Economics of Cyber Security

Risk Management Summer Course
Mon 4th – Fri 15th July 2016

Maciej Korczyński
Delft University of Technology

12 July 2016, Delft, The Netherlands

What is economics of cyber security?

What is economics of cyber security?

- Economics

What is economics of cyber security?

- Economics
- Computer science

What is economics of cyber security?

- Economics
- Computer science
- Policy

What is economics of cyber security?

- Economics
- Computer science
- Policy
- Governance
- …

What is economics of cyber security?

security
computer
hang
night
data
safe
guard
perform
fraud
meets
geeks
using
risk
cyberpeace
like
keep
decision-making
policy/internet
approaches
great
zeros
scientist
subjects
break
economics
support
cybersecurity
administrator
bums
ph.d
human
internet
ones
protecting
statistical
cybercrime
governance
evangelist
network
information
teach
help
abuse
work
technical
scourges
candidate
research
guys
prism
analytical
banks
reality
systems
science
cyber
privacy
excellent
around
bad

Research questions

Agenda

- Framework (interplay between costs benefits, and levels of security)

Agenda

- Framework (interplay between costs benefits, and levels of security)
- Security reputation metrics
  - What to measure?
  - Measuring security levels

securityMETRICS ✓Certified

Agenda

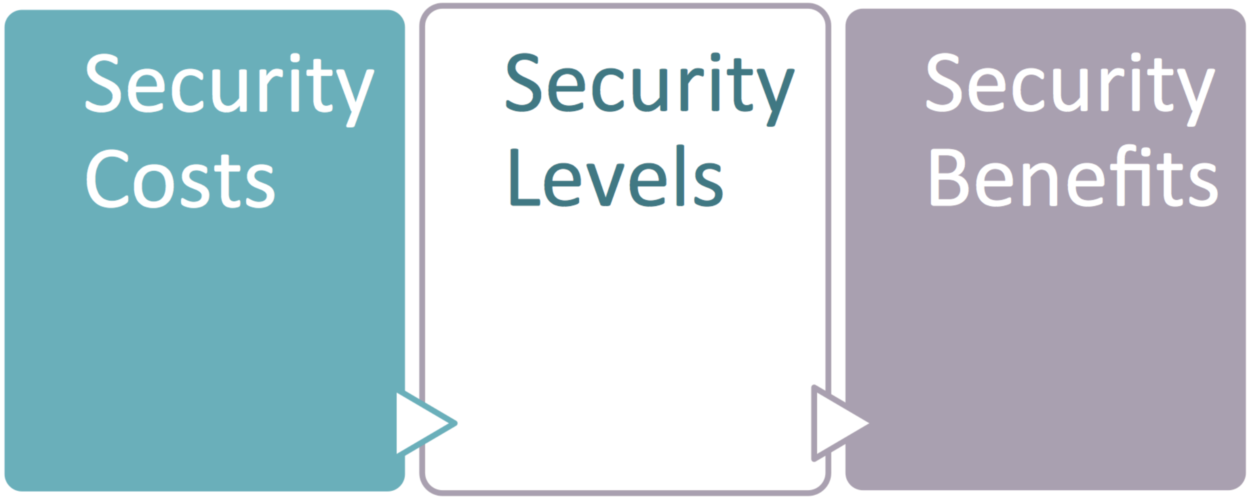
- Framework (interplay between costs benefits, and levels of security)
- Security reputation metrics
  - What to measure?
  - Measuring security levels
- Practical examples
  - Security reputation metrics for top-level domains
  - Security metrics for hosting providers

Agenda

- Framework (interplay between costs benefits, and levels of security)
- Security reputation metrics
  - What to measure?
  - Measuring security levels
- Practical examples
  - Security reputation metrics for top-level domains
  - Security metrics for hosting providers

Cost, benefit, and levels of security

- Resources for information security are very limited



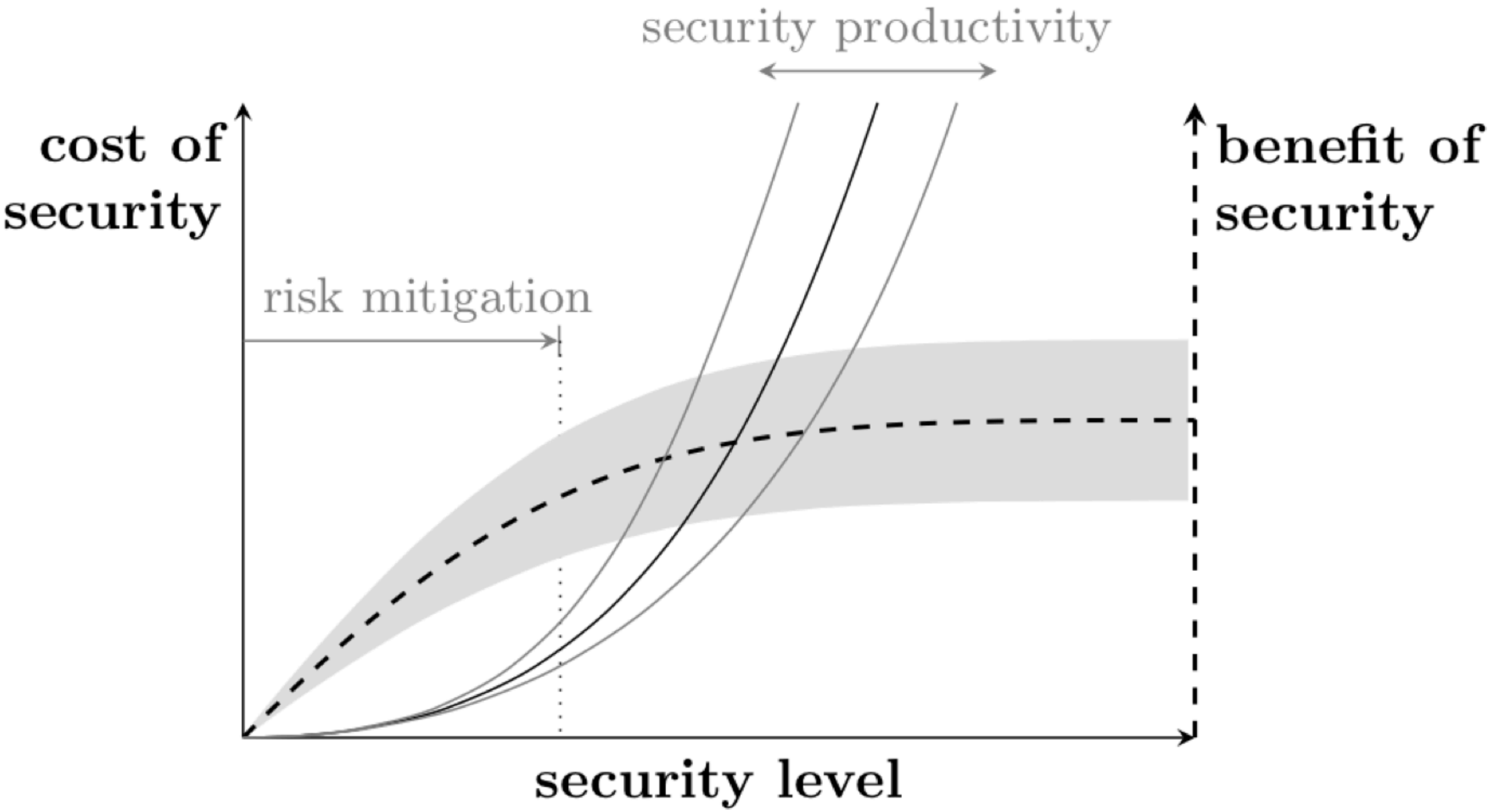
Security Costs

Security Levels

Security Benefits

Source: "Economics of Cyber security: What to measure?"

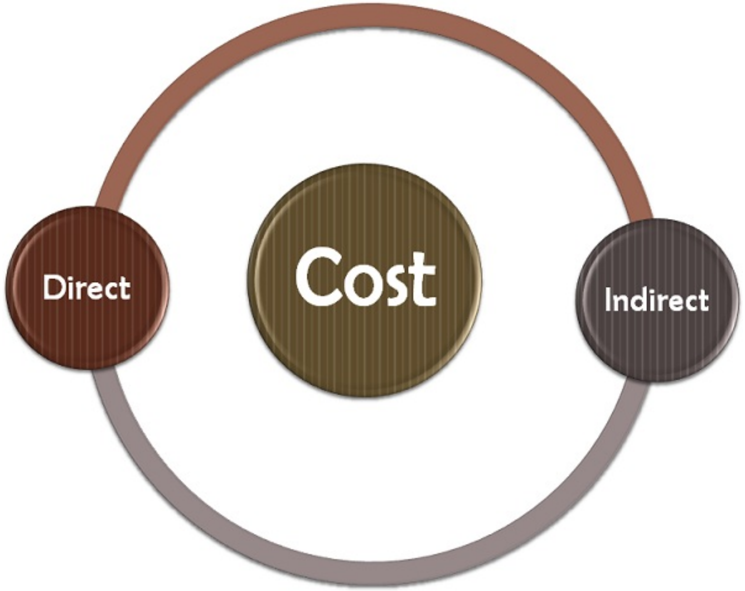
Cost, benefit, and levels of security



Source: “Economics of Cyber security: What to measure?”

Cost of security

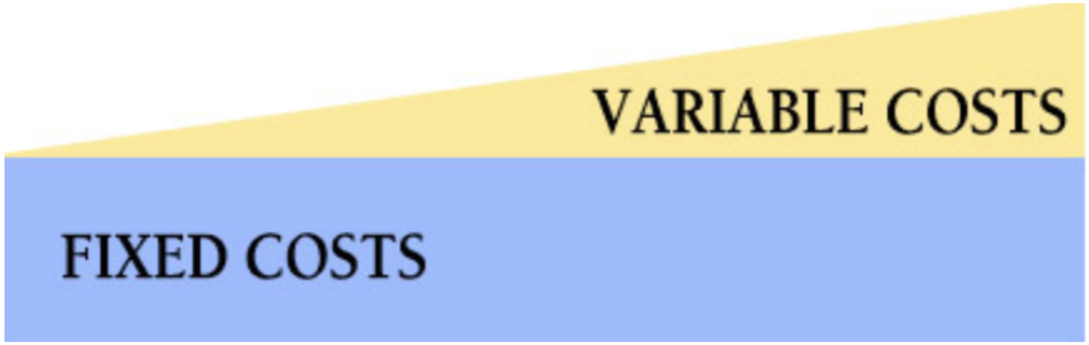
- Direct versus indirect costs



Cost of security

- Direct versus indirect costs
- Fixed versus variable costs:

  (in)dependent of the activity in the core business



Cost of security

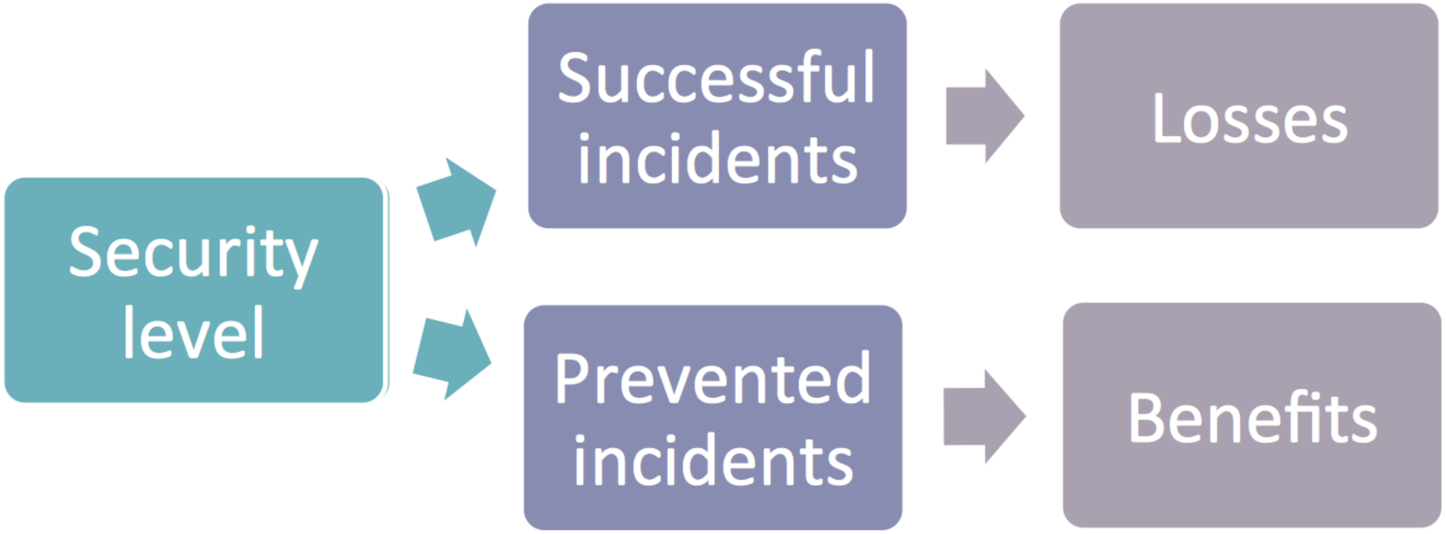
- Direct versus indirect costs
- Fixed versus variable costs:

  (in)dependent of the activity in the core business
- Periodical costs:
  - Onetime, recurring, sunk, recoverable

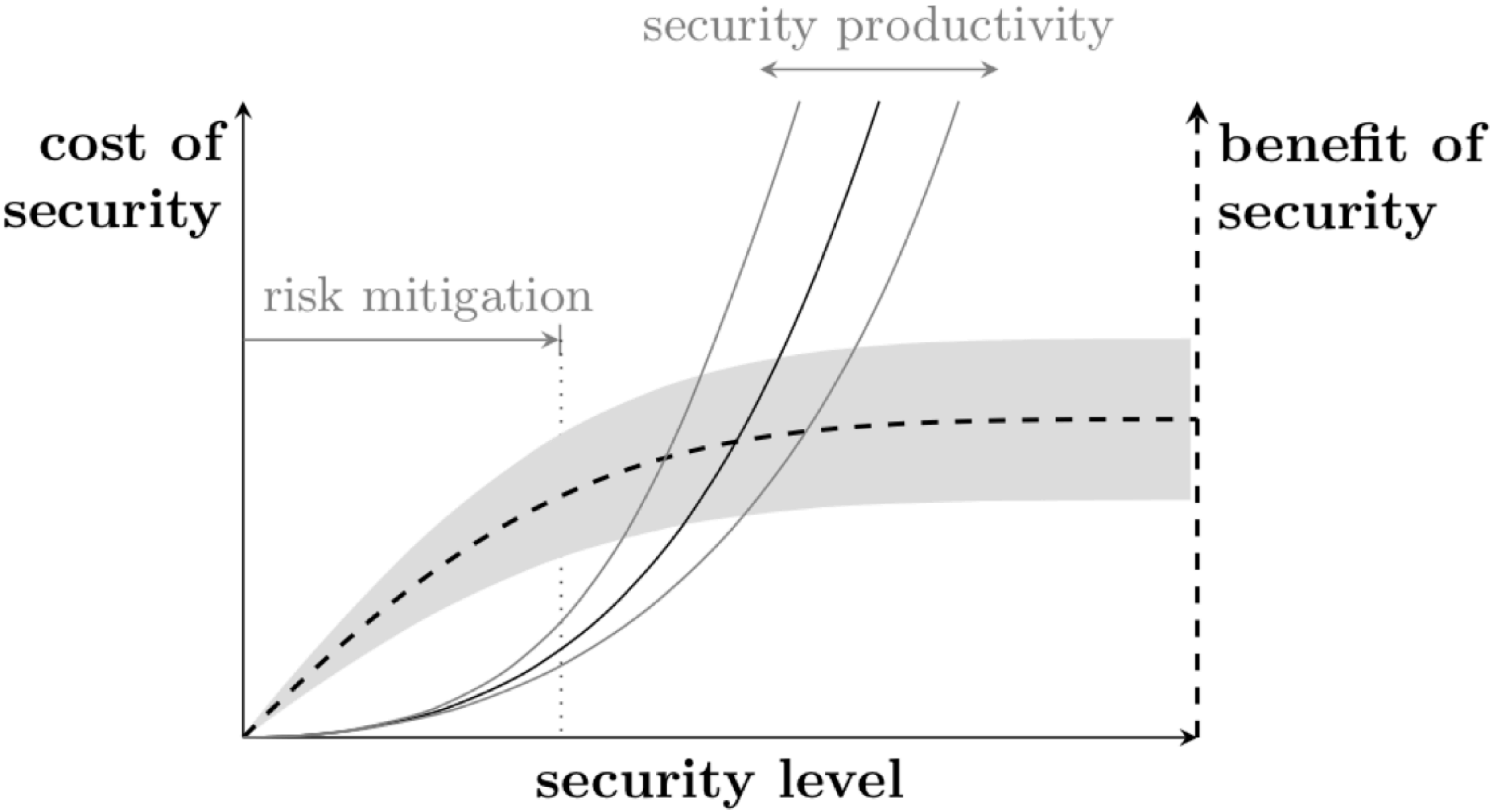
Security level

- Deterministic indicators:
  - Software vulnerabilities
  - Virus scanners
- Stochastic indicators:
  - Compromised machines
  - Stolen (e.g. phished) credential

Benefit of security



Cost, benefit, and levels of security



Source: “Economics of Cyber security: What to measure?”

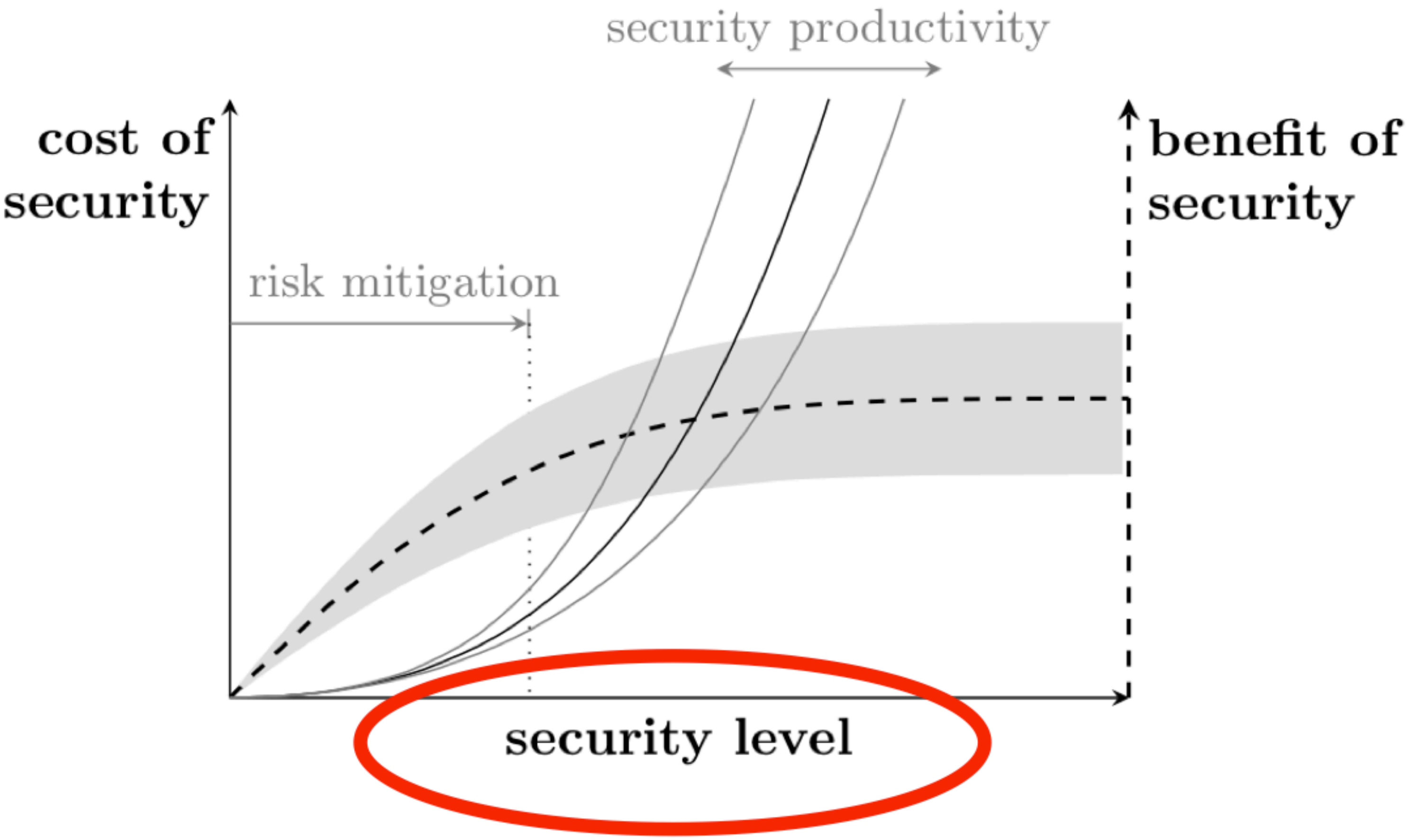
Agenda

- Framework (interplay between costs benefits, and levels of security)
- Security reputation metrics
  - What to measure?
  - Measuring security levels

securityMETRICS ✓Certified

- Practical examples
  - Security reputation metrics for top-level domains
  - Security metrics for hosting providers

Security level



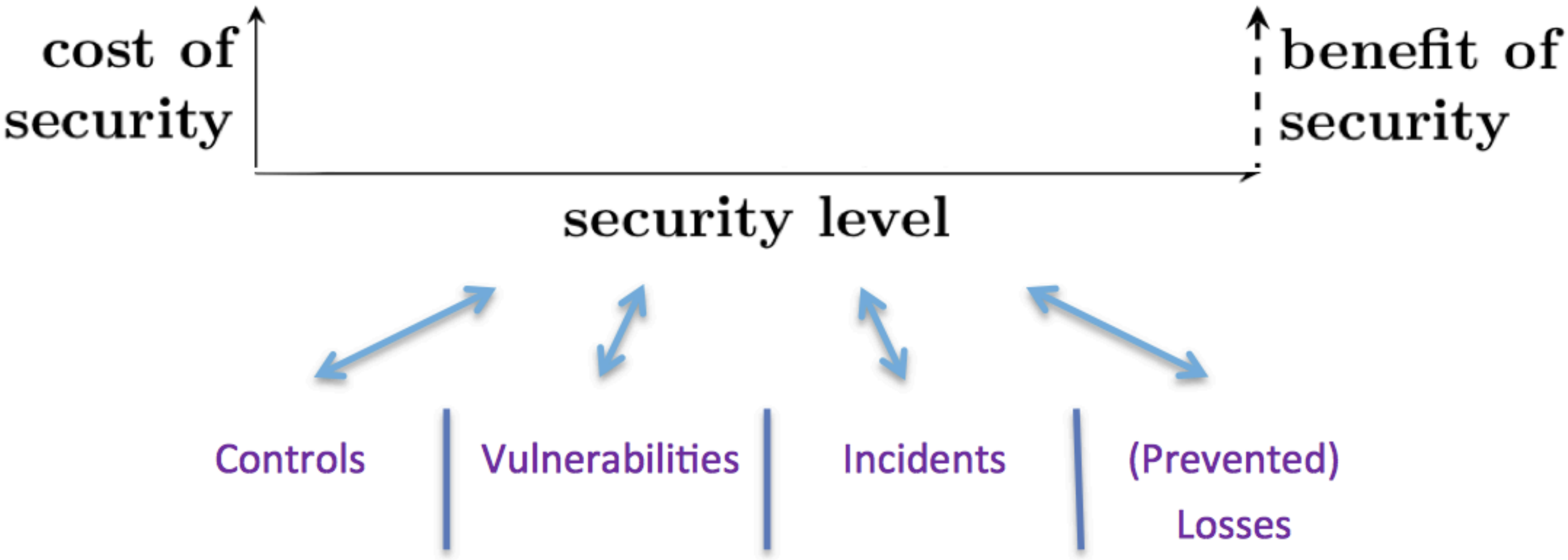
Source: "Economics of Cyber security: What to measure?"

What is measurable?

What is measurable?

- Security level cannot be observed or measured directly
- We can define and measure indicators or metrics that reflect different aspects of the security level
- Together, the metrics give us an estimation of the security level

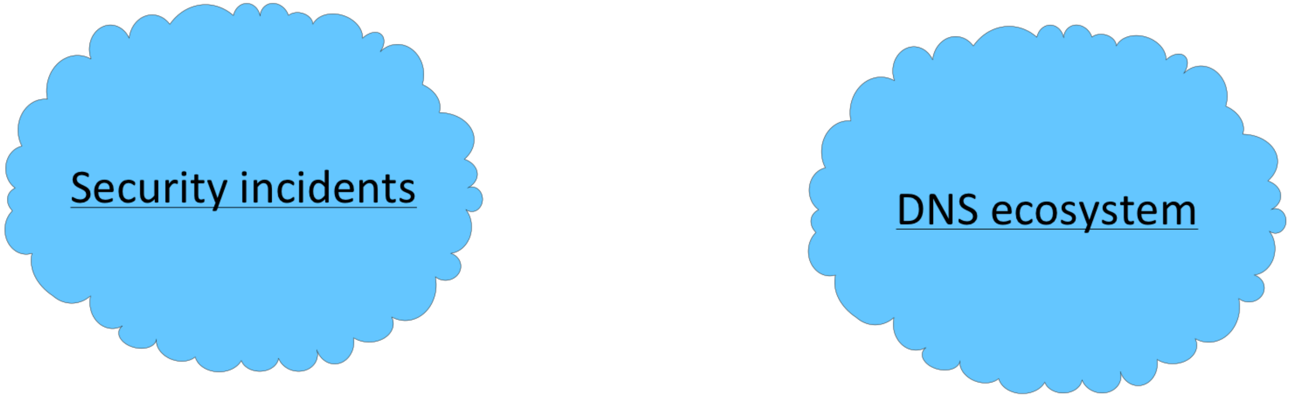
Types of metrics



Agenda

- Framework (interplay between costs benefits, and levels of security)
- Security reputation metrics
  - What to measure?
  - Measuring security levels
- Practical examples
  - Security reputation metrics for top-level domains
  - Security metrics for hosting providers

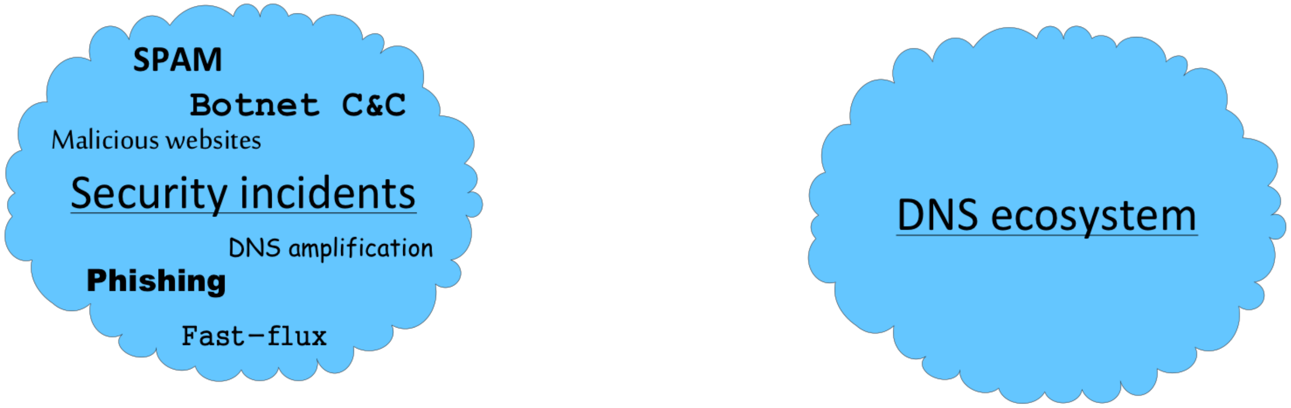
Security reputation metrics for DNS ecosystem



Security incidents

DNS ecosystem

Security reputation metrics for DNS ecosystem



SPAM

Botnet C&C

Malicious websites

Security incidents

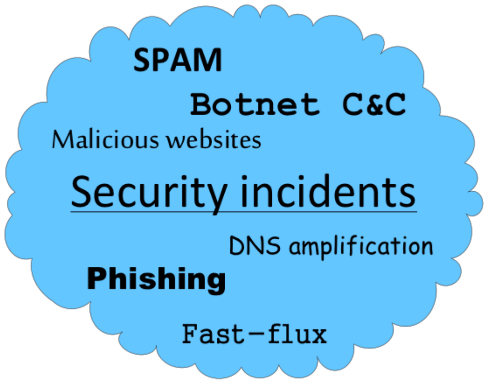
DNS amplification

Phishing

Fast-flux

DNS ecosystem

Security reputation metrics for DNS ecosystem



SPAM

Botnet C&C

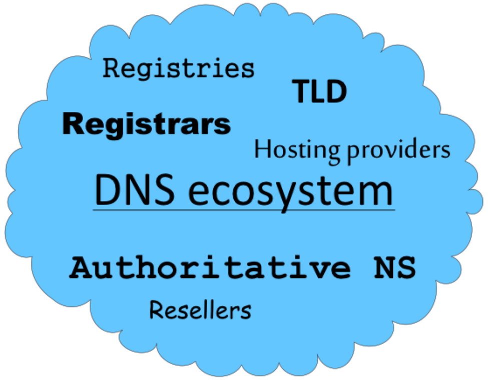
Malicious websites

Security incidents

DNS amplification

Phishing

Fast-flux



Registries

TLD

Registrars

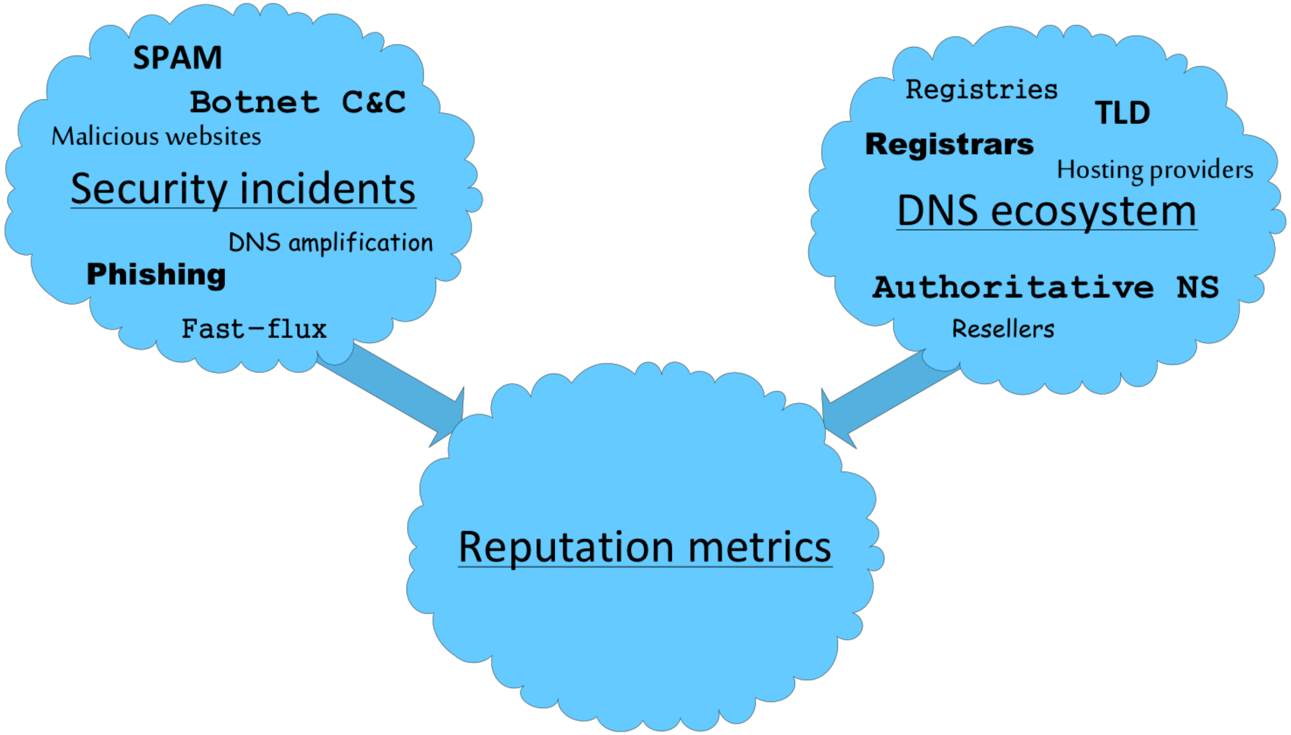
Hosting providers

DNS ecosystem

Authoritative NS

Resellers

Security reputation metrics for DNS ecosystem



SPAM

Botnet C&C

Malicious websites

Security incidents

DNS amplification

Phishing

Fast-flux

Registries

TLD

Registrars

Hosting providers

DNS ecosystem

Authoritative NS

Resellers

Reputation metrics

Security incidents

- StopBadware
- Anti-phishing working group (APWG)
- Phishtank
- ZeusTracker
- Child abuse material
- ShadowServer
- …

Security reputation metrics for DNS ecosystem

- Different layers of security metrics:
  - Top Level Domains (TLDs)
  - Market players (infrastructure providers): hosting providers, registrars, etc.
  - Network resources managed by each of the players, such as resolvers, name servers

Agenda

- Framework (interplay between costs benefits, and levels of security)
- Security reputation metrics
  - What to measure?
  - Measuring security levels

- Practical examples
  - Security reputation metrics for top-level domains
  - Security metrics for hosting providers

Security metrics for TLDs

- Type of reputation metrics
  - Concentration of malicious content:
    a) Number of unique domains

Security metrics for TLDs

- Type of reputation metrics
  - Concentration of malicious content:
    a) Number of unique domains (e.g. **malicious.com**)

Security metrics for TLDs

- Type of reputation metrics
  - Concentration of malicious content:
    a) Number of unique domains
    b) Number of FQDN

Security metrics for TLDs

- Type of reputation metrics
  - Concentration of malicious content:
    a) Number of unique domains
    b) Number of FQDN

       facebook.malicious.com, **ebay.**malicious.com, …

Security metrics for TLDs

- Type of reputation metrics
  - Concentration of malicious content:
    a) Number of unique domains
    b) Number of FQDN
    c) Number of URLs

Security metrics for TLDs

- Type of reputation metrics
  - Concentration of malicious content:

    a) Number of unique domains

    b) Number of FQDN

    c) Number of URLs

    e.g. malicious.com/**file1**, malicious.com/**file2**, malicious.com/**file3**, etc.

Security metrics for TLDs

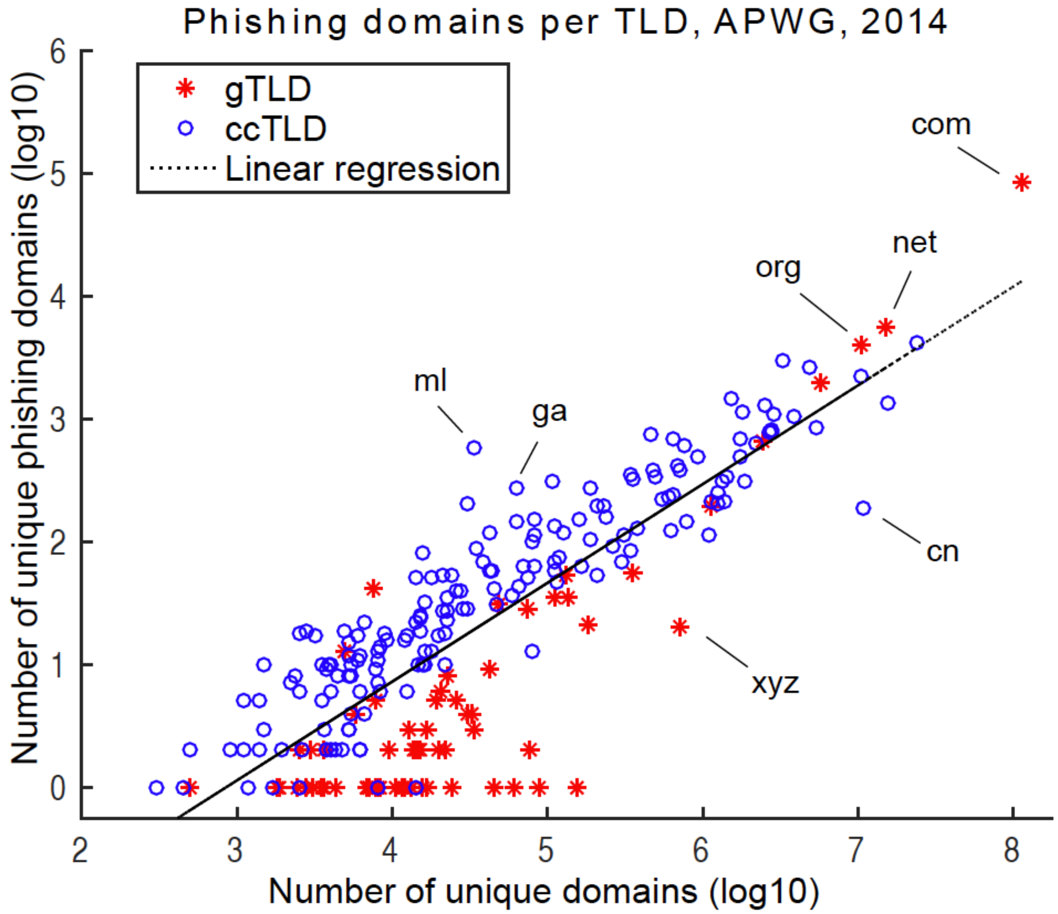
- Type of reputation metrics
  - Concentration of malicious content:
    a) Number of unique domains
    b) Number of FQDN
    c) Number of URLs

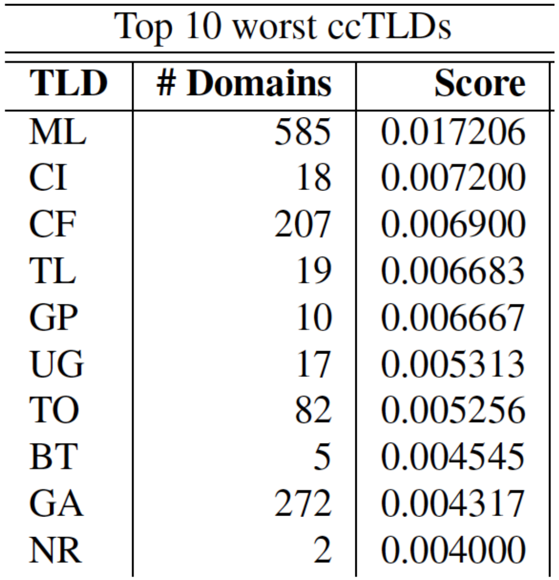
Security metrics for TLDs

- Type of reputation metrics
  - Concentration of malicious content:
    a) Number of unique domains
    b) Number of FQDN
    c) Number of URLs
  - Size matters!

Security metrics for TLDs

- Estimation of the amount of badness



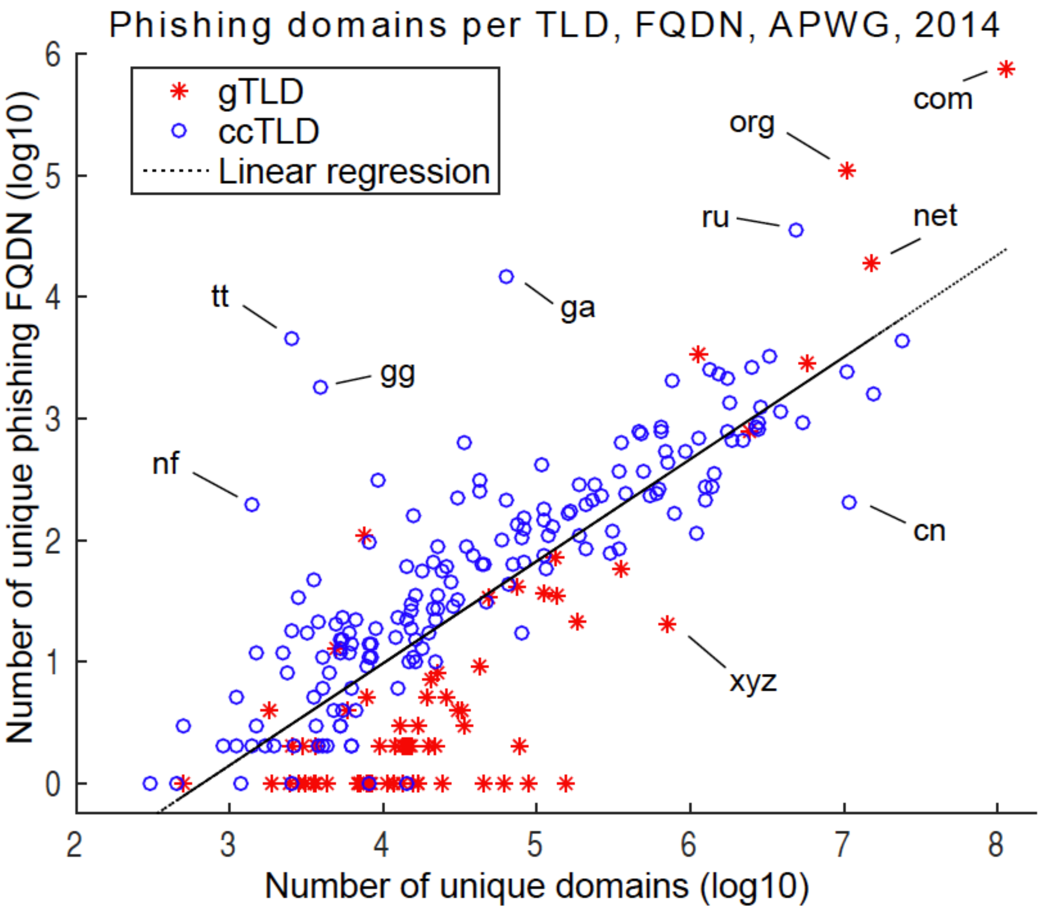


Top 10 worst ccTLDs

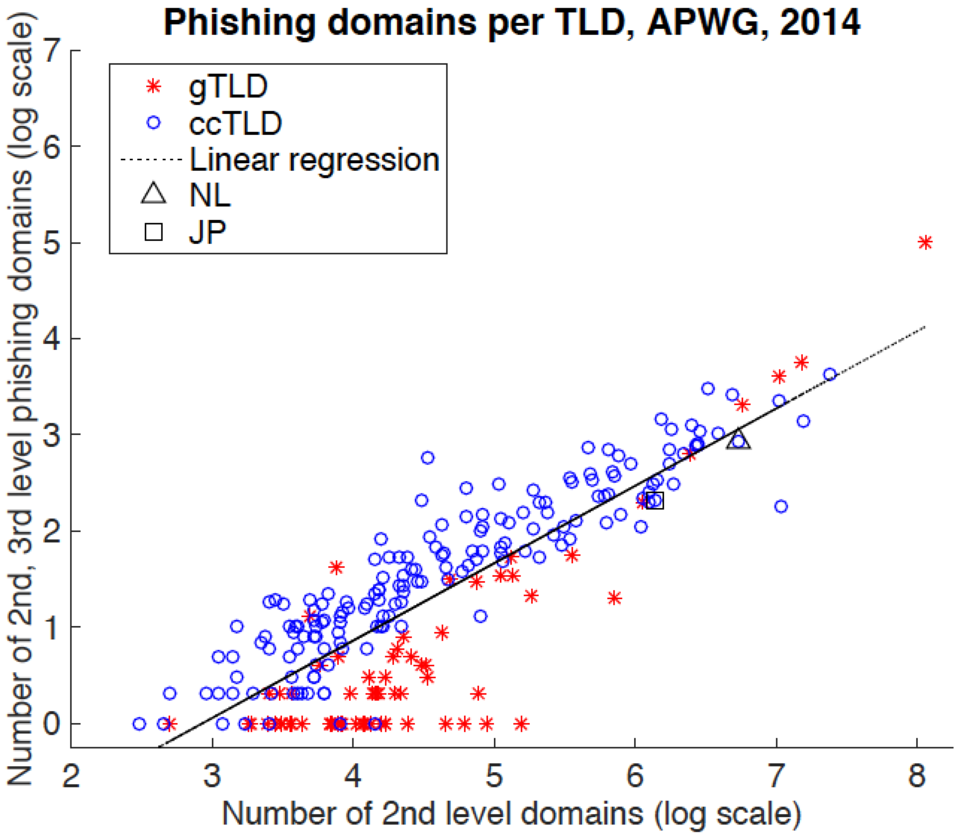
TLD	# Domains	Score
ML	585	0.017206
CI	18	0.007200
CF	207	0.006900
TL	19	0.006683
GP	10	0.006667
UG	17	0.005313
TO	82	0.005256
BT	5	0.004545
GA	272	0.004317
NR	2	0.004000

Security metrics for TLDs

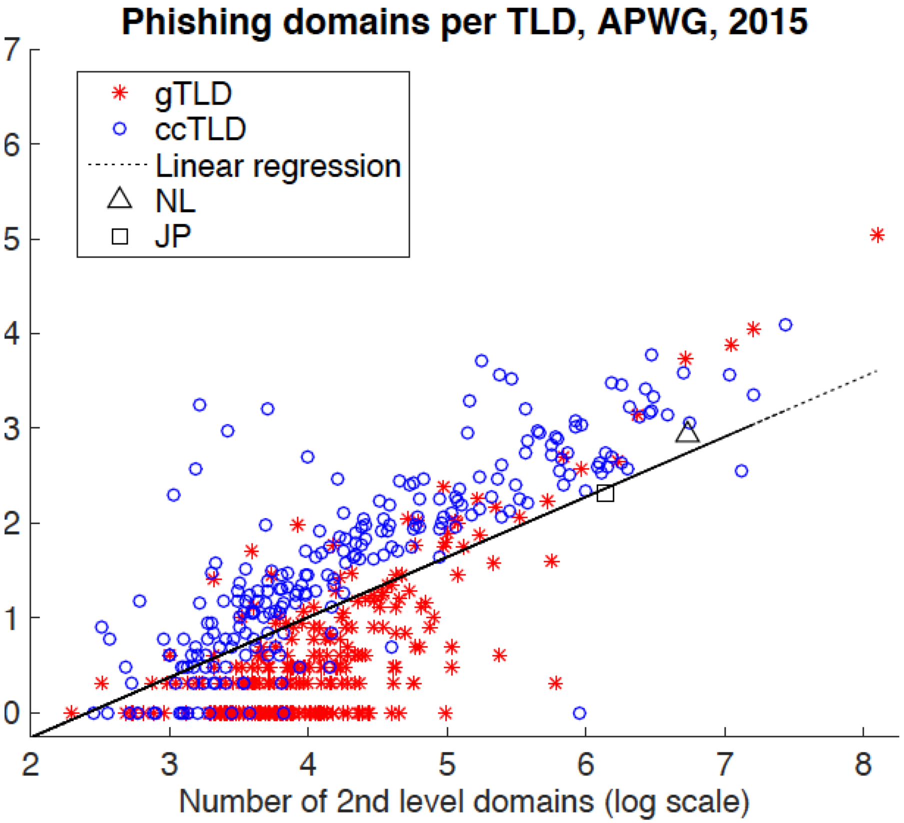
- Estimation of the amount of badness



Security metrics for TLDs (2014 vs. 2015)

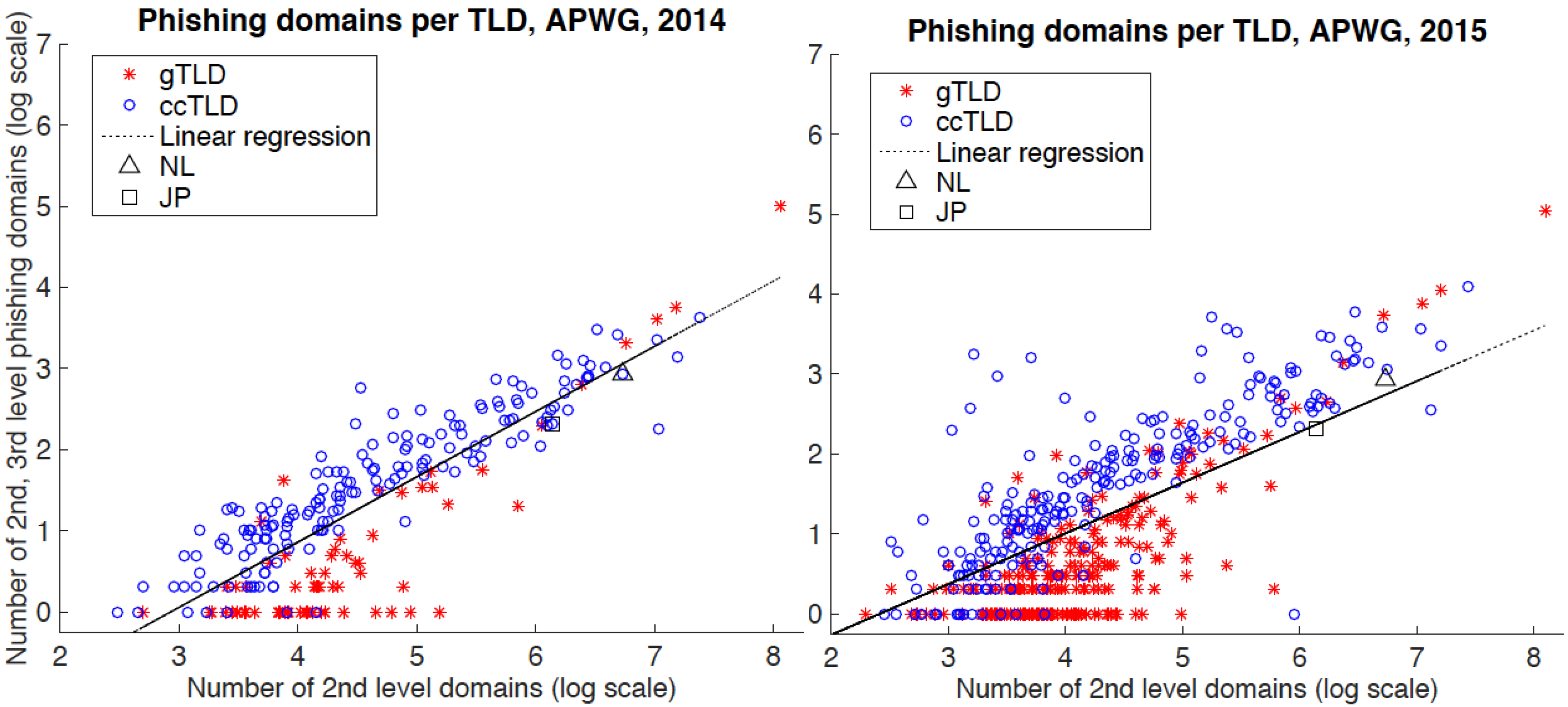


Phishing domains per TLD, APWG, 2014



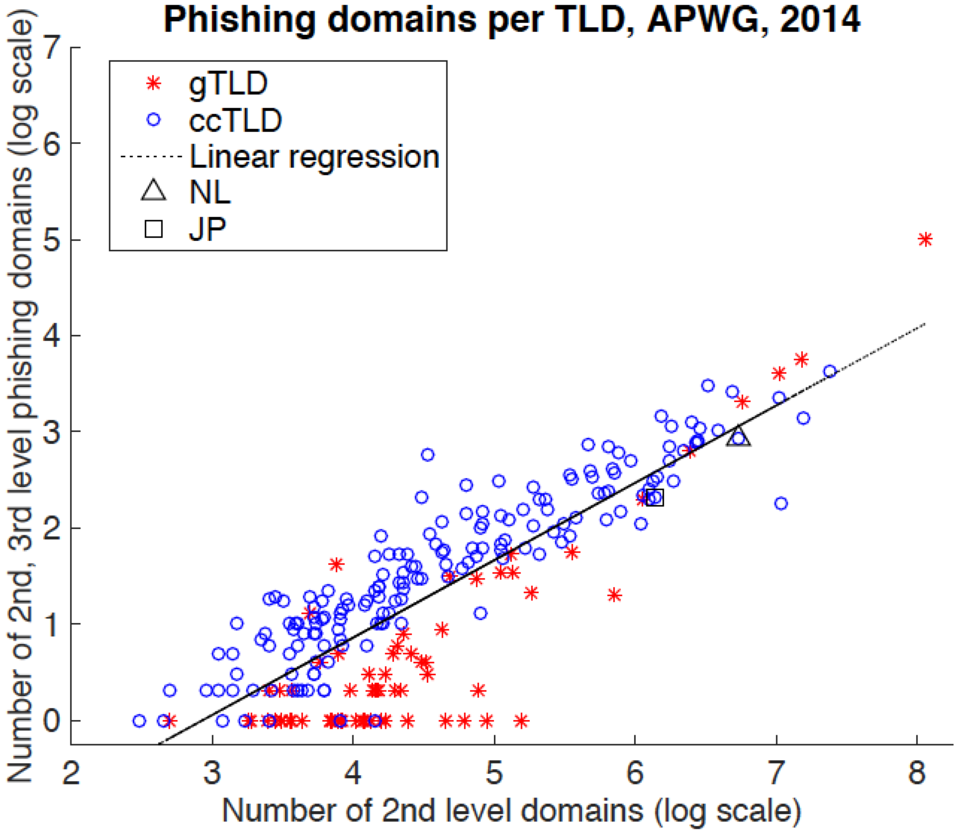
Phishing domains per TLD, APWG, 2015

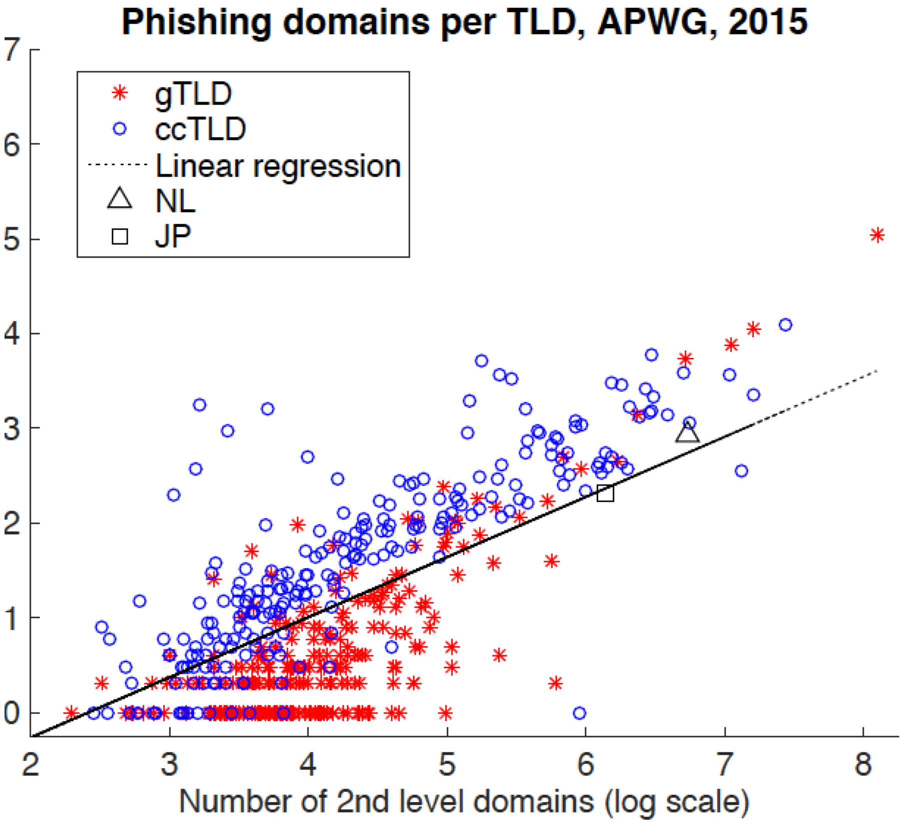
Security metrics for TLDs (2014 vs. 2015)



SIZE:	Phishing: domains	FQDN	URLs
NL 2014: 5460852	867	919	2995
NL 2015: 5614561	1169	1252	6366

Security metrics for TLDs (2014 vs. 2015)





SIZE:	Phishing: domains	FQDN	URLs
NL 2014: 5460852	867	919	2995
NL 2015: 5614561	1169	1252	**6366**

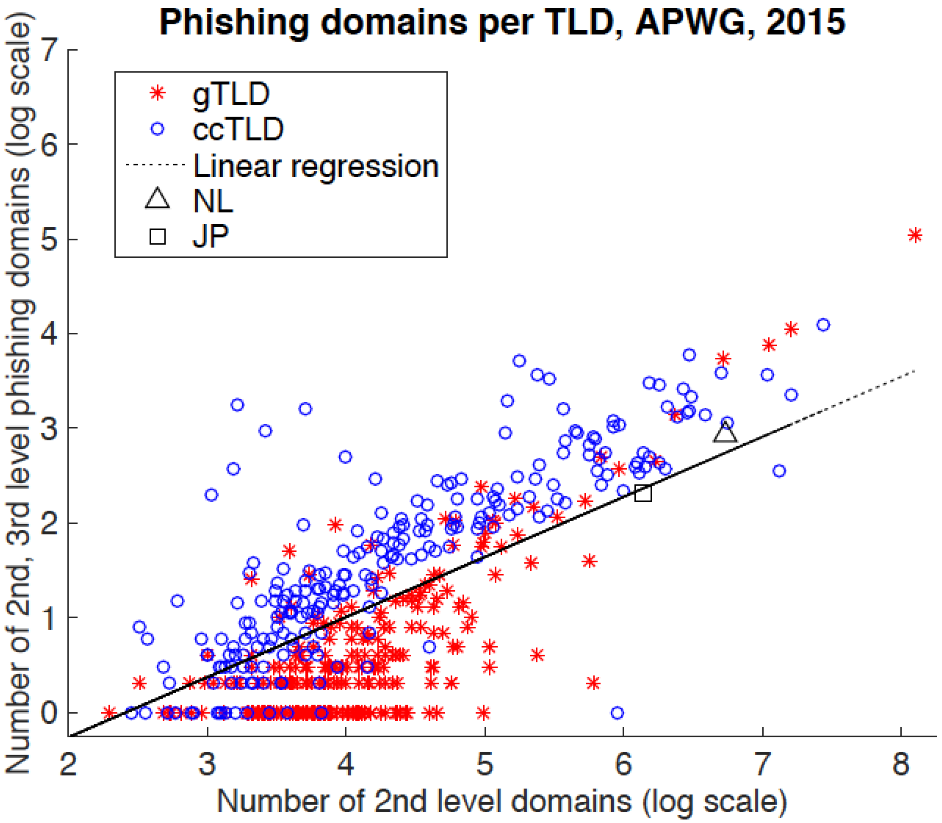
Security metrics for TLDs

	SIZE:	Phis: domains	FQDN	URLs:
NL 2014:	5460852	867	919	2995
NL 2015:	5614561	1169	1252	**6366**

URL shorteners!

http://bitly.nl/	1678
http://no.nl/	552
http://mini-url.nl/	55
http://iturl.nl/	45

Security metrics for TLDs (2014 vs. 2015)



Only size matters? What else?

Security metrics for TLDs

- Type of reputation metrics
  - Up-times of maliciously registered/compromised domains
  - Problems:
    - Maliciously registered domains vs. compromised websites
    - Reinfections, blacklisting…
    - Definition of first seen
    - Highly depends on the measurement technique

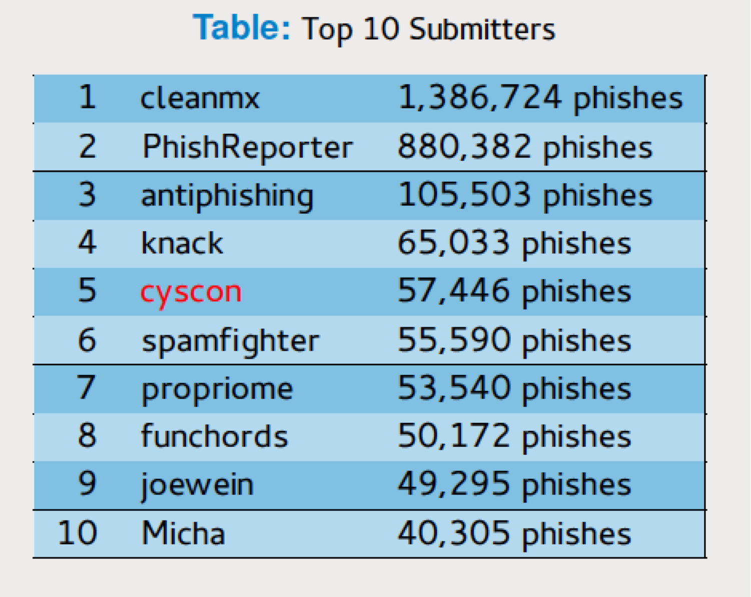
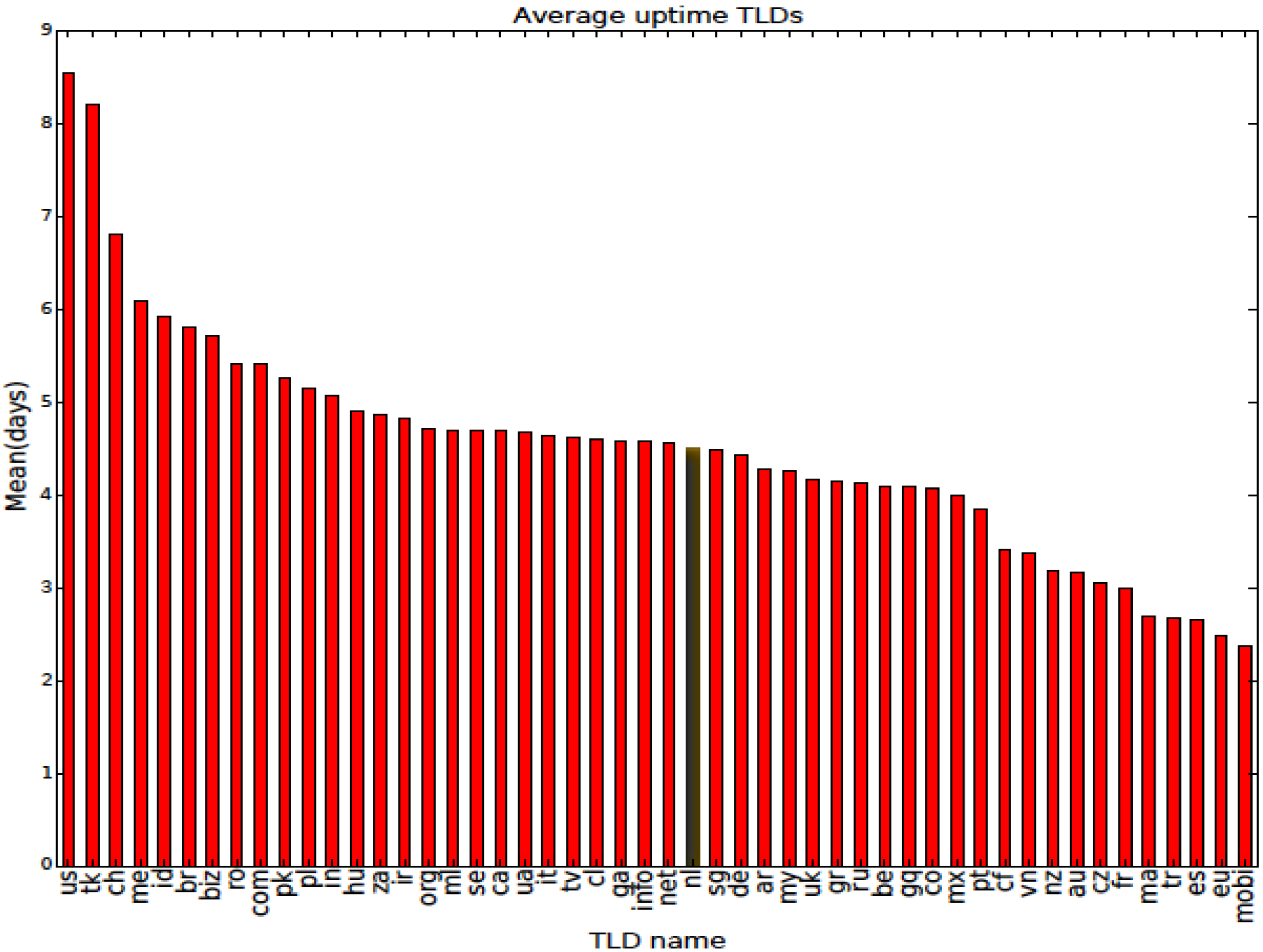
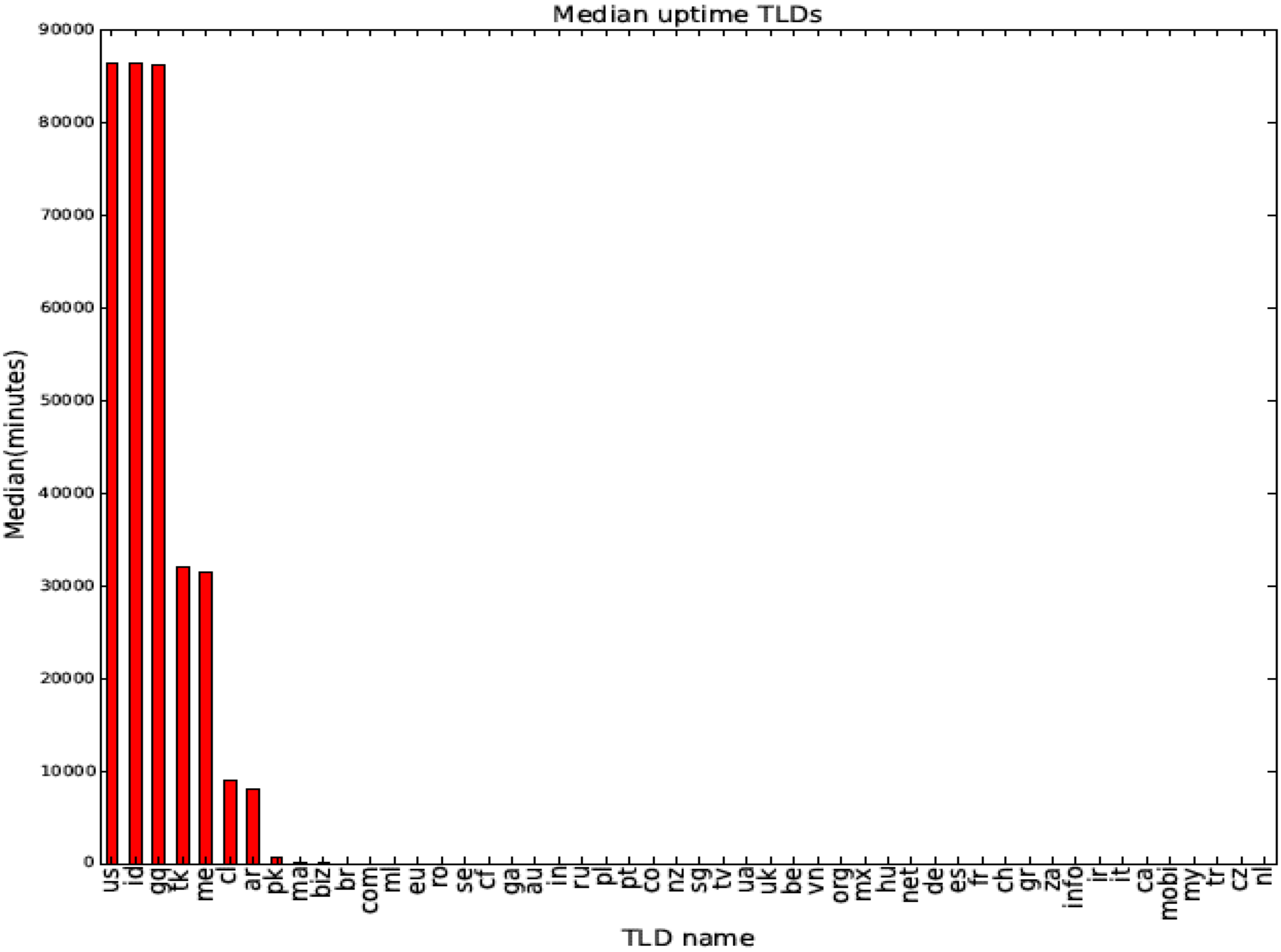


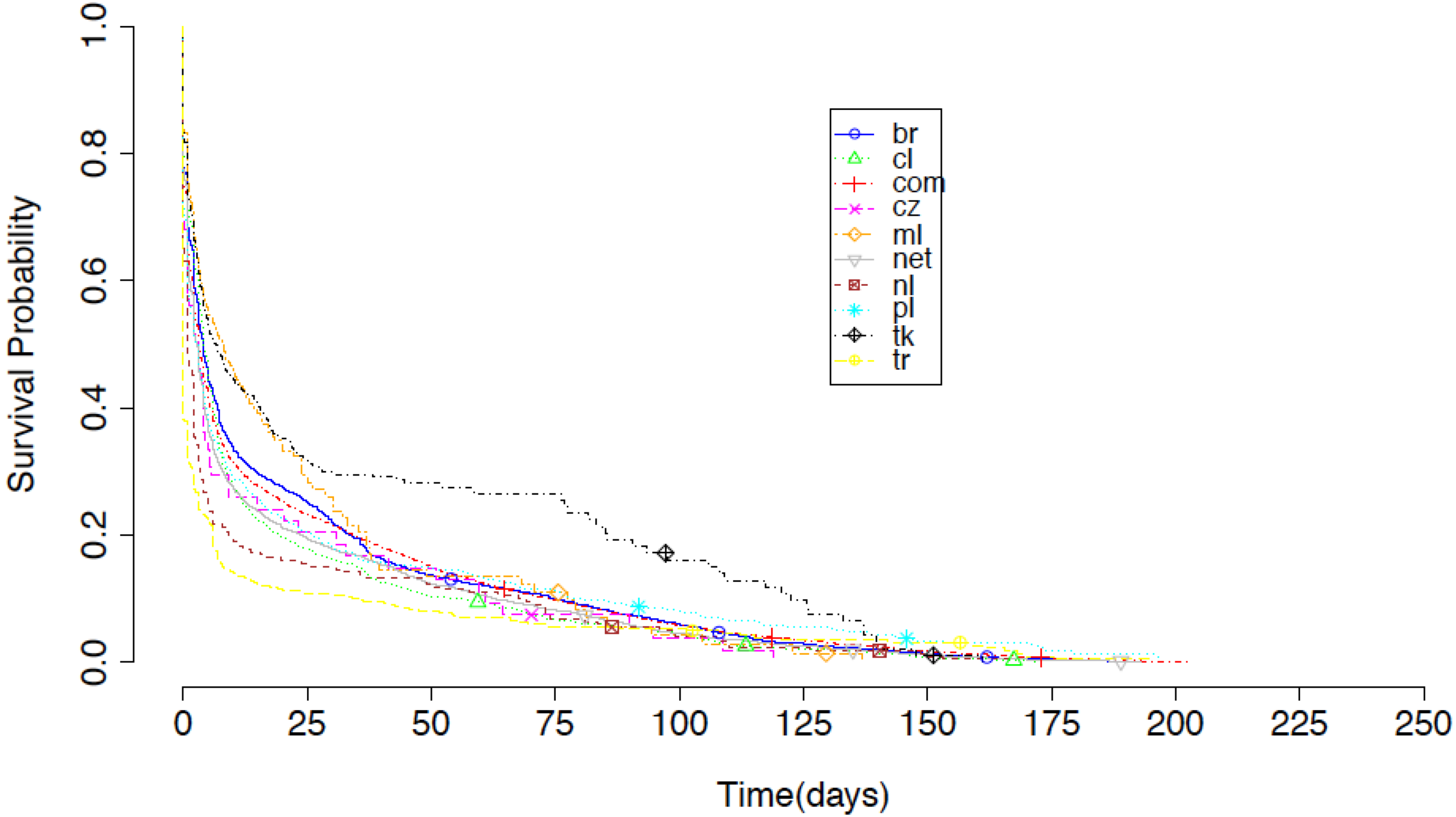
Table: Top 10 Submitters

1	cleanmx	1,386,724 phishes
2	PhishReporter	880,382 phishes
3	antiphishing	105,503 phishes
4	knack	65,033 phishes
5	cyscon	57,446 phishes
6	spamfighter	55,590 phishes
7	propriome	53,540 phishes
8	funchords	50,172 phishes
9	joewein	49,295 phishes
10	Micha	40,305 phishes


Average uptime TLDs
Mean(days)
TLD name
0
1
2
3
4
5
6
7
8
9
us
tk
ch
me
id
br
biz
ro
com
pk
pl
in
hu
za
ir
org
ml
se
ca
ua
it
tv
cl
ga
info
net
nl
sg
de
ar
my
uk
gr
ru
be
gq
co
mx
pt
cf
vn
nz
au
cz
fr
ma
tr
es
eu
mobi

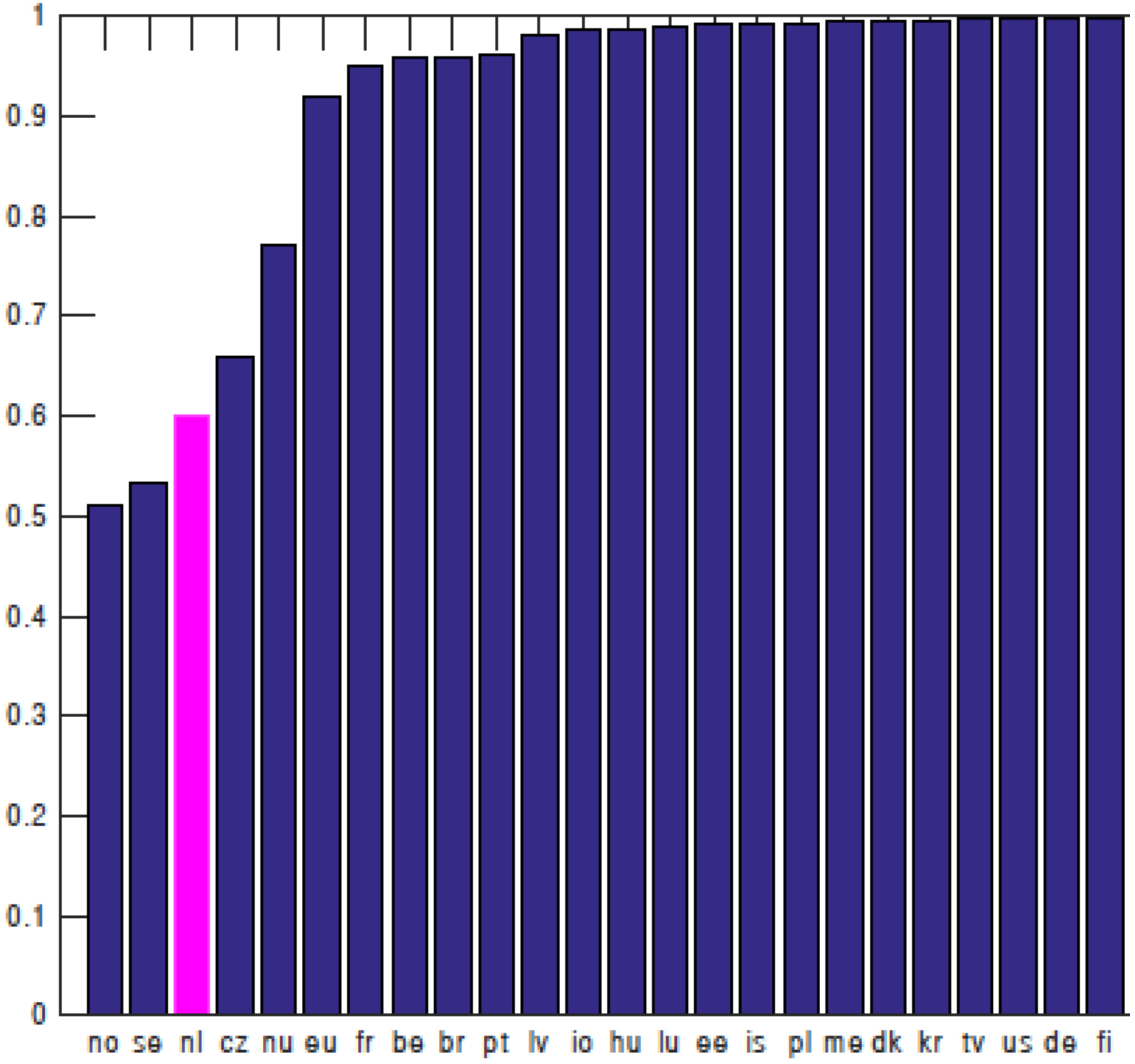

Median uptime TLDs
Median(minutes)
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
us
id
gg
tk
me
cl
ar
pk
ma
biz
br
com
ml
eu
ro
se
cf
ga
au
in
ru
pl
pt
co
nz
sg
tv
ua
uk
be
vn
org
mx
hu
net
de
es
fr
ch
gr
za
info
ir
it
ca
mobi
my
tr
cz
nl
TLD name

Security metrics for TLDs



Security metrics for ccTLDs

- No DNSSEC



Which market players are responsible?

Agenda

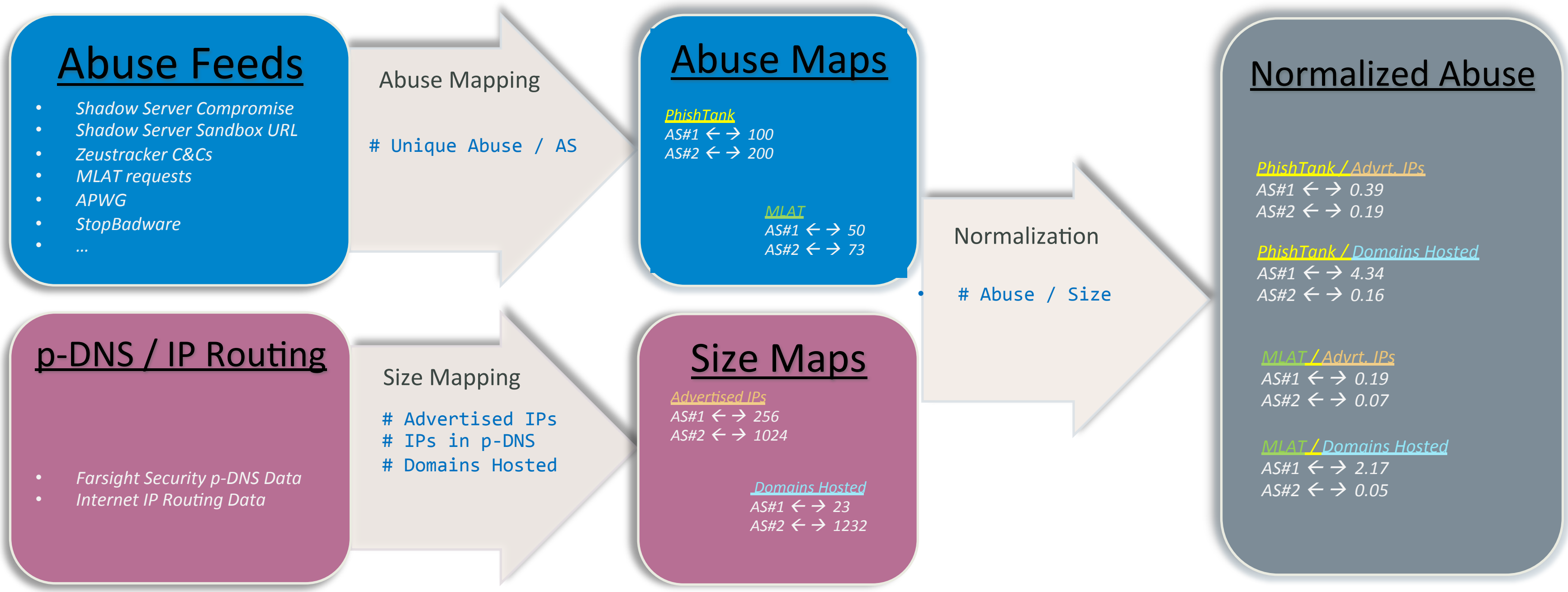
- Framework (interplay between costs benefits, and levels of security)
- Security reputation metrics
  - What to measure?
  - Measuring security levels
- Practical examples
  - Security reputation metrics for top-level domains
  - Security metrics for hosting providers

Security metrics for hosting providers

Indicators of Abuse	Why	Challenge
Occurrence of Abuse (How often abused?)	*Signals network hygiene and vulnerability*	*Hard to isolate provider efforts from other factors*
Uptime of abuse (How long abused?)	*Signals effectiveness of abuse handing*	*Hard to measure at scale*

Security metrics for hosting providers

1. Count badness per AS across different data sources
2. Normalize for the size of the AS (in 3 ways)



Abuse Feeds

- *Shadow Server Compromise*
- *Shadow Server Sandbox URL*
- *Zeustracker C&Cs*
- *MLAT requests*
- *APWG*
- *StopBadware*
- *…*

Abuse Mapping

`# Unique Abuse / AS`

Abuse Maps

PhishTank
AS#1 ←→ 100
AS#2 ←→ 200

MLAT
AS#1 ←→ 50
AS#2 ←→ 73

p-DNS / IP Routing

- *Farsight Security p-DNS Data*
- *Internet IP Routing Data*

Size Mapping

```
# Advertised IPs
# IPs in p-DNS
# Domains Hosted
```

Size Maps

Advertised IPs
AS#1 ←→ 256
AS#2 ←→ 1024

Domains Hosted
AS#1 ←→ 23
AS#2 ←→ 1232

Normalization

- `# Abuse / Size`

Normalized Abuse

PhishTank / Advrt. IPs
AS#1 ←→ 0.39
AS#2 ←→ 0.19

PhishTank / Domains Hosted
AS#1 ←→ 4.34
AS#2 ←→ 0.16

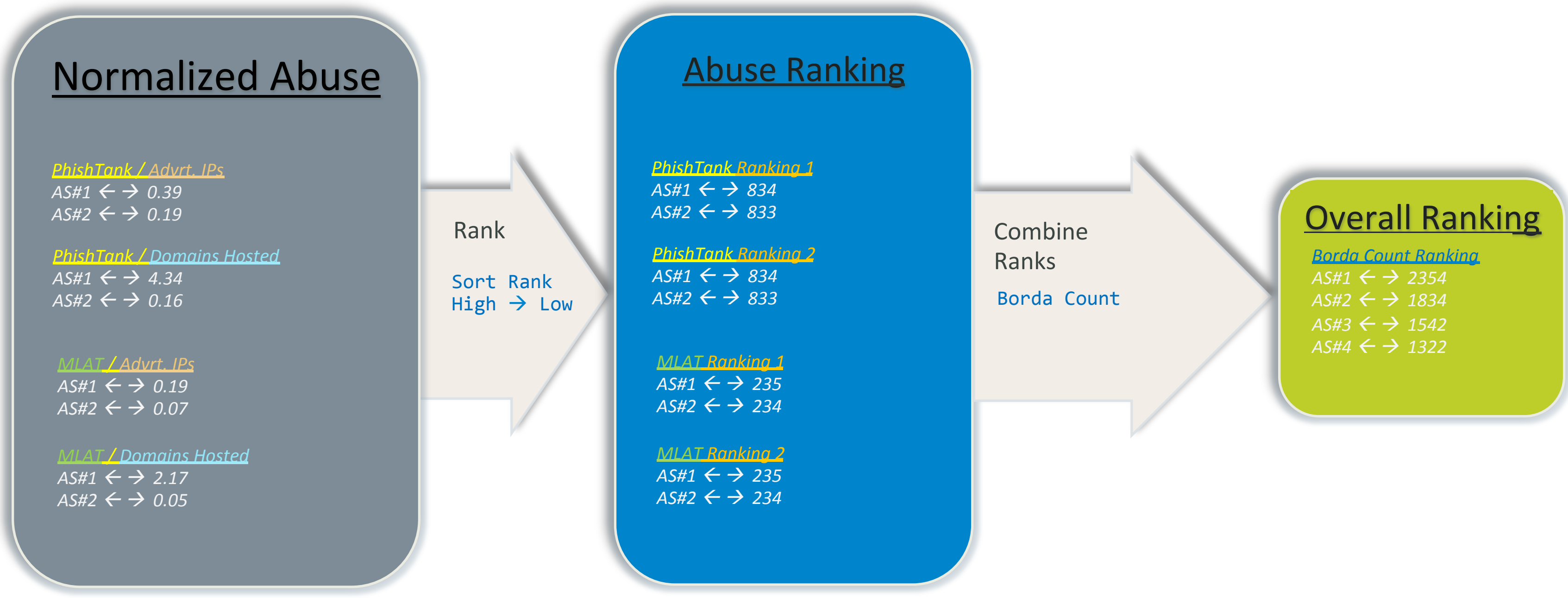
MLAT / Advrt. IPs
AS#1 ←→ 0.19
AS#2 ←→ 0.07

MLAT / Domains Hosted
AS#1 ←→ 2.17
AS#2 ←→ 0.05

*"Developing Security Reputation Metrics for Hosting Providers", Arman Noroozian, Maciej Korczyński, Samaneh Tajalizadehkhoob, and Michel van Eeten, *USENIX CSET'15*

Security metrics for hosting providers

3. Rank ASes on amount of badness
4. Aggregate rankings (Borda count)
5. Identify ASes with consistently high concentrations of badness



Normalized Abuse

PhishTank / Advrt. IPs
AS#1 ← → 0.39
AS#2 ← → 0.19

PhishTank / Domains Hosted
AS#1 ← → 4.34
AS#2 ← → 0.16

MLAT / Advrt. IPs
AS#1 ← → 0.19
AS#2 ← → 0.07

MLAT / Domains Hosted
AS#1 ← → 2.17
AS#2 ← → 0.05

Rank

Sort Rank
High → Low

Abuse Ranking

PhishTank Ranking 1
AS#1 ← → 834
AS#2 ← → 833

PhishTank Ranking 2
AS#1 ← → 834
AS#2 ← → 833

MLAT Ranking 1
AS#1 ← → 235
AS#2 ← → 234

MLAT Ranking 2
AS#1 ← → 235
AS#2 ← → 234

Combine Ranks

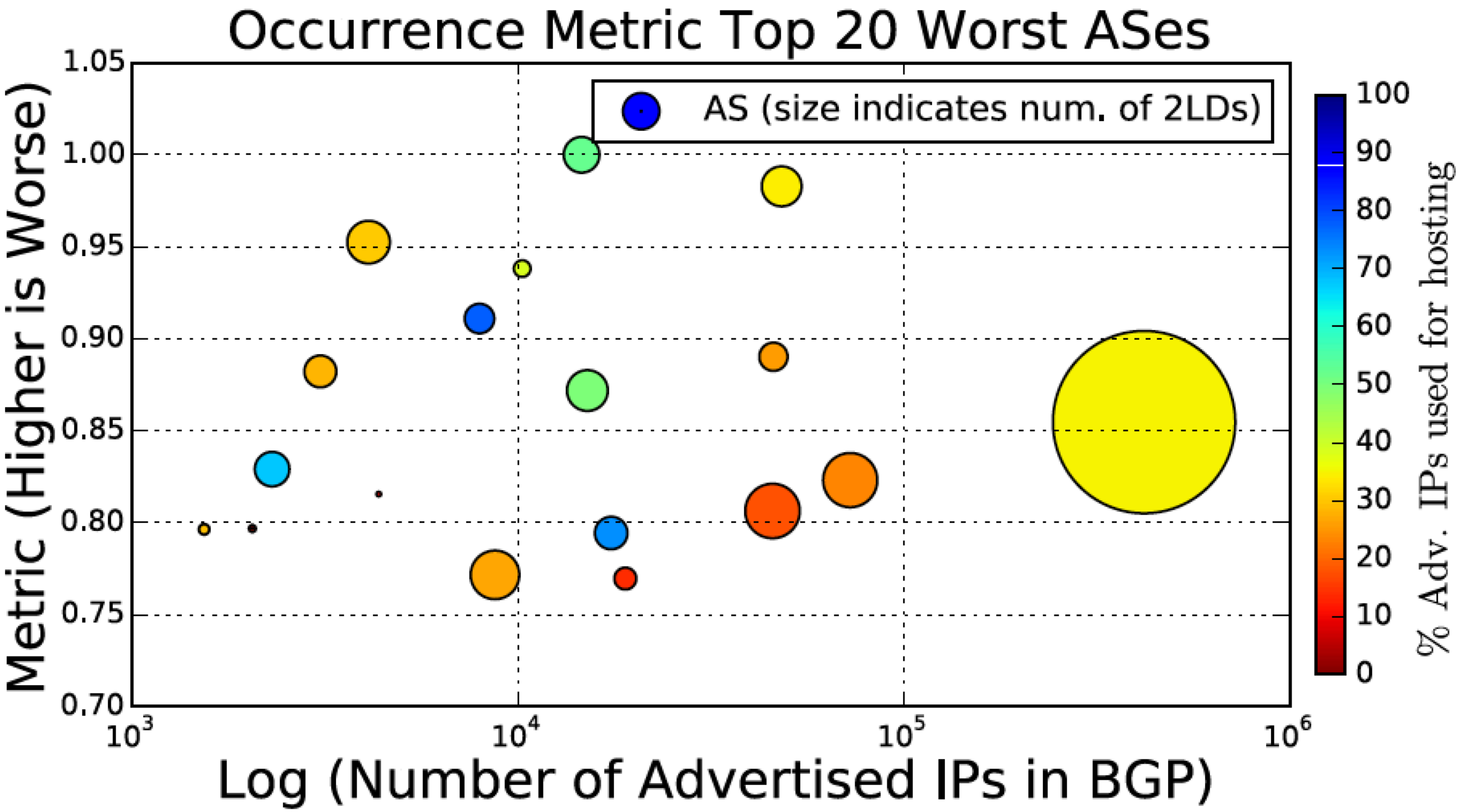
Borda Count

Overall Ranking

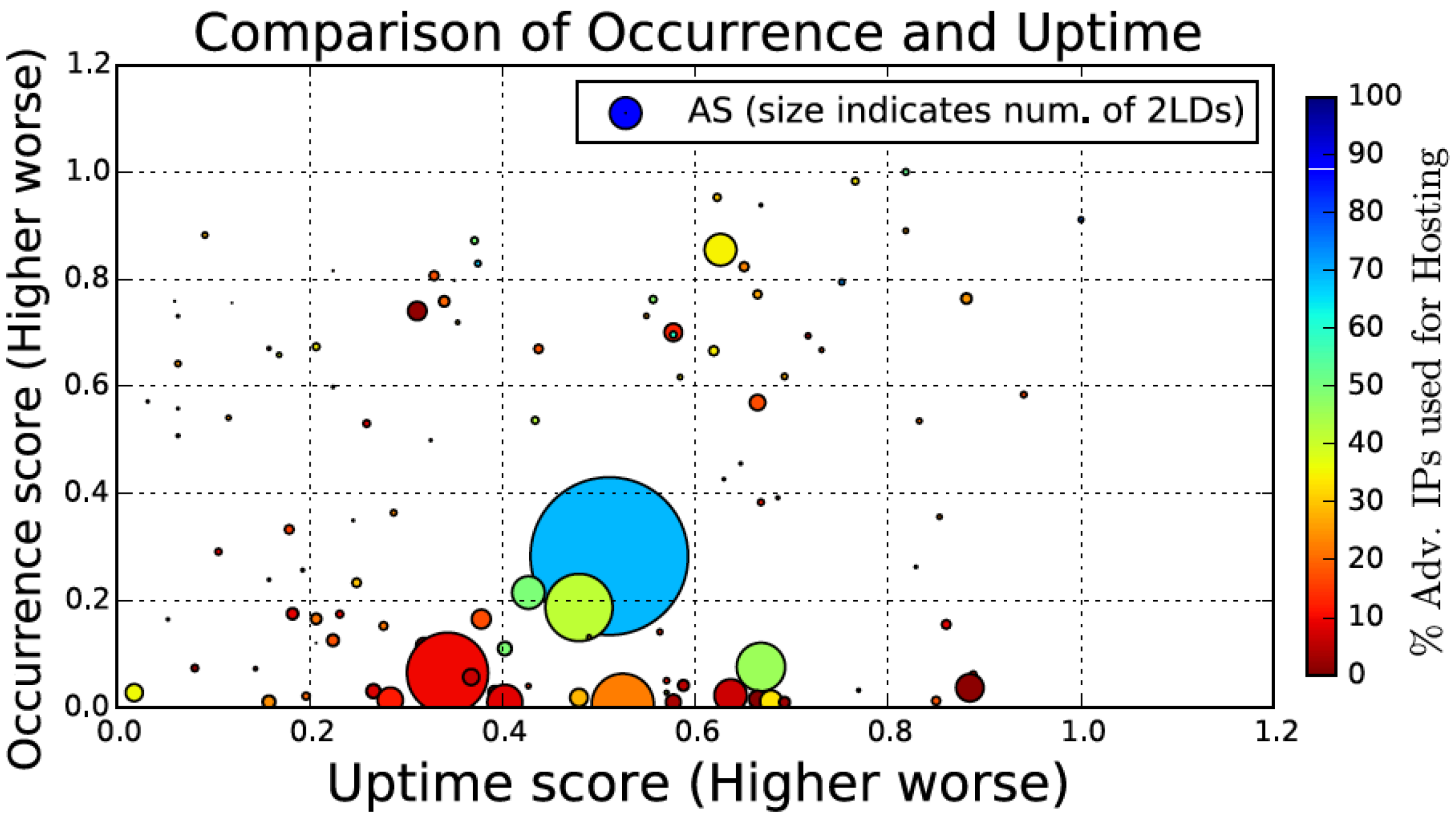
Borda Count Ranking
AS#1 ← → 2354
AS#2 ← → 1834
AS#3 ← → 1542
AS#4 ← → 1322

TUDelft

Security metrics for hosting providers



Security metrics for hosting providers



Security metrics for hosting providers

- “Clean Netherlands”: Enhance self cleansing ability of the Dutch hosting market by
    - Promoting best practices and awareness
    - Security metrics *
    - Driving factors

*"Developing Security Reputation Metrics for Hosting Providers", Arman Noroozian, Maciej Korczyński, Samaneh Tajalizadehkhoob, and Michel van Eeten, *USENIX CSET'15*

Summary

- Cost, benefit, and levels of security
- Practical examples:
  - Security reputation metrics for top-level domains and hosting providers

Question?

Maciej Korczyński
Delft University of Technology
maciej.korczynski@tudelft.nl