Topic 1: SE intro / information gathering

Social Engineering (II909)

Kaido Kikkas

Different understandings

- Actually different concepts in different disciplines:
  - **Social sciences:** a scientific/philosophical approach to influencing large social processes and groups of people (alike to what education does to individuals). As such, a positive (kind of) term, but borders with propaganda and media manipulation
  - **Infosec:** manipulations with people (to cause certain actions or acquire restricted information). Typically a multi-step approach, often combined with more technical methods

Starting point

- This course treats SE as another method of breaching information security defenses
- An important component in the Mitnick formula about security:
  - Technology
  - Training
  - Policy
- Note: SE attacks can target all three

Examples from earlier times

- Many stories from the Bible (Adam & Eve, Jesus vs the Pharisees etc)
- The original Trojan Horse
- Carlo (Charles) Ponzi – Boston, around 1920
- Victor Lustig – Eiffel Tower 1925
- Frank Abagnale Jr – globally, around 1965
- …

From the IT era

- Stanley Mark Rifkin 1978
- Mark Abene (Phiber Optik) 80s
- Kevin Mitnick
- Susan Headley (Suzy Thunder)
- Kevin Poulsen (Dark Dante)
- ...

Techniques

- Generic:
  - Pretexting
  - Quid pro quo
  - Time pressure
  - Stress the position
  - Poor thing
  - Praise the fool, the fool will jump
- Tech:
  - Phishing
  - Vishing
  - Baiting
  - Waterholing

Techniques 2

- Tactical:
  - Shoulder surfing
  - Dumpster diving
  - Tailgating
  - Mimicry
- More on these things in a later lecture!

Robert Cialdini's six principles

- In *Influence: The Psychology of Persuasion* (1984):
  - **Reciprocity** – people reply in kind (and are nice)
  - **Commitment/consistence** – people stick to things they believe in, even if the incentive disappears
  - **Social proof** – people do what they see others doing

...

Authority – people obey authorities, even if they do questionable/evil things

- **Liking** – people do the bidding of likable people
- **Scarcity** - “rare/expensive stuff cannot be bad”

- (more of this stuff will come in Lecture 4)

3 x 5

- *Ninja Hacking* by Thomas Wilhelm and Jason Andress:
  - **Five Elements** (earth, water, fire, wind and void), each tied to a personality type (in terms of exploitability)
  - **Five Weaknesses** (same elements) – laziness, anger, fear, sympathy and vanity
  - **Five Needs** – security, sex, wealth, pride and pleasure

Information gathering

- A common model in SE:
  - Use different (mostly legal) channels to create pretext/context – without burning the source
  - Create an attack vessel (e.g. identity suitable for the task)
  - As a result, obtain more information
  - Rinse and repeat (possibly in another setting, using the recently acquired information)
- Thus, the initial step is of great importance!

Trust building

- Trust is a major currency in SE
- Various aspects in building trust include
  - Personality
  - Background (incl. education, culture etc)
  - Common experiences
  - …
- Today, a major source of relevant information is social media (“Networks of trust”)

Other sources

- Websites
- Google! (site:victim.com filetype:pdf etc)
- Shodan (https://www.shodan.io/)
- Libraries and “old media”
- Direct observation
- Dumpster diving
- Profiling software and services

Hadnagy's points for communication

- From *Social Engineering: The Art of Human Hacking*:
  - Never take for granted that the receiver has the same reality as you
  - Never take for granted that the receiver will interpret the message the way it was intended
  - Communication is not an absolute, finite thing
  - Always assume as many different realities exist as there are different people involved in the communication

Communication models

- Various exist
- Main components:
  - Source
  - Channel
  - Message
  - Receiver/Target
  - Feedback/Result
- A 5-minute exercise: based on the components above, design a phishing message to a retired male ex-businessman

To be continued...

- ...with elicitation (next week)