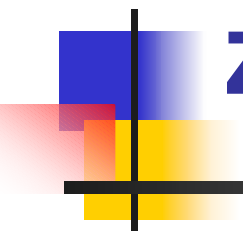


Zasebnost in nadzor na internetu

Matej Kovačič
http://www.ljudmila.org/matej

ZASEBNOST V VIRTUALNEM PROSTORU

- Tehnologije svobode in poostritev mehanizmov nadzora.
- Če je na začetku kazalo da je neobstoj s strani države potrjenih pravil na internetu priložnost za razvoj svobode, se danes čedalje bolj zdi, da ta neregulacija dopušča možnost različnih zlorab in omejitev svobode.
- Če se je še pred nekaj leti zdelo, da je internet tehnologija svobode, se danes zdi, da je panoptičnost že vgrajena v internet.
- Organizacija Privacy Rights Clearinghouse ugotavlja, da "pravzaprav ne obstaja nobena on-line aktivnost, ki bi omogočila popolno zasebnost".

ZASEBNOST V VIRTUALNEM PROSTORU

- Drugačna uporaba zbranih podatkov: primer Toysmart.
- "Social engineering" – goljufije, lažno predstavljanje, opazovanje preko rame, goljufije z URL naslovi in lažne spletne strani....

ZASEBNOST V VIRTUALNEM PROSTORU

- Pridobivanje informacij o računalniku, vključenem v omrežje.
  - Fiksni IP, NAT, ICMP, ping.
  - Interaktivni sistemi (ICQ, MSN, Yahoo!, AIM,...).

ZASEBNOST V VIRTUALNEM PROSTORU

- Elektronske sledi pri ponudniku dostopa do interneta.
  - Datoteke aktivnosti.
  - Carnivore (DCS1000).
  - Podatki iz DNS-ov.
  - Portali.

ZASEBNOST V VIRTUALNEM PROSTORU

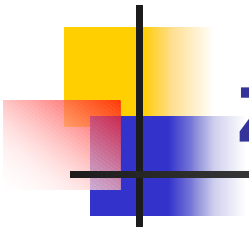
- Elektronske sledi pri ponudniku internetnih storitev in vsebin.
  - Spremenljivke o uporabnikovem okolju.
  - Klepetavost brskalnikov (*browser chattering*).
  - Uporaba JavaScripta (http://www.ljudmila.org/matej/netspeed/).
  - Multimedijska opremljenost računalnikov -> serviranje reklam.
  - Piškotki (*cookies*): session, persistent ter first-party, third-party.
  - Spletni hrošči (*web bugs*), pixel tehnologija, DoubleClick, personalizirane povezave, ugotavljanje off-line identitete.
  - Časovni napad (izkoriščanje lastnosti spletnega medpomnilnika).

ZASEBNOST V VIRTUALNEM PROSTORU

- Povezovanje in zbiranje razpršenih podatkov.
  - Podatkovni nadzor (*dataveillance*).
  - Povezovanje zapisov.
  - Roboti (*robot, bot, spider, worm, harvester*).
  - Virusi.
  - Podtaknjena JavaScript koda.
  - afna.telekom.si, spam mail.

ZASEBNOST V VIRTUALNEM PROSTORU

- Prestrezanje informacij preko omrežja.
  - Prestrezanje paketkov (*packet sniffing*).
  - Spremljanje prometa v Ethernet omrežjih.
  - Kraja gesel (*password sniffing*).
  - Brezžična omrežja (WLAN 802.11b) in *warchalking*.



ZASEBNOST V VIRTUALNEM PROSTORU

- Prestrezanje elektronske pošte.
  - Plain text.
  - Tehnično kot razglednica, praktično kot pismo v ovojnici.
  - Prenosni poštni strežniki (*relay servers*).
  - Prometni podatki.
  - SpamAssasin.

ZASEBNOST V VIRTUALNEM PROSTORU

- Vdiranje v sisteme.
  - Malomarnost pri nastavitvah pravic dostopa.
  - Izkoriščanje znanih varnostnih pomankljivosti.
  - SATAN (*Security Administrator's Tool for Analyzing Networks*), 1995.
  - Back Orifice, 1998. NetBus. Stranska vrata.
  - Instruktivni virusi.
  - Magic Lantern (*keyboard sniffing device*), FBI, 1999 (primer Scarfo). Antivirusna podjetja in sodelovanje z FBI.
  - Spyware, E. T. aplikacije.
  - Melissa in GUID.

ZASEBNOST V VIRTUALNEM PROSTORU

- Prestrezanje podatkov in informacij v okolici sistema.
  - TEMPEST - *Transient Electromagnetic Pulse Emanation Surveillance Technology* (tehnika prestrezanja oddanih začasnih elektromagnetnih signalov; tempest pa v angleškem prevodu pomeni vihar).
  - 1985: Wim van Eck, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk*?
  - Markus in Anderson, University of Cambridge.
  - Možnost nastanka posebnega virusa, ki bi s pomočjo povečane aktivnosti npr. procesorja ali trdega diska oziroma preko ohrajevalnika zaslona oddajal sporočila v obliki elektromagnetnega sevanja.