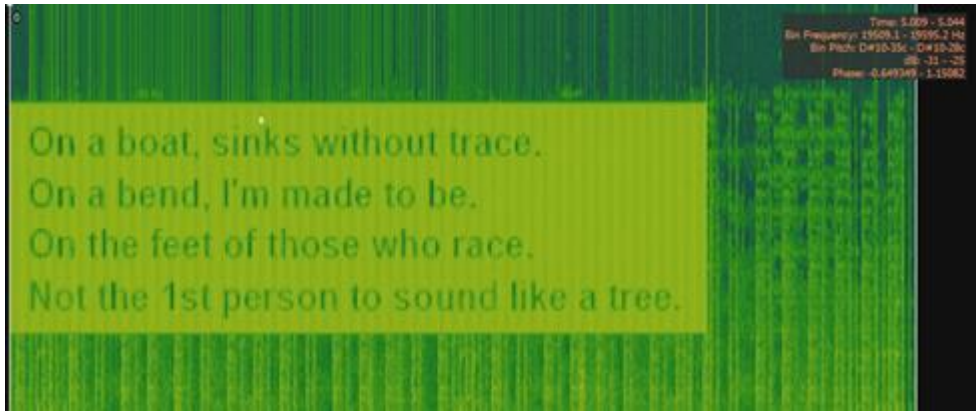
Answer

- 35/05/1989 (04/06/1989)
- Date of Tiananmen Square protests
- 35/05 not valid date, but used to refer to 4th June in China
- Fulfils all conditions (prime factors, day-month = age at next birthday)
- “Add a square”:



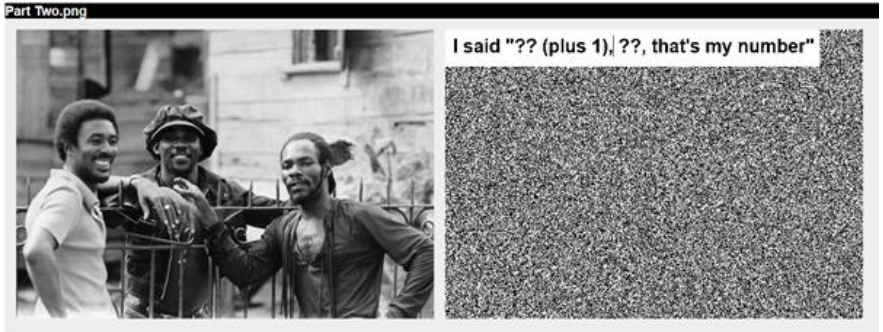
Example 2: Finding location (multi-stage)

- 3-part puzzle to give location of team event day
- Parts 1 and 2 released simultaneously, then Part 3
- But answer available with Part 3 alone also
- Part 1 = WAV file of “Never Gonna Give You Up”
- With riddle embedded in spectrogram (answer = “U”)



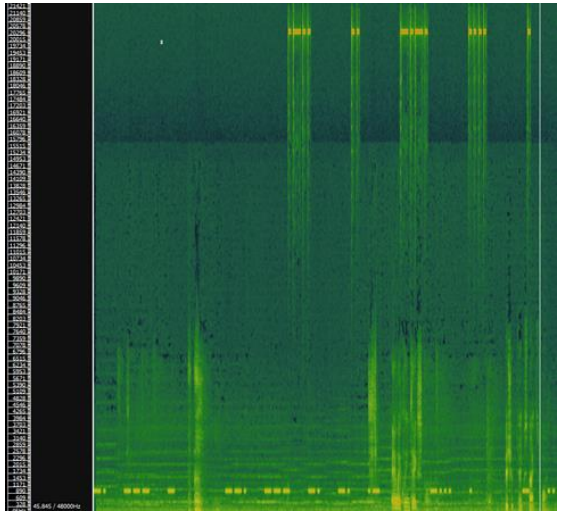
Example 2: Finding location (multi-stage)

- Part 2 = image with LSB steganography
- Google search reveals answer: “55 46”



Example 2: Finding location (multi-stage)

- Part 3 = video of *2001: A Space Odyssey* chess scene
- Alphanumeric string appears at end
- Obvious Morse code audio over scene
- Spelt out: “NOT GONNA BE THAT EASY”
- Ultrasonic Morse code: “LICHESS DOT ORG”

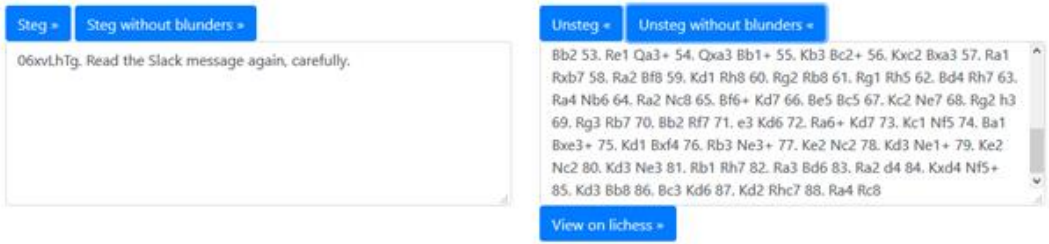


Example 2: Finding location (multi-stage)

- Video brightness also flashed in Morse code: “LICHESS URL”
- Punctuation (periods and hyphens) in riddle message also spelt out Morse code for “LICHESS”
- Lichess.org + alphanumeric string = chess game on Lichess

Example 2: Finding location (multi-stage)

- Decoding chess steganography



- Original message – first letter of each sentence spells out PASTEBIN
- Pastebin.com + string above =

text 0.17 KB

```
1. A Sagittarian's vision, destroyed in a fire.
2. Restored by the heart of PwC.
3. If this place's name you seek to acquire:
4. You have answers, so change them - with hex as key.
```

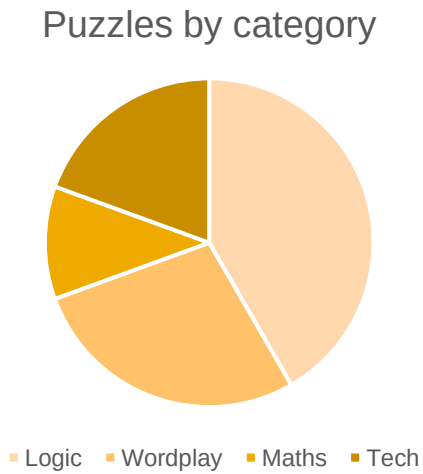
Example 2: Finding location (multi-stage)

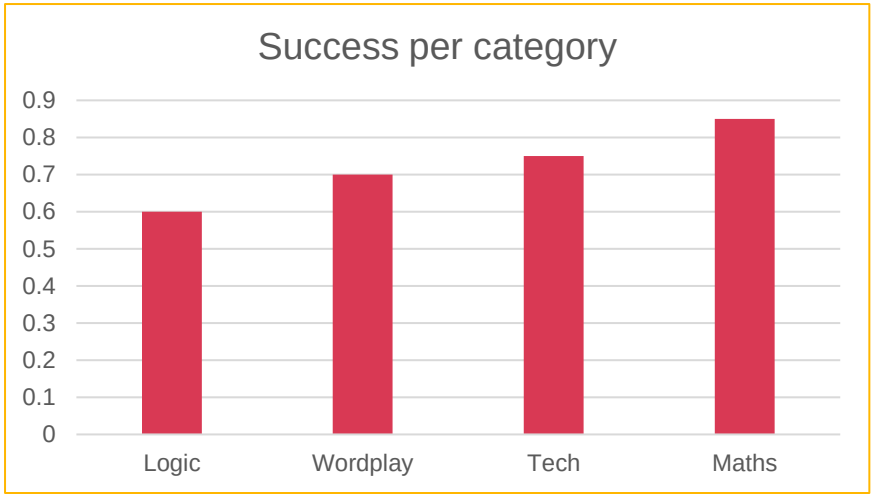
- “With hex, as key [ASCII]”
- Hex (u) = 0x75
- ASCII (55 46) = U F
- Put together = 0x75UF = OX7 5UF = postcode of location

OR

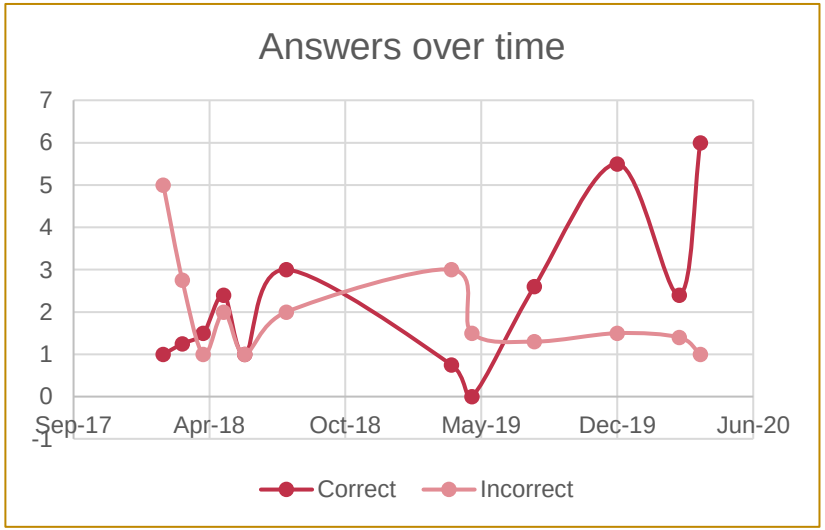
- "A Sagittarian's vision" - the architect was Thomas *Archer*
- "Destroyed in a fire" - a fire in 1831 destroyed a lot of the site
- "Restored by the heart of PwC" - architect Alfred *Waterhouse* was commissioned to rebuild it
- Search 'archer fire waterhouse’ and the location comes up

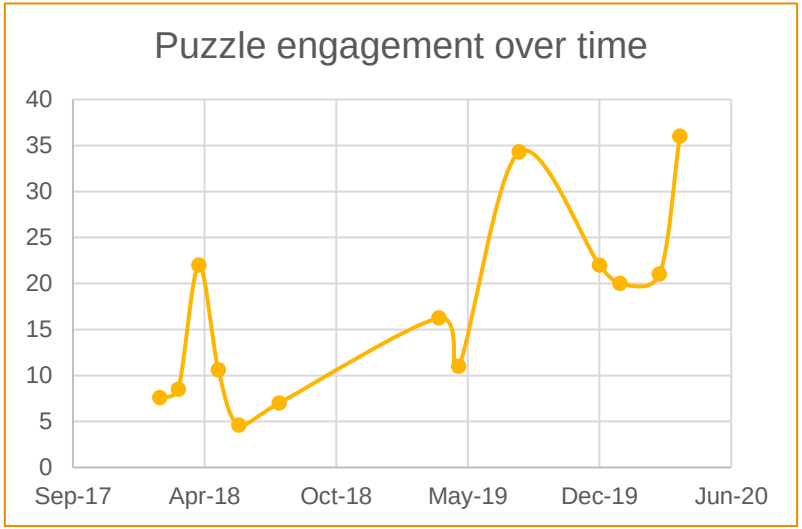
Category breakdowns



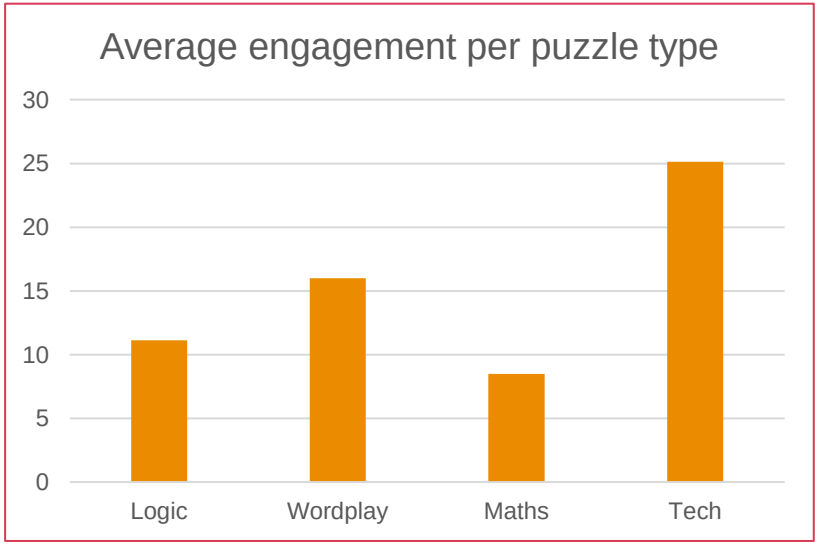


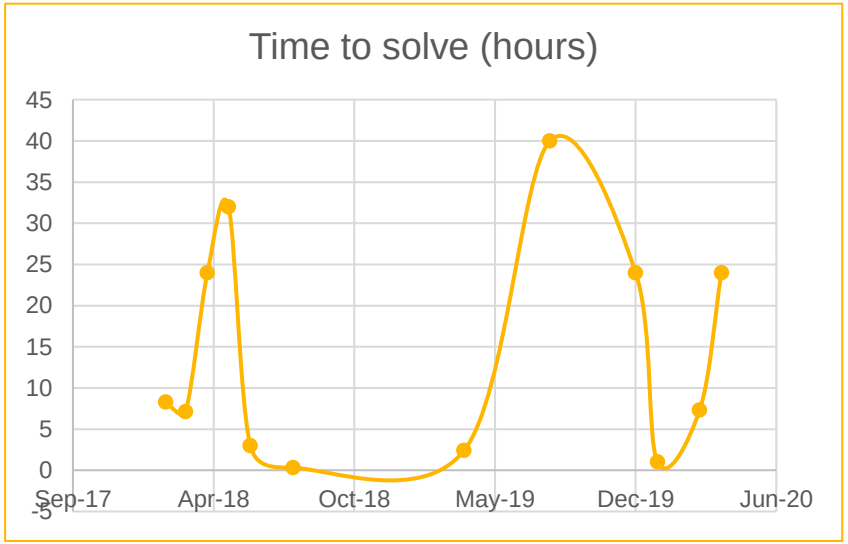
Answers and engagement over time





Engagement per category and time to solve





Unexpected answers and collaboration

"As 35/05 isn't a valid day/month combination in the Gregorian calendar, I was hoping you'd discount it in the previous stages!" - yes, yes I did 😬

Ah so I wasn't imagining it! , I have 1500+ frames

i wa Oh good grief @matt.wixey

How did I not spot that???

Hah, he kept me going, I'd have thrown the towel in long before if I was on my own.

Unexpected solutions

"Here's this wonderfully complex puzzle"

"Cool, I've got a bulldozer. and it's going through the middle"

Not gonna lie, I figured it would be easier to just wait until someone told us the answer

4

Just look at the colour of hat they are wearing, surely?

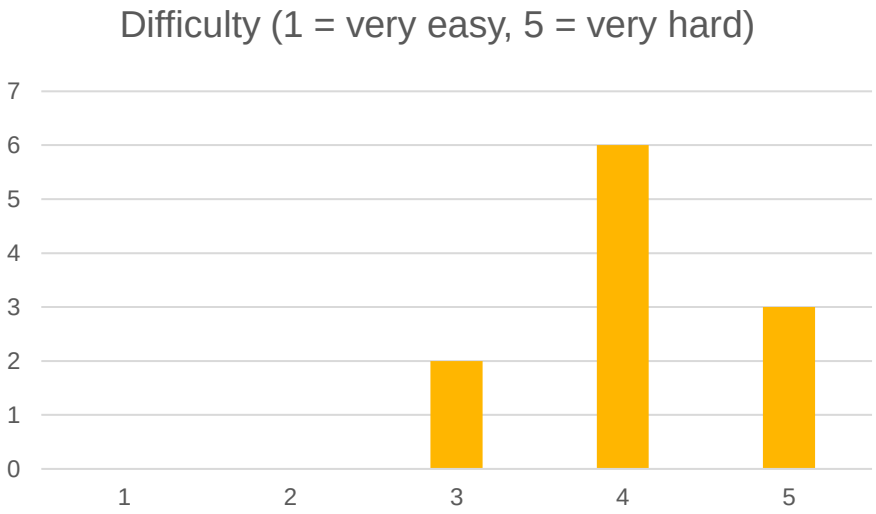
Kill both knights, open one door. If full of tigers, kill all the tigers

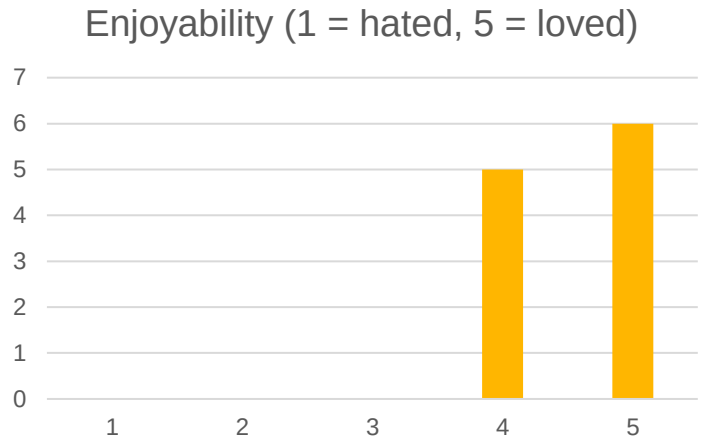
Matt Wixey 11:48 AM

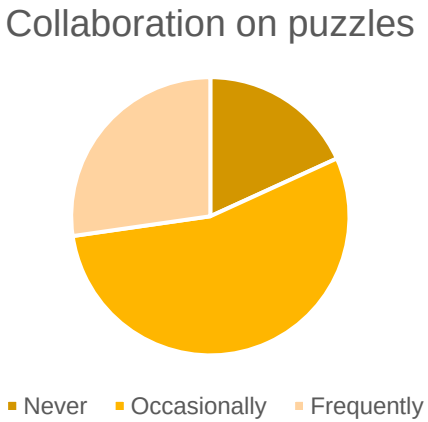
There is a brutal elegance about the phrase "If full of tigers, kill all the tigers"

2

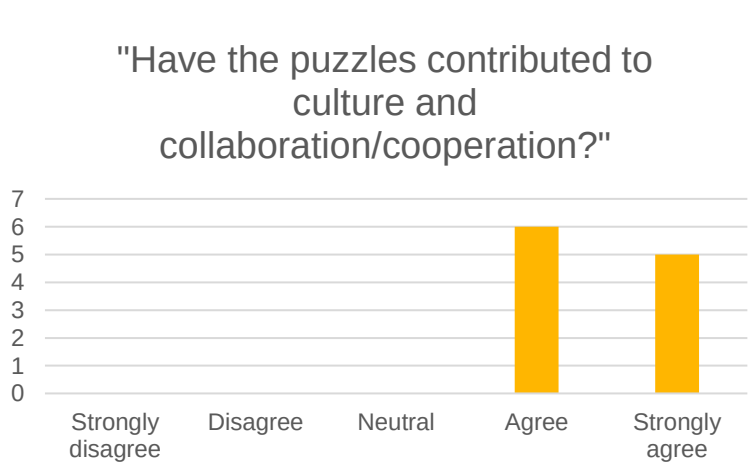
Straw poll

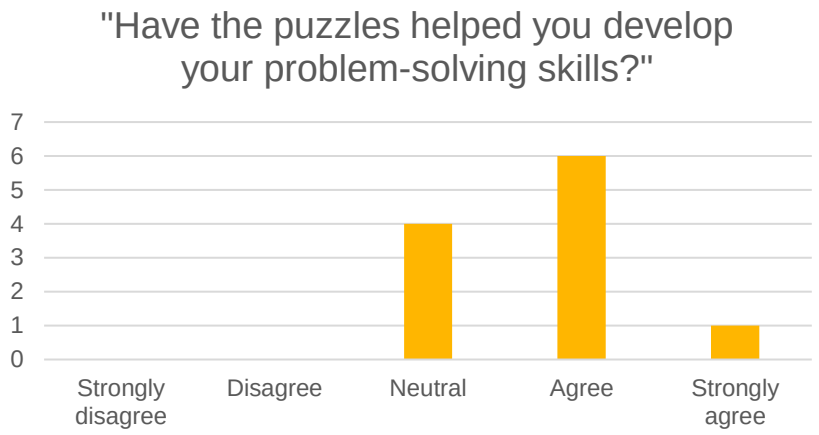

Difficulty (1 = very easy, 5 = very hard)
7
6
5
4
3
2
1
0
1
2
3
4
5

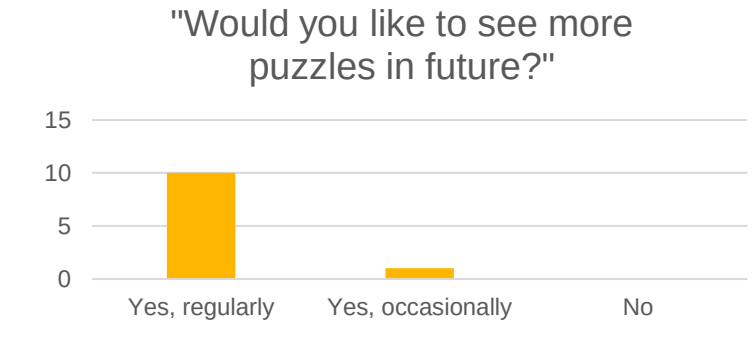

Enjoyability (1 = hated, 5 = loved)
7
6
5
4
3
2
1
0
1
2
3
4
5

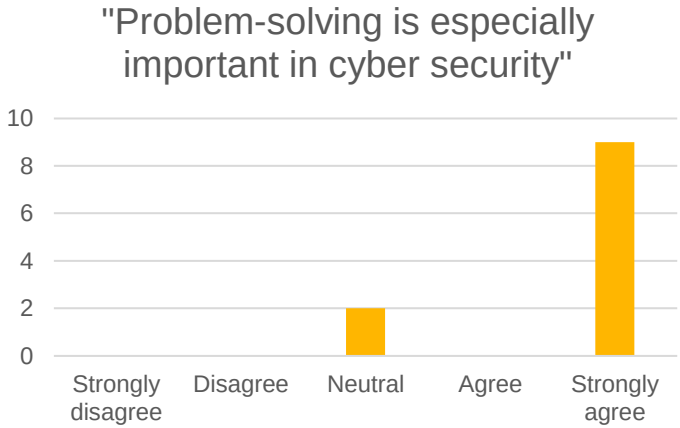

Collaboration on puzzles
Never
Occasionally
Frequently

Straw poll

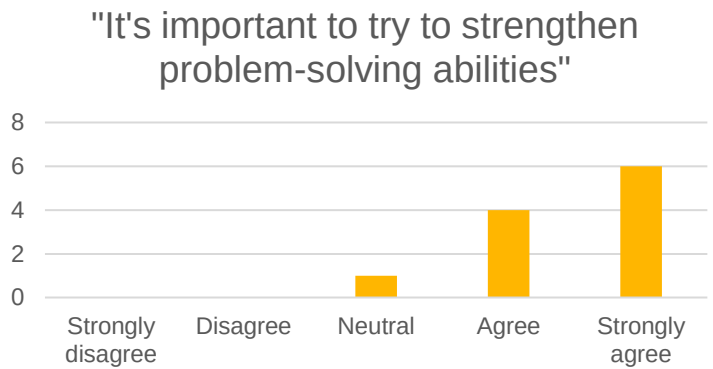

"Have the puzzles contributed to culture and collaboration/cooperation?"
7
6
5
4
3
2
1
0
Strongly disagree
Disagree
Neutral
Agree
Strongly agree

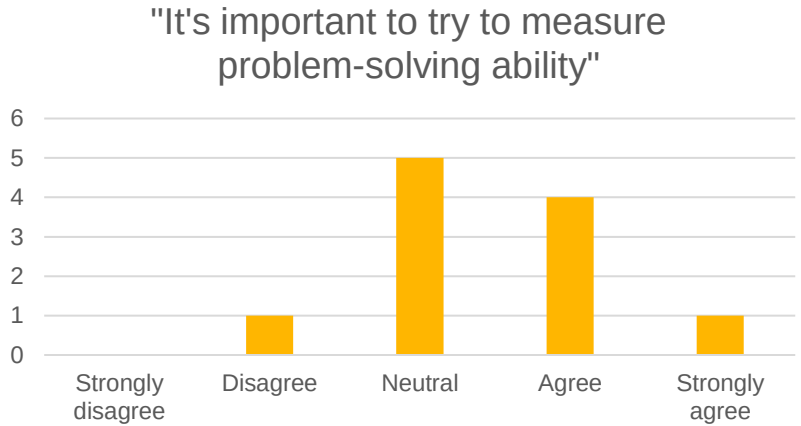

"Have the puzzles helped you develop your problem-solving skills?"
7
6
5
4
3
2
1
0
Strongly disagree
Disagree
Neutral
Agree
Strongly agree

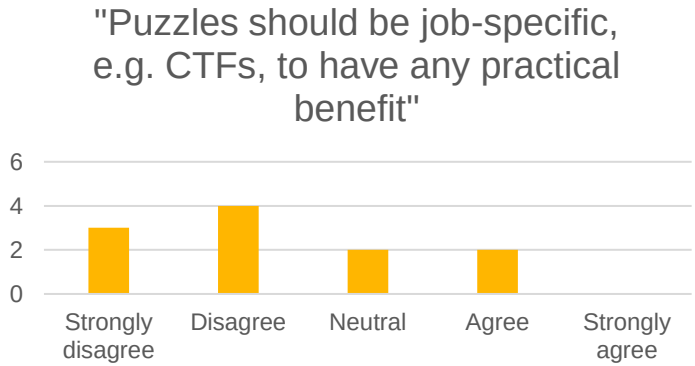

"Would you like to see more puzzles in future?"
15
10
5
0
Yes, regularly
Yes, occasionally
No

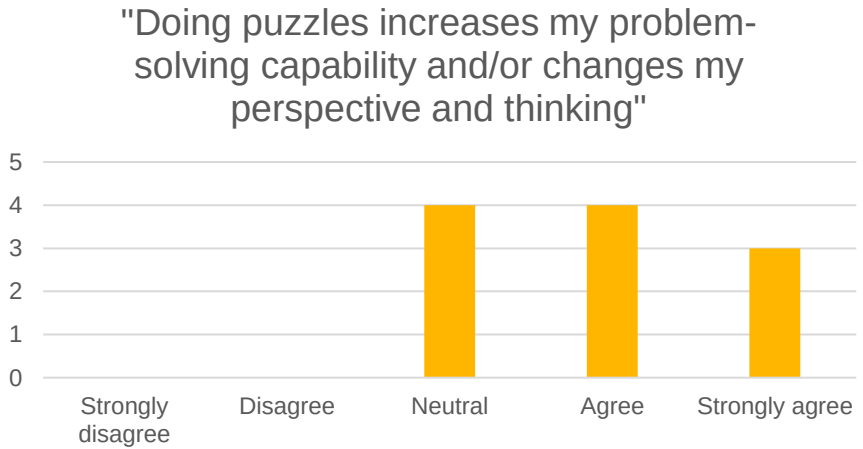

"Problem-solving is especially important in cyber security"
10
8
6
4
2
0
Strongly disagree
Disagree
Neutral
Agree
Strongly agree

Straw poll


"It's important to try to strengthen problem-solving abilities"
8
6
4
2
0
Strongly disagree
Disagree
Neutral
Agree
Strongly agree


"It's important to try to measure problem-solving ability"
6
5
4
3
2
1
0
Strongly disagree
Disagree
Neutral
Agree
Strongly agree


"Puzzles should be job-specific, e.g. CTFs, to have any practical benefit"
6
4
2
0
Strongly disagree
Disagree
Neutral
Agree
Strongly agree


"Doing puzzles increases my problem-solving capability and/or changes my perspective and thinking"
5
4
3
2
1
0
Strongly disagree
Disagree
Neutral
Agree
Strongly agree

Applied learning and benefits

“Taking a step back and looking at the larger picture”

“it is a good illustration of the 'greater than the sum of parts' idea as other people's ideas and strengths can enable you to solve a problem none of the team would have been able to on their own”

“all used in my day to day role”

“Not directly, but I think there is a correlation between solving your puzzles and puzzle solving in life / work”

“I feel that puzzles keep my problem solving skills sharp, and that is helpful for a range of situations at work”

“Definitely reading between the lines! and trying to think beyond what could be immediately obvious.”

“it feels like sometimes the puzzle show an application of a cyber concept which I had only previously just read about (e.g. steganography)”

Important attributes for problem-solving

"Open mind, lateral thinking"

"Being able to think outside the box. Deliberation"

"Ability to think holistically at a problem as well as in detail. Being able to let go of a chain of thinking so it doesn't bias future attempts"

"Quickly assimilating new information and taking further actions on it even if you didn't have any domain knowledge prior to attempting the task"

"Structuring one's thoughts, being able to prioritise issues, linking pieces of information"

"Seeing the bigger picture"

"Curiosity and stubbornness!"

"Ability to 'divide and conquer' the problem to accurate sub-problems. This helps to improve teamwork and collaboration"

Case study: SandGrox

- Coming up with various ways to detect and evade sandboxes for red-teaming
- Lateral-thinking: novel forms of detection (e.g. environmental)
- Challenging assumptions: what can a sandbox detect?
- Sub-goaling – test if technically feasible, then test against end state
- Avoiding rabbit-holes
- Spontaneous thought and incubation
- Avoidance of bias, esp. self-serving and hindsight bias
- Problem isomorphs – HCI, bot detection, antivirus evasion

Starting your own puzzle programme

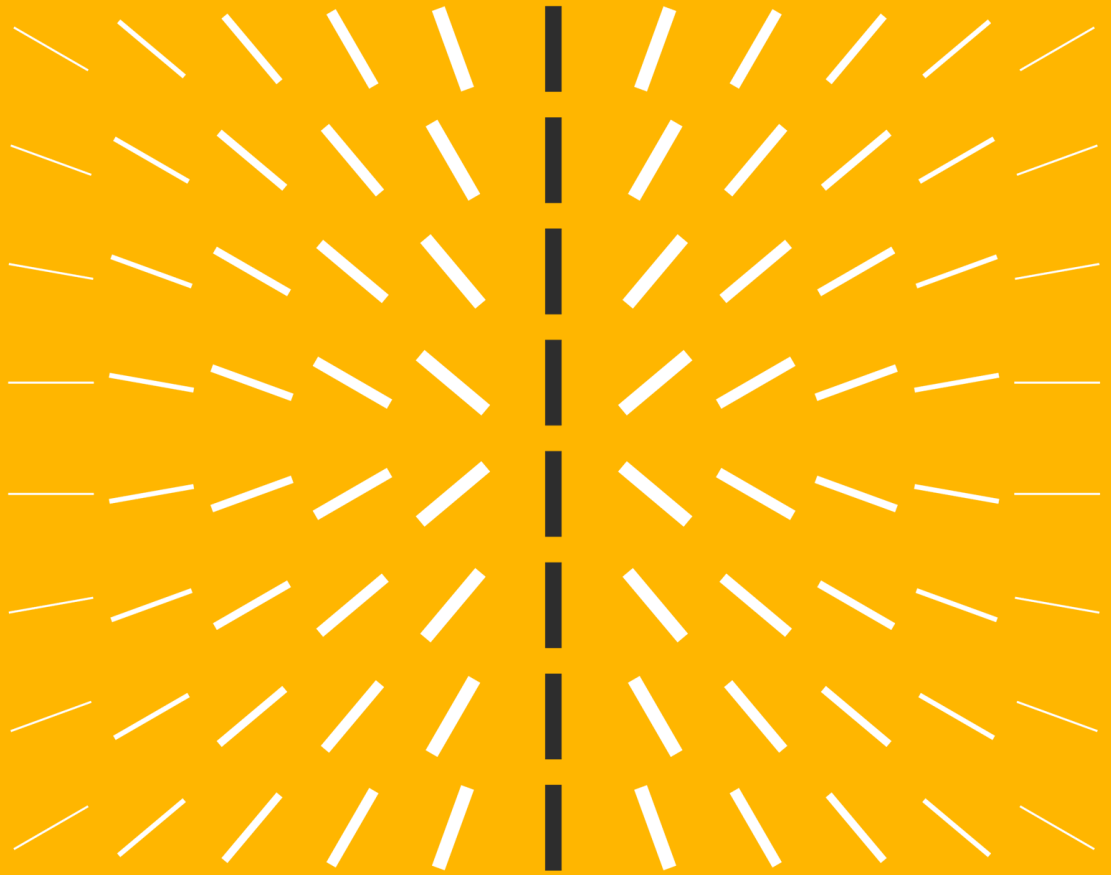
- Can start off with pre-existing ones
- Creating puzzles from scratch = time-consuming (14+ hrs)
- Good resources:
- https://puzzling.stackexchange.com/
- Puzzles on TED-Ed YouTube channel
- Cryptic crosswords in newspapers
- CTFs, DEF CON challenges, etc

Lessons learnt

- Mix up formats and genres to broaden appeal
- Measure engagement and stats
- Link to other organisational activity
- Encourage collaboration (e.g. teams)
- Incentives – prizes etc
- Encourage inclusivity – don’t alienate would-be participants

5

Summary



Key takeaways

- Problem-solving is a skill, with specific processes underpinning it
- There are specific strategies for improvement – not just a case of doing more
- And specific biases associated with it
- Puzzles are a great way to develop problem-solving
- And contribute to culture and engagement
- The design and type of puzzle is important, and it needs thought!

Future work

- Will create a repository of cyber-related puzzles for everyone to use
- Add yours! Plus stats, critiques, analysis, etc
- Gap in research on the psychology of security-related problem-solving
- Don’t forget to have a crack at the crossword!
- **thedarkartlab.com/crossword20**

References

Ajayi, B. (1990). Riddles and the Child. International Journal of Moral and Social Studies, 5(5), 251-261.

Anderson, J. R. (1993). Problem solving and learning. American Psychologist, 48(1), 35.

Bar-Hillel, M., Noah, T., & Frederick, S. (2018). Learning psychology from riddles: The case of stumpers. Judgment & Decision Making, 13(1).

Butler, S. A. (2010). Solving business problems using a lateral thinking approach. Management Decision.

Butler, S. A., & Ghosh, D. (2015). Individual differences in managerial accounting judgments and decision making. The British Accounting Review, 47(1), 33-45.

Butler, S.A. and Ghosh, D. (2006). The effect of individual differences in comprehensive thinking on judgments and decision making. Working paper, School of Accounting, University of Oklahoma, Norman, OK.

Cacioppo, J.T. and Petty, R.E. (1982), "The need for cognition", Journal of Personality and Social Psychology, Vol. 42, pp. 116-31.

Chi MTH, Bassok M, Lewis M, Reimann P, Glaser R. 1989. Self-explanations: how students study and use examples in learning to solve problems. Cogn. Sci. 15:145–82

Chi MTH, VanLehn K. 1991. The content of physics self-explanations. J. Learn. Sci. 1:69–105

Chi, M. T. H., Glaser, R. & Rees, E. (1982). Expertise in problem solving. In R. J. Sternberg (Ed.), Advances in the Psychology of Human Intelligence. Hillsdale, NJ: Erlbaum.

Christoff, K., Gordon, A., & Smith, R. (2011). The role of spontaneous thought in human cognition. In Neuroscience of decision making (pp. 271-296). Psychology Press.

Dunbar, K. (1998). Problem solving. A companion to cognitive science, 289-298.

Fitts PM. 1964. Perceptual-motor skill learning. In Categories of Human Learning, ed. AW Melton, pp. 243–85. New York: Academic

Gick, M.L. & Holyoak, K.J. (1980). Analogical problem solving. Cogntive Psychology, 12. 306-355

References

Gick, M.L. & Holyoak, K.J. (1983). Schema induction and analogical transfer. Cognitive Psychology, 15, 1-38.

Hayes, J. R. & Simon, H. A. (1974). Understanding written problem instructions. In L. W. Gregg (Ed.), Knowledge and Cognition. Hillsdale, NJ: Erlbaum. Reprinted in H.A.Simon (1979 Models of Thought, New Haven, CT: Yale University Press.

Hofstadter, Douglas R. "Analogy as the core of cognition." The analogical mind: Perspectives from cognitive science (2001): 499-538.

Jeffries, R., Turner, A.A., Poison, P.G. & Atwood, M.E. (1981). The processes involved in designing software. In J.R. Anderson (Ed.), Cognitive Skills and Their Acquisition. Nillsdale, NJ: Eribaum.

Kane, M. J., Brown, L. H., McVay, J. C., Silvia, P. J., Myin-Germeys, I., & Kwapil, T. R. (2007). For whom the mind wanders, and when: an experience-sampling study of working memory and executive control in daily life. Psychological Science, 18(7), 614-621.

Klinger, E., & Cox, W. M. (1987). Dimensions of thought flow in everyday life. Imagination, Cognition and Personality, 7(2), 105-128.

Langley, P., Magnani, L., Schunn, C., & Thagard, P. (2005). An extended theory of human problem solving. In Proceedings of the Annual Meeting of the Cognitive Science Society (Vol. 27, No. 27).

Lewis, C. (1981). Skill in algebra. In J. R. Anderson (Ed.), Cognitive Skills and their Acquisition. Hillsdale, NJ: Lawrence Erlbaum

Mitchell, M. B., Cimino, C. R., Benitez, A., Brown, C. L., Gibbons, L. E., Kennison, R. F., ... & Lindwall, M. (2012). Cognitively stimulating activities: effects on cognition across four studies with up to 21 years of longitudinal data. Journal of aging research, 2012.

Newell A, Rosenbloom P. 1981. Mechanisms of skill acquisition and the law of practice. In Cognitive Skills and Their Acquisition, ed. JR Anderson, pp. 1–56. Hillsdale, NJ:Erlbaum

References

Newell, A. (1980). Reasoning, problem-solving, and decision processes: The problem space as a fundamental category. In R. Nickerson (Ed.). Attention and performance VIII (pp. 693-718). Hillsdale. NJ: Erlbaum

Nickerson, R. S. (2011). Five down, Absquatulated: Crossword puzzle clues to how the mind works. Psychonomic bulletin & review, 18(2), 217-241.

Papert, S. (1980). Mindstorms: Children, Computers and Powerful Ideas.. New York, NY: Basic Books.

Pepicelloo, W. J., & Green T. A. (1984). The Language of Riddles New Perspectives. Columbus: Ohio State University Press

Shultz, R. T. (1974). Development of the Appreciation of Riddles. Child Development, 45(1), 100-105. http://www.jstor.org/stable/1127755.6/1/12

VanLehn, K. (1988). Problem solving and cognitive skill acquisition (No. AIP-32). CARNEGIE-MELLON UNIV PITTSBURGH PA ARTIFICIAL INTELLIGENCE AND PSYCHOLOGY PROJECT.

VanLehn, K. (1996) Cognitive skill acquisition. Annual review of psychology 47, no. 1: 513-539.

Wang, H. X., Xu, W., & Pei, J. J. (2012). Leisure activities, cognition and dementia. Biochimica et Biophysica Acta (BBA)-Molecular Basis of Disease, 1822(3), 482-491.

Witkins, H.A., Oltman, P., Raskin, E. and Karp, S. (1971), A Manual for the Embedded Figures Test, Consulting Psychologists Press, Palo Alto, CA.

Wixey, M. (2017). SandGrox: Detecting and bypassing sandboxes. Proceedings of CRESTCon 2017. youtube.com/watch?v=VnlL3lKX5p8

Zhao, Qingbai, Zhijin Zhou, Haibo Xu, Shi Chen, Fang Xu, Wenliang Fan, and Lei Han. "Dynamic neural network of insight: a functional magnetic resonance imaging study on solving Chinese 'chengyu' riddles." PloS one 8, no. 3 (2013).

Get in touch!

@darkartlab
matt.wixey@pwc.com

pwc.com