Privaatsusest nii ja naapidi

TPK2012
Kaido Kikkas

Privaatsus

- Enne tehnoloogia võidukäiku oli täiesti saavutatav – tuli minna teistest eemale ja jälgida, et keegi ligi ei hiiliks
- Niipea, kui tuli mängu distants, oli aga ka privaatsus ohus – kullerite ”rajalt mahavõt-mine”, kirjade avamine, salasõnumite dekodeerimine jpm eksisteerisid ammu enne IT-ajastut
- Tänapäeval on suundmikrofonid, paraboolantennid, laserinterferomeetrid ja muu peen kraam - privaatsust on jälle sellevõrra vähem

”Kõike, mida te ütlete, võidakse kasutada teie vastu”

- Vanasti oli väga raske püüda lendulastud sõnu – oli võimalik ainult konkreetses kohas (N: kohtus) sõna sõna vastu seada
- Siis hakati neid üles kirjutama...
- … ja siis salaja talletama (kirjutama, salvestama)
- Tegelikult ei ole see ka kunagi tõsiselt inimõiguste teema olnud (privaatsus tervikuna on seda küll)!

Privaatsus ja seadused

- Juudi seadustes (Talmud): kes ehitab maja vastu naabri aknaid, peab tegema akna vähemalt neli küünart kas madalamale või kõrgemale. Lisaks oli otsene keeld kiibitsemise suhtes
- Mõned aspektid hilisemast ajast:
  - õigus autonoomsusele, sh olla rahule jäetud
  - õigus kontrollida enda kohta levivat infot
  - õigus saladusi hoida ja eraviisiliselt edastada
  - õigus üksindusele, intiimsusele ja anonüümsusele

Privaatsus ja privaatsus

- Sõltub ka kultuurikontekstist ja traditsioonidest – näiteks jaapanlane vs rootslane
- Mõnel juhul piirab privaatsust ka
  - isiku enese valik (avaliku elu tegelased)
  - mugavus (internetipank on mugav, kuid eeldab enese identifitseerimist)
- Privaatsus on aga eraldi punktina sees nii 1948. aasta Inimõiguste Ülddeklaratsioonis kui 1967. aasta Rahvusvahelises Inimõiguste Leppes

Internet ja salastamine läbi aegade

- Sõjaline - tippsaladus
- Teadus - mõneti salajane
- Haridus ja NGO - mitte eriti
- Äri - mõneti salajane
- Isik – privaatsus!

Interneti privaatsusparadoks

- Ühelt poolt soodustab ebaisikulisust ning ano- ja pseudonüümsust (nn. kuvaripeitus)
- Teisalt - alati on pealtkuulamise/vaheltlõike võimalus
- Tuvastada saab enamasti tagantjärele, kui tulemus juba avaldunud
- Väliseid erinevusi "puhta" ja "lõigatud" info vahel ei ole või on neid raske avastada

Kaks tähtsat mõistet

- Privaatne suhtlemine mistahes kanalis eeldab sõnumi
- Autentsust (*authenticity*) – sõnum tuleb tõepoolest sealt, kust seda väidetakse tulevat
- Ehtsust (*integrity*) – sõnum jõuab kohale samal kujul kui saadeti ja keegi ei ole seda vahepeal torkinud

Minu kodu on minu kindlus?

- Võrreldes traditsioonilise privaatsusega
  - Olukorda raskem kontrollida
  - Tagantjärele tarkus
  - "Kõike, mida ütlete, võidakse kasutada teie vastu" - otseselt või kaudselt, kohe või aastaid hiljem
  - Identiteedivargus on lihtsam kui varem, selle tagajärjed aga võivad minna üsna tõsiseks
  - Seadusandlik kaitse on nõrgem

Privaatsus kui äriobjekt

- Kaks leeri:
  - Säilitamisega teenivad (turvamehed, adminnid)
  - Rikkumisega teenivad (vargad, spammerid)
- Võimalik ka kokkumäng

Jälle see inimfaktor!

- Konkreetne näide lähiminevikust – üks ameerika tibi, kes Valges Majas selle tollase peremehega trikke tegi
- Tibi rääkis asjast telefonitsi ”sõbrannale”, kes jutu tema teadmata salvestas ja prokurörile edasi saatis
- NB!!! Kui tibil oleks olnud kasutada kindlalt turvaline sideliin, oleks tulemus olnud veel hullem – jutt oleks olnud veelgi avameel-sem ning sõbranna sigatsemine oleks saanud veel suurema mõõtme. Sama kehtib ka netisuhtluse korral!

Ekskurss: krüptograafia

- Krüpteerimine on kasutusel hallidest aegadest
- Alguses lihtne asendusšiffer – tähestiku mingi täht asendati mingi teisega. Iseenesest piisava kombinatsioonide arvuga, ent murtav konkreetse keele tähtede esinemissagedusi ja tähekombinatsioone arvestades
- Järgnesid muutuva tähestikuga šifrid – esmalt oli tähestike järjestus väikese-arvuline ja korduv, hiljem aga ühekordne ja muutuv

Näide: Vigenère'i süsteem

- Luuakse samapalju eri tähestikke kui tähestikus tähti, iga tähestiku esitäht on erinev. N:
  - U S I P N A M S ...
  - B I U E R K A S ....
  - T O J S I N E R ...
  - ...
- Võti moodustatakse tähestike esitähtedest: U B T E R O F H ...
- Sõnumi esitäht kodeeritakse U-tähestikus, järgmine B-tähestikus jne

Ühekordne numbrikrüpteering

- Levinud meetod II maailmasõja ajal
- Näiteks olgu antud sõnum ”kohtume aadressil Mustamäe tee 18-45 5. juunil 2012 kell 13.45"
- Kodeeritult: 25 18 45 05 06 20 12 13 45 (siin on 25 võetud Mustamäe tee koodiks)
- Kodeeritakse võtmega 33 23 98 54 01 83 22 43 66
- Kodeeritud sõnum: 58 41 43 59 07 03 34 56 11
- Saaja lahutab kodeeritud sõnumist võtme

Ühekordse kodeeringu probleemid

- Suures koguses oli raske genereerida unikaalseid võtmeid (VENONA 1942-45 - NL vajas alanud sõjas suurt hulka koodi-raamatuid, milles tüüpilise nõukavärgina kasutati osasid lehekülgi topelt. Britid said teada ja lugesid mitu aastat NL sidet)
- Sõnumi pikkus piiratud võtme pikkusega
- Raudne reegel – ühtegi kodeerituna edastatud sõnumit ei tohi hiljem edastada samal kujul lahtise tekstiga (ka siis, kui sisu enam üldse mingi saladus pole)

Tänapäevane igamehekrüpto

- Asümmeetrilised, avaliku võtmega süsteemid (PKI – *Public Key Infrastructure*)
- Kui A saadab B-le sõnumi, võtab ta B avaliku võtme ja krüpteerib sõnumi sellega. B kasutab avamiseks enda privaatvõtit
- Digiallkiri – A saadab B-le sõnumi, mis on krüpteeritud A privaatvõtmega. B kasutab A avalikku võtit – kui sõnum on loetav, oli selle saatjaks A
- Sertifikaat – avaliku võtme ehtsuse kinnitus

Info kogumine: motiiv määrab

- Andmete kogumine on neutraalne, eetiline hinnang saab lisanduda vaid kasutamisele
  - Perearst
  - Elion, EMT vmt suurfirma
  - Reklaamibürood
  - Spammerid
  - Kriminaalid

Miks nii palju kisa?

- Taandub kahele Interneti suurele võimalusele
  - Jälgida teiste tegevust nende teadmata
  - Koguda, süstematiseerida ja pikaajaliselt säilitada järjest suuremaid infomahtusid
- Privaatsus eeldab teatavaid kirjutamata reegleid – s.t. osaliste teatud küpsustaset (*consenting adults*)
- Enamasti on netireaalsus aga teistsugune
- Tulemus: privaatsuse ja turvalisuse vägikaikavedu nendevahelise koostöö asemel

Mis ripakil, see ära

- Info kogumine üha enam võimalik täiesti legaalsel teel
- Ka kõige väiksemad "ämbrid" saab registreerida
- Hoidmine pole probleem - infot saab kasutada kõige soodsamal momendil (näit. valimisvõitluses). Enamasti mõjub juba "väljakaevamine", harilikult aga lisatakse mingis vormis santaaž

Kaevur Mati ja nuhk Albert

- Kiirelt arenenud tegevusala - andmekaeve *(data mining*). Muuhulgas sisaldab ka isikliku info hankimise võimalust objekti teadmata (näiteks teise inimese koduleheküljelt)
- Võimalik kokku panna Imre Perli loomingu sarnaseid andmekogusid (kes ei mäleta – tegu oli 90-ndatel ringlusse pääsenud illegaalsete isikuandmebaasidega)

Toimikuefekt

- Võrk soodustab info süstematiseerimist
- Kipub tekkima kiusatus koguda ka isikuandmeid
- Paljude firmade kliendiandmebaasid - toimikud?
- Riigivõim pole ka puhas poiss

Privaatsus vs mugavus

- Igapäevased anonüümsed asjad
  - Haiguste testimine
  - Mobiili kõnekaart
  - Sularaha
- Teisalt asjad, kus privaatsus jääb alla mugavusele
  - mobiiltelefon – raadioside ja sellisena murtav
  - suvalise arvuti kasutamine (hotell, netikohvik)
  - läpakas – võhiku käes ohtlik mitmes aspektis
  - WiFi (lahtine või WEP-iga ning ilma turvakanalita)

Negatiivne anonüümsus

- Läbi aegade on anonüümkirju peetud Pahaks Asjaks
- Võrgu puhul suhtus traditsiooniline netikett pikka aega üsna samamoodi – ehkki sõnavabadus on üks võrgu põhialuseid, siis anonüümsus (vähemal määral ka pseudonüümsus!) on halva maiguga
- Uuemal ajal on suhtumine hakanud muutuma – ja seda just neti kiire levi ja elukutseliste privaatsuseründajate paljunemise tulemusena

Internetis

- Pluss:
  - Oluline roll vaba suhtluskeskkonna arengus
  - "On Internet, nobody knows you're a dog!" (Dogbert)
  - Vilepuhumise võimalus
- Miinus:
  - Autorsus- ja omandiküsimused
  - Rämpsulevi
  - Viha- ja lollpost

Arengust

- TCP/IP – paketitasemel pole anonüümsus võimalik
- ISP = *Internet Surveillance Project* ...?
- Lihtsaim viis - kasutada "postkastina" teist inimest
- Võimalused võltsida meilipäist
- Anonüümsed e-posti- ja veebisüsteemid
- Tänaseks ka keerukamad lahendused

Kokkuvõtteks

- Privaatsus sarnaneb tulirelvade küsimusega:
- Piirangud vähendavad juhuslike väärkasutuste arvu
- Piirangud vähendavad ka ausate inimeste kaitsevõimet ühelt ja inimväärikust teiselt poolt
- Eelkõige tuleks kogu valdkonda rohkem tutvustada ja teadvustada – üheksa korda mõõda, üks kord lõika

Aitab kah...