LATVIJAS UNIVERSITĀTE
ANNO 1919

Drošības virstēriņa minimizēšana ZERO Ethernet pār IP tunelēšanas protokolā

Artūrs Lavrenovs al07058

Vadītājs: profesors Dr. dat. Guntis Bārzdiņš

28.01.2015.

LATVIJAS UNIVERSITĀTE
ANNO 1919

Prezentācija

- Kas tika stāstīts iepriekšējā reizē?
- Kas tika darīts pēc tam?
- Kas šobrīd tiek darīts?
- Ko plānots darīt nākotnē?

ZERO

- Hipotēzes – ir iespējams
  - Atrisināt problēmas
  - Risinājums bezvadu tīklos
  - Iegūt ātrdarbību un stabilitāti, kas tiecas uz bez tuneļa rādītājiem
- Kā to paveikt
  - Jāsamazina katras individuālās datu paketes virstēriņu
  - Jāiegūst minimālu protokola virstēriņu
  - Jānovērš datu pakešu fragmentāciju

LATVIJAS UNIVERSITATE
ANNO 1919

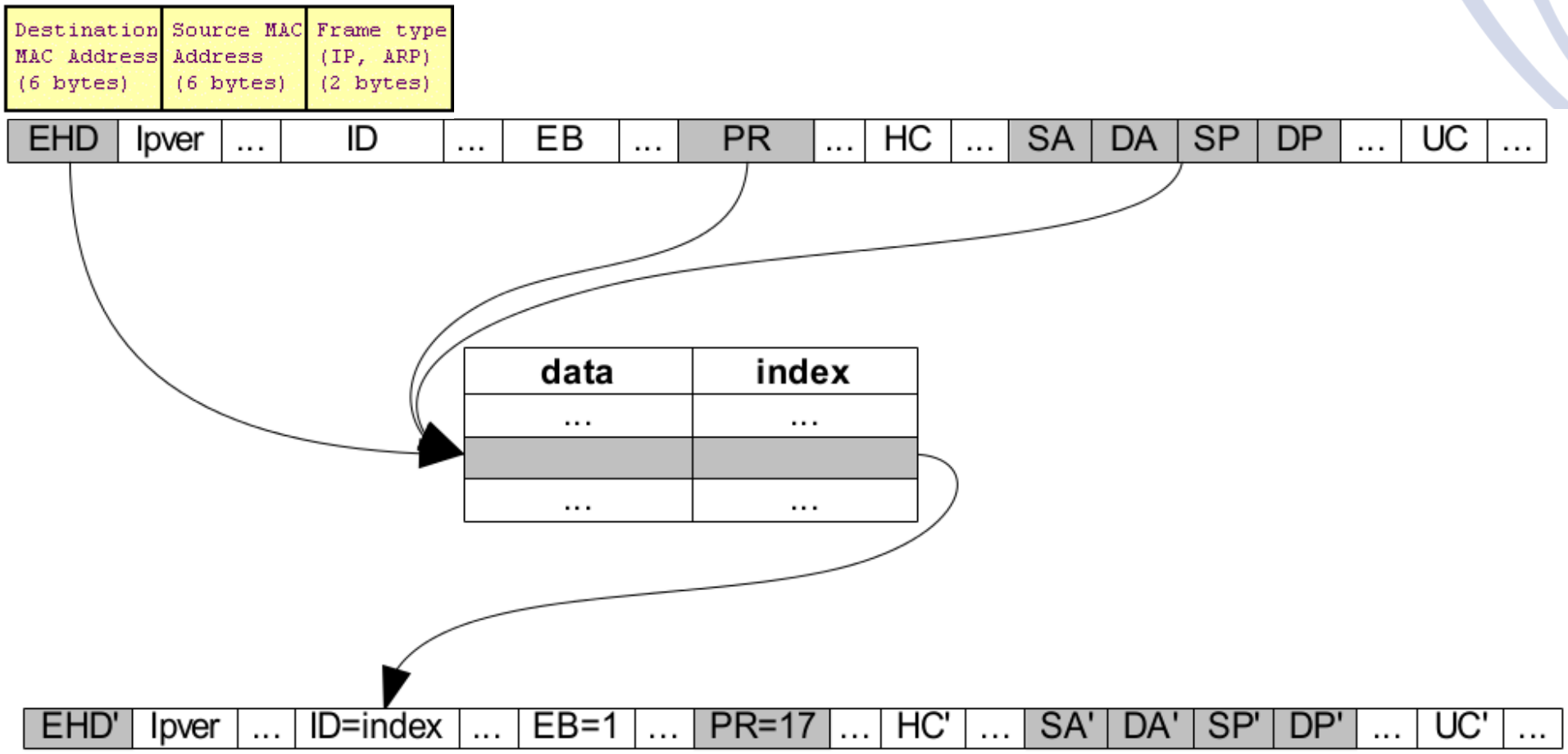
ZERO realizācija

- L2 pār IP tunelis
- Pilnībā novērst fragmentāciju nav iespējams, bet pilnībā pietiek ar tiekšanos uz 100%, novērš fragmentāciju visbiežākajos (NICE) gadījumos
  - UDP un TCP paketes
  - Nav izmantoti specifiskie tehniskie lauki
- Eksperimentāli maksimāli sasniegts līdz pat 99.94% pakešu pārsūtīšana bez fragmentācijas
- Efektīvi komunikāciju sesijām

ZERO saspiešana

- Pārpietiekamu datu saspiešana OSI L2
  - Izvēlas tādus datu laukus, kas mainās reti komunikāciju sesiju ietvaros
- Tiek veidota vārdnīca
- Vārdnīca tiek sinhronizēta pēc iespējas retāk
- Sinhronizācijā konkrētajā paketē tiek pārsūtīta kopā ar datiem, izraisot fragmentāciju tikai sinhronizācijas brīdī
- Vārdnīcas identifikators tiek iekodēts bez virstēriņa, lietojot “brīvos” laukus, novēršot fragmentāciju

ZERO darbībā



Pētījuma virzieni

- **Drošība**
- Internet of things
- Implementācija gala iekārtās (mobilās, iegultās, serveri u.c.)
- Uzticamie tīkli
- L2 mākoņi
- Jauni IP tīkla projektējuma modeļi
- Pielietojumi, kas šobrīd neizmanto tunelēšanu

LATVIJAS UNIVERSITĀTE
ANNO 1919

Pēc stāstījuma

- Neilgi pēc iepriekšējā stāstījuma tēma tika *atlikta*
- Problēmu nav
  - Izdomāt un teoretizēt
- Problēmas
  - Plika teoretizēšana neiet cauri šajā nozarē
  - Ļoti daudz inženieriska darba
  - Zema līmeņa programmēšana (individuāla problēma)
    - Prasība prototipiem ir būt efektīviem, ieinteresētās puses grib redzēt rezultātus reālā dzīvē
  - Grūti iegūt publicējamus rezultātus

NTP

- Apstākļu sakritības rezultātā saskāros ar NTP lietām
- 2013. gada Ziemassvētkos pirms ~1gada+1mēneša sākās NTP DDoS
- NTP - Pulksteņu sinhronizācija
  - Laiks ir svarīgs daudzās iekārtās
  - Izmanto datori, portatīvie datori, serveri, mobilās iekārtas, tīkla iekārtas u.c.
  - Bieži šajā iekārtās pulksteņi ļoti neprecīzi vai to nav vispār

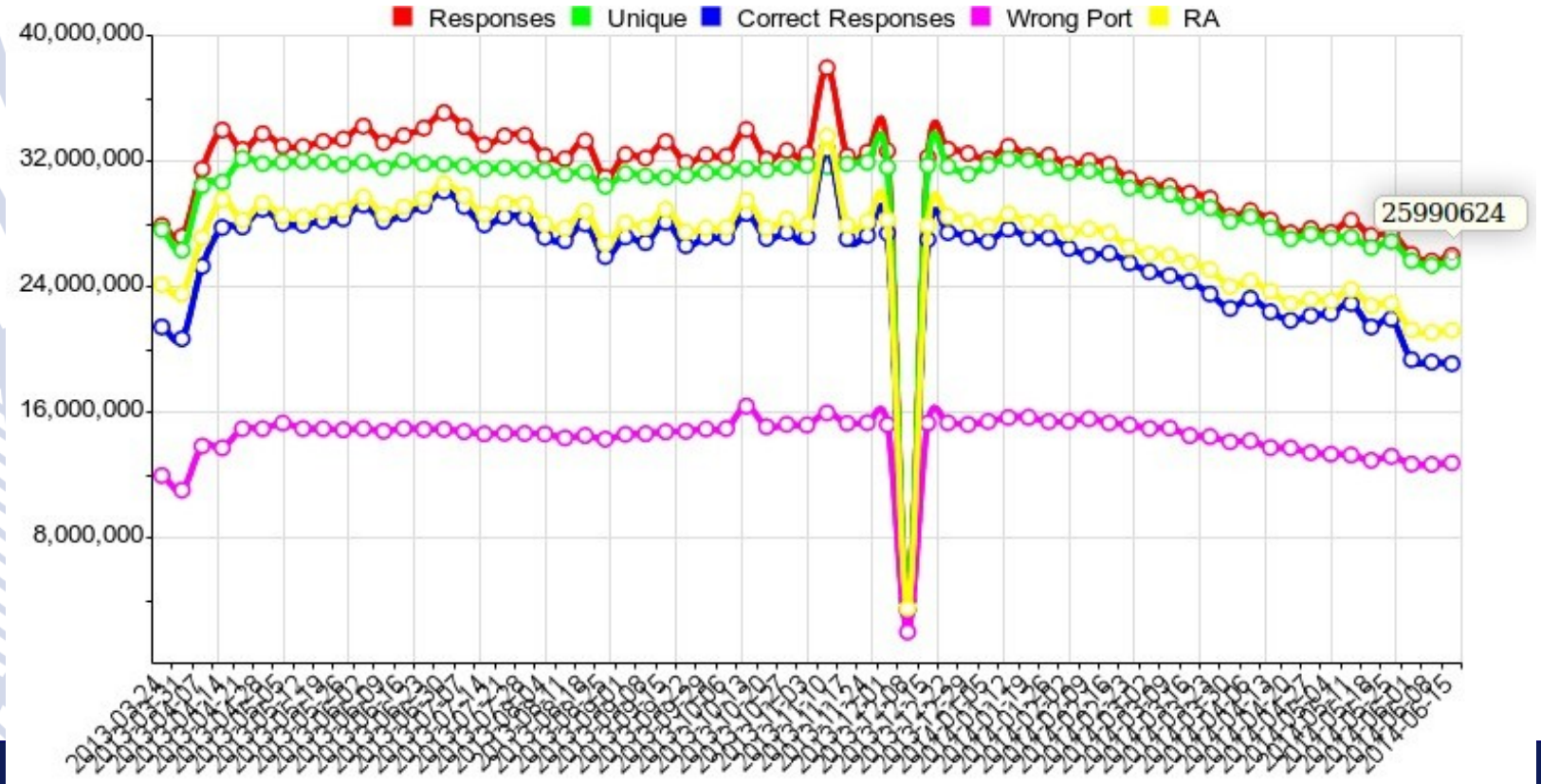
LATVIJAS UNIVERSITATE
ANNO 1919

DDoS

- Pakalpojuma atteices uzbrukumi
- Sen zināma reāla problēma Internetā
- Daudz pētījumu un publikāciju
- Pētnieciskās metodes
  - Darknet
  - Transit / Victim logs
  - Procotol analysis
  - Internet scanning and measuring
  - Honeypots

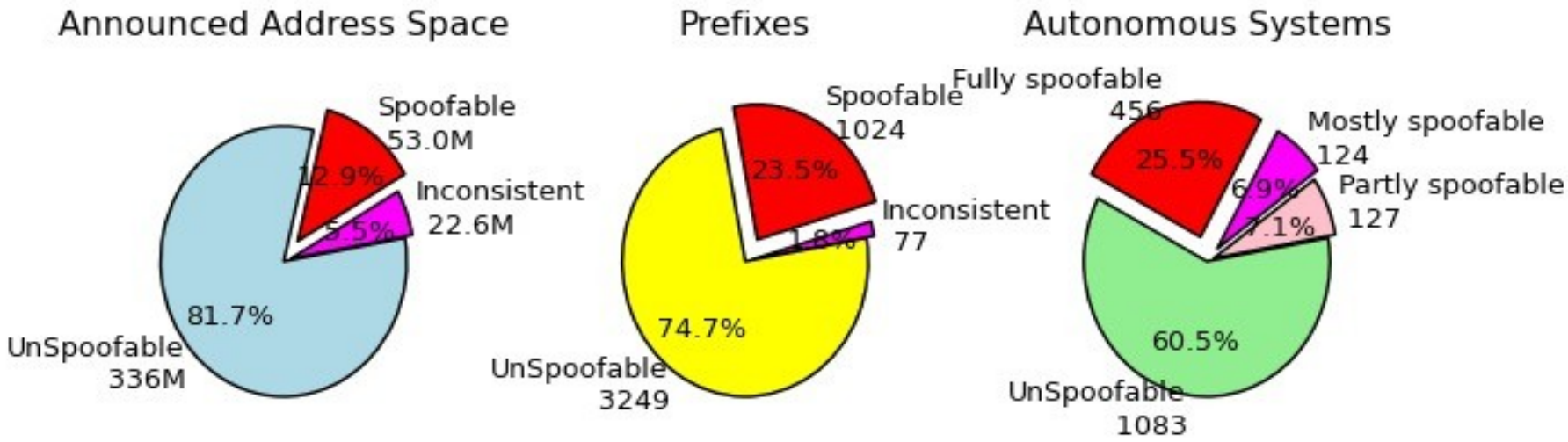
DDoS cēlonis #1

- Internetā brīvi pieejami pakalpojumi
- Piemēram, DNS, NTP u.c. (UDP)
- DNS piemērs no OpenResolverProject



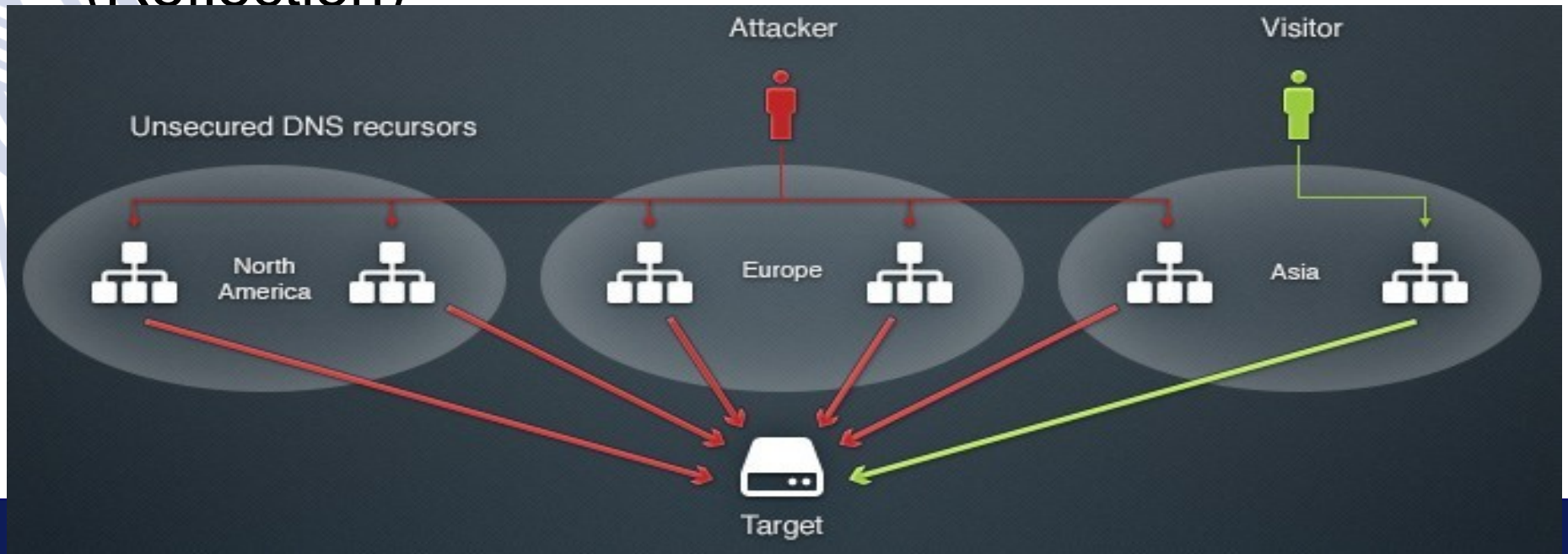
DDoS cēlonis #2

- IP adrešu viltošana (spoofing)



DDoS sekas

- Uzbrucējs vilto paketes ar upura IP adresi (Spoofing)
- Izveido paketes ar pēc iespējas lielākām sagaidāmām atbildēm (Amplification)
- Sūta paketes Internetā pieejamiem serveriem (Reflection)



NTP pētījums

- Paver iespēju analizēt DDoS upurus novērotājiem no malas
  - Viss pārējais vai nu nepubliska informācija vai nepilns skats
- Nekad šādas iespējas nav bijis
- Nav publikāciju par šādu tēmu
- Atbilstoši Darjas Šmites mācītajam – neslēpt, ja kāda pētniecības ideja rodas
  - Nevienam liela sajūsma neradās

LATVIJAS UNIVERSITATE
ANNO 1919

NTP problēma

- *monlist* komanda
- Nav protokolā, tikai un vienīgi implementācijas *debug* iespēja
- Pēdējie 600 klienti
- Maksimālās standarta amplifikācijas faktors 4670
- Vēsturiski lielākie DDoS uzbrukumi – 400Gbps, 2014.g. janvāris-marts

NTP *monlist* izpēte

- *monlist* komandas rezultāts
- Ko šie dati nozīmē?

```
Client IP       Client port                    Count
...
54.72.96.203              80 0.0.0.0           17842 7 2      0      0   59149
184.105.139.112        54032 0.0.0.0               1 6 2      0      0   59782
...
```

NTP *monlist* izpēte

- Skenējam visu Internetu (/0)
- Atrodam visus NTP laika serverus Internetā (~14 miljoni)
- Atrodam visus NTP, kas atbild uz monlist, pirms gada >1 miljons, šobrīd <100 tūkst.
- Saglabājam visas saņemtās *monlist* atbildes

LATVIJAS UNIVERSITATE
ANNO 1919

NTP anomālijas

- Lielākā anomālija uz vienu pieprasījuma UDP paketi, tiek saņemti miljoni atbilžu pakešu (daudz GB)
- Daži 10 šādu IP adrešu, var pielietot DDoS
- Viss Japānā, izskatās pēc kādas maršrutēšanas cilpas
- Sabojāja daudz mērījumus, jāsāk no jauna

Daži NTP rezultāti

- Redzam lielākos upurus (DoD, CSC)
- Redzam lielākos uzbrucējus
  - Dažādi IPS, kas piedāvā pakalpojumus biznesam
  - Pārsvarā ar sliktu pārvaldību, t.sk., vairāki no Krievijas
- Redzam lielākās upuru klases
  - Tīmekļa bāzēti risinājumi
  - Spēļu industrija, pārsvarā indivīdi
- Citi – uzbrukumu identificēšana, uzbrukumu izmēri, aktuālā uzbrukumu kapacitāte

Pasaulē publicēts

- Oktobrī pasaulē parādās publikācijas par konkrēto tēmu
- *Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks*
  - *... the **first study** to measure amplification-type DDoS attack activity via a direct global survey of records on the amplification hosts themselves ...*
- Pasaules līmeņa autori
- Viss manis izpētītais tur jau ir iekšā, bet augstākā kvalitātē
- Ko no tā varu secināt?
  - Tātad pētījuma ideja, dizains, darbs bija pareizā virzienā
  - Uzvarēt sacensībā ar pasaules milžiem izredžu nav

Pētījumu jēga

- Šāda veida pētījumi mēģina iegrožot problēmu
- Izglītot publiku, t.sk., industriju
- Ļaundaru aktivitāšu uzraudzība
- Jaunas zināšanas, ko varētu pielietot nākotnē līdzīgā situācijā

NTP citas iespējas

- Mēģinājumi turpināt kaut ko NTP virzienā, lai viss ieguldītais laiks nebūtu pilnīgi bezjēdzīgs
- Detalizēta upuru izpēte
  - Ikdienas *monlist* ievākšana
  - Upuru identificēšana un klasificēšana
  - Uzbrukumu mērīšana
  - Ko dara upuri? (Metodoloģija?)
- BAF precīza mērīšana
- Izmaiņu analīze

IM

- Internet Measurement
- Pētnieki nevar īsti saprast, kas tā ir par nozari, tādēļ izdala savu ar savām konferencēm (ACM IMC) un žurnāliem
  - Daļa vispār neuzskata par vērtīgu
- Mēram kādus faktorus Internetā, izdarām secinājumus – esam ieguvuši jaunas zināšanas – atbilst pētniecībai
- Parasti pārklājas ar citām nozarēm – datortīkli, drošība u.tml.

IM kā disertācija

- +Vai IM ir atzīta nozare?
  - Ir konferences, ir žurnāli, pasaulē ir laboratorijas
- +Vai man ir interese?
- ~Vai Es spēju publicēties IM nozarē?
  - Pagājušā gada mēģinājums ir izgāzies, jauni mēģinājumi šobrīd
- -Vai es varu iegūt *labās* publikācijas
  - Šobrīd nav skaidrs
- -Vai var sakombinēt pētījumus disertācijā?
  - Šobrīd skaidras vīzijas nav

Tuvākā nākotne

- Mēģinājumi glābt vismaz kaut ko no NTP darba
- DDoS novirzienā citas tēmas
- Citas IM un drošības pārklāšanās vietas
- Mēģināt vairākus novirzienus vienlaicīgi, lai vismaz kaut kas sanāktu, ja kāds cits publicējas
- Studēt publicētos pētījumus, kas nav IM, bet publicējas tajos pašos izdevumos

Pētniecība citur

- CERT.LV nav pazīstama publicējama pētījuma koncepcija
- Čehu un citos certos jau labāk, pārsvarā uz vizualizāciju
- Zviedru projektos vairāk uz virtualizāciju
- Specsemināra “IT drošība” ietvarā mēģinām popularizēt pētniecību, publicējamu rezultātu pagaidām nav
- Rezultātā šobrīd viens pats Latvijā, kam interese dotajā IM/drošības nozarē

Ja IM neizdodas

- ~6 mēnešos varētu būt skaidrs, vai IM kaut kas izdodas
- Potenciāli atgriezties pie ZERO
- PTL implementācija potenciāli samazina zema līmeņa programmēšanas apjomu
- Atkarīgs no tā, kas turpmāk notiks ar ZERO
- Bet sākt no otra gala – no daudzajiem virzieniem izvēlēties tos, kur visvairāk publicēšanās iespēju

LATVIJAS UNIVERSITĀTE
ANNO 1919

Paldies par uzmanību!

Jautājumi?