Social Engineering

Lecture 4: Pretexting

Kaido Kikkas

Wiktionary says:

- Etymology

  From French *prétexte*, from Latin *praetextum* ("an ornament, etc., wrought in front, a pretense")

- pretext (plural pretexts): A false, contrived, or assumed purpose or reason; a pretense
  - Example: The reporter called the company on the pretext of trying to resolve a consumer complaint

Different aspects

- Warfare: (typically fabricated) excuse to interfere:
  - WWII: Westerplatte (Poland), Mainila (Finland)
  - WMD in Iraq
  - Ukraine
- Legislation: false reasons for legal action, e.g. pretextual arrest – arrest first, search later
- Information security: creating and using an invented scenario to increase the chance that the victim will divulge information or perform actions unlikely in ordinary circumstances

Recap from last week

- The Matron: “Every human being is a puzzle of need. Learn to be the missing piece and they will give you anything”
- The Frame:
  - Bridging (match the expectation)
  - Amplification (show that you actually match and then some more)
  - Extension (add new aspects)
  - Transformation (reframing/redefinition)

https://www.imdb.com/title/tt2873282/mediaviewer/rm1242911744/?ref_=tt_md_2

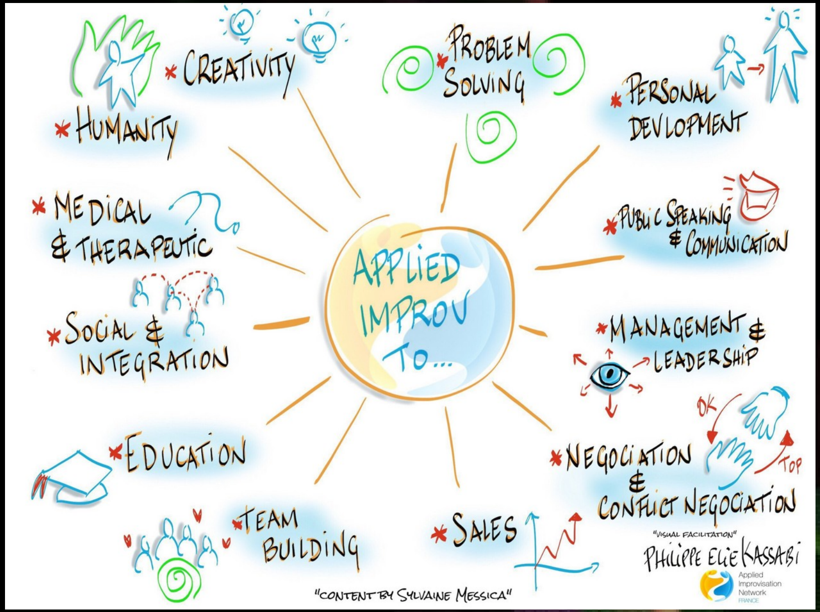
Hugo Weaving: the opposites

https://en.wikipedia.org/wiki/Elrond#/media/File:Elrond11.jpg

https://en.wikipedia.org/wiki/Agent_Smith#/media/File:Agent_Smith_(The_Matrix_series_character).jpg

Excursus: improv

- Improvisational theatre: a form of cooperative theatre where there is no fixed script/scenario, and the line between the actors and the audience is blurred or gone
- Applied improvisation: using the same techniques in business or other setting (education, therapy…)
- Internet history knows MUSE/MUSH/MUX environments – essentially a MUD for improv



https://en.wikipedia.org/wiki/Applied_improvisation#/media/File:Applied_Improvisation_-_Apllied_Improv_to.jpg

…

- Main principles of improv
  - Trust: players should trust each other
  - Acceptance: “yes, and…” or a) accept the idea/person, and b) contribute something in turn (essentially, brainstorming)
  - Attentive listening: awareness and understanding of other players
  - Spontaneity: collective creation ‘in the moment’
  - Storytelling: developing a narrative (story) together
  - Nonverbal communication: face and body language
  - Warm-ups: techniques to create rapport and achieve the mindset needed for improvisation
    - https://www.researchgate.net/publication/238623530_Whose_Classroom_Is_It_Anyway_Improvisation_as_a_Teaching_Tool

Discussion break

- Think about the principles of improv mentioned above – how can they be applied to a social engineering setting?
- Are there any notable differences (things done differently in SE)?

Two important parts

- A pretext should include
  - Situation – a plausible, believable description of what has happened and why the targeted person needs to act in a certain way
  - Character – the persona through whom the situation is brought to the targeted person. May be a victim, but also a bystander - or even an adversary!

Mimicry

- … in nature:
  - zoomimesis (look like someone nasty)
  - phytomimesis (look like a plant/tree)
  - allomimesis (look like an object)


- … in pretexting, quite the same:
  - look like someone nasty
  - look like a plant (i.e. not equal)
  - look like an object (i.e. belonging to the background)




Pictures: Wikimedia Commons

A well-known case

© Peter Steiner, The New Yorker 1993

Character creation (impersonation)

- What would this individual wear?
- How presentable would he/she be?
- Would the person carry any specific type of equipment?
- What kind of accent is he/she likely to have?
- How well-spoken would he/she be?
- What sort of vocabulary would the person use?
- What kind of body language would this person present?
- What skills would he/she have?
  - *Social Engineering Penetration Testing* by Gavin Watson et al

Some main principles (Hadnagy 2018)

- Think through your goals (the first idea may be not the best one)
- Understand reality vs fiction (e.g. social media picture vs actual situation)
- Know how far to go (the 4 questions; keeping the focus; don’t be greedy)
- Avoid short-term memory loss (cannot use memory aids!)
- Get support for pretexting (prepare for the role – tools, props, knowledge)
- Execute the pretext (without a script!)

- NB! In case of more complex attack (several different pretexts for different steps), a ‘safe haven’ can help (relatively safe area for regrouping and mental preparation for the next step/role, e.g. a cafeteria); changing outfits can be done in e.g. toilets/bathrooms)

More points (Hadnagy 2011)

- The more research you do, the better the chance of success
- Involving your own personal interests will increase success
- Practice dialects or expressions
- Many times social engineering effort can be reduced if the phone is viewed as less important. But as a social engineer, using the phone should not reduce the effort put into the social engineering gig
- The simpler the pretext, the better the chance of success
- The pretext should appear spontaneous
- Provide a logical conclusion or follow through for the target

And yet some more

- Hadnagy 2011:
  - Try to forget your own feelings (excitement, anxiety, fear…)
  - Don’t take yourself too seriously
  - Get out of your head and into the world (or, learn to identify what is important/relevant)
  - Seek experience (less unexpected situations)

Discussion break

- Think of a scenario where you will have to sneak some (suspicious) software into your boss’ desktop computer in his/her office. What would be the suitable pretext?
  - Plausible situation
  - Character

Note: technology

- Technology-heavy pretexts (technician, sysadmin etc):
  - Need more preparation (must be reasonably able to use the tech and talk the talk!)
  - Come with an authority bonus (“Put that USB stick in – we need NVIDIA version 3.4.0 drivers!”)...
  - ... that may also backfire (“the last guy was way nicer!”)
  - often used for either technological (baiting, planting, local phishing) or environment/access-gaining (tailgating, shoulder surfing, dumpster diving, some types of mimicry) attacks, sometimes also for elicitation (authority bonus!)

Note: disasters and emotions

- Aftermath of large-scale disasters (9/11, New Orleans, Fukushima etc) gives ample possibilities to create both plausible situations and characters; likewise do accidents with celebrities
- Proven, documented (and emotional!) events mixed with fictional situations and characters (ct “Based on a true story” in movies!)
- Rapport through common suffering (evident in many cases, e.g. survivors of concentration camps, shipwrecks and plane crashes, natural disasters)

Note: (ab)using the taboos

- Saved by the ladies' room (Alistair MacLean, *Where Eagles Dare*)
- Rather many modern (corporate) policies contain Political Correctness and related taboos:
  - Never ask one's gender over the phone (a male can use a female pretext!). In the more recent times, this can be expanded further
  - Never talk about some issues (or vice versa - a quick way out of the conversation: "Are you for Trump, too?", "Are you saved?"...)
  - Be especially sensitive (read: do not poke too much!) with minorities
  - https://www.researchgate.net/publication/353432841_POLITICAL_CORRECTNESS_IN_BUSINESS_COMMUNICATION

Note: let them come

- Advanced-level pretexting (aka reverse social engineering)
- The persona and scenario are chosen so that the victim will contact the attacker (rather than vice versa)
- May need preliminary steps (e.g. baiting with ‘accidentally dropped’ USB sticks that contain some interesting data, including phone numbers and/or e-mails)
- Can validate the pretext stronger than with direct pretexting (“Hey, I am NOT an idiot! So, he really has to be that person!”)
- Can also involve multi-person attacks (bad cop, good cop) or the Introduction – Sabotage – Assist approach

Short vs long game

- Different approaches for different tasks
- Short: tactical, limited timeframe, one-time (burning may be OK):
  - reset password
  - phone survey
  - e-mail phishing
- Long: strategic, can be multi-part, different episodes with different pretexts - much more attention on character development and background study
  - Example: journalist Ryan Parry – successfully infiltrated the Buckingham Palace in 2003 (https://www.mirror.co.uk/news/real-life-stories/buckingham-palace-queen-tupperware-philip-13663437)

Excursus: online training grounds

- More specific:
  - Old-school MUSHes (as mentioned earlier; the MUDs, or text-based environments, which focus strictly on roleplay – as opposed to hack'n'slash)
  - Second Life and its descendants (OpenSimulator etc)
- General:
  - chatrooms/talkers
  - generic MMORPGs (WoW etc)
  - social media (we have to invent something for that...)

Summing up

- Pretexting is the art of being there for a reason without raising suspicion (character/impersonation), as well as eliciting information ‘by being there’ (situation/story)
- Some overlap with applied improvisation
- Can be part of short (tactical) or long (strategic) game
- Next week: some human psychology

Thanks