Social Engineering

Lecture 2: Information gathering

Kaido Kikkas

Intro

- 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!

An example from Hadnagy's book

- A penetration tester had to test a company with very little online presence
- Found a top manager in a postage stamp forum, using corporate e-mail address
- Looked for old stamp pictures online, created a website (with an exploit for Internet Explorer in a frame – it happened a while ago)
- Contacted the manager, told a story of inheriting some stamps
- Hijacked the manager's PC using the exploit

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”)

Sources

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

Websites

- Among other things:
  - Contacts/staff
  - Main profile
  - Physical locations
  - Open jobs (pretext!)
  - Some personal information of key people (biographies)
  - Pictures of premises (sometimes)
  - Dress code and corporate style (formal vs relaxed, etc)
  - Some corporate personal profiles link to more personal stuff

Social media

- All the above, plus
  - Networking (six degrees of separation!)
  - Relationships
  - FOMO
  - Important: networks of trust
- Generic social media (FB/Meta, Instagram) vs more specific (LinkedIn, Flickr, SlideShare, AO3, DeviantArt, SoundCloud…) - note: created material can tell a lot about the person!
- Twitter/X and other ‘shorties’ – watch out for ‘fingers move ahead of brain’! A (quite old by now) example www.social-engineer.org/wiki/archives/BlogPosts/TwitterHomeRobbery.html
- There are also shadier networks (just the presence there will count!)

Social media: the power

- Examples from Hadnagy 2018
- LinkedIn:
  - Your job history
  - Where you got your education from
  - Where you went to high school
  - Clubs and academic achievements you’re involved in
  - People who endorse your skills
- Facebook/Meta:
  - Your favorite music
  - Your favorite movies
  - Clubs you belong to
  - Your friends
  - Your family
  - Vacations you’ve taken
  - Your favorite foods
  - Places you’ve lived at
  - Much, much more
- Twitter/X:
  - What you are doing right now
  - Your eating habits
  - Your geolocation
  - Your emotional state (within 280 characters)

Discussion break

- Personality, background and common experiences were named above as trust-building aspects. Can you find some more?
- Suggest a persona (fictional but realistic human profile) and find the best ‘personal information hunting ground’ for this persona among common social media services

Google

- Simple search may do (but in this case, use other engines like Duckduckgo as well)
- Google hacking/dorking:
  - https://www.googleguide.com/advanced_operators_reference.html (updated in early 2022)
  - https://www.exploit-db.com/google-hacking-database
  - https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf
- BEGIN (CERTIFICATE|DSA|RSA) filetype:key; robots.txt...
- May combine with local language (Google Translate)

Specialized search engines

- Shodan.io
  - a search engine for IoT and various hardware
  - Among other things, lists open ports, virtual domains, locations, sometimes people...
- CriminalIP.io
  - a search engine for IP addresses
  - Displays various kinds of cybersecurity-oriented information
- Sometimes, combining these two can provide interesting results

Whois

- Unix/Linux command or on the Web: whois.com
- More recently, somewhat reduced in efficiency (GDPR etc) – but can still find interesting information about domains (and their owners)
- Example:
  - check the expiry deadline, send a phish about extending the registration etc
  - poison the DNS (more difficult, but possible in some cases)

Old school

- Library – books and archived periodicals (often from the very beginning), plus occasional chances to SE more information
- Physical (old) media
- Can also be used to create pretexts (many newspapers have certain reader profiles, such as political affiliation)

Direct observation

- Learning the environment (entrances/exits, lifts, security)
- Learning the ways (people, dress, communication, routines)
- Being present / not raising alarm (“this guy belongs here”)
- Can also photograph/film/record (usually covertly)

Dumpster diving

- Sometimes, the trash can actually be treasure: www.social-engineer.org/wiki/archives/BlogPosts/LookWhatIFound.html
- Extremes aside, interesting things can be found (the Post-It note example)
- Sometimes, shredding is not enough
- Can also be outsourced (bribe a janitor)

Profiling tools

- Background checkers – largely an American thing, e.g. https://www.intelius.com/ ; A number of large companies, including Equifax, Dun & Bradstreet, Palantir and others
- Social media can serve in that role, too
- Some other tools: pipl.com, webmii.com, https://www.maltego.com/maltego-community/
- https://www.mayerbrown.com/files/uploads/Documents/PDFs/2016/April/A-Global-Guide-Background-Checks.pdf
- Perhaps more fitting to large-scale business intelligence, but can moonlight in this role (e.g. someone's company is already a customer of similar services)

Discussion break

- Of the methods mentioned above, how would the profile of the target influence the choice of tools?
- For some brief play-around (can go on later at home):
  - Google dorking (try some queries with e.g. filetype or inurl); https://www.googleguide.com/advanced_operators_reference.html
  - Shodan.io (e.g. try “Webcam”, “Logitech”, some domain…)
  - Webmii.com – look up yourself

Remarks on communication

- From Hadnagy 2011:
  - 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
- Read more from https://en.wikipedia.org/wiki/Models_of_communication

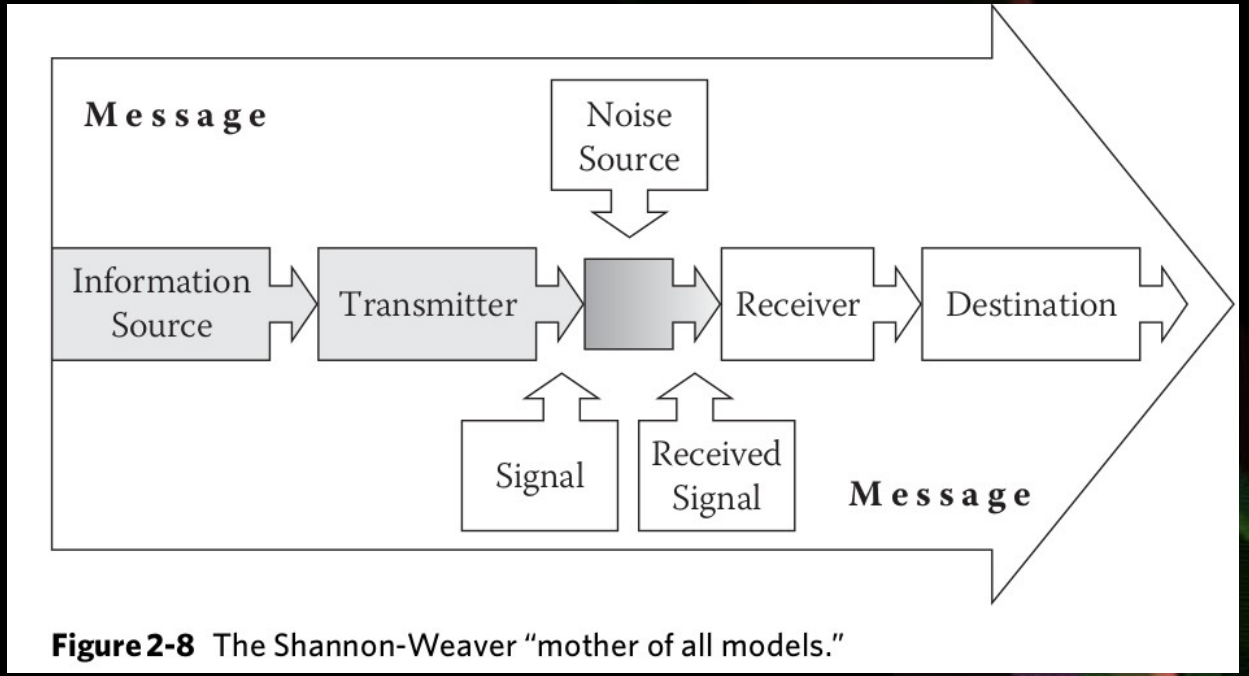


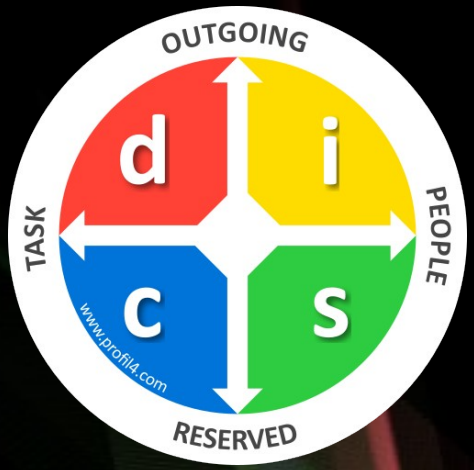
Figure 2-8 The Shannon-Weaver "mother of all models."

From Hadnagy (2011)

The crucial first seconds

- Christopher Hadnagy suggests that during the first 5-10 seconds of contact, the other person would think about four questions:
  - Who are you?
  - What do you want?
  - Are you a threat?
  - How long will this take?
- Setting the stage during that time:
  - Pretext
  - First words
  - Body language and facial expressions

DISC



https://en.wikipedia.org/wiki/DISC_assessment#/media/File:DISC_wheel.png

- William Moulton Marston 1928
- A (somewhat contested!) theory of personality:
  - D: direct/dominant
  - I: influencing
  - S: steady/supporter
  - C: conscientious/compliant
- Some keywords:
  - D - direct, results-oriented, firm, strong-willed, forceful
  - I - outgoing, enthusiastic, optimistic, high-spirited, lively
  - S - even-tempered, accommodating, patient, humble, tactful
  - C - analytical, reserved, precise, private, systematic

Horizontal vs vertical

- Horizontal: communication between peers/equals
- Vertical: communication from a position of authority
- Hadnagy's examples (2018) of different communication modes:
  - DV: Be direct and brief, set firm boundaries, answer the *what*
  - DH: Stress the *what*, focus on result, logic, facts and positions
  - IV: relaxed, let them talk, define the actions, answer the *who*
  - IH: Stress on special, give and take, no dictate, quote experts
  - SV: systematic yet friendly, answer the *why*, define what to do
  - SH: patience, focus on team, ask *how*
  - CV: details, be dependable, recognize, ask *how*
  - CH: reliability, statistics/data, facts and logic

Discussion break

- Based on the components above, design a phishing message to a retired male ex-businessman
- Define the components of the communication model in the previous example – source, channel, message, receiver and feedback
- What kind of communicator are you, according to the DISC model?

Try it out

- Spend some time in a lobby of a large building (e.g. the main hall of the university) observing:
  - Layout, entries and exits, adjoining facilities fast ways out, perimeter/surroundings
  - People (general profiles)
  - Staff (security and other)
  - …
- Play some more with the things we tried earlier (e.g. Google or Webmii)

Conclusion

- Information gathering is a gradual – and sometimes recurring – process, rather slow than fast
- Both technical and non-technical (interesting point: some overlap with the main components of the DISC model)
- Communication (and ability to adapt it) is a key component

- Next week: elicitation

Thanks