Topic 3: pretexting

Social Engineering (II909)

Kaido Kikkas

Motto (sort of)

- “The first basic law of human stupidity:

  Always and inevitably everyone underestimates the number of stupid individuals in circulation”

  – *The Basic Laws of Human Stupidity* by Carlo M. Cipolla

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, an excuse to interfere:
  - WWII: Westerplatte (Poland) and maybe Pearl Harbor
  - WMD in Iraq
- 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

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 adversary!

A case of pretexting

Creating a character: impersonation

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

More points by Hadnagy

- 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

– *Social Engineering: The Art of Human Hacking*

Watch out for those emotions

- A major tactic used by nastier people
- Aftermath of large-scale disasters (9/11, Fukushima etc) gives ample possibilities to create both plausible situations and characters
- Likewise do deaths of celebrities

Being spontaneous

- Christopher Hadnagy has the following pointers:
  - 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)

Short game vs long game

- Different approaches for different tasks
  - Short: tactical, one-time
    - reset password
    - phone survey
    - e-mail phishing
  - Long: strategical, can be multi-part, different episodes with different pretexts, much more attention on character development and background study

Example: Stanley Mark Rifkin

- A computer consultant at Security Pacific National Bank in Los Angeles in October 1978
- Wire transfer room had the daily transfer code… posted on the wall, easy to memorize
- A bit later, supposedly a local employee Mike Hansen called, ordering a transfer of 10.2 mln USD to a bank account in New York
- Contacted a diamond dealer in LA and negotiated a purchase of diamonds from Rosalmaz in Geneva (about $8 000, 43,200 carats)

...

- Smuggled back to the US, sold some but was turned in by 3rd buyer
- Full story at https://www.social-engineer.org/wiki/archives/Hackers/hackers-Mark-Rifkin-Social-Engineer-furtherInfo.htm
- Read other case studies at social-engineer.org too!

Example: Hadnagy at airport

- Christopher Hadnagy recounts a story in his book
- He took a flight to another city and had forgotten a full set of cracking tools (including lockpicks and RFID scannner) in his bag
- Stopped by security and asked about his stuff
- All he had to do was to show a business card and say “I’m a security professional”
- After that, he deliberately repeated it five times

A little exercise

- Task: install some software into your boss' desktop computer in his/her office
- Everything should be left intact and working

- What would be the suitable pretext? I.e.
  - Plausible situation
  - Character

Thanks!

- Next time, some psychology behind SE