Social Engineering and DoS notes

Agile Development

* Conversational Development.
  + Development should go both ways.
  + A conversation between developers and businesspeople.
* Interest in the science and knowledge.
* Dark patterns
  + A UI made to encourage users to do something there might not be in their best interest.
    - Manipulating users to buy trivial Insurance on products for example.
    - Buy this for free!
  + Programmers need to reject this.
    - We are responsible for the software we write.
* Impact judgement
  + We as developers are partly responsible for our software’s impact on the world.
  + Where are we going to apply our talents?
  + Alienating atmosphere
    - Is the software industry a meritocratic industry?
    - Harassment
  + Privacy
    - Important to all of us.
* We are a profession, and not just code monkeys.

Social Engineering er ikke bare at snyde folk, men er også etikken ved den måde vi vælger at udvikle software på.

Vishing

* Voice phishing is the criminal practice of using social engineering over a telephone system to gain access to private, personal and financial information.

Reciprocity (gensidighed)

* People tend to return a favor (good cop/bad cop)

Commitment to consistency

* Brainwashing – “I’ll sign up later” vs. “No thanks I prefer not making money”.
* Continue to pressure until people give in.

Social engineering principles (psychological):

* Social proof
  + The other do so…
  + A way to trick other into doing something by convincing them that others do this as well.
  + Social pressure.
* Authority
  + If someone of authority speaks, often people will just listen with asking questions.
  + Fake requests from higher up’s or big respected concerns/people.
* Linking
  + What would others do or think
  + Blackmailing others by presenting linked data to them and threaten their social life or social network.
* Scarcity
  + Limited time
  + Force someone to act irrationally, by saying that they have a limited time to act.
  + The same mechanism used when people buy large amounts of food on sale, thinking they are making a good deal.

Social engineering vectors:

* Vishing
  + Voice phishing
* Phishing
  + Links til falske hjemmesider, der udgiver sig for at være den rigtige vare.
  + Homophone for fishing
  + Spear phishing uses highly customized content
    - specifying content to trick a specific person or target.
    - To research and combine known/gathered information about the target to better blend in and look legit.
  + Water holing uses knowledge about favourite sites.
    - Customizing towards pages that a lot of people use and try to hit a larger range of targets.
  + Do some research first, and then use that research to access places where you shouldn’t be allowed.
    - Combination of having authority and being nice with a bit of inside information, can cat you access to a lot of things.
* Smishing
  + SMS phishing
    - Overbevisning og snyd gennem SMS.
* Impersonation
  + Attackers trying to impersonate other people or corporations to trick the target.
  + An example is to send mails using the addresses of a legit company or person, while hiding the actual senders mail address.

How can you secure yourself against this?

* Hardware
  + Adding more multifactor authentication, and more security layers.
  + Hardware is not necessarily a solution in most cases though.
* Education
  + Educating your employees awareness about these types of attacks.
  + In most cases, social engineering attacks has to do with human error.
    - Humans are social animals

Denial of service DoS

* Crash Service
* Flood Service
* Distributed Attacks DDoS
  + Man burger en masse zombie computere til all at angribe målet.
    - Der er folk der specialiserer sig i at hacke computere så de senere kan bruges som zombie computere.
* Application Layer Attacks
* Network Layer Attacks

Jo længere ned man vil angribe i lagene, jo mere adgang og jo tættere på skal man være.

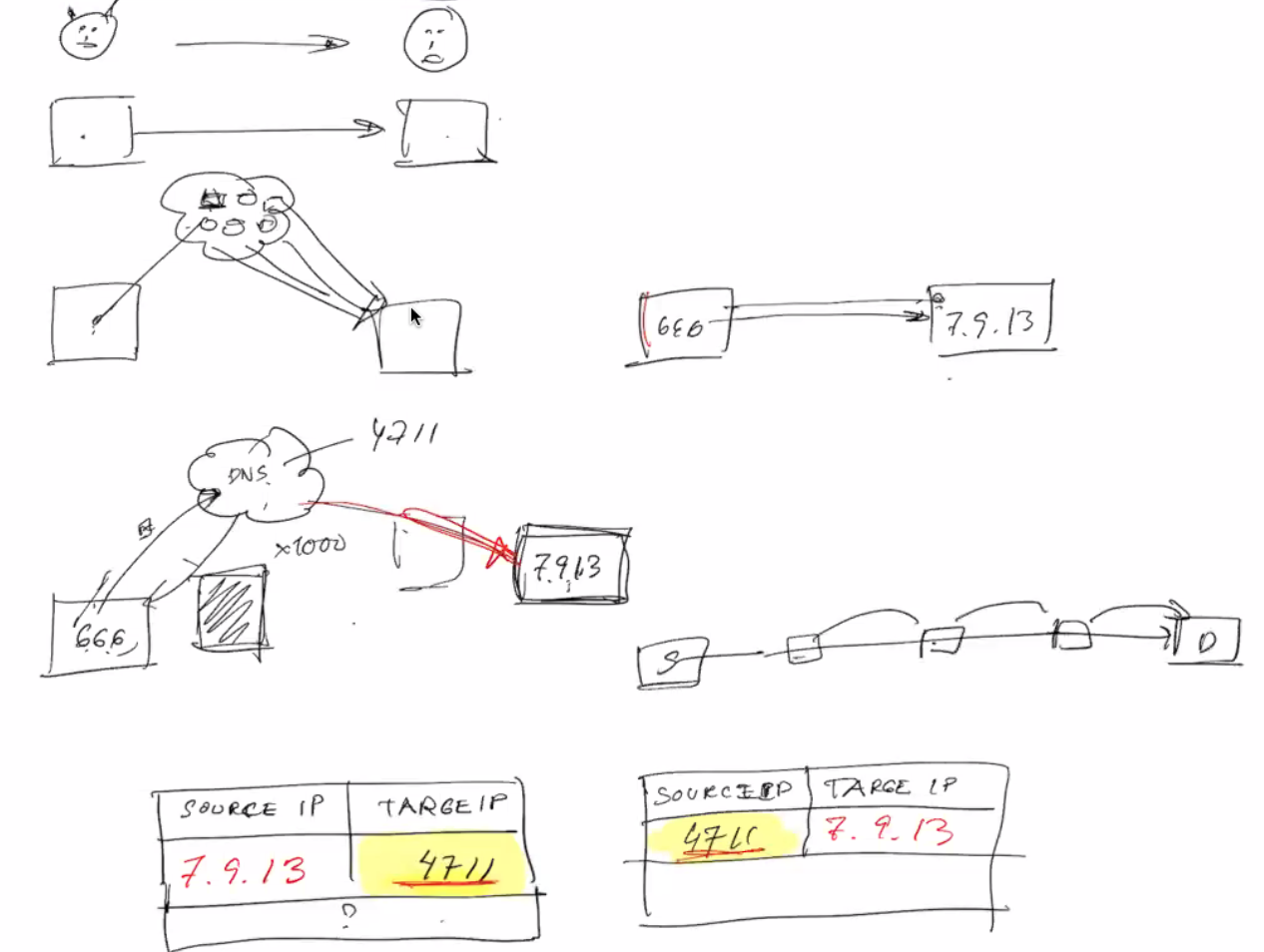
* Eks hvis man vil angribe Network layer, skal man næsten være med på lokalforbindelsen.

Man skal næsten skal have lige må meget computer kræft på den angrebene side som på den modtagende side man vil lave DoS på.

* Typisk bruger man derfor distribuerede DDoS kald til at lægge større maskiner/servere ned.

Man kan også skalere sit angreb op ved at vi gennem kommunikationen med et DNS-system, sender en masse små pakker med målets Ip adresse som source, så DNS-serveren så videresender en større pakke til målet. Dette er en nem måde at opskalerer sit angreb med en faktor x1000 da den pakke der videresendes er 1000 gange større end den vi selv sendte. Dette kaldes amplification.

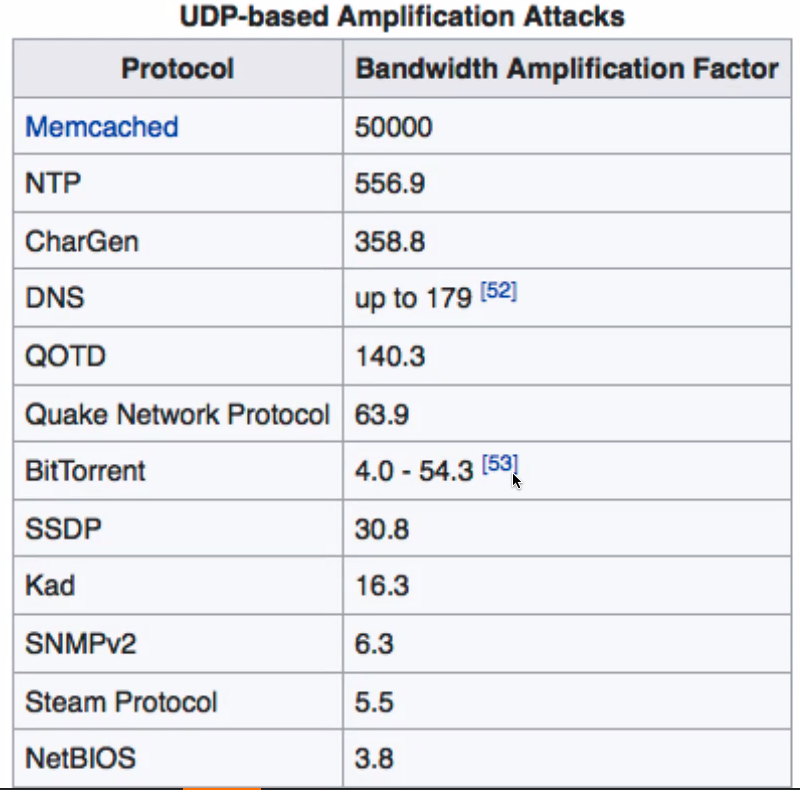
* En UDP-pakke har typisk 4 felter med et Source IP, et Target IP, et Source port og et Target port.
  + Det er her hvor vi kan bytte om på source IP’en så den store pakke som vi skulle modtage som svar på vores request, bliver videresendt til målet og opskalerer intensiteten af vores angreb, da pakker der bliver spammet til målet vil være større end hvis vi sendte dem direkte.
  + Man kan forstå det som at vi sender et brev til Social Styrelsen, hvor vi sætter en anden persons adresse på og bederstyrelsen om at sende os flere breve. Da jeg ændrede personadressen, vil den nye adresse blive spammet med breve, hvor alt det tog fra min side var et brev.



Denial of service DoS

* Degradation of service
* Denial of service level 2
  + Make the service block as a defence mechanism
* Distributed denial of service attacks
  + Hard to close down since there is not a single IP flooding
* HTTP POST DoS attack
* Internet Control Message Protocol Attack
  + Den går under radaren for en helt masse ting
* Permanent DoS attacks - phlashing
  + Destroy Server e.g. By updating firmware.

Amplification

* DNS amplification is a DDoS attack that leverages DNS resolvers to overwhelm a victim with traffic.
* Here are the different application factors for different bandwidths.
* 

Hvad kan vi gøre imod DoS angreb

* Elastic cloud services
* Blackholing – sinkholing
* ISP based prevention
  + Lave en aftale med sin internetservice provider ISP.
* DoS Defense System (DDS) based defense
* Firewalls
  + Kan for eksempel udelukke de IP’er og routers der forsøger eller tidligere har forsøgt at floode.
* Routers
* Upstream filtering

