Social Engineering

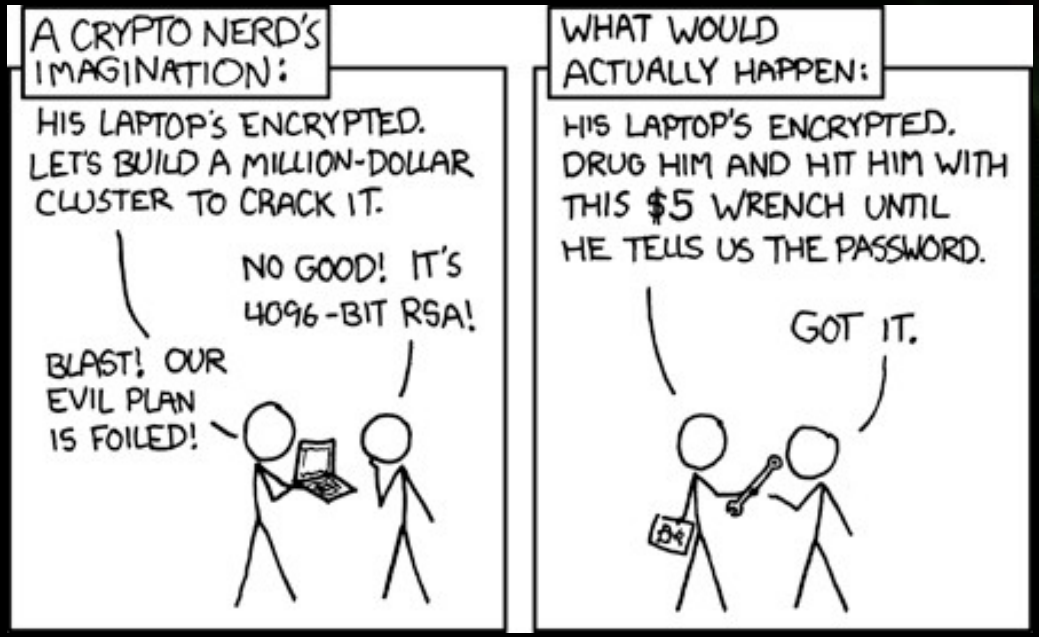
The Way of the Ninja

Kaido Kikkas

Hey, ain’t that a different art?

- The course is about social engineering…
- ...but sometimes the best result will come from combining social skills with some physical ones
  - Example: to create a pretext of an engineer at a project, one needs the project documentation – which happens to be locked into a drawer
- And some parallels are quite interesting (especially as they were around so much earlier)

Obligatory XKCD



https://xkcd.com/538/

Main sources

- *Ninja Hacking* (2011) by Thomas Wilhelm and Jason Andress
- *Cyberjutsu* (2021) by Ben McCarty (more IT-centric)
- Surprisingly good takes in adapting several aspects of medieval Japanese ninjutsu to modern times, including
  - exploitation of current events
  - disguise and impersonation
  - infiltration (timing, weak points, distraction)
  - tools (entry, concealment, covert listening)
- The [B|M]ansenshukai – an alleged ninjutsu manual used by the Imperial Army during WWII (Cummins & Miname 2013)
- Also recommended: The Art of War, Go Rin no Sho, Hagakure

Two modes

- *in-nin* (the art/person of darkness) – infiltration while unseen (darkness, underground, hiding…)
- *yo-nin* (the art/person of light) – infiltration in plain sight (disguise, pretext, mind tricks…)

- Note: parallel with ‘pure’ SE vs technical measures; in a similar way, the arts were often used together

Disguise (aka pretext)

- Once upon a time, in the Land of Rising Sun…
- *Hensōjutsu* (art of disguise), *Gisojutsu* (art of impersonation) and *Shichi ho de* (7 ways of going):
  - *akindo* (merchant or tradesman)
  - *hokashi* (musician)
  - *komuso* (itinerant priest)
  - *sarugaku* (entertainer, showman)
  - *shukke* (Buddhist monk)
  - *tsunegata* or *rōnin* (wandering samurai for hire)
  - *yamabushi* (mountain warrior ascetic)

Skills

- *Hengen kasha no jutsu* (immersion in the illusion):
  - Appearance (e.g. a businessperson with dirty fingernails?)
  - Knowledge (professional, local, personal)
  - Language (London or Manchester accent?)
  - Geography (“Which branch office were you from?”)
  - Psychology (a lot of things we have covered before)

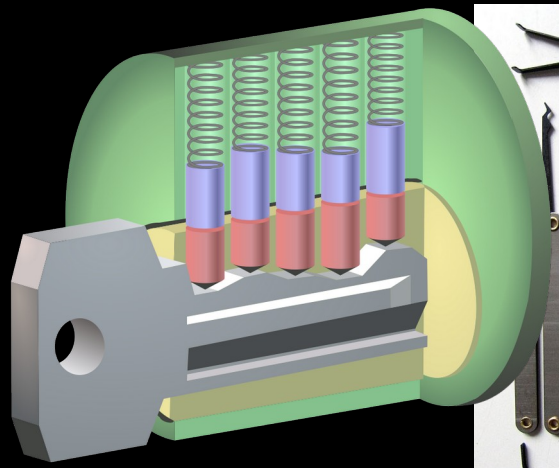
Discussion break

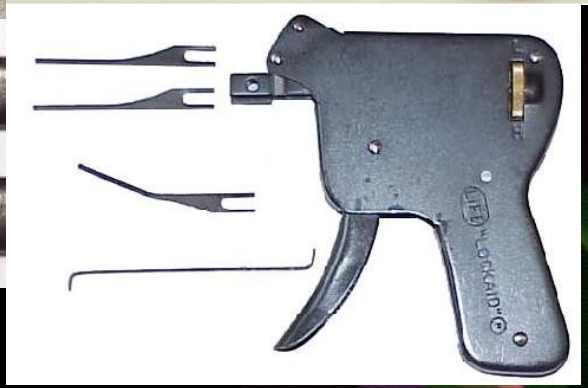
- Propose a version of the *Shichi ho de* for the modern Western society
- Prioritize the *Hengen kasha no jutsu* (illusion) skill categories for the pretexts of
  - a high-ranking government official
  - a fisherman
  - an aspiring actress (“girl next door goes to Hollywood”)
  - a pilot (think of Frank Abagnale…)

Shichi ho de in modern times: two takes

- Stephen K. Hayes:
  - Scholastic
  - Business
  - Rural
  - Religious
  - Public figures
  - Labo(u)r
  - Uniformed
- Kaido's version:
  - Professional (lawyer, doctor, businessperson)
  - Government official/clerk
  - Emergency worker (rescue/medic/police/security)
  - Media person (journalist, writer, TV host)
  - Student/intern
  - Support staff (technician, repairman, driver, janitor)
  - Delivery (courier, pizzaboy)

Infiltration: lockpicking

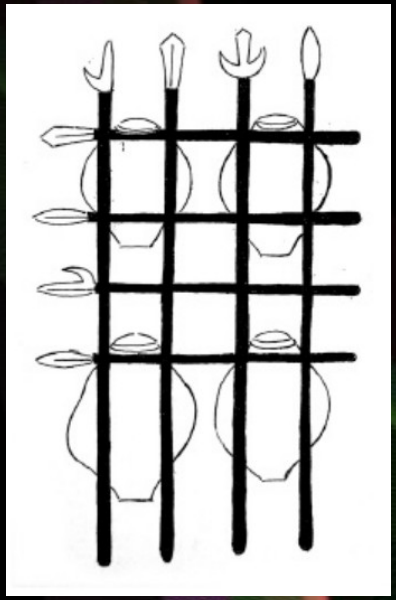




Wapcaplet, https://commons.ikimedia.org/w/index.php?curid=5466624
GeoTrinity. https://commons.wikimedia.org/w/index.php?curid=54899397
Willh26, https://commons.wikimedia.org/w/index.php?curid=47403638
Madox at Polish Wikipedia, https://commons.wikimedia.org/w/index.php?curid=2527579
Public Domain, https://en.wikipedia.org/w/index.php?curid=10881158

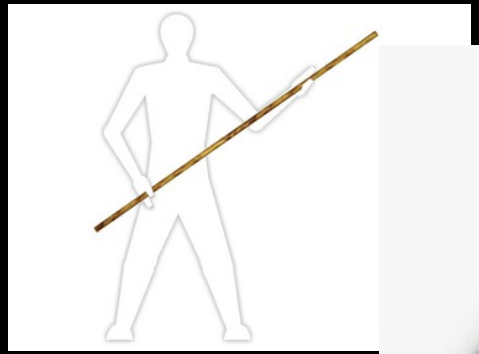
Notes on equipment

- Many tools are alarming or incriminating if spotted (e.g. lockpicks or keyrings)
- Ways to carry (in-nin vs yo-nin)
- Use of ‘innocent’ equipment
  (historical parallel: Ryukyu Kobujutsu)
- Improvization skills



A raft made of jars and pole weapons
(from the Bansenshukai)

Example from ancient times: farming tools



https://commons.wikimedia.org/wiki/File:Bo(weapon).png
https://commons.wikimedia.org/wiki/File:A_standard_sai_1.jpg
https://commons.wikimedia.org/wiki/File:Tonfas.jpg
https://commons.wikimedia.org/wiki/File:Nunchaku.JPG
https://commons.wikimedia.org/wiki/File:Kamas.jpg
https://commons.wikimedia.org/wiki/File:Tekk%C5%8D.svg
https://commons.wikimedia.org/wiki/File:Suruchin.gif
https://commons.wikimedia.org/wiki/File:Timbei%26Rochin.svg

Example from today: everyday items

https://en.wikipedia.org/wiki/Kubotan#/media/File:Ku2.JPG

http://www.themartialist.com/wp-content/uploads/2009/12/koppo2-150x150.jpg

https://www.covertproductsgroup.com/products/covert-g10-credit-card-knife

https://scotcps.org.uk/improvised-weapons/

A more extensive collection: https://info.publicintelligence.net/LA-DisguisedWeapons.pdf

Infiltration: alarms and cameras

- False positives (“the boy who cried wolf”)
- Impersonation
- *Metsubishi* (sight removing) – works on both guards and cameras; the latter can be physical (blinding) or networked (DDoS on control systems)

Infiltration: timing

- Daily routines
- Weak points in environment (slow doors)
- Maintenance times (repairs, upgrades)
- Tailgating
  - Two time-tested pretexts: smoking and fake injuries/disability
  - Also possible in cyber-forms (session hijack, logging in at high-traffic times etc)

More on timing

- Japanese hours of the day (<= Chinese zodiac):
  - Hare: 05.00 – 07.00
  - Dragon: 07.00 - 09.00
  - Snake: 09.00 – 11.00
  - Horse: 11.00 – 13.00
  - Ram: 13.00 – 15.00
  - Monkey: 15.00 – 17.00
  - Rooster: 17.00 – 19.00
  - Dog: 19.00 – 21.00
  - Boar: 21.00 – 23.00
  - Rat: 23.00 – 01.00
  - Ox: 01.00 – 03.00
  - Tiger: 03.00 – 05.00

- Some aspects:
  - Awake / sleep (Tiger!)
  - Start / End of day
  - Meals
  - Shifts
  - Service/maintenance
  - Other timed routines
  - …

- Impact to most steps of SE (from information gathering to attack and getting out)

Infiltration: weak points in infrastructure

- Dumpster diving
- Surplus/discarded hardware (what’s left inside)
- Cyber-versions: phishing, Google hacking

Infiltration: inside help

- Recruiting a *minomushi* (worm agent):
  - People with recent hard or unfair sanctions/punishments
  - Overqualified people (Peter Principle)
  - Unnoticed or poorly rewarded overachievers
  - Talented people with dumb and arrogant bosses (contempt)
  - Exploited experts (e.g. recent immigrant)
  - People torn between their job and convictions (e.g. religion)
  - Dark Triad types (disloyal and amoral)
  - People with tainted reputation (black sheep)

Discussion break

- Find examples of targets where timing of the SE attack (a specific time of day) would possibly be advantageous – where, at what time and why?
- Suggest two different cases of worm agent (insider) use – what type of person would be the best and why?

A version of ninja SE

- Five elements
  - Earth (*chi*) - stable
  - Water (*sui*) - emotional
  - Fire (*ka*) - aggressive
  - Wind (*fu*) – wise, kind
  - Void (*ku*) - creative

Five weaknesses	Five needs
laziness	security
anger	sex
fear	wealth
sympathy	pride
vanity	pleasure

Distraction

- Large events
  - holidays and festivals
  - sporting events
  - business/company events
- Natural events (*force majeure* – fires, floods, outages)
- Panic rousers (fake news, identity theft etc)
- Malware

Surveillance and communication

- Smartphones – 2 cameras, mic, GPS
- Burner (throwaway) phones – either physical or app-simulated (https://www.burnerapp.com)
- Wearables (https://www.spyshopeurope.com/)
- GPS tracking devices

Discussion break

- Think of various people and “buttons to press” on them, using the Five Elements system (examples can be suggested, but try not to interfere with privacy!)
- Panic rousing can sometimes be a good way to achieve the goal. What are the risks?
- Browse the Spyshop web and comment. :)

Conclusion

- We are dealing with an ancient art (or also science)
- While SE is mostly about humans, various tools can be handy
- Equally high and low tech
- “There is no problem that cannot be solved with a proper amount of high explosive” (on a bomb squad car)

- (and although pirates might be cooler than ninjas, the latter are way better social engineers)

- Next (and the last) time: some countermeasures

Thanks