

„Loll saab Internetis kah peksa”  
(eesti vanasõna, XXI saj)

Kaido Kikkas  
2019/2020

**Kaido Kikkas 2019. Käesoleva dokumendi paljundamine, edasiandmine ja/või muutmine on sätestatud ühega järgnevatest litsentsidest kasutaja valikul:**

**\* GNU Vaba Dokumentatsiooni Litsentsi versioon 1.2 või uuem**

**\* Creative Commonsi Autorile viitamine + Jagamine samadel tingimustel 3.0 Eesti litsents (CC BY-SA) või uuem**

# Paar mõtet alustuseks

- „Suurim turvarisk asub alati klaviatuuri ja tooli vahel“ - IT aksioom
- „Lollikindlat masinat ei ole võimalik luua, sest lollid on ülimalt leidlikud.“ - üks amishi talumees Howard Rheingoldile
- „Ei ole küsimus, KAS süsteemi sisse murtakse, vaid MILLAL.“ - Kevin Mitnick
- „We are Samurai... the Keyboard Cowboys... and all those other people who have no idea what's going on are the cattle... Moooo.“ - The Plague

# Turvalisus = tehnoloogia x koolitus x eeskirjad

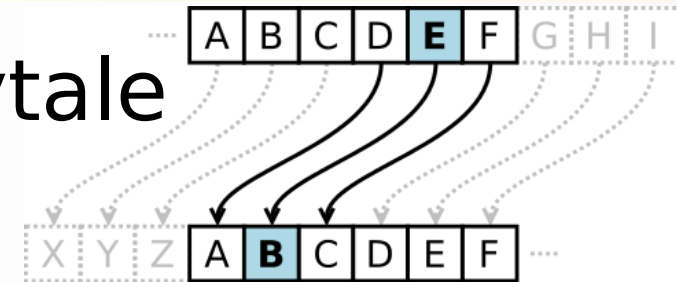
- Pealkirjas toodud lause pärineb Kevin D. Mitnickilt – turvalisus tuleneb tehnoloogiast, kasutajakoolitusest ja protseduurireeglitest
- Mitte summa, vaid korrutis (kui üks kolmest on 0 või peaaegu, on seda ka kogutulemus)!
- N: firma ostab uusima tippturvalisusega serveri, adminid jäetakse välja õpetamata ja/või ei panda mängureegleid paika.  
Tulemus on SNAFU

# Sisse astuvad Karl Marx ja Freddie Mercury

- Mida need sellid SIIN teevad?
  - Marx: “vastandite ühtsus ja võitlus”
  - Mercury: “I can't live with you, I can't live without you....”
- Point: seisu muudab veelgi segasemaks asjaolu, et andmeturve on suur äri, kus võib rääkida ka huvide konfliktist.  
**Kas McAfee või Symantec oleks õnnelik, kui ühel päeval oleks kogu pahavara ilmast kadunud...?**

# Andmeturve läbi aja

- Antiikaeg: Caesari šiffer ja scytale
- Turing ja bombed
- UKUSA lepe ja ECHELON
- Pätid ärkavad esimestena:
  - IBM PC 1981 ja 80-ndate viirused
  - Internet ja Morrise uss (02.11.1988)
  - Ärikeelu kadumine 1991 ja spämmiuputus
  - Sotsiaalmeedia ning petised ja trollid



Siin ja edaspidi kasutatud pildimaterjal pärineb Wikimedia Commonsisist (ühe viidatud erandiga)

# Vanasti oli rohi rohelisem

- Tsiteerime veel kord Steven Levy't
- MIT häkkerikogukond tajus juhtkonna poolt sisseviidud paroolinõuet mitte kaitseabinõu, vaid privaatsusele suunatud ründena
- Reaktsioon: soovitati kõigil kasutajatel jätta parool tühjaks (1/5 kasutajaist tegi seda)
- Pool sajandit hiljem on aga olukord väga tublisti muutunud

. . .

- Vanasti olid arvutid elitaarsed => vähe inimesi, kõrge haridustase, äri ei olnud eriti reaalne
- Tänapäeval võib läänemaailmas olla arvuti isegi kodutul (vt <https://thehomelessguy.wordpress.com/>)
- Tulemus – ühelt poolt minek massidesse ja tubli tõuge ühiskonna arenguks, teisalt aga
  - omapärane arusaam ärist
  - palju otseseid kaabakaid ja kurjameid
  - veelgi rohkem hästivarustatud lolle



# Mõned põhivaldkonnad

- Pahavara
- Identiteedivargus
- Ressursihõive
- Netipettused
- Manipulatsioonid
- Rämpspost
- Trollimine
- Häktivism
- Suur Vend
- Kübersõda



# Pahavara

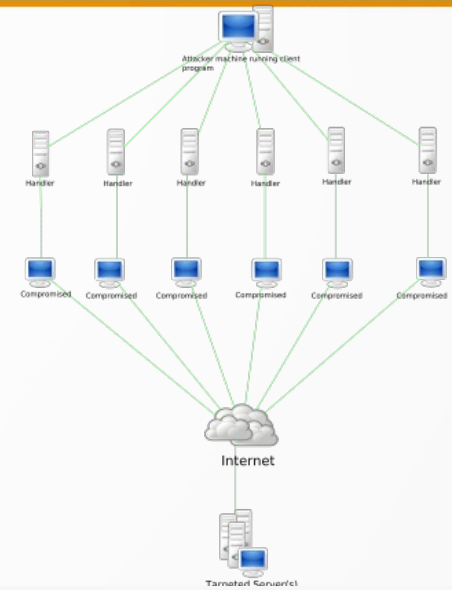
- Viirused
- Trooja hobused
- Ussid
- Juurkomplektid
- Nuhkvara
  - klahvinuhk
- Lunavara
- Veebiründed (XSS, CSRF jt)
- Lisaks paar mehhanismi:
  - Aegsütik (N: Michelangelo 1991 – 6.03)
  - Ümbersuunaja (N: Rove Digital 2007-11)
- Hall tsoon - kaughaldus:
  - Back Orifice, Netbus, Sub7
  - TeamViewer (!)

# Identiteedivargus

- “Tõesta, et pole sebra!”
- Google aitab – ka pätti
- Õngitsemine (*phishing*)
- “Ligupidamisega Hansapanga administratsioon” 2002 (<http://anton.tkwcy.ee/kraam/tekstid/hanza.html>)
- WiFi ja *evil twin* -võrk
- *Bluejacking/bluesnarfing*
- Võltsnimed ja homoglööfründed

# Ressursihõive

- Suur erisus võrreldes 80-ndate viirustega
- Arvuti teeb haltuurat kellegi teise heaks:
  - Leebe variant: kaevandab bitimünte
  - Kuri variant: sigatseb täiega (rämps, DDOS)
- Superarvuti võimsus!
- Tänane uus sihtmärk: nutistu (Mirai)



|            |        |        |         |
|------------|--------|--------|---------|
|            | 1000   | 5000   | 10,000  |
| World MIX  | 25 \$  | 110 \$ | 200 \$  |
| EU MIX     | 50 \$  | 225 \$ | 400 \$  |
| DE, CA, GB | 80 \$  | 350 \$ | 600 \$  |
| USA        | 120 \$ | 550 \$ | 1000 \$ |

[https://webrootblog.files.wordpress.com/2013/02/malware\\_infected\\_hosts\\_as\\_a\\_service\\_international\\_europe\\_usa1.jpg](https://webrootblog.files.wordpress.com/2013/02/malware_infected_hosts_as_a_service_international_europe_usa1.jpg)

# Netipettused

- Häda Nigeeriaga
- Algas sarnaselt spämmiga – seadusi ei olnud
- Levinumad tüübid:
  - Ettemaksupettused (419)
  - “Aita raha vasakule lükata” (pangateenus)
  - Autopettused
  - Tibitillikad (kohtingupettused)

# Kõrvalepõige: miks Nigeeria?

- Miks ikkagi?
  - pikaaegne ebakindlus ja korrupsioon (rikas maa ebakindla võimu all, pikk sõjaväevõimu periood)
  - vaesus ja ebavõrdsus – 60% elanikest on allpool vaesuspiiri, 80% naftatuludest läheb 1%-le elanikkonnast
  - suur maa, palju rivaalitsevaid hõime
  - inglise keel kui ühiskeel (muid keeli ca 250)
  - kirjaoskuse protsent ca 70, üsna hea haridustase
  - üsna hea tehno-infrastruktuur (korralik keskmik)
  - pikk pettustetraditsioon (ammu enne Vörku)

# Laud teistpidi: scambaiting ehk pätikottimine

- Uus spordiala (ka nimega *mugu-baiting*) - EETILINE HALLTSOON!!
- Põhiidee: vastatakse mõne “Dr Mobutu” kirjale, mängitakse Lolli Valget Meest (stiilipunkte annab endale võimalikult napaka nime väljamõtlemine nagu Gerald Womo Milton Glockenspiel) ja üritatakse seejärel õnnetu “ettevõtja” igasuguseid asju tegema panna
- Parimad pojad on saanud ise raha, lasknud totraid pilte teha või lennutanud õnnetu päti (tema enda kulul ikka) New Yorki kohtuma
- Vt näiteks [whatsthebloodypoint.com](http://whatsthebloodypoint.com), [scamorama.com](http://scamorama.com), [419eater.com](http://419eater.com)

# Sotsiaalmanipulatsioonid

- *Social engineering, no-tech hacking*
- Eelinfo, ettekäänded ja rollimäng (*pretexting*)
- Prügistuhnimine (*dumpster diving*)
- Üleõlapiilumine (*shoulder surfing*)
- Sappavõtmine (*tailgating*)
- Mimikri!
- Vt Johnny Long, Christopher Hadnagy, Kevin Mitnick



# Näide 1: Martin, audiitor

- Osakonna raamatupidaja tädi Maalile helistab „Martin Meri siseauditi osakonnast“. Küsib järjekorras selliseid küsimusi:
  - Mitu töötajat on teie osakonnas?
  - Kui palju on kõrgharidusega töötajaid?
  - Kui tihti korraldatakse osakonnas täienduskooolitusi?
  - Mis on osakonna personalikulude kontonumber raamatupidamises?
  - Mitu töötajat on lahkunud viimase aasta jooksul?
  - Milline on osakonna üldine tööõhkkond?
- Mis siin valesti on...?

# Näide 2: abivalmis itimees

- Vajalik varustus: mobla + kõnekaart
- 1. kõne: firma raamatupidamisse hr. Sepale; mängida helpdeski ja küsida, kas kõik on ikka korras ja jätta „igaks juhuks“ oma telefon. Muu hulgas küsida ka võrgukaabli pesa numbrit
- 2. kõne: firma IT-osakonda. Jätta mulje, et räägitakse „hr. Sepa kontorist“ ja paluda konkreetse numbriga kaablipesa välja lülitada
- Oodata, kuni hr. Sepp paanikasse läheb ja „helpdeskile“ oma probleemiga helistab

. . .

- Tunnikese pärast on asi korras – muidugi tuleb helistada vahepeal uuesti IT-osakonda ja paluda ühendus sisse lülitada
- „Et seda enam ei juhtuks“, paluda hr. Sepal alla laadida üks programm ja käima panna. See ei tee midagi nähtavat – vabandada, et „oih, ei tööta“ ja paluda allalaetu kustutada
- Korras: sniffer/rootkit/trooja hobune on paigas
- (Telefon pärast prügikasti - muidugi enne teha mälu tühjaks ja võtta aku välja)

# Ettevaatust, veisepuuk!

- Enamik sotsiaalseid võrgustikke moodustavad nn usaldusvõrgustikud (sõbralisti liikmed on „omad“)
- Kohati kaugelt liiga palju isiklikku infot!
- Enamik manipulatsioone algab usalduse tekitamisest – sellise võrgustiku puhul on väga suur hulk tööd tihti juba ette ära tehtud
- Suur probleem – teenuste põimumine!
- Gazzag.com'i juhtum 2006. aastal

# Rämpspost

- Algas: 1978, Greg Thuerk spämmib üht DECI projektiüritust 600-le ARPAneti kasutajale
- Suur jama algab 1991 – esimesena ärkavad taas pätid
- Kõrgaegadel oli maht ca 200 miljardit rämpssõnumit päevas, 75-90% kogu netiliiklusest
- 2019. aastal eri andmetel 50-60% liiklusest
- Ravimid ja dieet-tooted, “püstitajavad” asjad, võltsdiplomid...
- Suurim probleem: odavus (~0,00001 senti tükk)
- Varem USA, Hiina ja Venemaa, nüüd tuleb ka Euroopast

# Trollimine

- Inimeste sihilik seaksvihastamine (*for lulz*)
- Algas Usenetis (*trolling for newbies*)
- Slashdot (*you must be new here*)
- Kurjaks keerab asi 4chanist alates ( /b/ ) - *doxing*
- Probleem: piiri kadumine sotsiaal- ja “päris” meedia vahel (sh tavameedia allakäik viimase ca 10 aasta jooksul)
- Leebem aspekt: tüngad ja meemid (*rickrolling, lolcat* jpt)
- Tänapäeval suurfirmade, parteide ja riikide tasemel (Internet Research Agency jt)



# Häktivism

- Poliitilise motiiviga küberrünne
- Algas 80-ndates  
(*Chaos Computer Club* Saksamaal)
- 4chan => Anonymous (ja LulzSec)
- Hiina (*honke*), Venemaa, Korea... aga ka Daesh/ISIS
- Kasvutendents ohtude osas





# Suur Vend

- 1948 - UKUSA (*Five Eyes*)
- Enne oli kombeks omaenda kodanike järel mitte nuhkida
- JOKK: USA>UK>AUS>NZ>CAN>USA...
- ECHELON
- Külma sõja ajal oli vaja “riigi turvalisuse huvides” jälgida kommuniste, tänapäeval igat sorti terroriste
- Wikileaks 2006



# Kübersõda

- Maa, meri, õhk, kosmos ja küberruum
- Stuxnet ~ 2010-12, Natanzi tsentrifuugid
- Eesti ja Gruusia 2007 – hübriidsõja eelproov?
- Tavakodanike roll kasvab (Eestis KL KKÜ, Hiinas *honke* jne)
- CCCoE Tallinna manuaal: <https://ccdcoe.org/tallinn-manual.html>

# Lahendused: tehnoloogia

- Pahavaratõrje
- Tulemüürid
- Nõrkuste avastajad
- Sissetungidetektorid
- Meepotid
- Logianalüüsi vahendid
- Autentimissüsteemid

# Lahendused: koolitus

- Märkus: Tiigrihüppe õppetund
- Muuhulgas oleks vaja:
  - Üldteadlikkus
  - Internetitehnoloogiad - veeb, e-post...
  - Manipulatsioonid
  - Andmekäitlus - säilitamine ja hävitamine
  - Füüsiline keskkond - lukud/uksed, kaugtöö, reisimine...
  - ...
- Kolm fookusgruppi: IT personal, tippjuhid, tugipersonal(!)

# Lahendus: eeskirjad

- Mängureeglid paika! Palju jama tekib ebaselgusest
- Füüsiline ligipääs – kuidas, kes, millal, mis tingimustel...
- Tehnoloogia – ligipääs, õigused, mobiilseadmed/VOSK, kaugtöö, külalised, jälgimine...
- Vt veebist – RIA ja ISKE

# Lisaks: tavakasutaja 10 käsku

- Ära võta liigseid õigusi
- Paroolid...
- 1 kasutaja, 1 konto
- Tunne ja kasuta kaitsetarkvara
- Tea, mis arvutisse on paigaldatud

. . .

- Oska andmekandjatel orienteeruda
- Uuenda tarkvara regulaarselt (võhik pigem automaatselt, oskaja pigem käsitsi)
- Tunne enda arvuti peamisi riistvaraosi
- E-postimanused...
- Viitsi uurida ja õppida



# Kokkuvõtteks

- Andmeturve on igaühe asi - nagu liiklusohutus
- Mitnicki valem!
- Turvalisus on VÄGA liikuv märklaud
- Tegelda tuleb kogu spektriga direktorist koristajani ja vanaisast põnnini

# Edasilugemiseks

- Kevin Mitnicki raamatud (eriti *The Art of Deception*)
- Johnny Long, *No Tech Hacking*
- Christopher Hadnagy, *Social Engineering*
- Nicky Hager, *Secret Power*
- Cliff Stoll, *Cuckoo's Egg*
- Bruce Sterling, *Hacker Crackdown*
- ...

**Aitab jorinast**