Lecture 4: psychology

Social Engineering (II909)

Kaido Kikkas

A word of caution

- This branch of psychology seems to be notoriously riddled with controversies and contradictions
- What is a solid theory for some, can be considered pseudoscience by others (e.g. neurolinguistic programming)
- Note: the phenomena and practical applications (incl. in social engineering) are not really disputed, scientific classification and explanations are
- Thus, read, think and decide by yourselves!

Cognitive biases

- There are bugs in human hardware - and some of them exist in animals as well
- See a list at https://en.wikipedia.org/wiki/List_of_cognitive_biases (a very good overview) and a diagram with links at https://upload.wikimedia.org/wikipedia/commons/6/65/Cognitive_bias_codex_en.svg (again, this is ONE possible interpretation!)
- Most of them can be – and are - used in social engineering!

Some examples: decision-making

- Bandwagon thinking (aka groupthink or herd mindset)
- Courtesy bias (aka political correctness / SJW; not offending anyone prevails honesty and truth)
- Curse of knowledge (aka ivory tower; difficulty in understanding 'lesser folks')
- Gambler's fallacy (connecting probabilities of unrelated events; "Heads vs tails")
- IKEA effect (aka "made with my own hands" giving intrinsic value – inflation of participation)
- ...

Examples: social biases

- Authority bias (aka “experts have said that”)
- Forer/Barnum effect (aka “this is exactly about me” - taking well-crafted generic information – e.g. horoscopes – as being personalized)
- Halo effect (aka “she is a good actor, let’s vote for her”)
- Just world hypothesis (aka “karma is a bitch” or “he must have deserved it!”)
- System justification / status quo effect (aka “do not rock the boat!”)
- ...

Examples: memory errors/biases

- Bizarreness effect (aka “can’t forget something that crazy!”)
- Cross-race effect (aka “The Chinese are all alike”)
- Hindsight bias (aka “I knew that all along!”)
- Picture superiority effect (aka “a picture is worth 1000 words”)
- Rosy retrospection (aka “the grass was greener then”)
- Suggestibility (aka “thanks for reminding, I remember that now”)
- ...

Rapport?

- The state of ‘clicking’ with another person
- Feeling ‘sync’, kinship, alikeness
- Some ways of building:
  - Coordination/mirroring
    - Emotional (“I am on your side”)
    - Posture (matching body language)
    - Voice (tone and tempo)
  - Attentiveness (showing connection, e.g. nodding)
  - Commonality (references to common interests etc)

Modes of thinking

- Sight/visual
  - Scenery, light/size/colour/movement, appeal
- Hearing/auditory
  - Sounds, volume/tone/pitch/tempo, wording
- Feeling/kinesthetic
  - Sensation, texture/temperature/weight, emotion

- Also reflects vocabulary (e.g. “I see” vs “sounds OK”)

Microexpressions

- Short-time, involuntary facial expressions (vs macroexpressions – longer, voluntary, can be faked)
- As defined by Paul Ekman:
  - Anger
  - Disgust
  - Fear
  - Joy
  - Sadness
  - Surprise
  - Contempt (added later)

Usage in SE: reorder the building blocks

- Experienced ‘engineers’ learn to use ‘natural’ microexpressions by adding hints of other feelings to them and/or provide alternate interpretation
- e.g. fear stemming from the actual risky mission can be re-interpreted in the context of pretext (“I need this document from the USB drive, or I’ll be fired!”)

Usage in detecting deception

- Contradictions – looking for related MEs in case of changing statements (“He is not there. OK, I will check.”)
- Hesitation – check for MEs at delayed replies
- Changing behaviour – check for MEs (e.g. the person starts looking around)
- Hand gestures – check for MEs during them (e.g. the person touching his/her face)

- Caution: MEs convey the emotion but not its cause!

Neurolinguistic programming

- Richard Bandler and John Grinder (1970s)
- A theory about connecting neurological processes to language and behaviour
- Various aspects and offshoots exist, some of them heavily contested
- Yet, the main point of social engineering – using language to activate some “bugs” in human mind to achieve desired behaviour – is close enough

The Voice

- (Not just the Jedi and Bene Gesserit ;))
- Playing with the tone:
  - "Don't you agree?" (▲) vs "Don't you agree?" (▼)
- NLP suggests using lower tone for subconscious commands:
  - "Remember how clean your room looked last Christmas?" (also refers to a pleasant memory)
- NB! Sentences must be well-crafted

Gestures and posture

- Can be a powerful boost to speech
- Cultural differences!
- Anchoring: repeated use of certain gestures in certain contexts (e.g. Churchill's famous use of "V", but also using right hand for good things, left for bad)
- Mirroring: using similar (but not same) body language
- Placement of hands:
  - Elbows: kept against body in danger
  - Hands: look for subconscious movements

Listening

- Pay attention
- Prove that you listen
- Give feedback
- Don’t interrupt (unless really needed)
- Respond the right way
- React to the message, not to the person

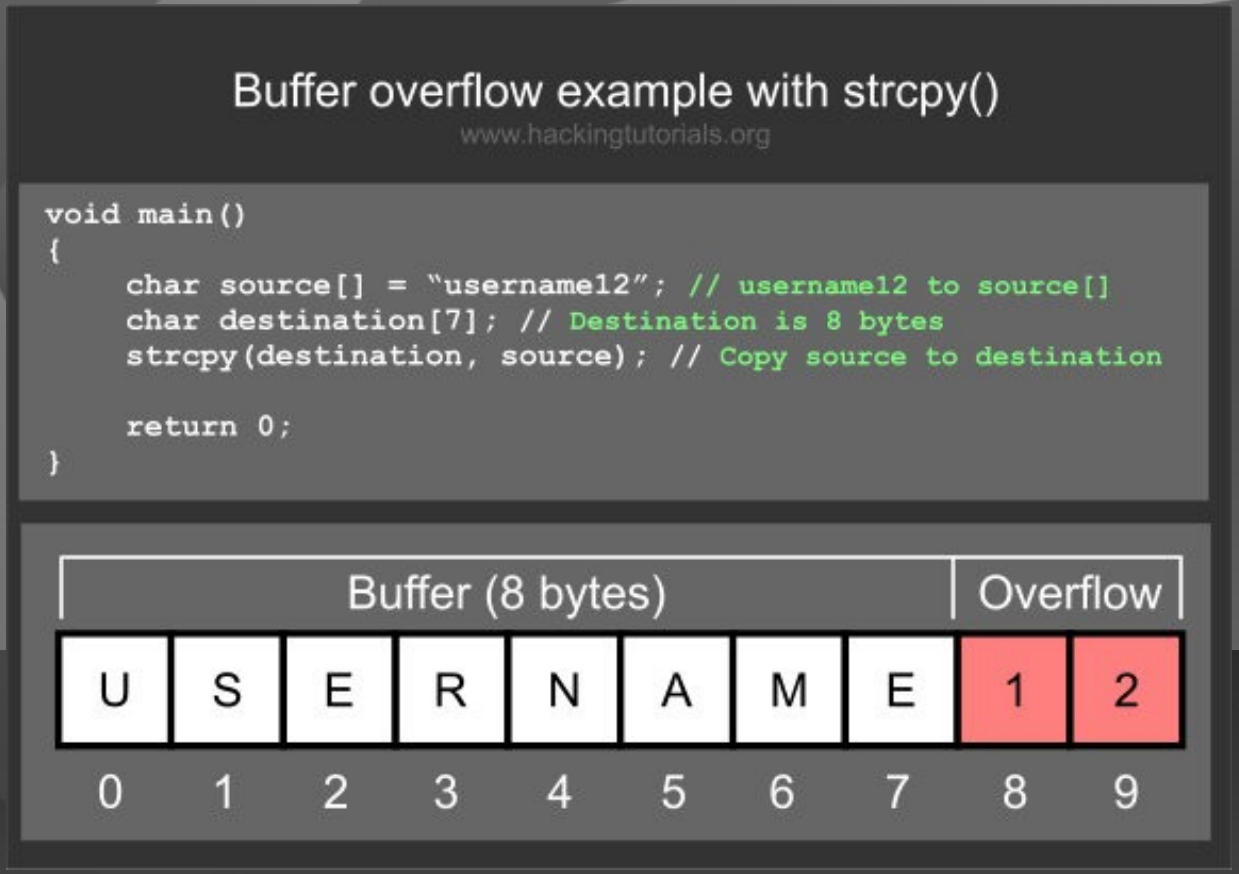
- Active listening + reflective responding (rephrasing, softening phrases “Seems like”, “Sounds that”)

...

- Empathy!
- Well-rounded general knowledge – plus some more in the field of chosen pretext
- Be curious (without being intrusive)
- Strive to meet people's needs (whether according to Maslow, Glasser, Torvalds/Wozniak or anyone else)

Crack the person

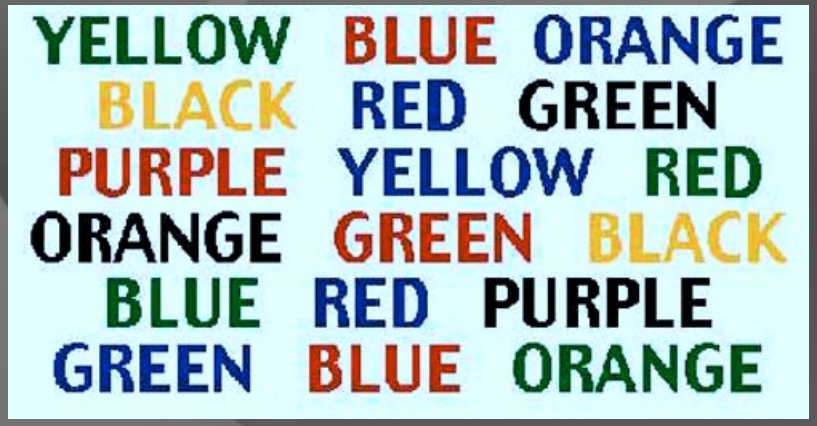
- Buffer overflows in programming:



https://www.hackingtutorials.org/exploit-tutorials/buffer-overflow-explained-basics/

...

- Similar things can happen with humans
- An example from Hadnagy's book:



- Try to say the ACTUAL colours of all words (NOT the colour that is written – i.e. the first one is "green"), the faster the better!

Fuzzing

- Again similar to a cracking technique using large amounts of random input
- The Law of Expectations – people tend to act as expected of them
- “Do you know my next door neighbor Ralph, always drives a green Ford Escort?”
- Ample information, yet the real question is “Do you know?”

Shell code for human OS

- Commands embedded in mental padding
- “Tom, I see you are heading to the kitchen, will you get me a cup of coffee with 2 creams please?”
- Main principles:
  - Short commands in longer sentences (padding)
  - Slightly emphasized within sentence
  - Suitable body language and mimics

Some more options

- Storytelling/parables (directing the target to think in a certain way)
- Negation (embedded command + forbidden fruit as an additional incentive)
- Engaging imagination ("Do not think about flying spaghetti" - first the brain has to form the concept, making it necessary to think before not thinking)

Conclusion

- There are some loopholes in human brain
- Social engineers have known many techniques long before researchers
- Most controversies are about theory and interpretation rather than the phenomenon itself
- Learning some of the concepts with a defensive angle in mind can help to avoid some attacks

Thanks!

- Next time, we go on with influence