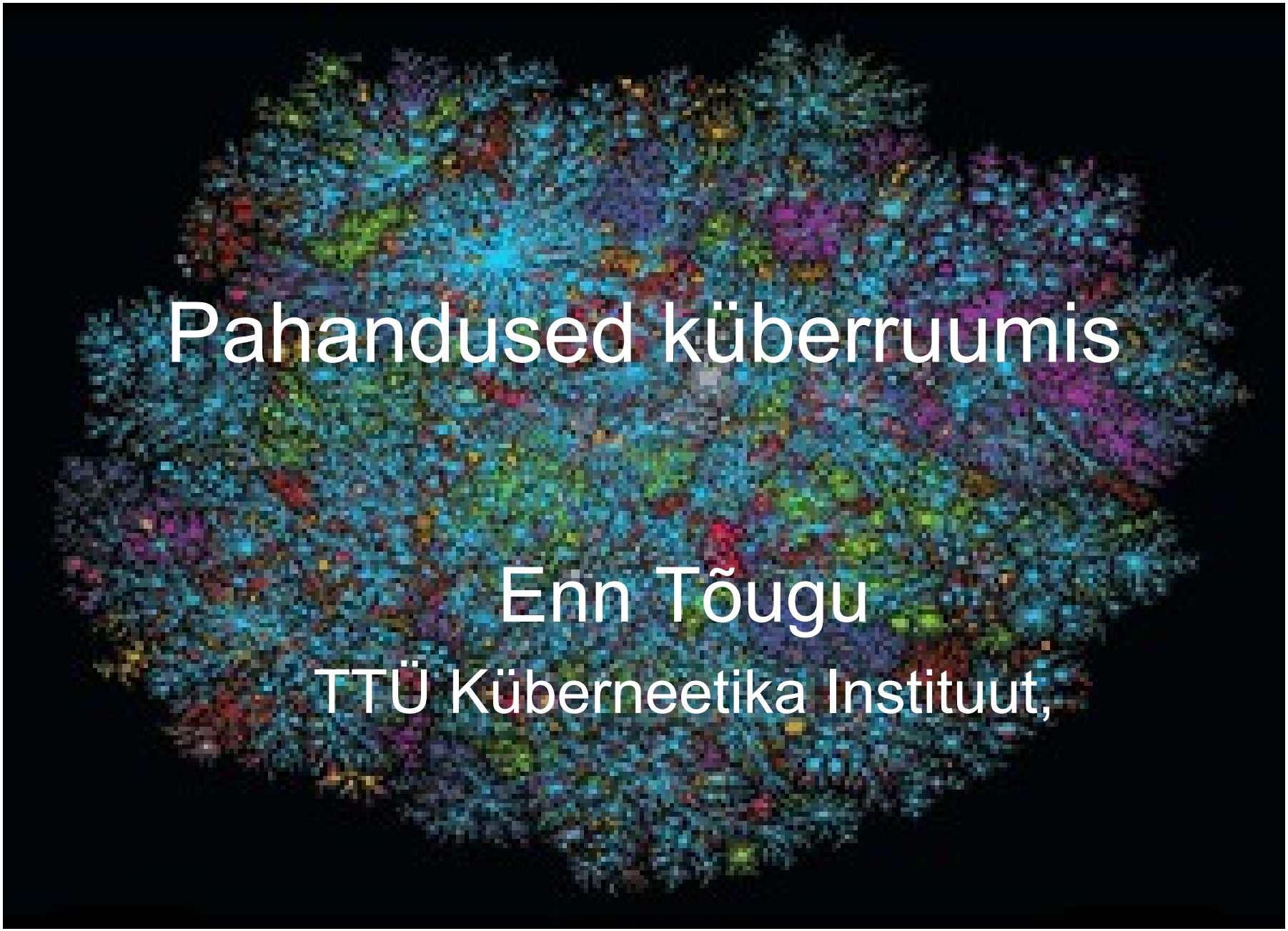
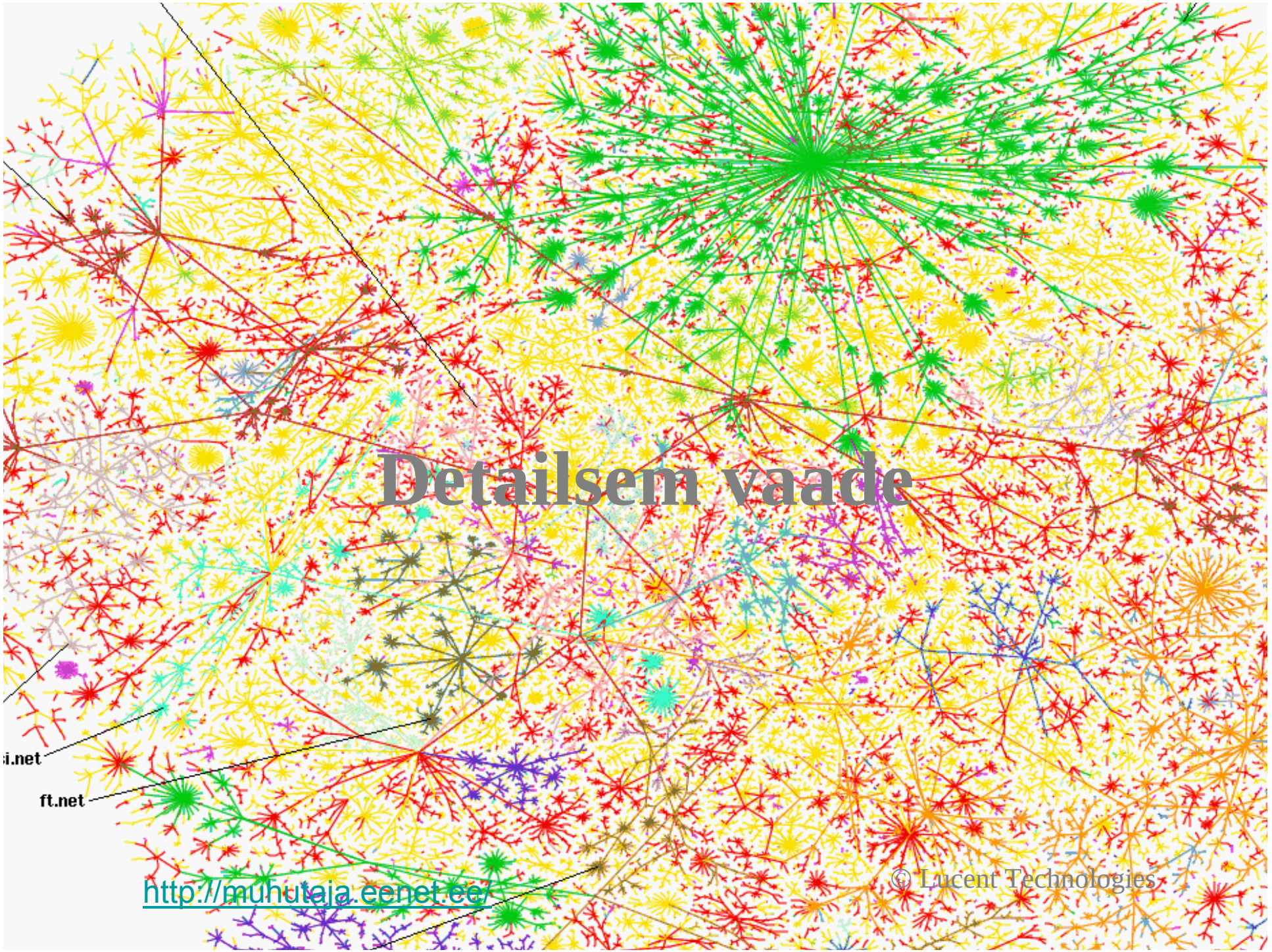

Pahandused küberruumis
Enn Tõugu
TTÜ Küberneetika Instituut,


Detailsem vaade
i.net
ft.net
http://muhutaja.eenet.ee/
© Lucent Technologies

Küberruum

- Küberruum on Internetipõhine keskkond, kus inimesed ja programmid suhtlevad.

Sõltume küberruumist

Eesti ühiskond on tugevasti sõltuv Internetist ja seal toimuvatest protsessidest – niinimetatud **küberruumist.**

Ei kodanikud ega ettevõtted ei saa Eestis normaalselt tegutseda enam ilma Interneti toeta.

- Üle 98% kõigist pangaoperatsioonidest tehakse meil elektroonselt.
- Interneti kaudu täidetakse enamus maksudeklaratsioone, kasutatakse avalikke teenuseid, saadakse infot, peetakse sidet, allkirjastatakse dokumente, osaletakse valimistel.
- Arvutivõrkude kaudu juhitakse energiasüsteeme ja liiklust.

IT kasutamine USA-s

- 1/3 valgekraedest töötavad kaugteel
- 1/3 riistvara vargusi tehakse insiderite poolt
- 1/3 töötajaist teab, mis neil arvutis on
- 1/3 suuremaid firmasid ei kaotanud arvuteid viimase aasta jooksul

Küberkuritegevus kasvab

- Küberkuritegude arv USA-s:

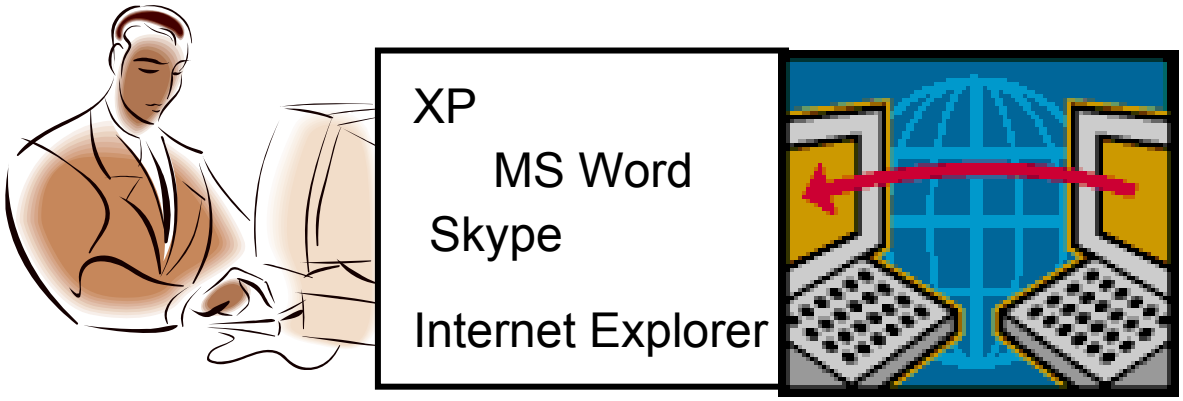
2006	*2007*	*2008 (eeldatav)*
80000	*271000*	*800000*

- 80% kuritegudest rahalisel eesmärgil

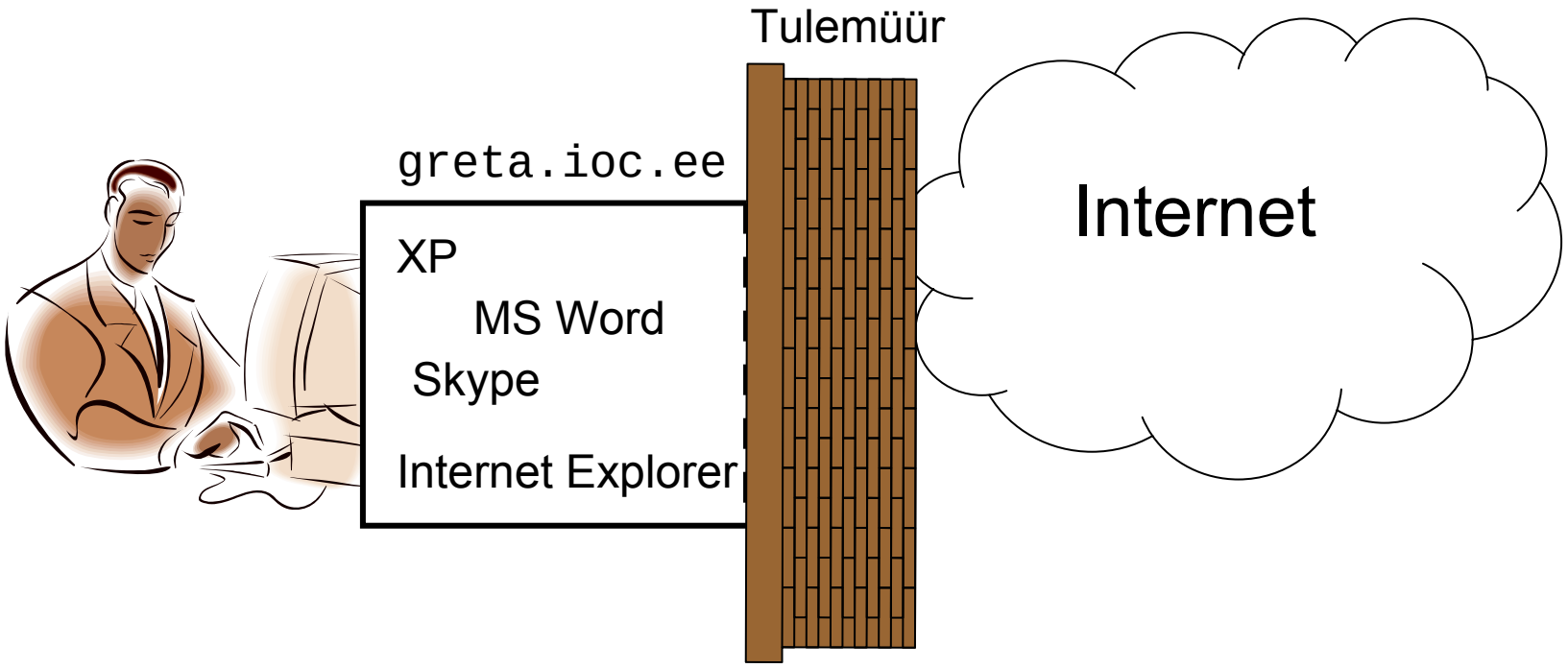
Esineb riiklikult tellitud küberründeid, mille skeem on sageli

riik → kurjategijad → rünnatav

Mina ja Internet



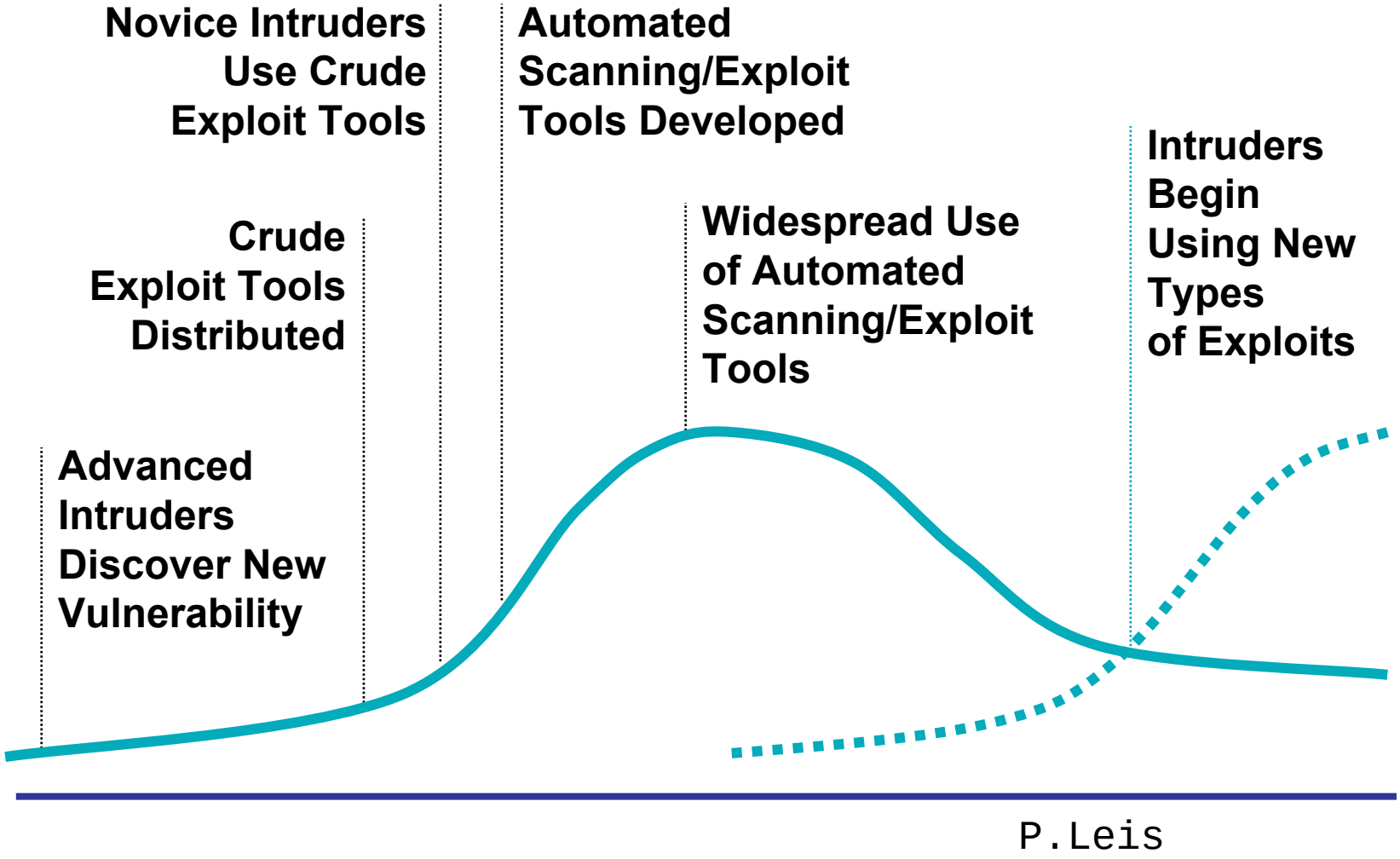
Arvuti ja Internet



Nõrkused ja ründed

- Tarkvara nõrkused -- **turvaaugud** võimaldavad teha **kurivara** ja korraldada **ründeid**. Pidevalt avastatakse uusi turvaauke, neid tekib juurde koos uue tarkvaraga.
- Tarkvara “lapitakse”, enamjaolt automaatselt.
- Turvaauke teatatakse kas avalikult või müüakse neid pahalastele (tavaline müügihind kõigub 100 ja 3000 dollari vahel, kalleim hind 2005.a. oli $4000, kuid on olnud turvaaukude pakkumisi ka $120000 peale).
- Eriti ohtlikud on 0-päeva (või 0-tunni) ründed -- sellised, mis tehakse värske kurivaraga, millele pole veel kaitset loodud.

Vulnerability Exploit Cycle



Kurivara

= Pogrammid, mis teevad halbu (keelatud, ebaeetilisi) toiminguid:

- Viirused
- Ussid
- Botid
- Troojalased
- Ebatuumad (rootkitid)

Need programmid toimivad suurel määral inimese vahetu osavõtuta.

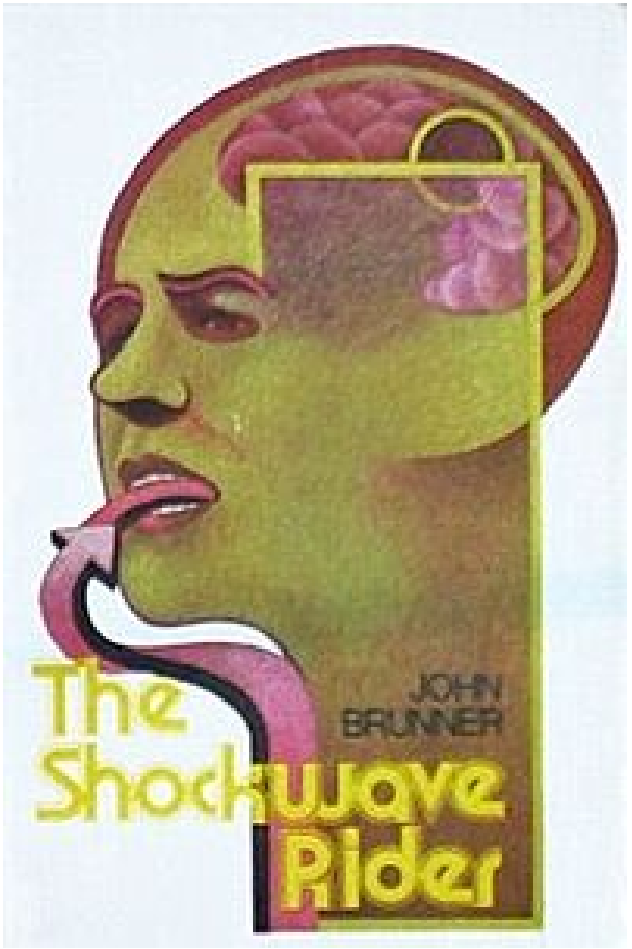
Viirused ja ussid

Arvutiviirus on programm, mis on peidetud mingi faili sisse, ja sealt võib käivituda ning arvutit nakatada. Viirus saatub arvutisse nakatatud faili arvutisse laadimisel, nt. viirus, mille nimi on "storm worm", mis tuleb e-posti manusest, n.t. nimega "*230 dead as storm batters Europe*."

Arvutiuss on programm, mis suudab turvaaugu kaudu arvutisse salvestuda, arvutis tööle hakata ja end sealt edasi levitada. Kui see kõik toimub automaatselt, võib uss levida väga kiiresti.

Arvutiussid tekkisid ammu

John Brunner, 1975.a.
tõi sisse arvutiussi mõiste
oma ulmeraamatus:



Suurt kahju tegi arvutiuss
Slammer 2003. a., levides
10 minutiga 75000 arvutisse.

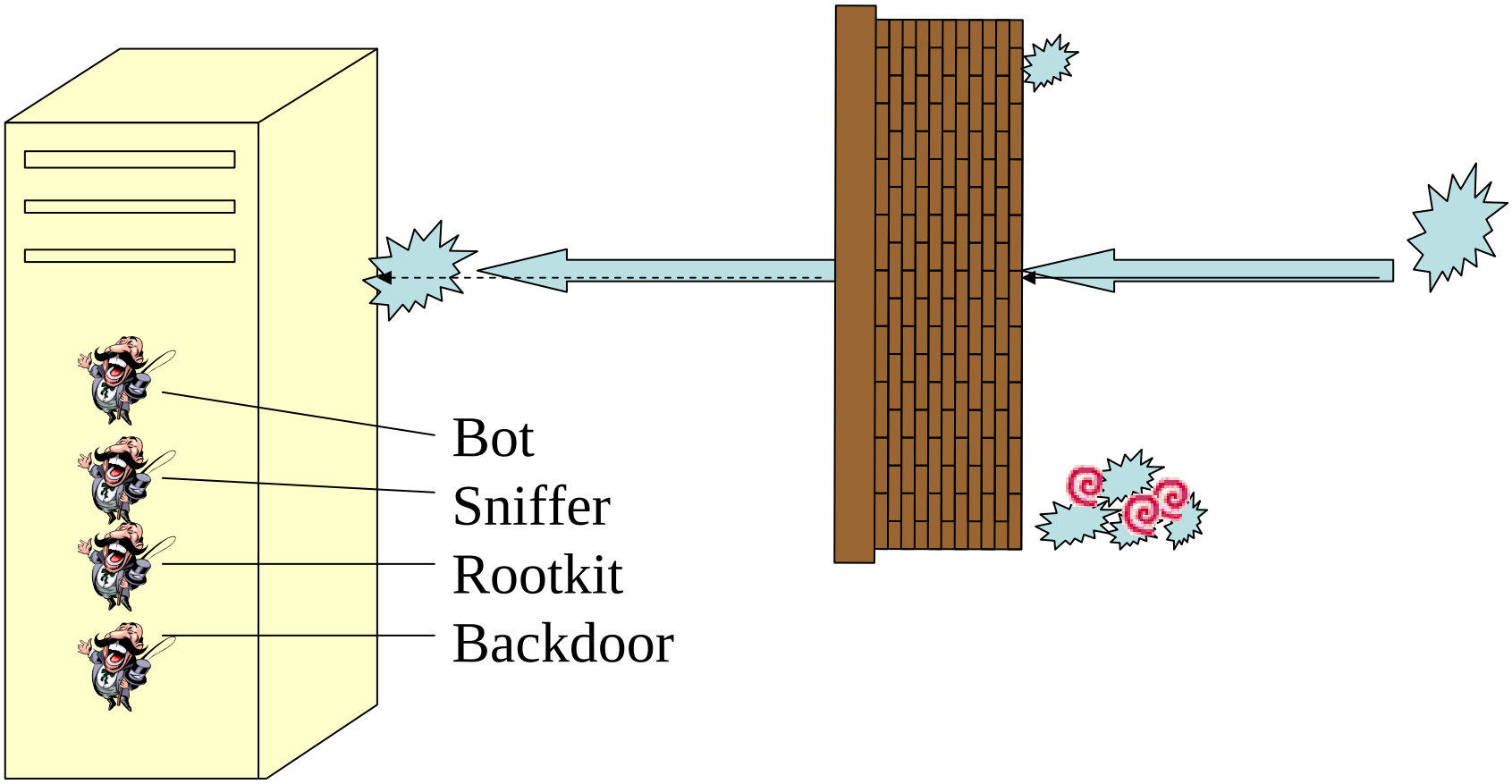
Botid, troojalased

Botiks kutsutaks juba arvutisse paigutunud kurivara, mis on võimeline üle Interneti suhtlema – sealt käske saama, andmeid ja käske edastama jne.

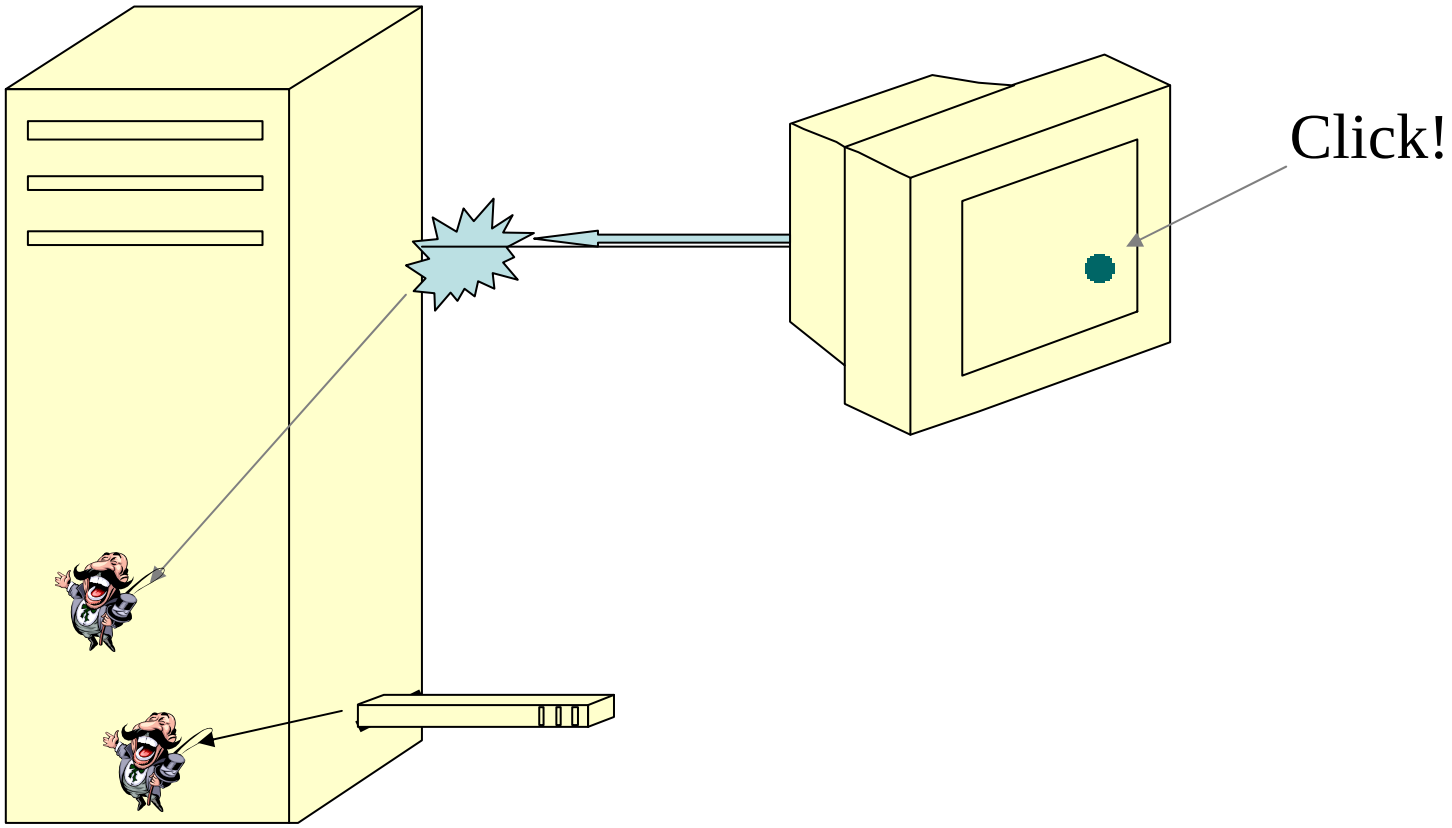
Troojalane on kurivara, mis näib olevat mingi tavaline ohutu programm, kuid sisaldab kahjulikke osi, mis võivad, näiteks olla:

tagauksed,
ebatuumad (rootkits),
snifferid.

Kuidas nakkus levib



Kuidas nakkus levib (2)



Kaitse

Kaitset kurivara vastu pakuvad:

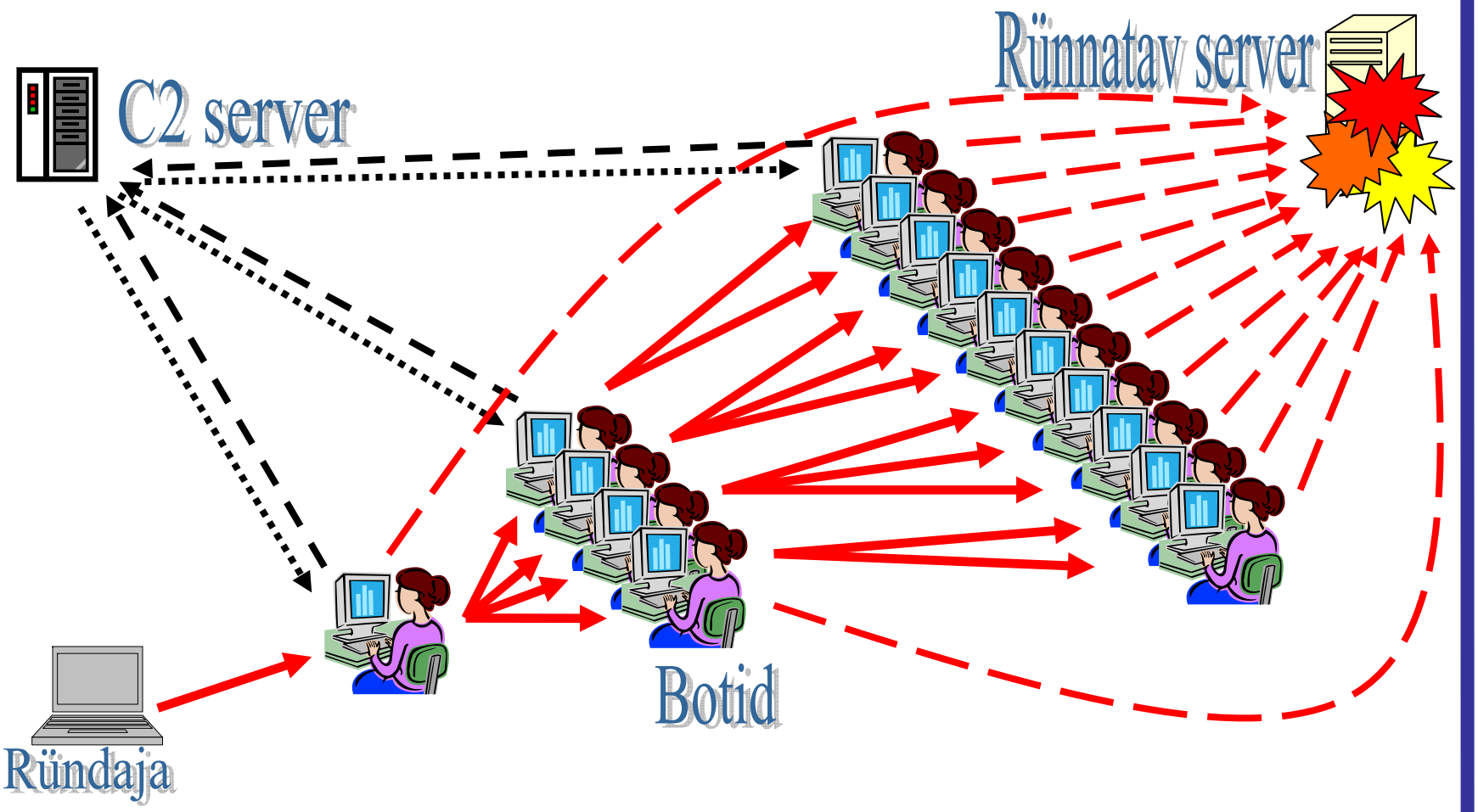
- Tulemüürid.
- Viirusetõrje programmid.
- Tarkvara parandused -- paigad, millega lapitakse tarkvara, et turvaauke kõrvaldada.
- Ettevaatus Internetis.

Igal juhul on vaja, et kaitstav arvuti saaks võimalikult ruttu parandused kätte, seda tehakse enamasti automaatselt.

Botivõrk

- Botivõrk on bottidest koosnev vägi Internetis, mida juhivad *kontrollijad*, kes täidavad neid omava inimese käske.
- Botnette koostatakse arvutite nakatamise ja neisse sel teel bottide tekitamise teel. (Selliselt nakatatud arvutit kutsutakse zombiks – ta ei “tea” mida ta teeb.)
- Botnettide suurus võib olla mõnest tuhandest kuni milojonite bottideni.

Teenusetõkestusrünne (DDoS)



Ründed Eesti vastu 2007 kevadel

Provotseeritud kübermäss (27-30APR) – rünnati riigi, meedia ja poliitikute veebisaite; üleskutse näide:

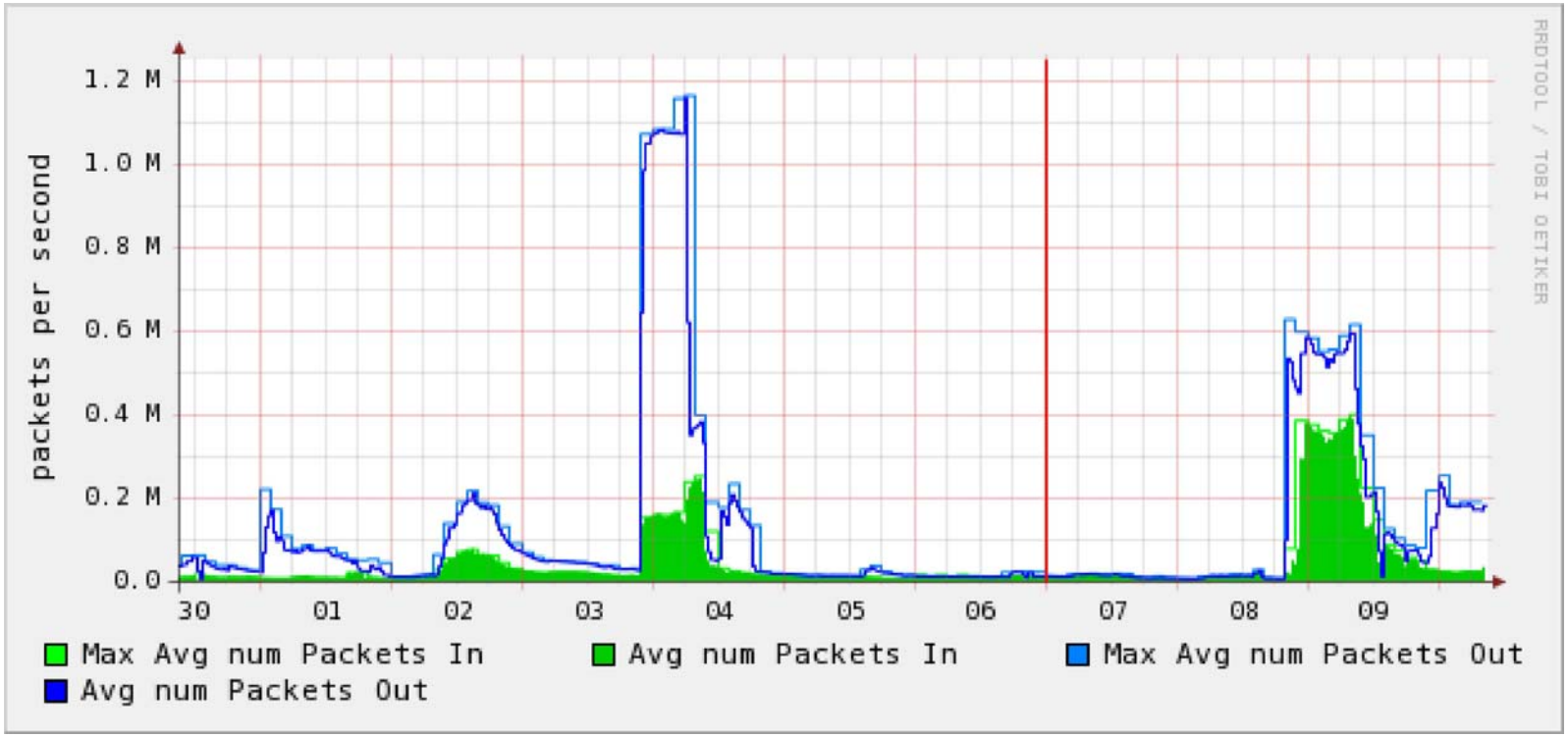
Сегодня, проводится грандиозная DoS-атака на сайт их правительства http://www.riik.ee/et/ ощуществить это легко - заходим в Пуск - Стандартные - командная строка, в открывшемся окне пишем :
ping -n 5000 -l 1000 http://www.riik.ee на это вы потратите 5 мегабайт исходящего трафика.

1. massilise ründe laine (04. mai) – ründe all ISP-d, pangad (Hansapank maas ca 1.5 tundi)
2. massilise ründe laine(08-11. mai) – ründed pankade ja ISP-de vastu
3. massilise ründe laine(15. mai) – ründed SEB vastu

Viimane suurem rünne (18. mai)

Ründed Eesti vastu

- DDoS ründed 04. mail 2007.



Ründed Gruusia vastu

- Riiklikud serverid võeti üle vaenlase poolt
- DDoS ründed Gruusia serverite vasu
- Muudeti pankade veebilehti – pandi üles valed valuutakursid
- Presidendi veebileht rikutud

Ründed Gruusia vastu

Oluliste veebilehtetede rikkumine:

- Pankade lehtedele valed valuutakursid
- Riigi lehtedele inetud pildid

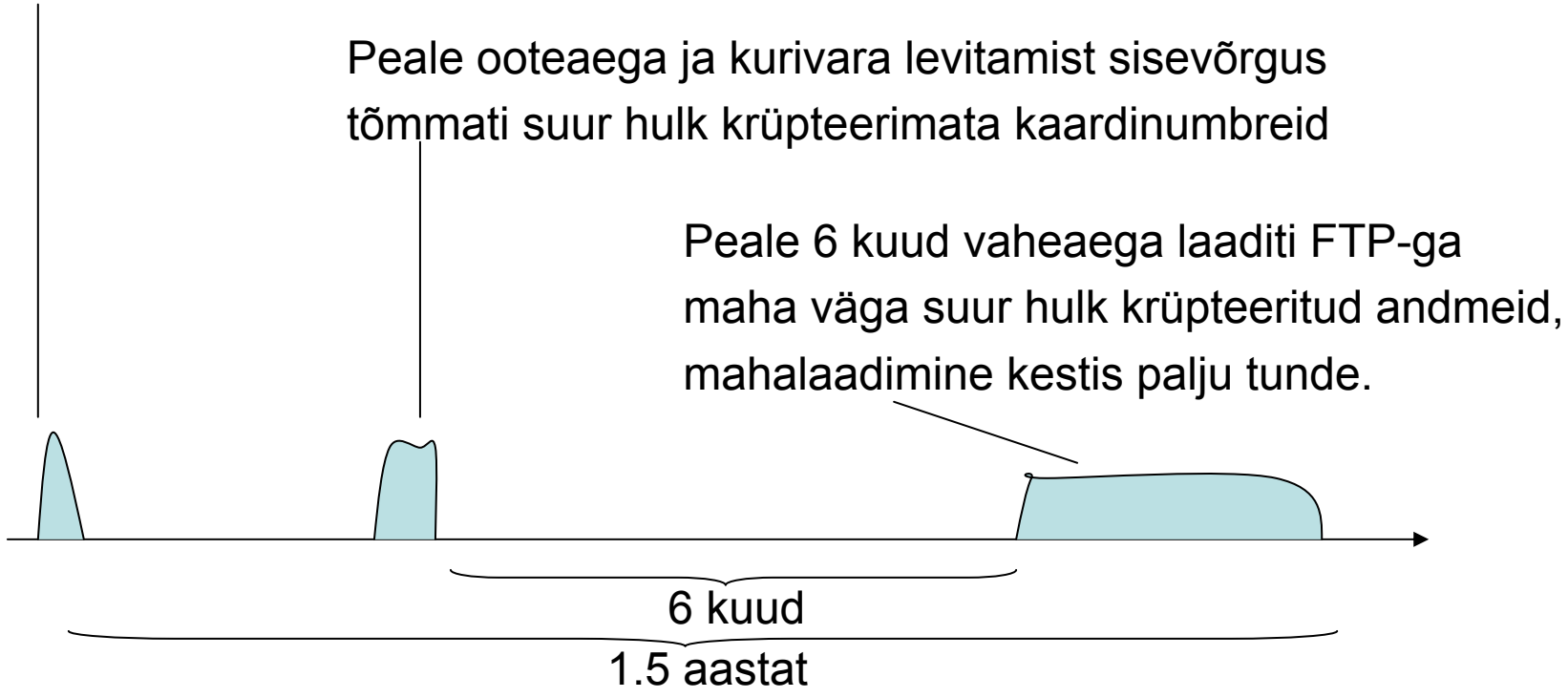
Suuremad pahandused viimasel aastal

- Varastati 45 miljoni TJX pangakaardi andmed, 11 kurikaela käes, üks neist Eestist.
- Jerome Kerviel rikkus reegleid ja Societe General kaotas ca 5 mlrd. Eurot.

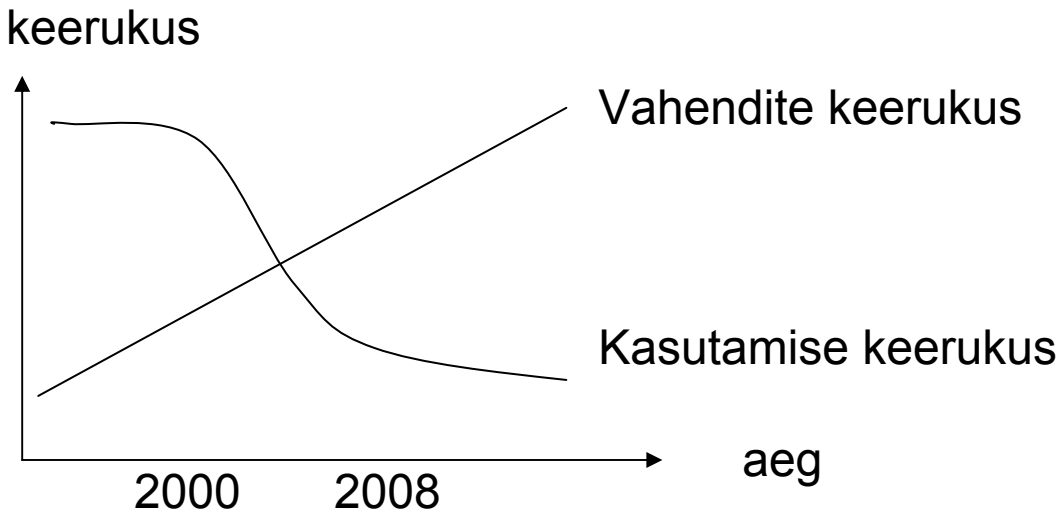
TJX pangakaartide info vargus

Kogu kuritöö kestis 1.5 aastat. Kokku varastati TJX andmebaasidest üle 45milojoni pangakaardi andmed.

Algas sellest, et WallMart poe WiFi kaudu saadi juurdepääs sisevõrku

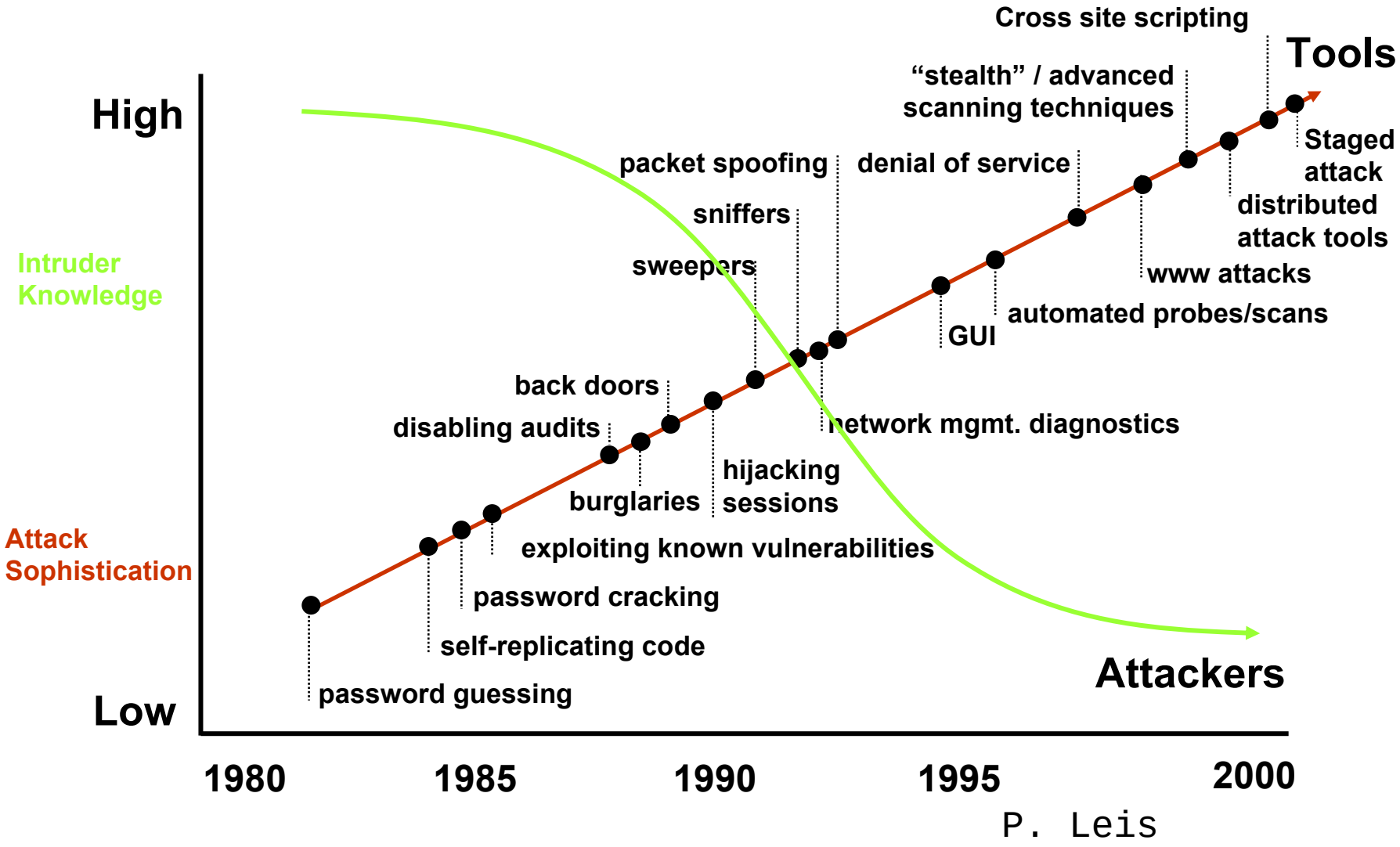


Küberründed muutuvad



- On teada ca 13 miljonit kurivara tüüpi, sh 50000 rootkitti.
- Küberründed on saanud proffide tegevuseks.
- Päevas toimub ca 500000 rünnet.
- Küberkuriteod muutuvad sündikaatide tegevuseks.

Attack Sophistication vs. Intruder Technical Knowledge



We Used to be Fighting these...

- **Chen-Ing Hau**
  Author of
  the CIH virus

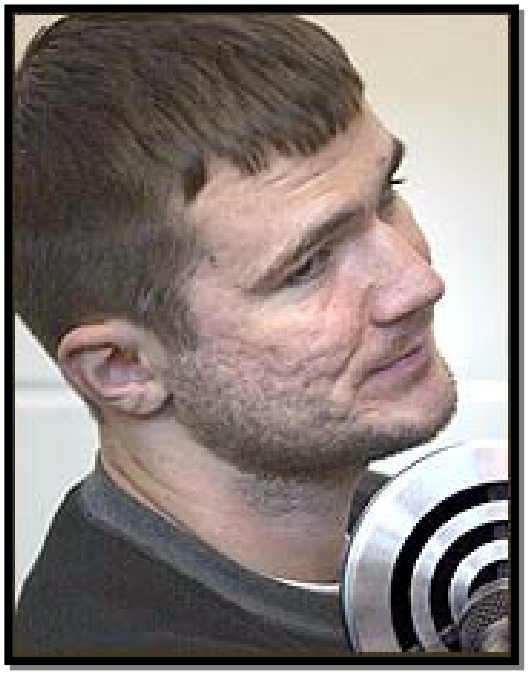
- **Joseph McElroy**
  Hacked the
  Fermi lab
  network

- **Jeffrey Parson**
  Author of
  Blaster.C

Today we are Fighting these!

- **Jeremy Jaynes**
  Millionaire,
  and a spammer

- **Jay Echouafni**
  CEO,
  and a DDoS attacker



- **Andrew Schwarmkoff**
  Member of Russian mob,
  and a phisher

Kes ma olen küberruumis?

Olen see,

- kellena end esitlen
- kellena mind teatakse
- mida ma teen
- mis on minu kohta Internetis.

Kübersootsium

Kas küberruum kui metsik lääs?

Tõepoolest, küberruumi sotsiaalne õhkkond on sellekohane:

- Anonüümsus
- Heade tavade vähesus
- Seaduste puudumine
- Kiire rikastumise võimalused
- Karistamatuse tunne

Siiski, valdav enamus küberruumis tegutsejatest on igati korralikud küberruumi kodanikud.

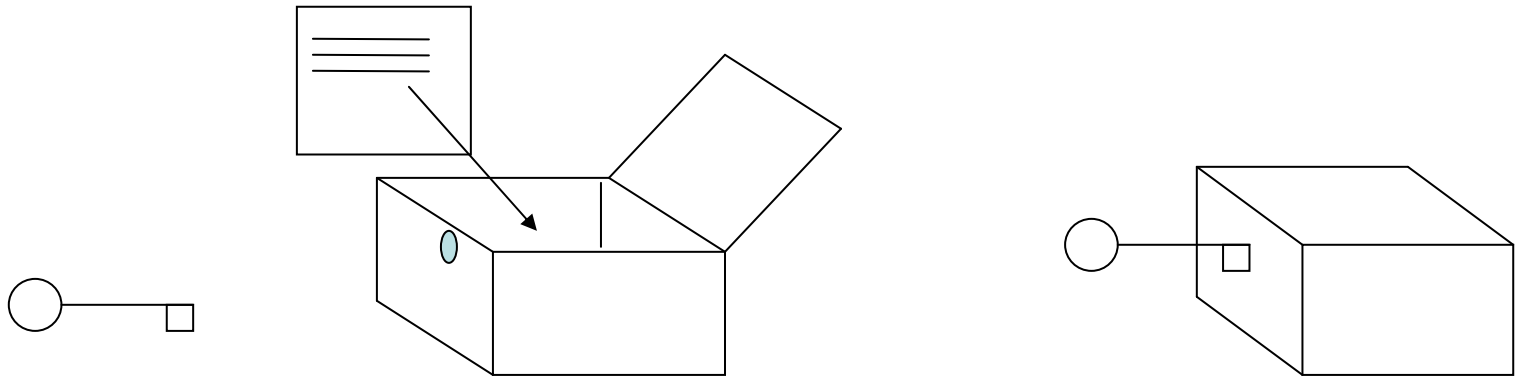
Infosõda

Küberruumi kontrollimatus võimaldab seal karistamatult pidada infosõda – levitada väärinfot, ässitada kuritegudele jne. Seda kasutati küberkallaletungidel Eesti ja Gruusia vastu.

- **Сегодня, проводится грандиозная DoS-атака на сайт их правительства http://www.riik.ee/et/ ооуществить это легко - заходим в Пуск - Стандартные - командная строка, в открывшемся окне пишем : ping -n 5000 -l 1000 http://www.riik.ee - на это вы потратите 5 мегабайт исходящего трафика.**

Krüpto

Oma andmetes sisalduva info kaitsmiseks saab andmeid krüpteerida e. šifreerida -- muuta võtme abil nii, et tekkivad andmed ei anna infot välja, kui võtit ei ole.



Avalikud võtmed

Kasutatakse ka sellist krüpteerimist, mil andmete salastamiseks on üks võti ja taastamiseks on teine võti. Sõltuvalt krüpteerimise otstarbest, ühe neist võtmeist võib avalikustada ja seda usaldusväärselt levitada. Kuid selleks on vaja mingit üldkasutatavat ja usaldusväärset süsteemi: avaliku võtme infrastruktuuri (PKI). Seda tuleb eriti kaitsta.

Mida teha?

- Kaitsta kriitilist info infrastruktuuri
- Õpetada turvalist arvutikasutust
- Arendada eetilist käitumist küberruumis
- Töötada välja turvalisemat tarkvara
- Töötada välja ja rakendada küberruumi seadused
- Arendada rahvusvahelist koostööd.