MASARYK UNIVERSITY
Czech Republic

Passive OS Fingerprinting Methods in the Jungle of Wireless Networks

NOMS Conference
26 April 2018

Martin Laštovička
lastovicka@ics.muni.cz

Brno Ph.D. Talent

MASARYK UNIVERSITY
Czech Republic

Motivation

- Results from static networks
  - ⇨ dynamic wireless network
- Rapid changes
  - ⇨ continuous passive monitoring
- Large network, lot of traffic
  - ⇨ IPFIX

MASARYK
UNIVERSITY
Czech Republic

Methods

MASARYK UNIVERSITY
Czech Republic

TCP/IP Parameters

synSize	winSize	TTL	OS	Confidence
52	8192	128	Windows 10.0	55.2 %
52	8192	128	Windows 6.1	31.9 %
52	65535	128	Windows 10.0	74.9 %
60	65535	64	Android 6.0	48.2 %
60	14600	64	Android 4.4	28.4 %
60	29200	64	Ubuntu	20.4 %
64	65535	64	Mac OS X 10.12	26.5 %
64	65535	64	iOS 10.3	10.3 %

MASARYK UNIVERSITY
Czech Republic

HTTP User-agent

- Mozilla/5.0 (**Windows NT 10.0**; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36

- Mozilla/5.0 (Linux; **Android 7.0**; SM-G930VC Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/58.0.3029.83 Mobile Safari/537.36

MASARYK UNIVERSITY
Czech Republic

Specific Domains

msftconnecttest.com
msftncsi.com
update.microsoft.com

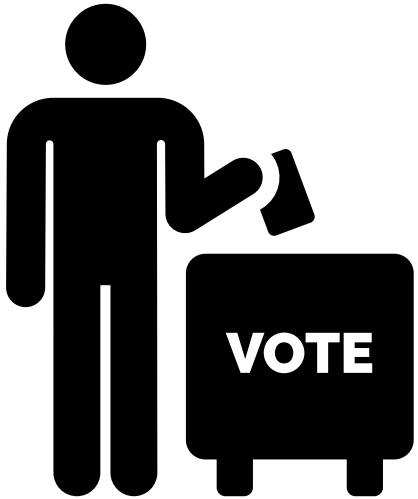
swcdn.apple.com
swdist.apple.com

clients3.google.com/generate_204
connectivitycheck.android.com

icc.blackberry.com

MASARYK UNIVERSITY
Czech Republic

Combination



MASARYK
UNIVERSITY
Czech Republic

Results

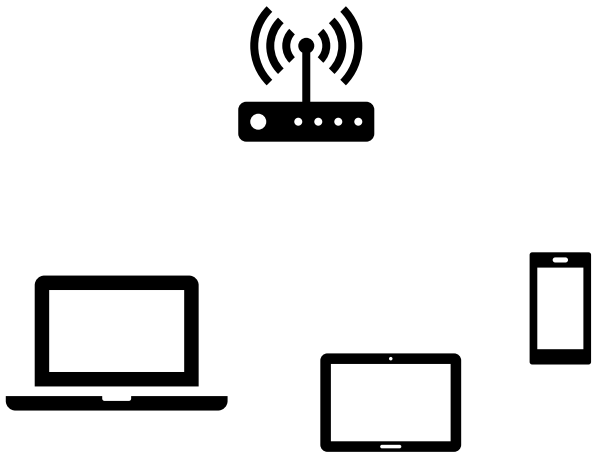
MASARYK UNIVERSITY
Czech Republic

OS hierarchy

Method	Vendor	OS Name	Major Version	Minor Version
TCP/IP	✓	✓	(✓)	(✓)
User-agent	✓	✓	✓	✓
Specific domain	✓	✓	✗	✗
Combination	✓	✓	✓	✓

MASARYK UNIVERSITY
Czech Republic

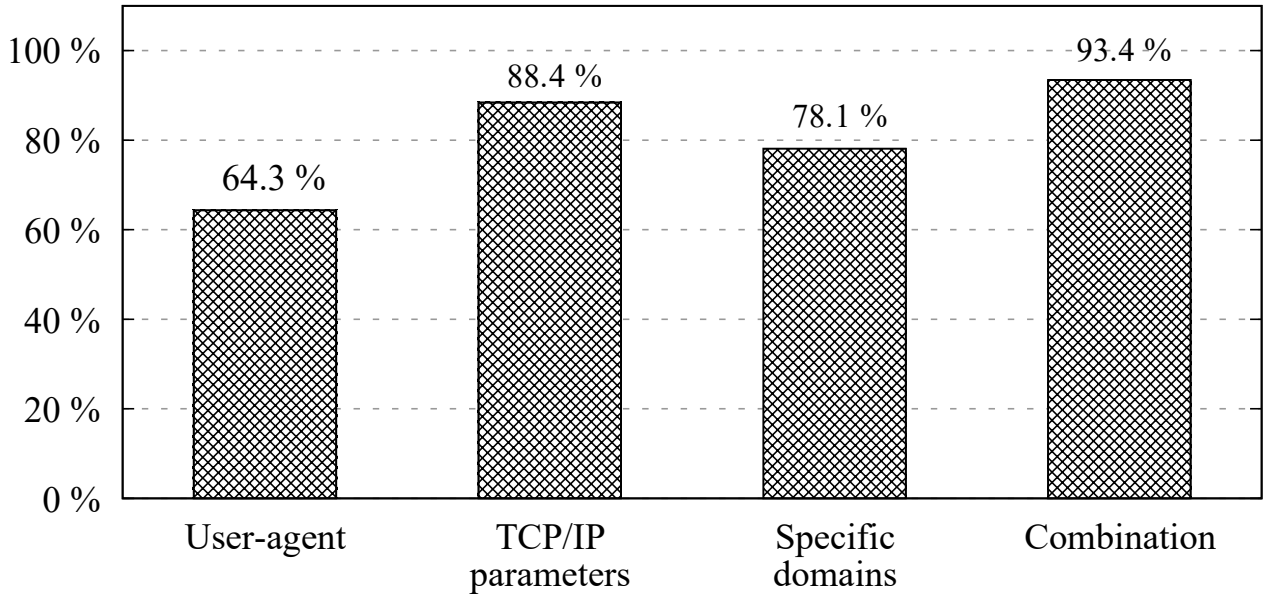
Dataset



- One week of flows + logs
  - 79 087 345 flows
  - 21 746 users
  - 25 642 unique MAC (1 692 vendor prefixes)
  - 253 374 Wi-Fi sessions
  - 6 104 unique IP addresses

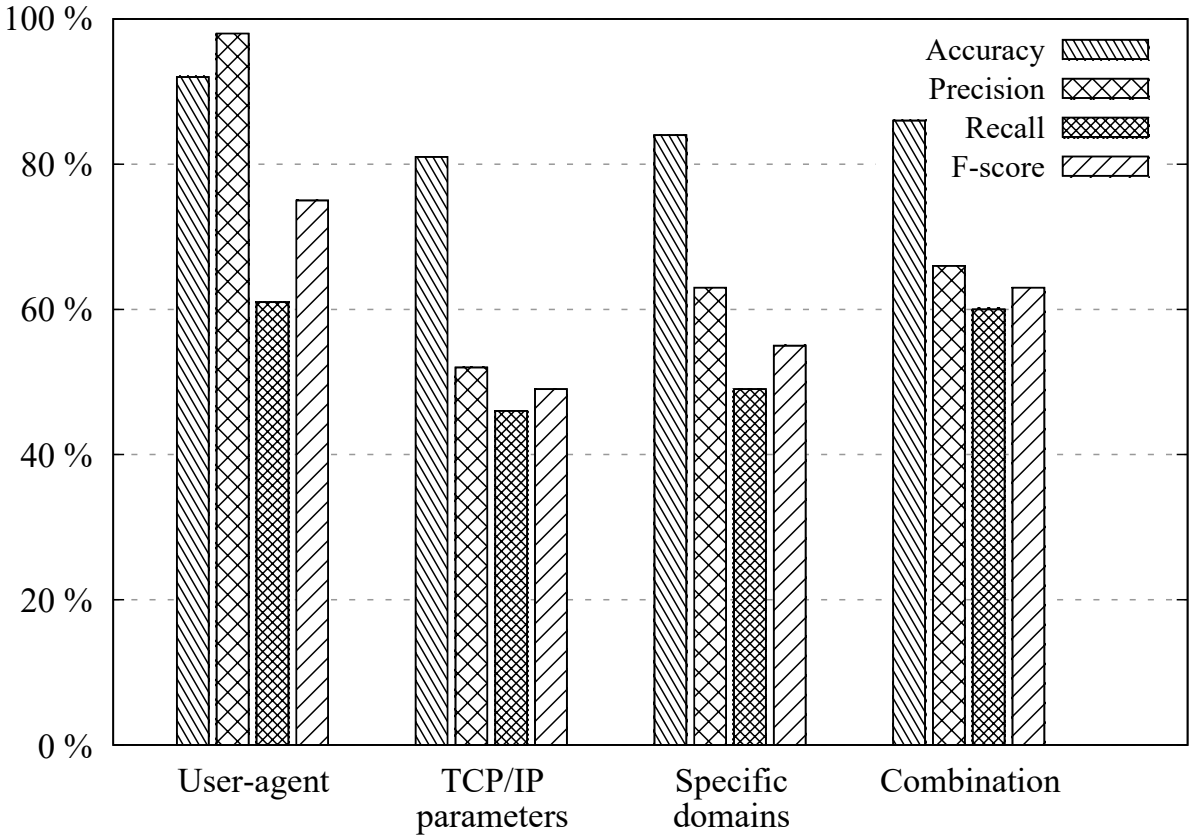
MASARYK UNIVERSITY
Czech Republic

Coverage



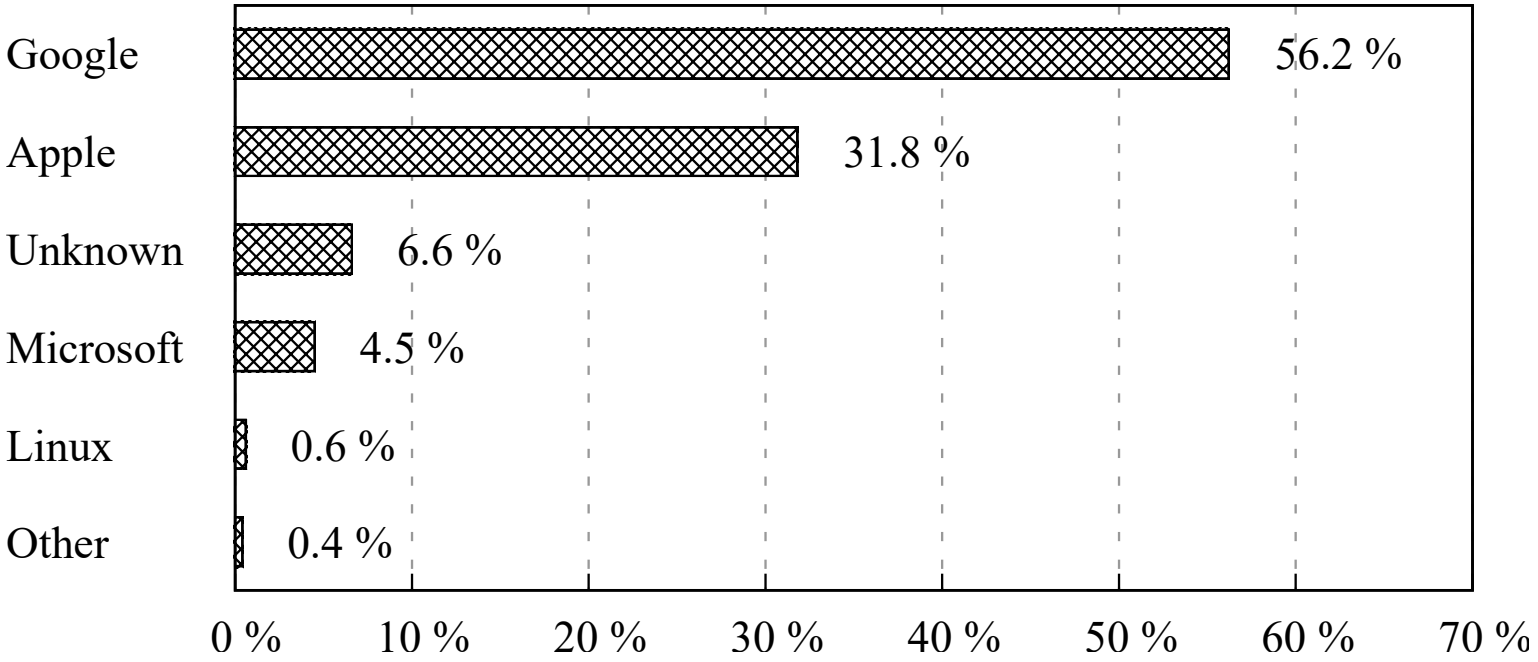
MASARYK UNIVERSITY
Czech Republic

Performance Measures



MASARYK UNIVERSITY
Czech Republic

OS Vendor Share



MASARYK
UNIVERSITY
Czech Republic

Lessons Learned

MASARYK UNIVERSITY
Czech Republic

Coverage Inconsistency

Bit offset	0-7										8-15										16-23										24-31									
0	Source port																				Destination port																			
32	Sequence number																																							
64	Acknowledgment number (if ACK is set)																																							
96	Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window size																									
128	Checksum																				Urgent pointer (if URG is set)																			
160+	Options, Data																																							

MASARYK UNIVERSITY
Czech Republic

Ground Truth

May	5 06:30:54 krakonos dhcpd: DHCPREQUEST	for 147.251.x.x from	98:0c:a5:x:x:x	(android-22d1bxxx)	via 147.251.x.x
May	5 06:30:54 krakonos dhcpd: DHCPACK	on 147.251.x.x to	98:0c:a5:x:x:x	(android-22d1bxxx)	via 147.251.x.x
May	5 06:31:17 krakonos dhcpd: DHCPREQUEST	for 147.251.x.x from	38:a4:ed:x:x:x	(Redmi3S-Redmi)	via 147.251.x.x
May	5 06:31:17 krakonos dhcpd: DHCPACK	on 147.251.x.x to	38:a4:ed:x:x:x	(Redmi3S-Redmi)	via 147.251.x.x
May	5 06:31:20 krakonos dhcpd: DHCPREQUEST	for 147.251.x.x from	9c:6c:15:x:x:x	(Windows-Phone)	via 147.251.x.x
May	5 06:31:20 krakonos dhcpd: DHCPACK	on 147.251.x.x to	9c:6c:15:x:x:x	(Windows-Phone)	via 147.251.x.x
May	5 06:36:24 krakonos dhcpd: DHCPREQUEST	for 147.251.x.x from	c0:f2:fb:x:x:x	(Barboras-iPhone)	via 147.251.x.x
May	5 06:36:24 krakonos dhcpd: DHCPACK	on 147.251.x.x to	c0:f2:fb:x:x:x	(Barboras-iPhone)	via 147.251.x.x

MASARYK UNIVERSITY
Czech Republic

Emerging Protocols

Method	HTTP/2.0 + TLS 1.3	IPv6	QUIC
TCP/IP	✓	✗	✗
User-agent	✗	✓	✗
Specific domain	✓	✓	(✓)

MASARYK UNIVERSITY
Czech Republic

Discussion

Martin Laštovička
lastovicka@ics.muni.cz

Brno Ph.D. Talent Scholarship Holder
Funded by the Brno City Municipality

Brno Ph.D. Talent