Social Engineering

Lecture 1: Course introduction +
some main concepts of SE

Kaido Kikkas

Motto (sort of):

- YOU ONLY HAVE TO ASK

  Activate the wealth corner of any
  crowded room by standing in it with
  a large kitchen knife and a sign that reads
  GIVE ME ALL YOUR MONEY.

  - Master Eu Plon Ka, in “The Little Book of Wrong Shui”

A little more seriously...

- PIBKAC/PEBKAC/EBKAC – the weakest link in an information system is often the human
- Many today's cyberattacks contain a social component (can have lower costs and risks, yet significant payout)
- One of the basic tenets of cybersecurity is to know one's enemies and their ways
- Important: remain on the Light side of the Force

The course

- Has in a similar form run once back in 2018, the current incarnation is the second run of the new version
- The course can be run both as a contact and an e-course – we will do the latter due to a number of EuroTEQ (distance) participants
- Note: lecturers are also still learners of the art – so one of the main points is to learn something useful together!

Chief engineers

- Kaido Kikkas (lectures, CotW seminars)

Source: https://opleht.ee/2022/02/zoomile-ei-pogus-pilguheit-distantsoppe-metoodikale/

- Kristjan Karmo (Hands-On seminars)

Source: https://www.asaquality.ee/akadeemia/koolitajad/

Course organization

- Social Engineering, university course code ICS0018
- Full synchronous e-course (due to participants from the distance)
- Total duration: 8 weeks (first half-term)
- Grading: pass/fail
- Starts with weekly lectures (which include a discussion component as well) by Kaido
- Four last weeks will add seminars - CotW seminars by Kaido, Hands-On seminars by Kristjan

Tools

- The university’s MS Teams (for contact events, i.e. lectures and seminars), needs logging in with the Uni-ID
- Course website at the IT College wiki: https://wiki.itcollege.ee/index.php/Social_Engineering (can also be reached from the wiki front page via “Sotsiaalmanipulatsioon”, or via the link https://akadeemia.kakupesa.net/SocEng .
- Wiki is free to read for everyone, editing (not required for the course, but can be done) needs logging in with the Uni-ID
- Visiting students (EuroTEQ) should have received their Uni-ID’s by now – if not, please let me know!

Syllabus (lectures)

- The main source for lectures: *Social Engineering* by Christopher Hadnagy (1. and 2. edition)
- Secondary sources include Kevin Mitnick, Johnny Long, Robert Cialdini, Jason Andress, Ben McCarty and several others

- Information gathering
- Elicitation
- Pretexting
- Psychological principles
- Influence and persuasion
- A sidestep to history (plus some tools)
- Prevention, mitigation and counters

Lectures

- The typical 1.5 hour time will be split into several shorter lecture parts with discussion time in between (a SE trick against napping during lectures...)
- We will have online sessions with a large enough number of participants – discussions will be held in written form (MS Teams chat) and deal with the topic of the day
- NB! We will not record any video in Teams, but the slides will be available on the website – and the chat history remains available during the course
- Chat will be open throughout the lectures, so typing a question/remark during the lecture part is OK, but it will be answered during the next discussion break (Kaido is not that good in multitasking yet)!
- NB! One of the criteria for passing is also **participation** – showing up in the chat is perhaps the easiest way to prove that ‘hey, I’m here!’

Hands-On (practical) seminars

- Held by Kristjan in the last four weeks
- Practical online tasks (Kristjan will join and tell you a bit about those next time on Feb 8!)
- The way to pass the course for the majority of students (for an alternative, see the next slide)
- Participation check!

CotW seminars

- Held by Kaido (Kristjan could attend sometimes, too) in the last four weeks
- Each will have up to three student presentations (~20 minutes) about a Crook of the Week (see the course website) followed by discussion (~10 minutes each):
  - short biography
  - motivation
  - main ways of SE
  - human weaknesses addressed the most
- An alternate way to pass the course (plus required attendance)
- Only 12 possible presentations => first come, first served! The rest will have to do the practical tasks
- Participation check!

Course schedule

- Lectures: On Thursdays at 10.00 Tallinn time (NB! CET + 1!), from February 1 to March 21 (8 times)
- Hands-On seminars: On Wednesdays at 08.15 Tallinn time, from February 28 to March 20 (4 times)
- CotW seminars: On Thursdays at noon (12.00) Tallinn time, from February 29(!) to March 21 (4 times)

Passing requirements (summed up)

- Either
  - A presentation at a CotW seminar
- or
  - Completing the tasks given at the practical seminars
- Plus
  - Attending 5 lectures and 5 seminars (each out of 8)

- NB! Means that some missed lectures/seminars will result in loss of information, but do not actually prevent passing the course!

Ideas/recommendations?

- The general framework and materials of the course are set (the university needs the formal programme etc), specific subtopics and smaller things can be adjusted to suit the audience – e.g. more case studies, psychology, specific techniques etc
- Let us know!

Contact

- Kaido:
  - kakk@kakupesa.net (other e-mail will redirect to it)
  - ICO-524 (up the stairs from the 4th floor, ring the bell)
  - If necessary, GSM +372 50 64 464 (but writing is preferred, as it leaves a footprint!)
- Kristjan:
  - kristjan.karmo@taltech.ee

Discussion break

- Anything that remained unclear about the course?
- Recommendations/ideas?

Social engineering: the term

- 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: manipulating people to cause certain actions or acquire restricted information. Typically a multi-step approach (e.g. pretext => small details => trust => actual target), often combined with more technical methods

A starting point

- This course treats SE as another method of breaching information security defenses
- An important component in the Mitnick's formula about security (we will come back to this later on):
  - Technology
  - Training
  - Policy
- Note: SE attacks can target all three

SE: art vs science

- The books by Christopher Hadnagy:
  - 2011: Social Engineering: The Art of Human Hacking
  - 2018: Social Engineering: The Science of Human Hacking
- Subjective or objective?
  - Many principles overlap with applied psychology and other disciplines
  - Instrumentalist vs virtuoso

Really old

- Look at
  - Folk stories and fairytales
  - Epics (from *The Iliad* to *Ramayana*)
  - Scriptures of various faiths
  - Historical records
- The actual examples are better to be left for the CotW seminars!

Techniques: a brief overview

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

Techniques: a brief overview 2

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

Discussion break

- Would you consider Mitnick's formula (tech, training, policy) valid?
- Would you think of SE as more an art or a science? Why?
- Did anything come to your mind right away about
  - literary and/or historical examples?
  - techniques of SE listed above?
- Do you have personal experience with any of the SE techniques listed above?

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"
- NB! More of this stuff will be in later lectures

3 x 5

- In *Ninja Hacking* (2010) 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
- Again, we'll return here later as well

Discussion break

- Bring an example of one of the Cialdini’s six principles
- Leaving aside the mysticism in the Five Elements, would the Five Weaknesses and Needs be still applicable? Would you drop or add anything?

Summing up for today

- SE is a multi-faceted discipline in many ways
- One can learn the moves… or master the art
- There are plenty of interesting examples to learn from

- Next week: information gathering

Thanks!