An Overview of DNS Security Measurements

Chaoyi Lu

Nov 7, 2023

DNS INFRASTRUCTURE

Why measure DNS security?

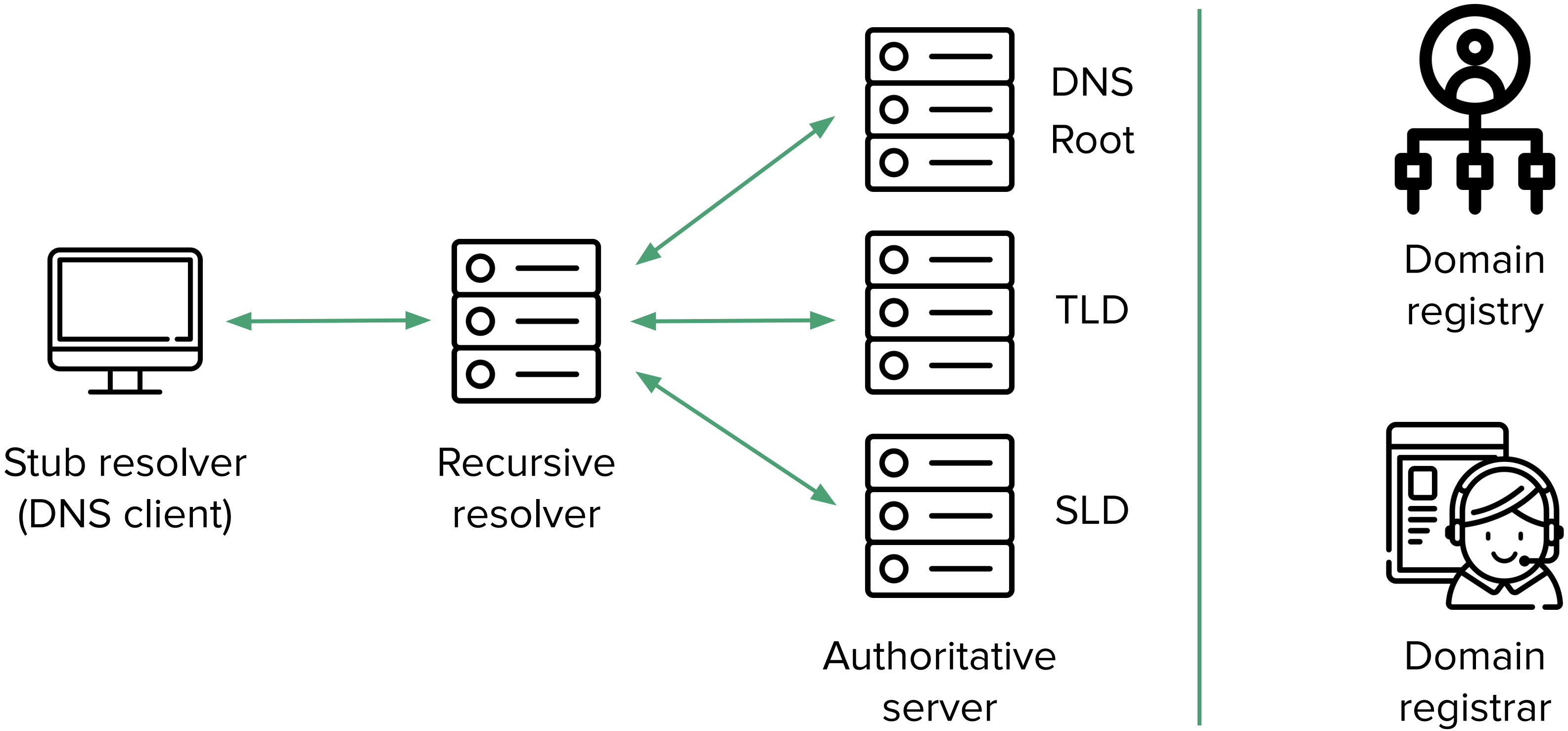
DNS is so fundamental.

But unfortunately, so vulnerable.

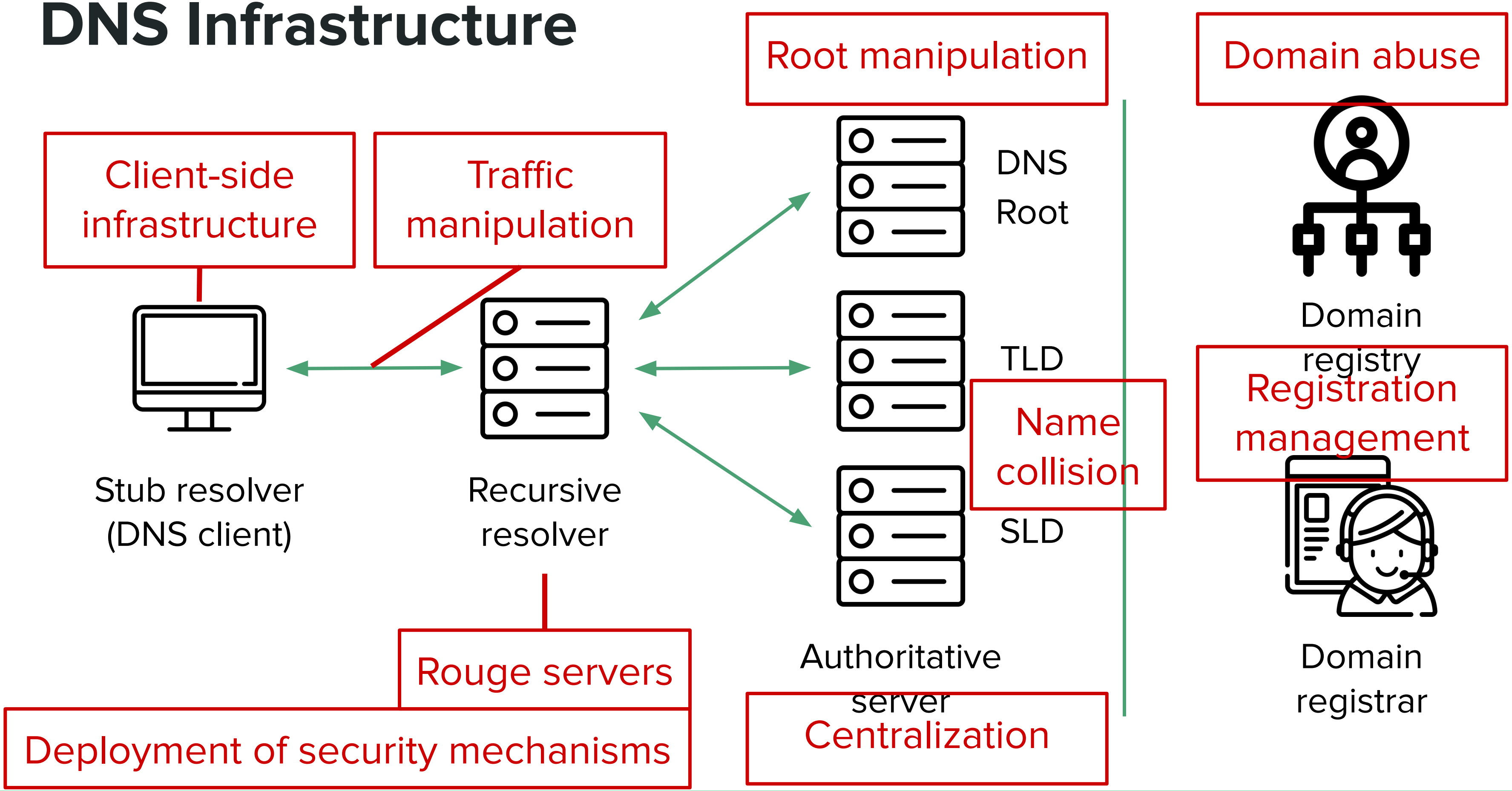
DNS Security Measurement Topics

Measuring security issues	Measuring operational status
Domain abuse	Client-side infrastructure
Packet interception	Encrypted DNS
Rogue servers	DNSSEC
Name collision	EDNS(0) Extensions

DNS Infrastructure

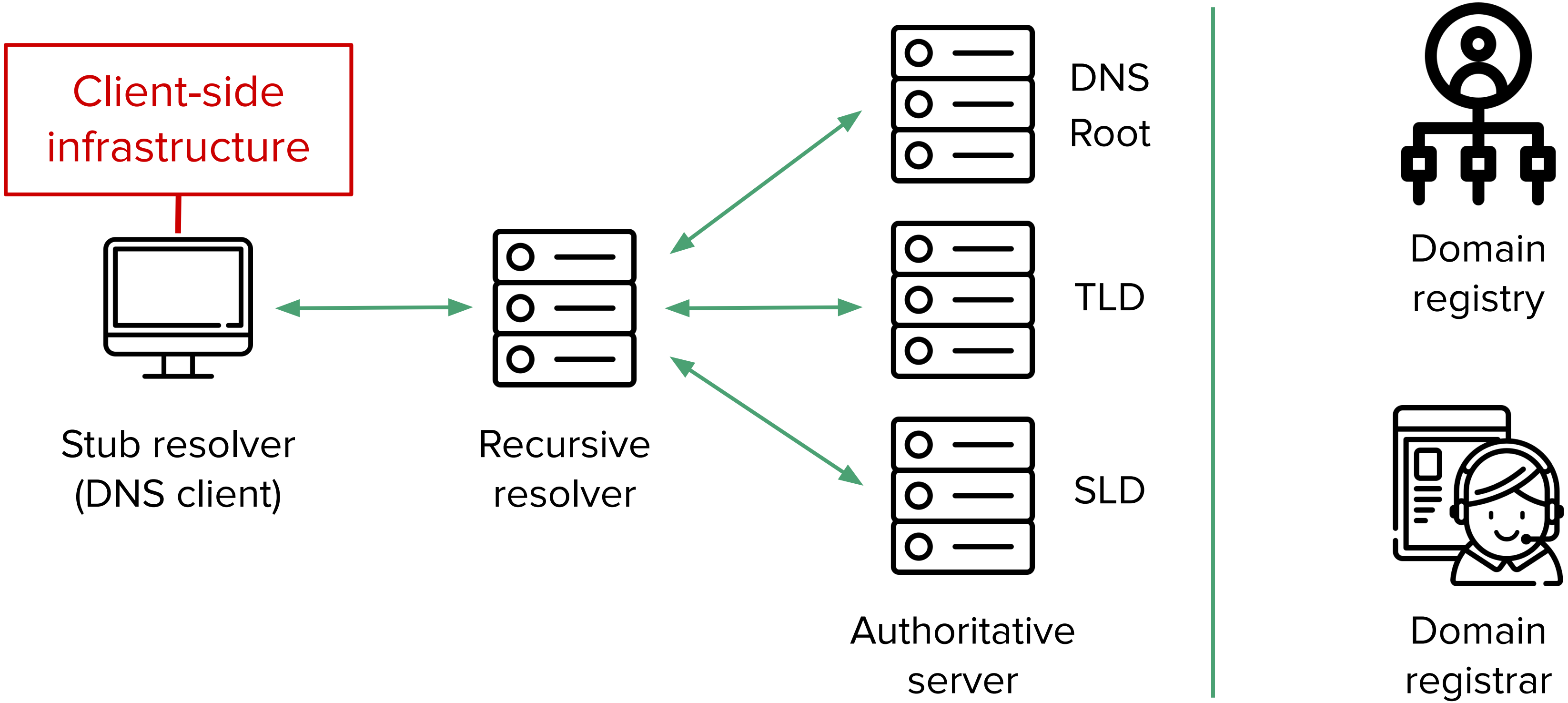


DNS Infrastructure



DNS SECURITY MEASUREMENTS

DNS Infrastructure



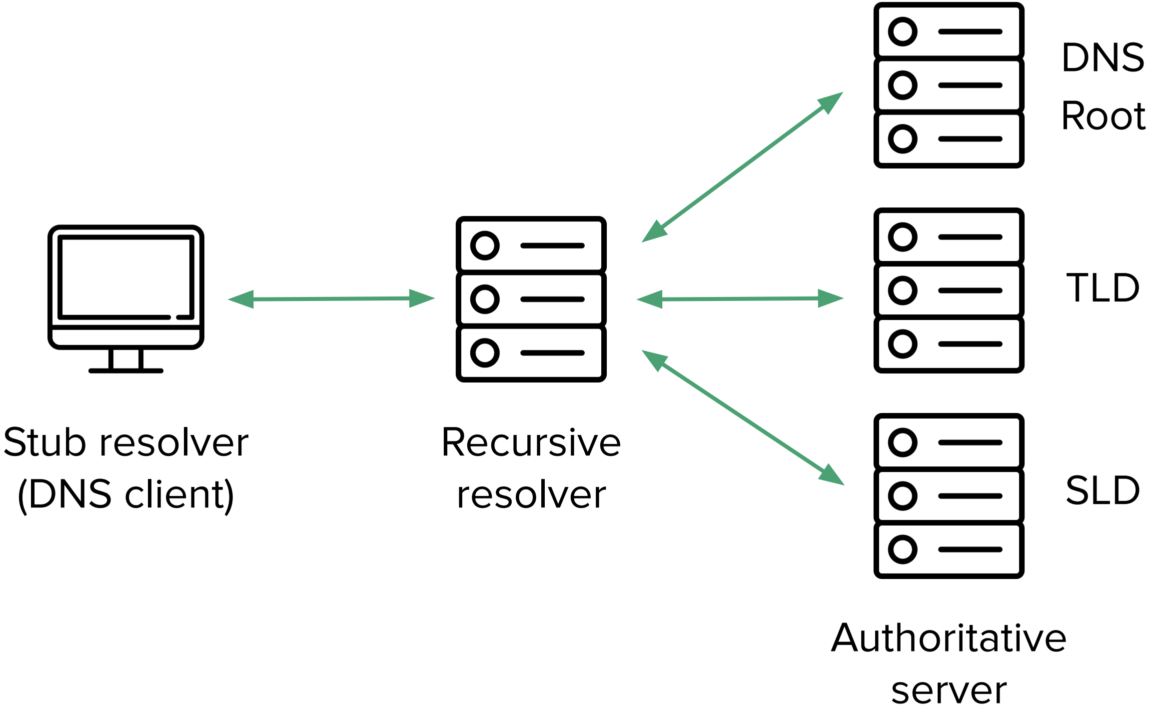
A. Client-Side Infrastructure

On Measuring the Client-Side DNS Infrastructure

Kyle Schomp[†], Tom Callahan[†], Michael Rabinovich[†], Mark Allman[‡]
[†]Case Western Reserve University, Cleveland, OH, USA
{kyle.schomp,tom.callahan,michael.rabinovich}@case.edu
[‡]International Computer Science Institute, Berkeley, CA, USA
mallman@icir.org

A. Client-Side Infrastructure

The client-side DNS infrastructure



A. Client-Side Infrastructure

The client-side DNS infrastructure

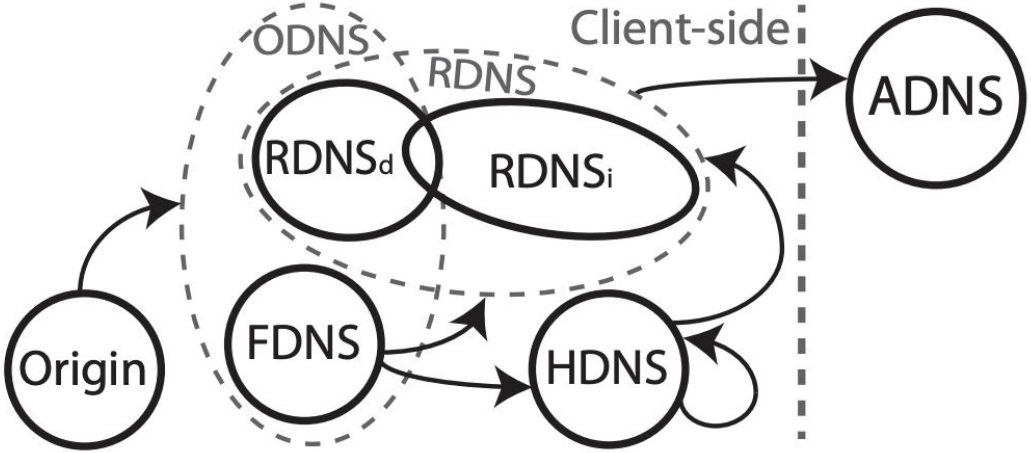
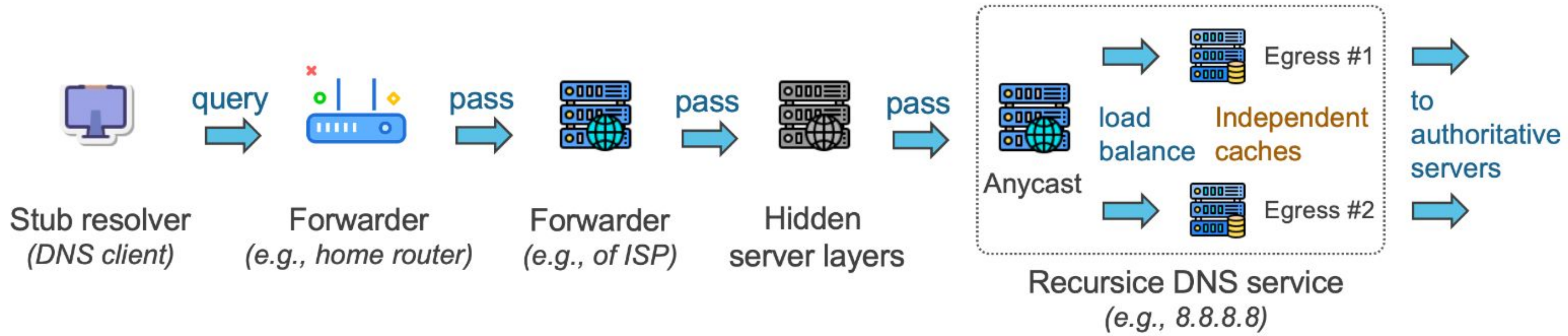


Figure 1: Structure of the client-side DNS infrastructure.

A. Client-Side Infrastructure

The client-side DNS infrastructure

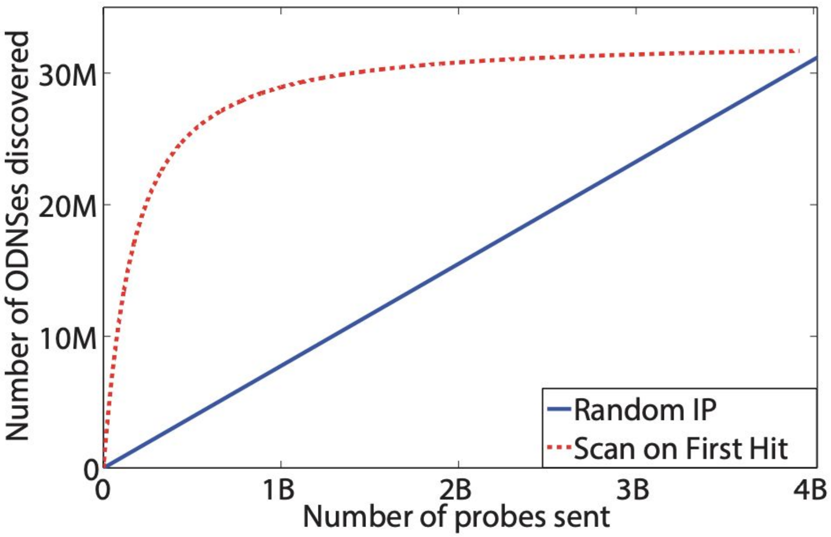
❖ A *typical* DNS resolution path now looks like this

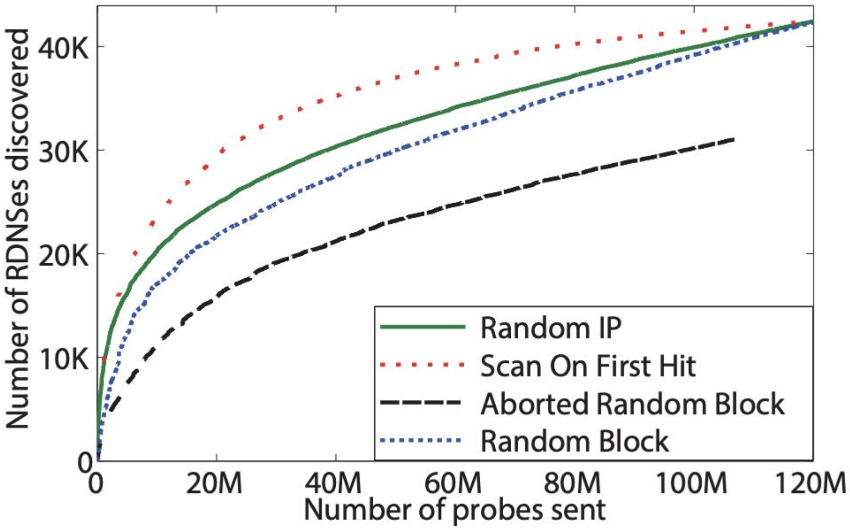


A. Client-Side Infrastructure

Count of ODNS & RDNS.

95% of ODNS are actually FDNS.





A. Client-Side Infrastructure

TTL & caching behaviors.

Behavior	Percentage of Measurements
Honest	19%
Lie on Initial	38%
Lie on Subsequent	9%
Constant TTL	7%
Increment TTL	1%

Table 3: Aggregate TTL Behavior

Expected (sec)	% <	% >	Mode Lie	
			Value	% of All Lies
1	0%	11%	10000	35%
10-120	$\leq$ 1%	$\leq$ 8%	10000	$\geq$ 37%
1000	1%	3%	10000	62%
3600	2%	2%	10000	51%
10000	5%	0%	3600	40%
10800	8%	0%	3600	27%
86400	16%	0%	21600	36%
100000	22%	0%	21600	27%
604800	22%	0%	21600	26%
1000000	64%	0%	604800	67%

Table 4: Aggregate TTL Deviations

Implementations are not always following the specifications.

A. Operational Statistics of the DNS

DNS Observatory: The Big Picture of the DNS

Pawel Foremski
Farsight Security, Inc. / IITiS PAN
pjf@fsi.io

Oliver Gasser
Technical University of Munich
gasser@net.in.tum.de

Giovane C. M. Moura
SIDN Labs / TU Delft
giovane.moura@sidn.nl

A. Operational Statistics of the DNS

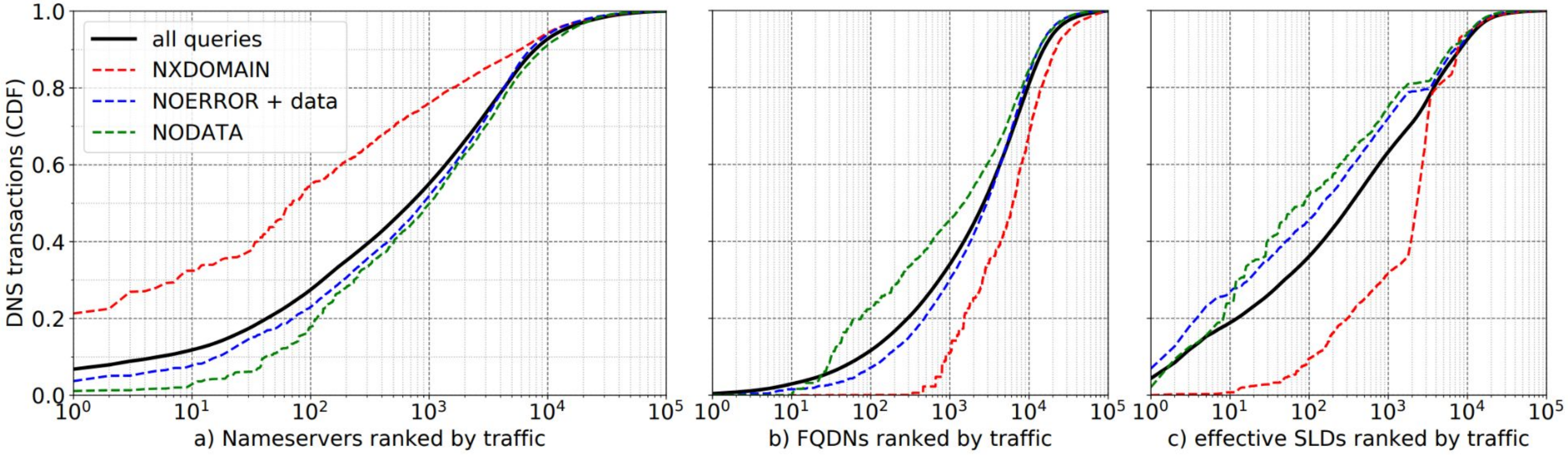
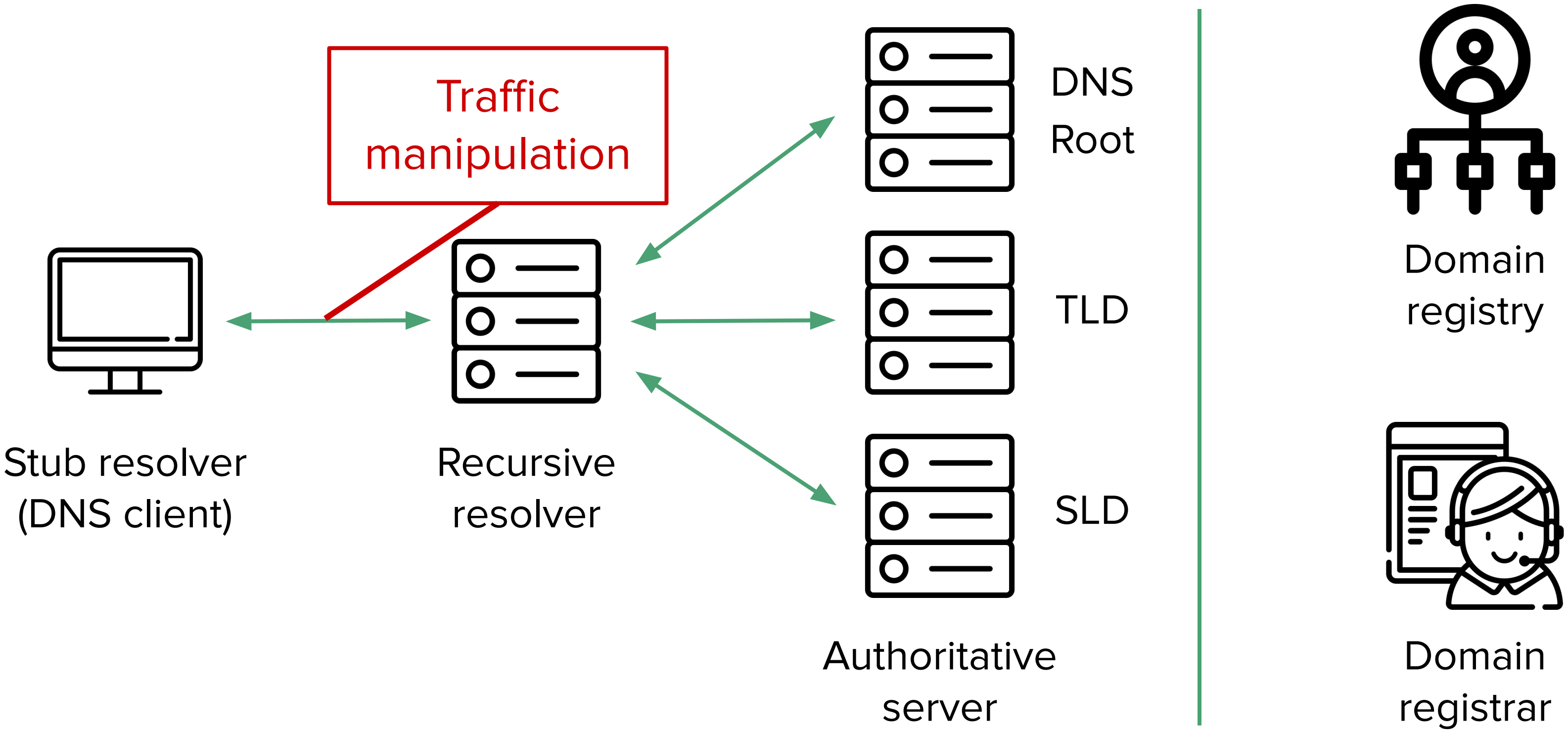


Figure 2: Traffic distributions for various Top-100K DNS objects, ranked by traffic. Note that the x-axis is log-scaled for improved readability.

A. Operational Statistics of the DNS

	QTYPE	global	data	nodata	nxd	err
1	A	**64%**	67%	**0.6%**	**22%**	11%
2	AAAA	**22%**	57%	**25%**	**5.9%**	11%
3	PTR	6.4%	45%	0.2%	29%	26%
4	NS	1.4%	9.4%	1.4%	**86%**	3.2%
5	TXT	1.4%	65%	4.1%	22%	8.1%
6	MX	1.2%	60%	3.3%	2.9%	**34%**

DNS Infrastructure



B. Packet Interception - Error Monetization

Redirecting DNS for Ads and Profit

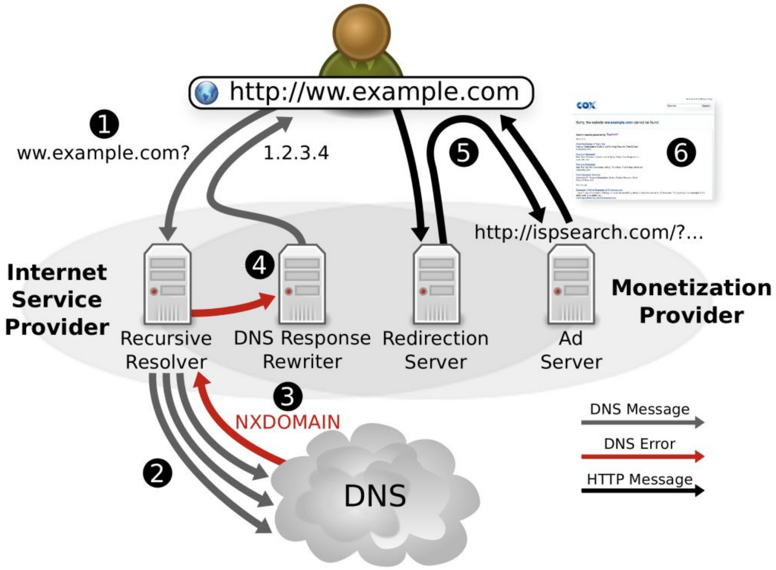
Nicholas Weaver
ICSI
nweaver@icir.org

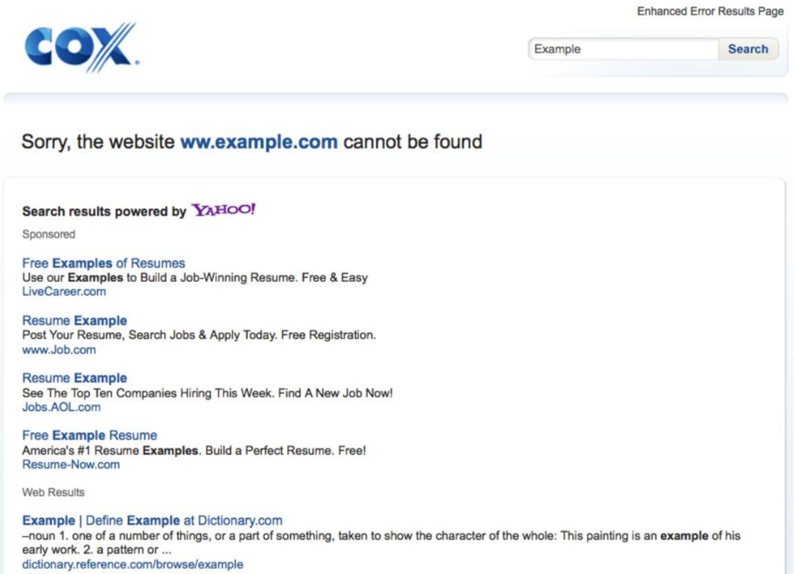
Christian Kreibich
ICSI
christian@icir.org

Vern Paxson
ICSI & UC Berkeley
vern@cs.berkeley.edu

B. Packet Interception - Error Monetization

Threat model





B. Packet Interception - Error Monetization

ISP	# Sessions	Country	Monetization Provider	Rewriting Rule	— User Opt-Out — Mechanism	% Rate
Alice DSL	3,761	DE	✘(AOL?)	www	Account Setting	25
Brazil Telecom	569	BR	✘	www	?	2
Charter	2,241	US	Paxfire → Xerocole	www	Account Setting	34
Comcast	17,362	US	FAST	www	Account Setting	27
Cox	2,633	US	Barefruit	all	Account Setting	18
Deutsche Telekom	12,671	DE	✘	all	Account Setting	30
Optimum Online	1,210	US	Infospace	www	Account Setting	15
Oi	657	BR	Barefruit	all	Cookie	25
Qwest	1,542	US	Barefruit	all	Account Setting	33
Rogers Cablesystems	1,197	CA	Paxfire	all	Cookie	4
Telecom Italia	1,429	IT	✘	all	?	33
Time Warner	7,287	US	Xerocole → FAST	www	Account Setting	20
UPC	964	NL	Infospace → Nominum	www	?	5
Verizon	4,751	US	Paxfire	www	Resolver Change	9
Virgin Media	1,890	UK	Nominum	www	?	28

Table 2: The 15 DNS-monetizing ISPs most prevalent in our Netalyzr dataset, their monetization providers, and monetization details. "→" indicates a provider switch, "✘" ISP-internal realization of the monetization service.

1-3 USD per customer of extra profit -> ISPs are willing to do this!

B. Packet Interception - Censorship

Global Measurement of DNS Manipulation

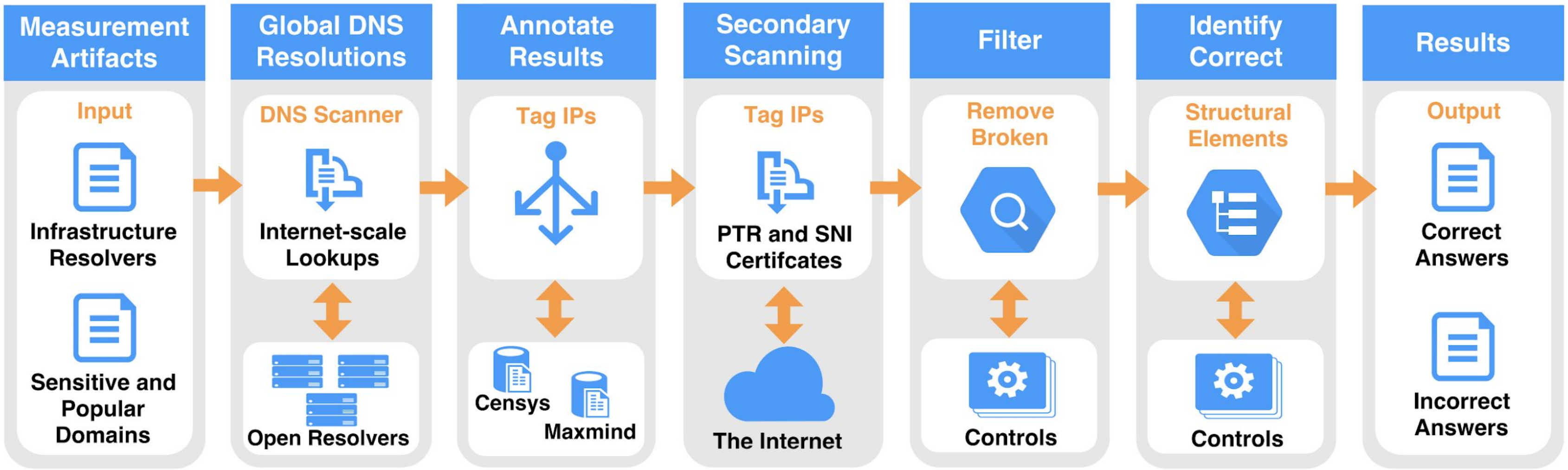
Paul Pearce[◇] *Ben Jones*[†] *Frank Li*[◇] *Roya Ensafi*[†]
Nick Feamster[†] *Nick Weaver*[‡] *Vern Paxson*[◇]

[◇]*University of California, Berkeley* [†]*Princeton University*
[‡] *International Computer Science Institute*

{pearce, frankli, vern}@cs.berkeley.edu *{bj6, rensafi, feamster}@cs.princeton.edu*
nweaver@icsi.berkeley.edu

B. Packet Interception - Censorship

Automatic detection of DNS manipulation



B. Packet Interception - Censorship

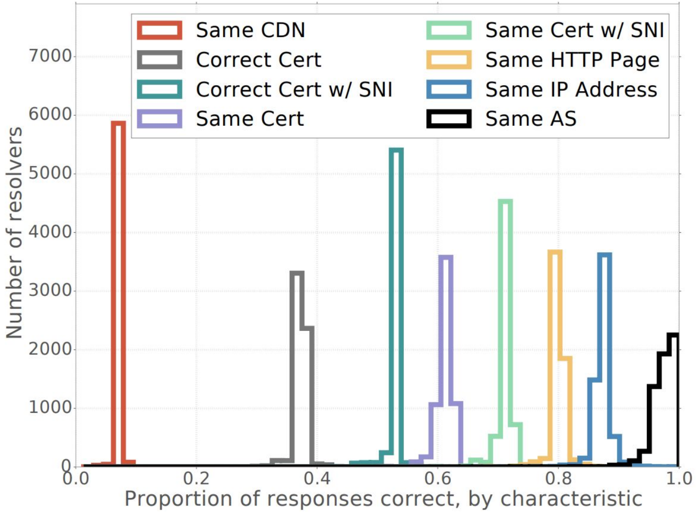


Figure 3: *The ability of each correctness metric to classify responses as correct. Table is ordered (top to bottom, left to right) by the lines on the graph (left to right).*

Several classification metrics

Rank	Domain Name	Category	# Cn	# Res
1	*pokerstars.com	Gambling	19	251
2	betway.com	Gambling	19	234
3	pornhub.com	Pornography	19	222
4	youporn.com	Pornography	19	192
5	xvideos.com	Pornography	19	174
6	thepiratebay.org	P2P sharing	18	236
7	thepiratebay.se	P2P sharing	18	217
8	xhamster.com	Pornography	18	200
9	*partypoker.com	Gambling	17	226
10	beeg.com	Pornography	17	183
80	torproject.org	Anon. & cen.	12	159
181	twitter.com	Twitter	9	160
250	*youtube.com	Google	8	165
495	*citizenlab.org	Freedom expr.	4	148
606	www.google.com	Google	3	56
1086	google.com	Google	1	5

Commonly manipulated domains

B. Packet Interception - Path Interception

Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path

Baojun Liu*, Chaoyi Lu*, Haixin Duan*, Ying Liu*✉, Zhou Li†, Shuang Hao‡ and Min Yang§

* Tsinghua University, † IEEE member,
‡ University of Texas at Dallas, § Fudan University

B. Packet Interception - Path Interception

Threat model

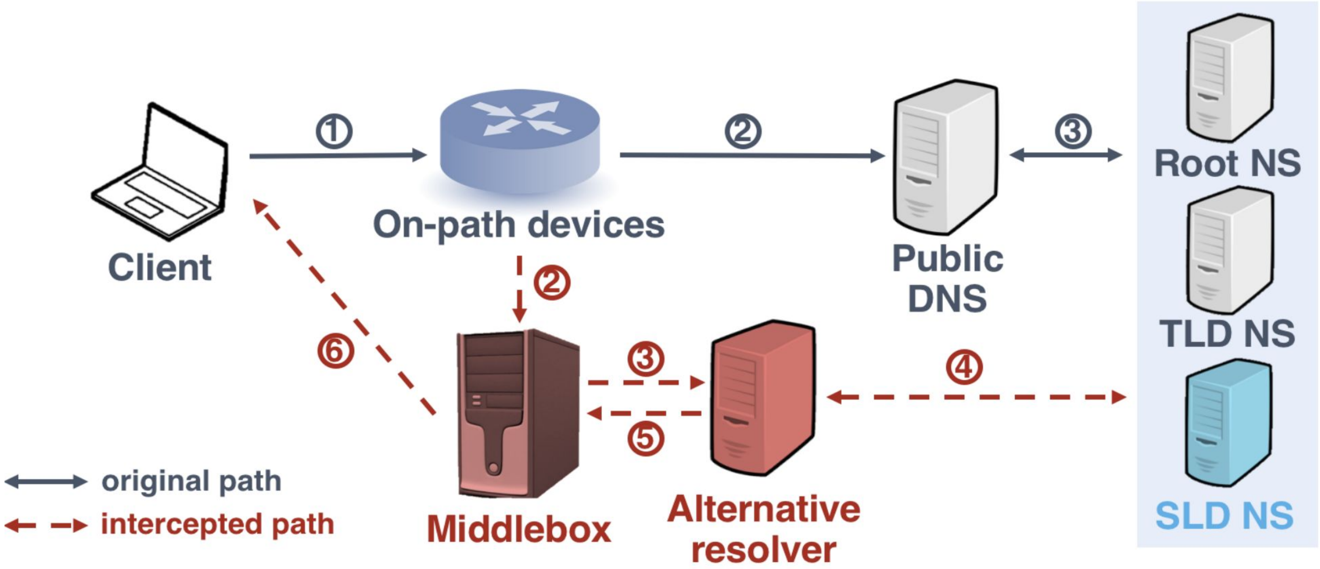
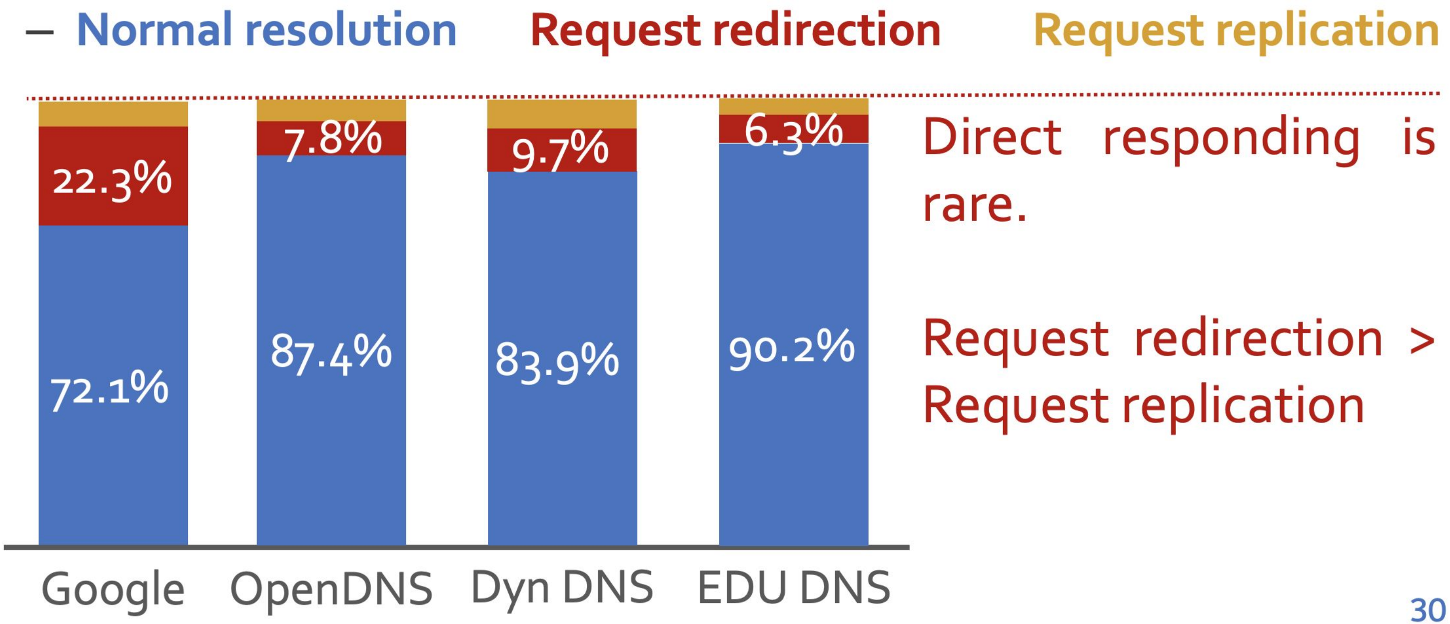


Figure 2: *Threat model*

B. Packet Interception - Path Interception



Direct responding is rare.

Request redirection > Request replication

30

B. Packet Interception - Path Interception

- Alternative resolvers' security
  - An analysis on **205 open alternative resolvers**

Only 43% resolvers support DNSSEC

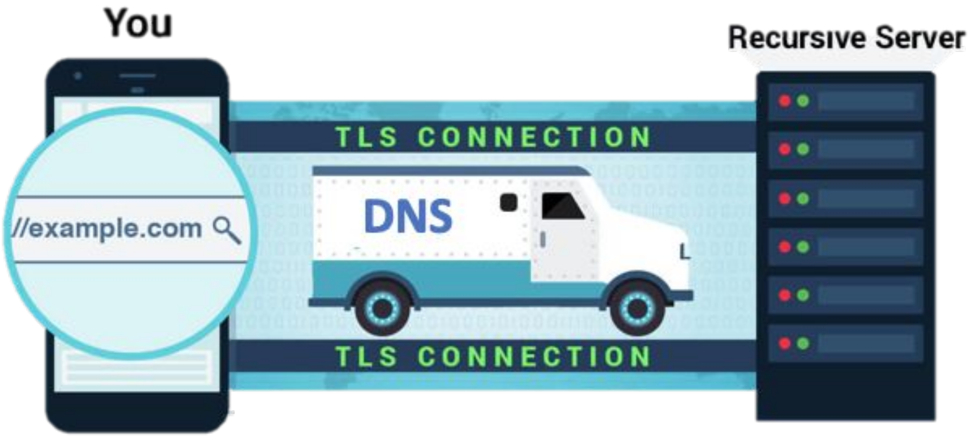
BIND
Berkeley Internet Domain Name

ALL BIND versions should be deprecated before 2009

B. Packet Interception - Recommendations

Deploy and use secure versions of DNS.

DNSSEC



Encrypted DNS

B. Packet Interception Defence - DNSSEC

A Longitudinal, End-to-End View of the DNSSEC Ecosystem

Taejoong Chung
Northeastern University

Roland van Rijswijk-Deij
University of Twente and SURFnet

Balakrishnan Chandrasekaran
TU Berlin

David Choffnes
Northeastern University

Dave Levin
University of Maryland

Bruce M. Maggs
Duke University and Akamai Technologies

Alan Mislove
Northeastern University

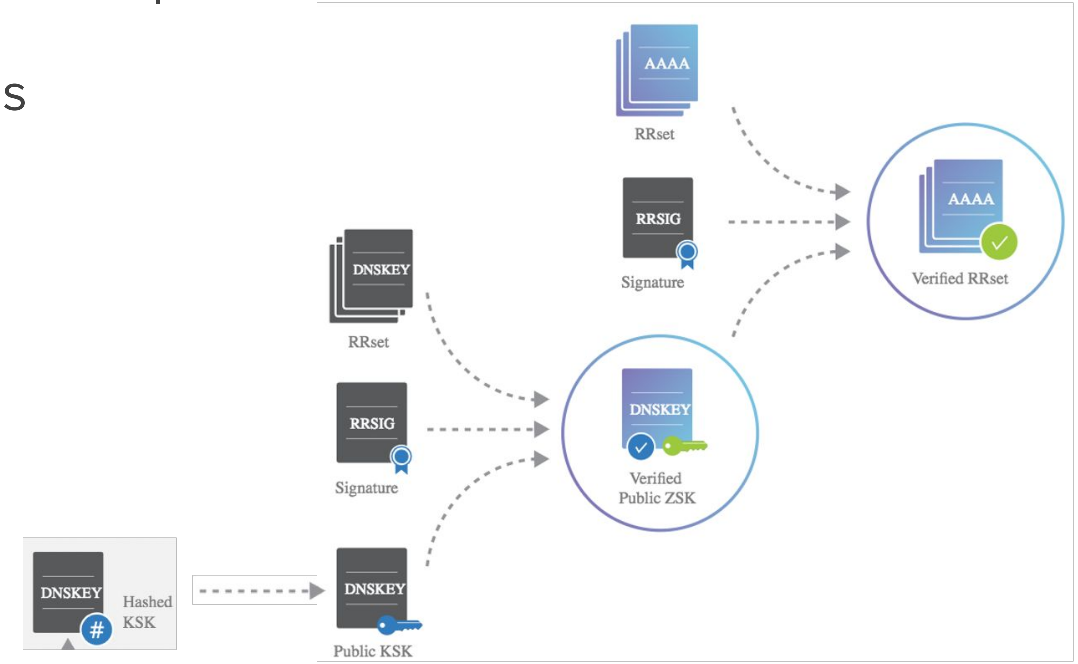
Christo Wilson
Northeastern University

B. Packet Interception Defence - DNSSEC

Gist: attach digital signatures to responses

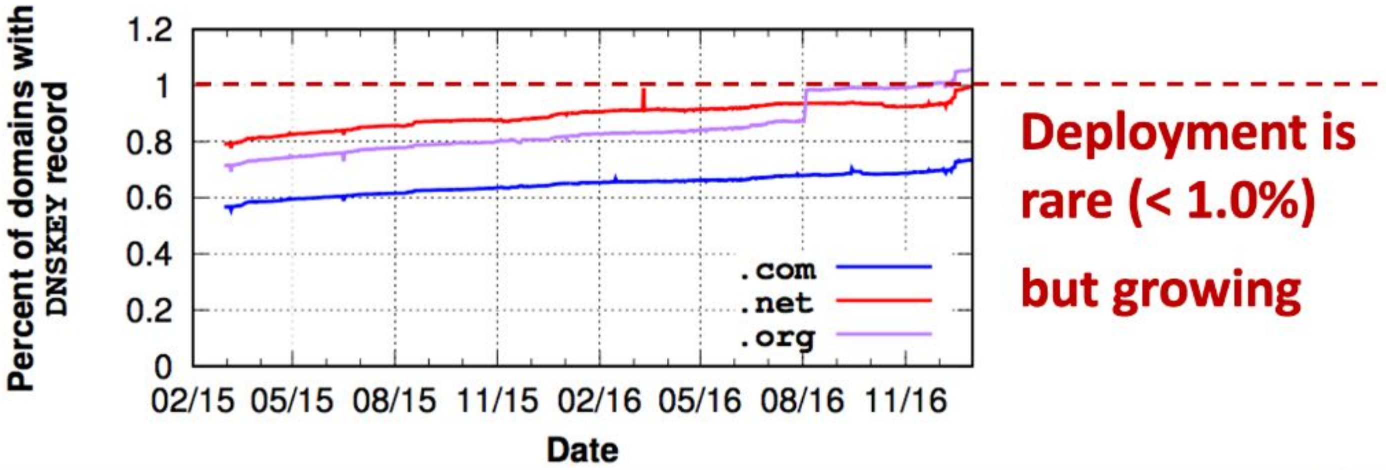
Domain owners **sign** domains

Resolver **validate** responses



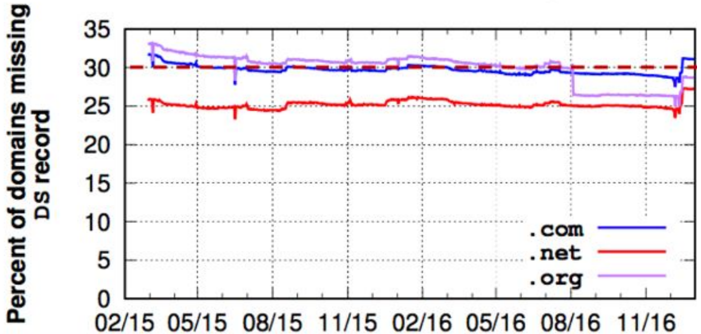
B. Packet Interception Defence - DNSSEC

- DNSSEC prevalence
  - Domain names with a DNSKEY record

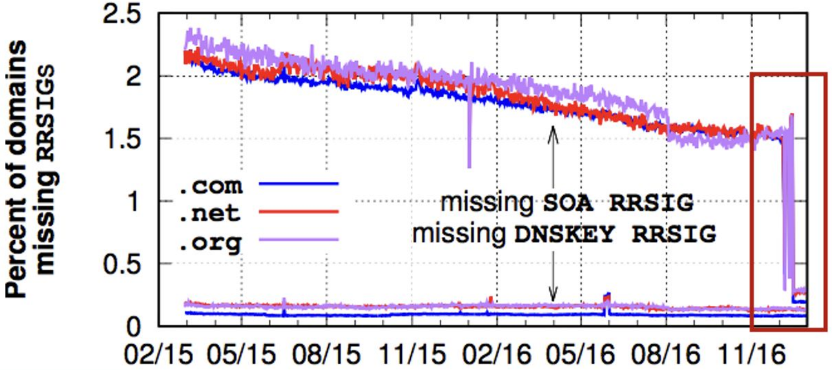


B. Packet Interception Defence - DNSSEC

- Missing DS records
  - Broken chain or trust
  - Domain owners need to contact registrar



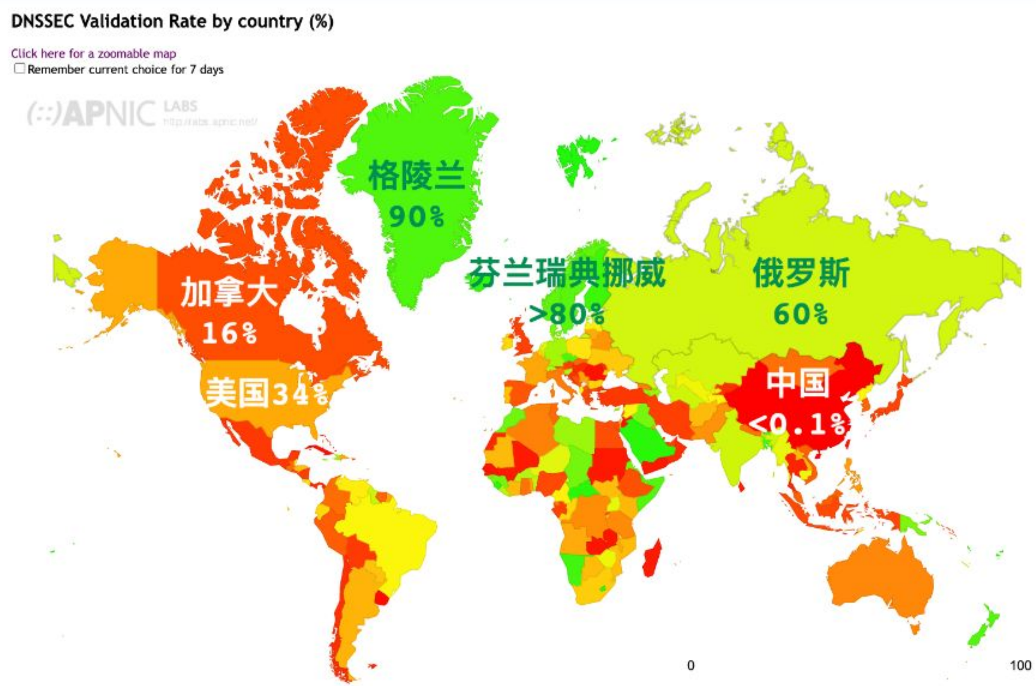
- Missing RRSIG records
  - No signatures to validate



30% domains have misconfigurations!

B. Packet Interception Defence - DNSSEC

Validation rate of recursive resolvers by country



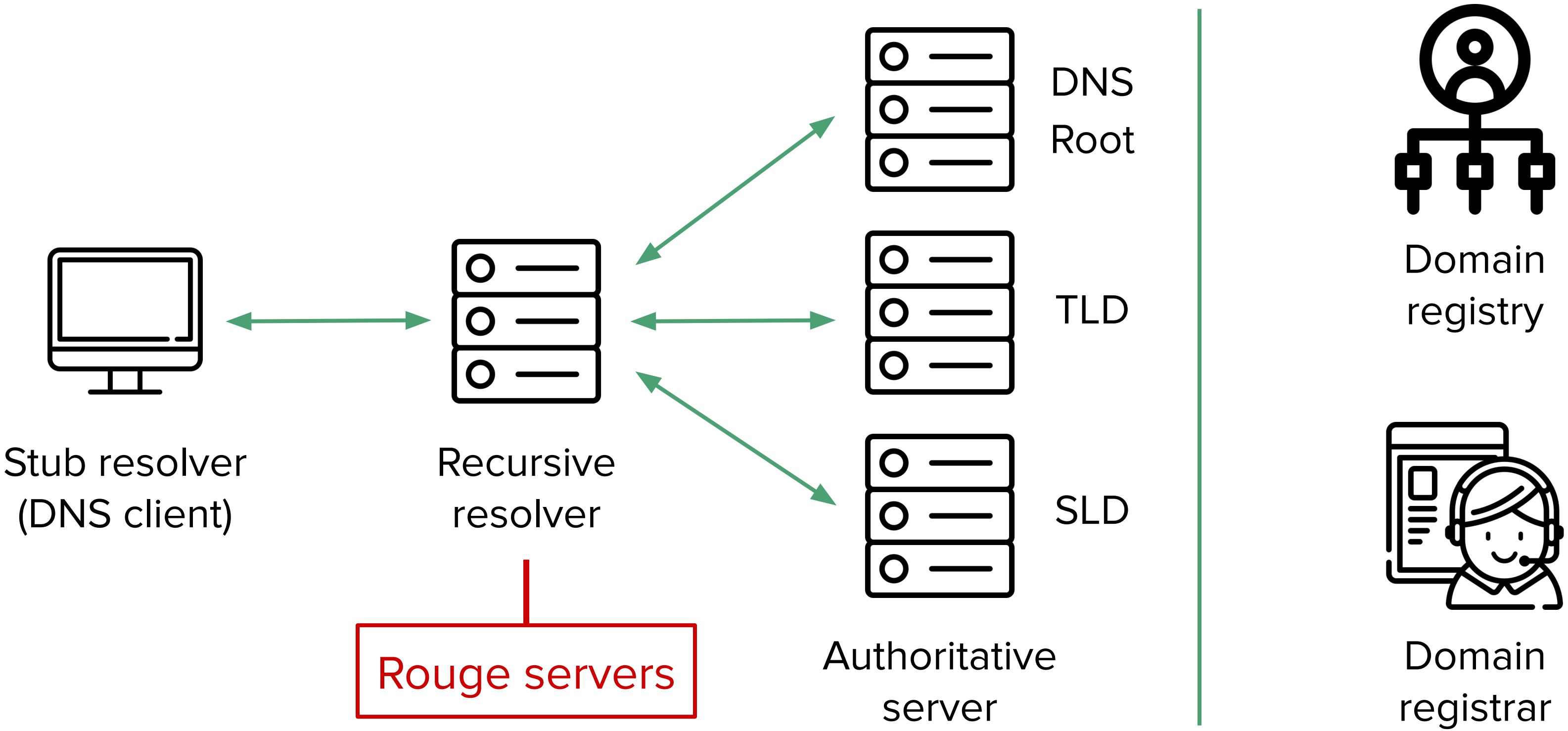
在多数国家，

服务器对DNSSEC签名的验证

比例仍然较低

推动DNSSEC的部署
需要域名所有者、域名
服务器的共同参与

DNS Infrastructure

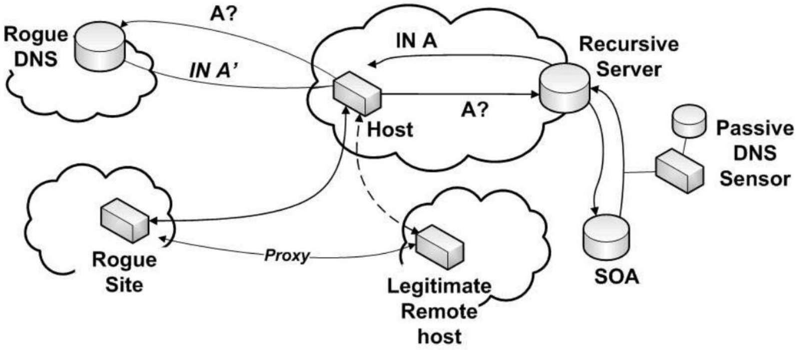


C. Rogue Servers - Resolver Altering

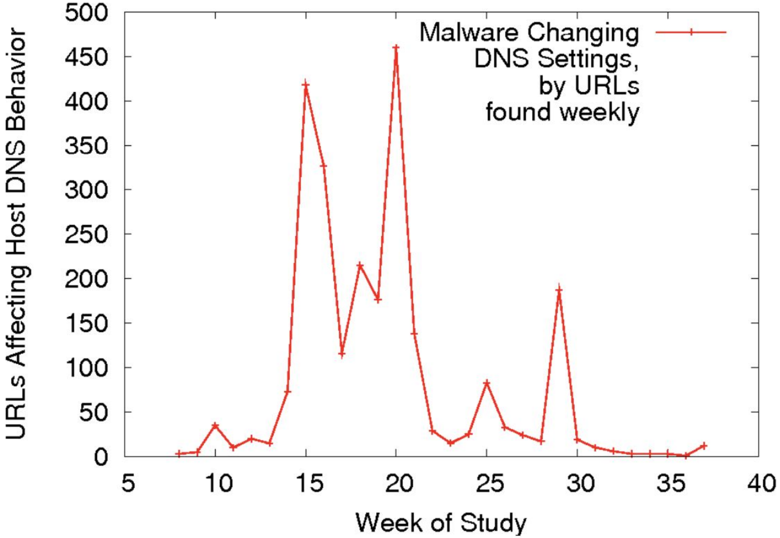
Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority

David Dagon[1] Niels Provos[2] Christopher P. Lee[3] Wenke Lee[1]
[1]College of Computing, Georgia Institute of Technology,
{dagon,wenke}@cc.gatech.edu
[2]Google Inc.
niels@google.com
[3]College of Engineering, Georgia Institute of Technology,
chrislee@gatech.edu

C. Rogue Servers - Resolver Altering



(a) DNS Resolution Paths



(a) URLs Altering Host DNS

C. Rogue Servers - Open Resolvers

Going Wild: Large-Scale Classification of Open DNS Resolvers

Marc Kührer
Ruhr-University Bochum
marc.kuehrer@rub.de

Thomas Hupperich
Ruhr-University Bochum
thomas.hupperich@rub.de

Jonas Bushart
Saarland University
s9jobush@stud.uni-saarland.de

Christian Rossow
Saarland University
crossow@mmci.uni-saarland.de

Thorsten Holz
Ruhr-University Bochum
thorsten.holz@rub.de

C. Rogue Servers - Open Resolvers

Resolver scan & classification.

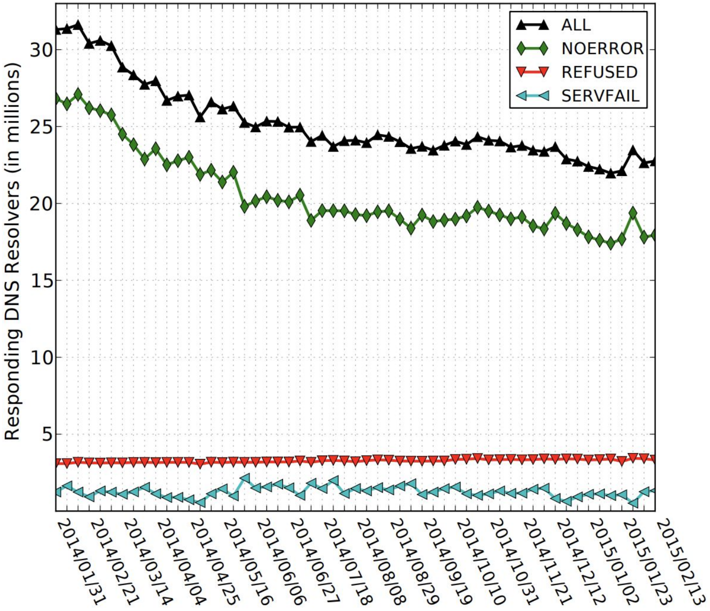


Figure 1: DNS resolvers identified in our weekly scans

Software	Resolvers	Released	Deprecated	CVE
BIND 9.8.2	19.8 %	Apr 2012	May 2012	IP Bypass, DoS Mem. Corr./Leak.
BIND 9.3.6	8.9 %	Nov 2008	Jan 2009	DoS
BIND 9.7.3	5.7 %	Feb 2012	Nov 2012	Mem. Overfl., DoS
BIND 9.9.5	5.2 %	Feb 2014	Sep 2014	DoS
Unbound 1.4.22	4.8 %	Mar 2014	Nov 2014	Mem. Overfl., DoS
Dnsmasq 2.40	4.6 %	Aug 2007	Feb 2008	RCE, DoS
BIND 9.8.4	3.9 %	Oct 2012	May 2013	IP Bypass, DoS Mem. Overfl.
PowerDNS 3.5.3	3.2 %	Sep 2013	Jun 2014	DoS
Dnsmasq 2.52	2.9 %	Jan 2010	Jun 2010	DoS
MS DNS 6.1.7601	2.5 %	Jun 2011	Aug 2011	DoS

Deprecated software versions are still in use.

	Hardware (in %)						
	Router	Embedded	Firewall	Camera	DVR	Others	Unknown
DNS	34.1	30.6	1.9	1.8	1.2	1.1	29.3

Routers & Embedded devices.

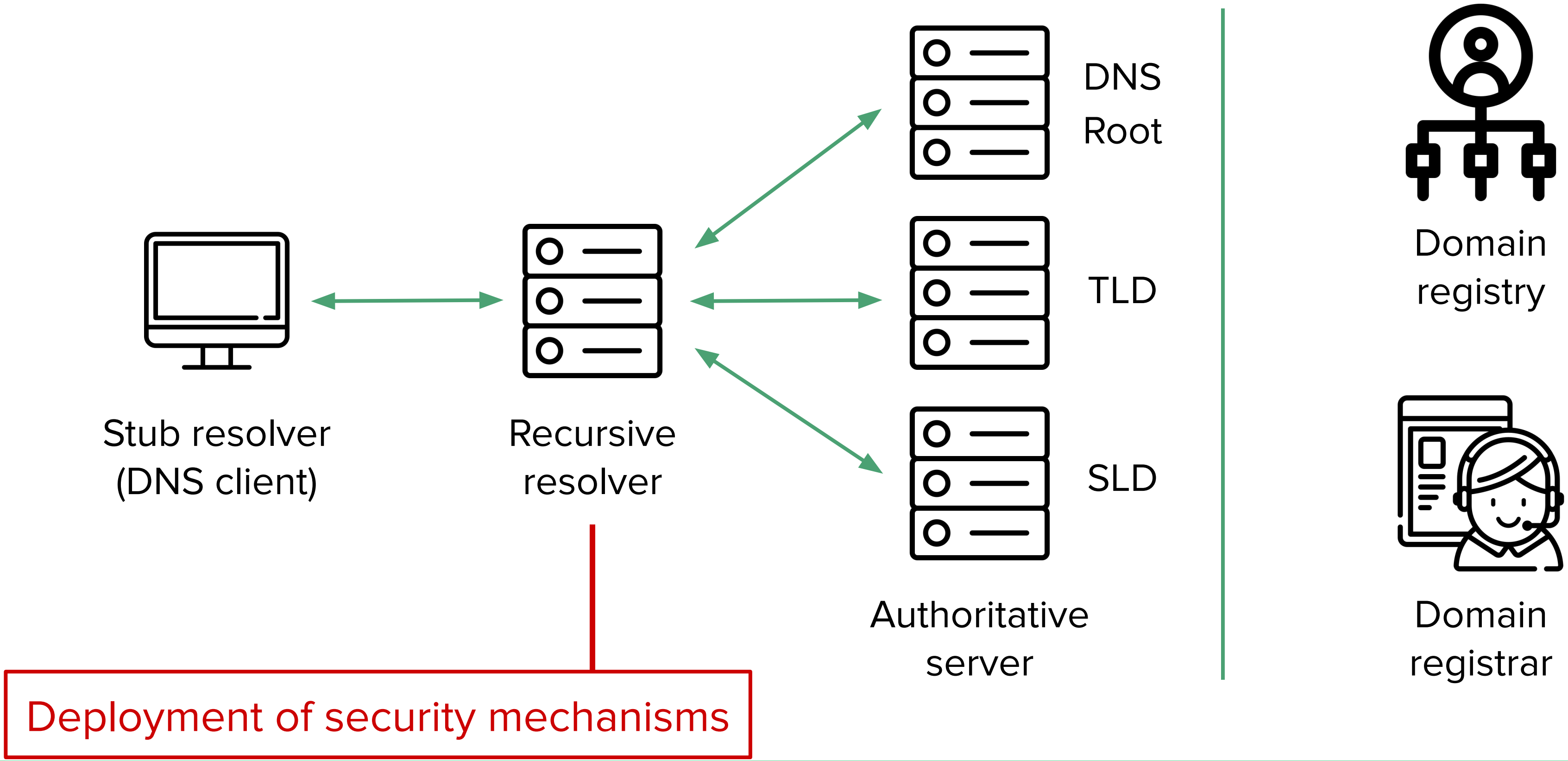
C. Rogue Servers - Open Resolvers

Analysis of bogus resolutions.

Table 5: Clustering and labeling results of the HTTP payload data for unexpected (*domain* ∘ *ip* ∘ *resolver*) tuples

Label	Ads	Adult	Alexa	Antivirus	Banking	Dating	Filesharing	Gambling	GroundTr.	Malware	Misc.	MX	NX	Tracking
	Average number of resolvers in % / (Highest number of resolvers seen for a domain in the particular dataset in %)													
Blocking	0.3	2.2	0.7	0.3	0.4	6.2	3.1	3.7	0.2	9.0	0.9	0.9	1.9	0.6
	(0.5)	(3.3)	(2.5)	(0.4)	(1.0)	(10.9)	(6.5)	(6.4)	(0.2)	(21.4)	(4.8)	(1.9)	(16.2)	(2.2)
Censorship	10.8	88.6	19.1	0.1	0.1	31.8	36.5	75.9	0.1	0.8	8.4	0.1	3.2	0.1
	(96.2)	(91.3)	(97.1)	(0.1)	(0.1)	(87.3)	(91.3)	(90.4)	(0.1)	(8.1)	(92.5)	(0.2)	(37.1)	(0.1)
HTTP Error	48.1	5.2	45.8	57.0	55.4	34.8	32.6	15.8	55.0	29.8	50.8	57.0	24.7	57.0
	(70.4)	(6.9)	(63.9)	(75.0)	(63.5)	(50.1)	(52.0)	(49.8)	(56.0)	(53.7)	(71.1)	(65.9)	(55.8)	(69.4)
Login	12.2	1.2	12.8	15.5	16.8	10.2	9.5	1.9	16.1	9.5	14.3	17.0	2.8	12.5
	(16.8)	(1.6)	(19.1)	(17.4)	(19.6)	(15.4)	(15.1)	(3.9)	(17.2)	(17.2)	(18.5)	(19.8)	(9.4)	(16.2)
Misc.	11.5	0.9	5.3	5.9	5.0	3.2	4.9	0.7	5.1	3.3	5.1	5.0	8.5	11.2
	(56.4)	(1.6)	(21.6)	(16.2)	(10.5)	(4.8)	(12.5)	(1.4)	(5.8)	(5.6)	(9.7)	(5.8)	(19.7)	(5.5)
Parking	17.1	1.8	16.1	21.2	22.2	13.8	13.4	2.0	23.4	26.2	20.5	20.0	23.2	18.6
	(23.9)	(2.4)	(24.0)	(25.0)	(24.3)	(21.5)	(22.4)	(2.4)	(23.9)	(92.1)	(83.6)	(23.4)	(42.4)	(24.0)
Search	0.0	0.1	0.2	0.0	0.1	0.0	0.0	0.0	0.1	21.4	0.0	0.0	35.7	0.0
	(0.1)	(0.1)	(2.7)	(0.1)	(0.1)	(0.1)	(0.0)	(0.0)	(0.6)	(69.3)	(0.5)	(0.1)	(65.1)	(0.0)

DNS Infrastructure



C. Deployment of Security Mechanisms

Fourteen Years in the Life:
A Root Server's Perspective on DNS Resolver Security

Alden Hilton*
Sandia National Laboratories
alden.hilton@sandia.gov

Casey Deccio
Brigham Young University
casey@byu.edu

Jacob Davis
Sandia National Laboratories
jacdavi@sandia.gov

C. Deployment of Security Mechanisms

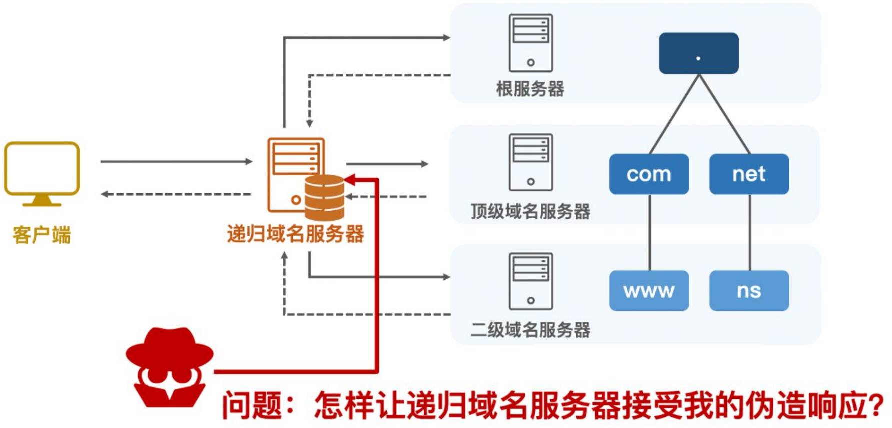
A. Src port & TXID randomization - defence for cache poisoning

缓存污染攻击

攻击模型：旁路注入（off-path injection）

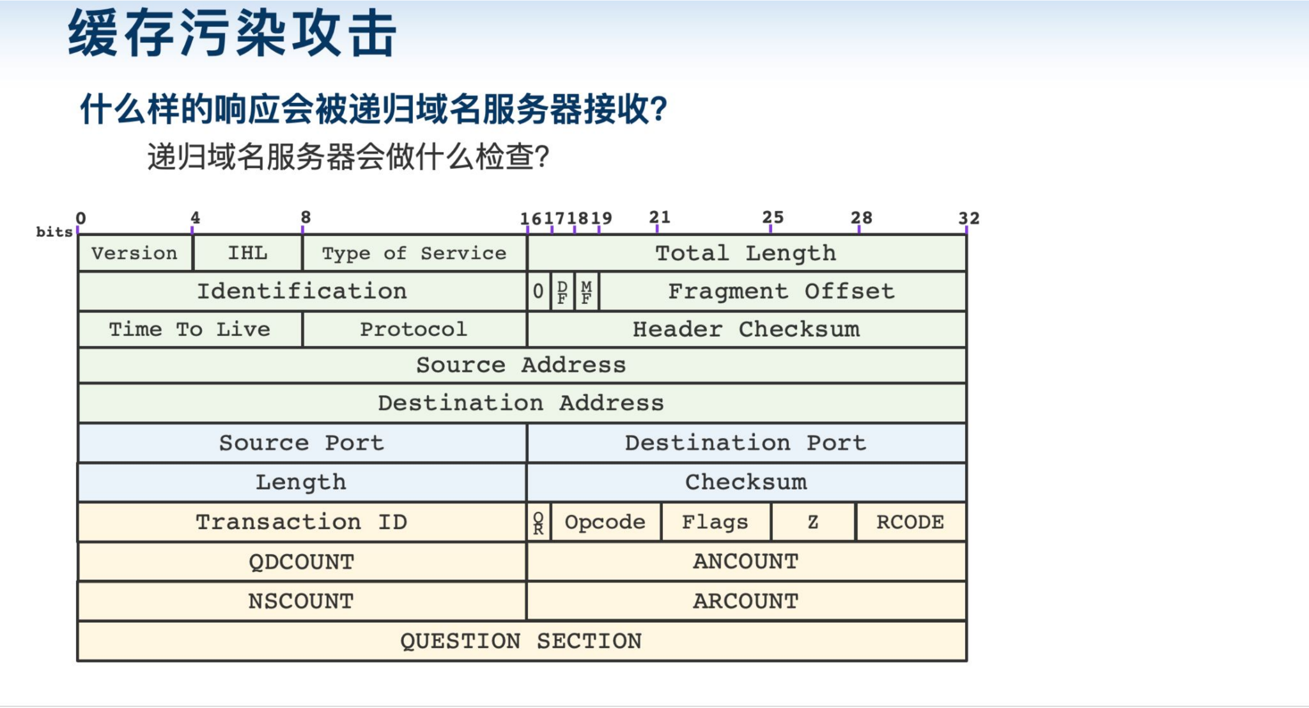
攻击者**并不位于域名解析链路上**，无法直接嗅探和修改报文

攻击者想要**注入一个伪造的响应**，使得递归域名服务器接受并写入缓存



C. Deployment of Security Mechanisms

A. Src port & TXID randomization - defence for cache poisoning



C. Deployment of Security Mechanisms

A. Src port & TXID randomization - defence for cache poisoning

缓存污染攻击

攻击者如何伪造符合上述条件的响应?

条件	备注	是否可控/可预知
IP地址匹配	响应源地址 = 权威服务器地址	是（通过查询实现）
	响应目的地址 = 递归域名服务器	是
端口匹配	响应源端口 = 53（DNS默认服务端口）	是
	响应目的端口 = 请求源端口	否
TXID匹配	响应TXID = 请求TXID	否
问题区域匹配	响应问题区域 = 请求问题区域	是（为什么？）
伪造响应先到达	伪造响应先于真实响应到达	是

C. Deployment of Security Mechanisms

A. Src port & TXID randomization - defence for cache poisoning

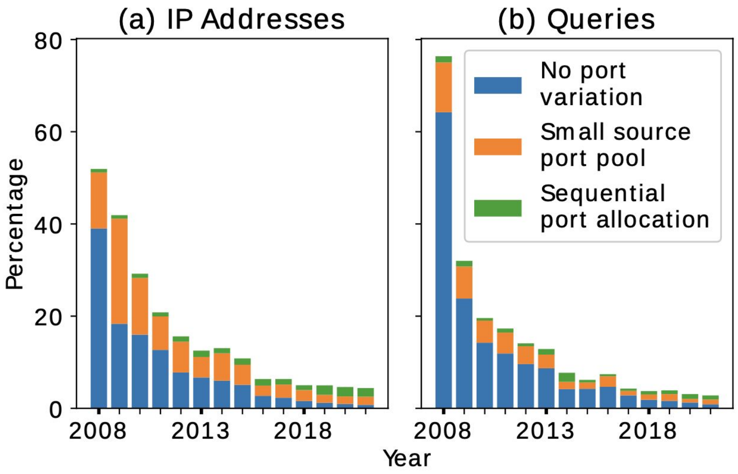


Figure 1: (a) The percentage of resolvers with poor SPR. (b) The percentage of queries from resolvers with poor SPR.

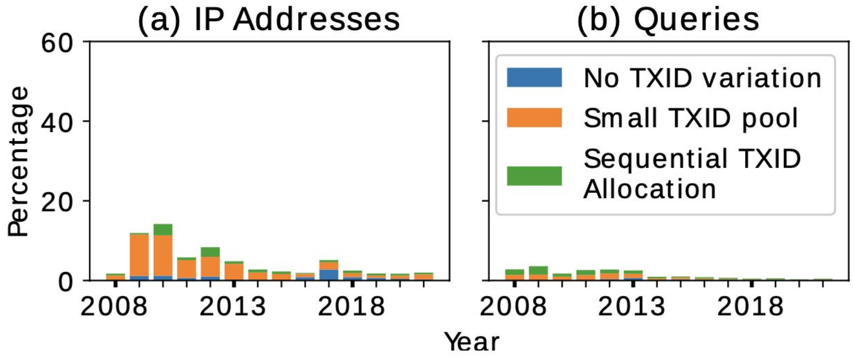


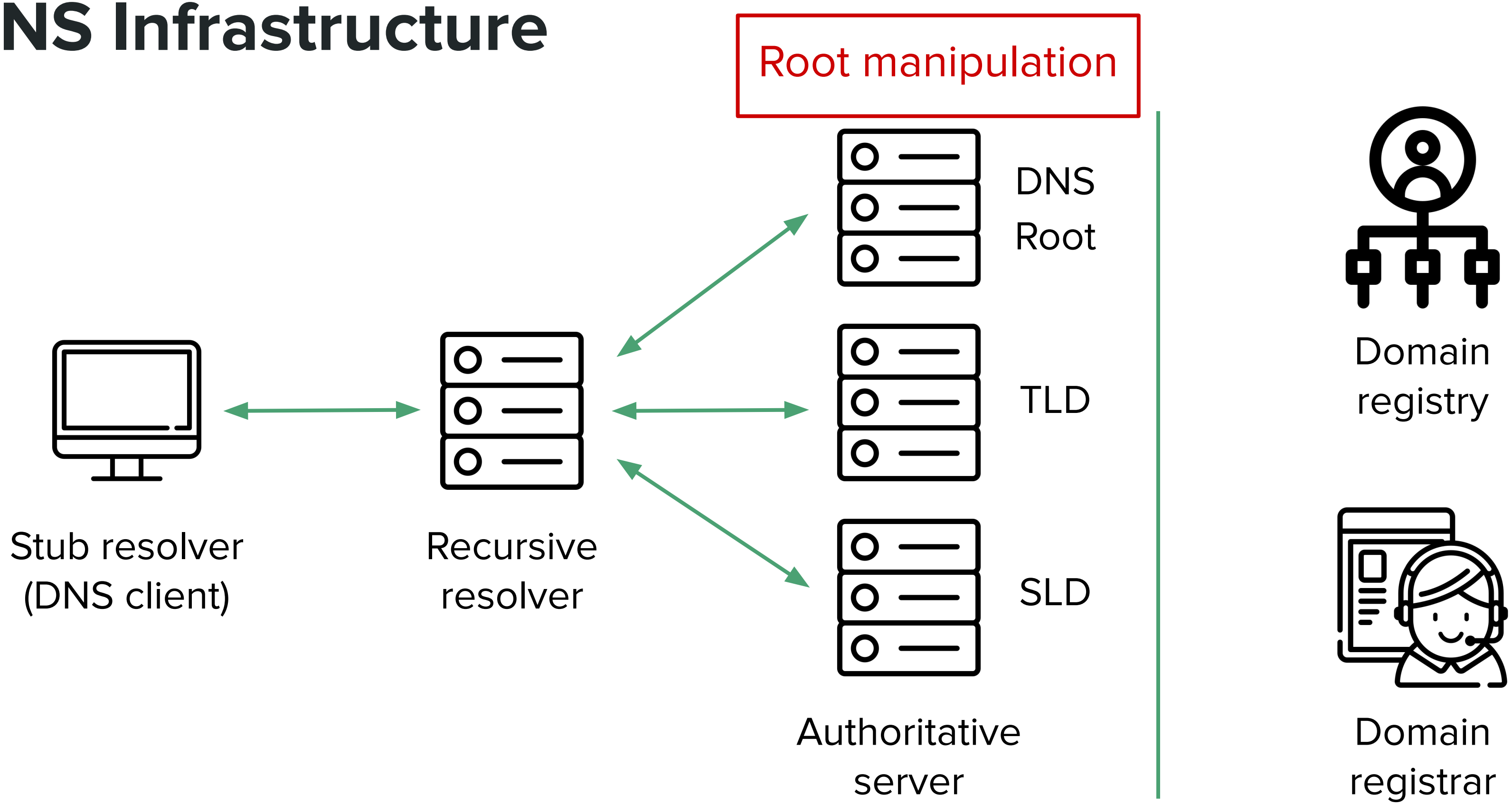
Figure 2: (a) The percentage of resolvers with poor TXID randomization. (b) The percentage of queries from resolvers with poor TXID randomization

C. Deployment of Security Mechanisms

B. Interactions between different security mechanisms

TXID	SPR	DNSSEC	0x20	Cookies	QMIN	IP Addresses		ASes		Queries	
						#	%	#	%	#	%
✓	✓	×	×	×	×	2,189,133	59.0%	40,173	79.8%	1,268	19.9%
✓	✓	✓	×	×	×	503,799	13.6%	26,486	52.6%	15,449	55.8%
✓	✓	×	×	✓	×	315,015	8.5%	13,168	26.2%	857	1.9%
✓	✓	×	×	×	✓	189,895	5.1%	7,956	15.8%	2,242	3.1%
✓	✓	✓	×	×	✓	157,278	4.2%	9,782	19.4%	7,895	8.9%
✓	✓	✓	×	✓	×	133,099	3.6%	12,398	24.6%	5,296	5.1%
✓	×	×	×	×	×	114,592	3.1%	6,931	13.8%	2,527	2.1%
×	×	×	×	×	×	47,069	1.3%	3,202	6.4%	383	0.1%
×	✓	×	×	×	×	24,192	0.7%	2,191	4.4%	849	0.1%
other						38,716	1.0%	5,471	10.9%	11,042	3.1%

DNS Infrastructure



D. Root Manipulation - Unauthorized Root

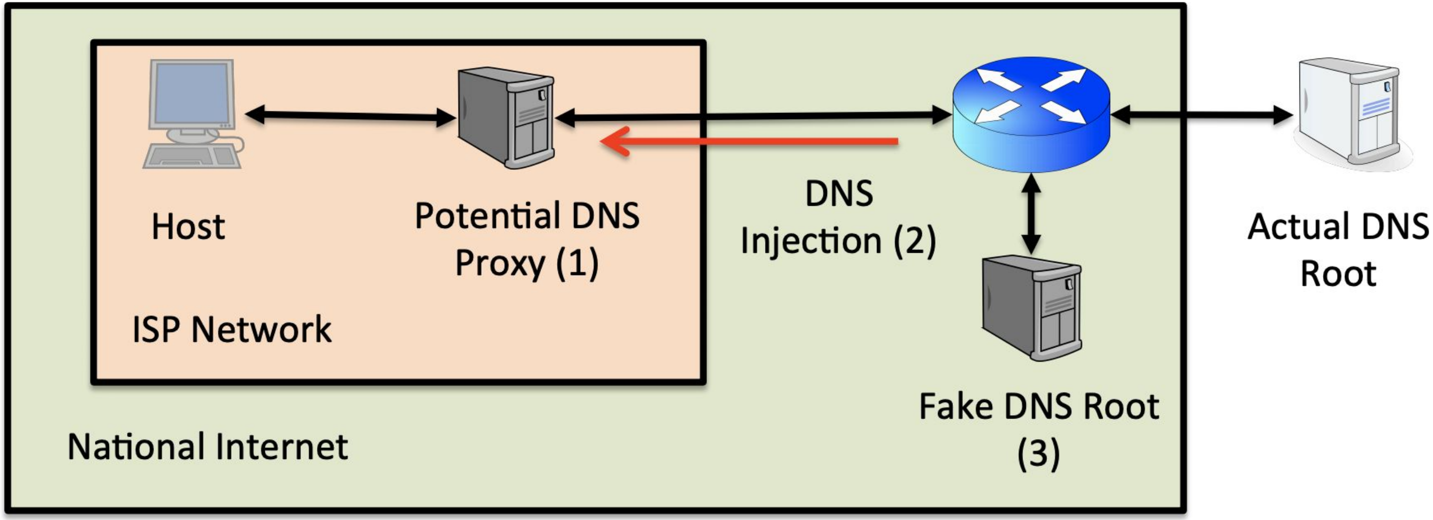
Detecting DNS Root Manipulation

Ben Jones[1], Nick Feamster[1], Vern Paxson[2,3], Nicholas Weaver[2], and Mark Allman[2]

[1] Princeton University
[2] International Computer Science Institute
[3] University of California, Berkeley

D. Root Manipulation - Unauthorized Root

Threat model



D. Root Manipulation - Unauthorized Root

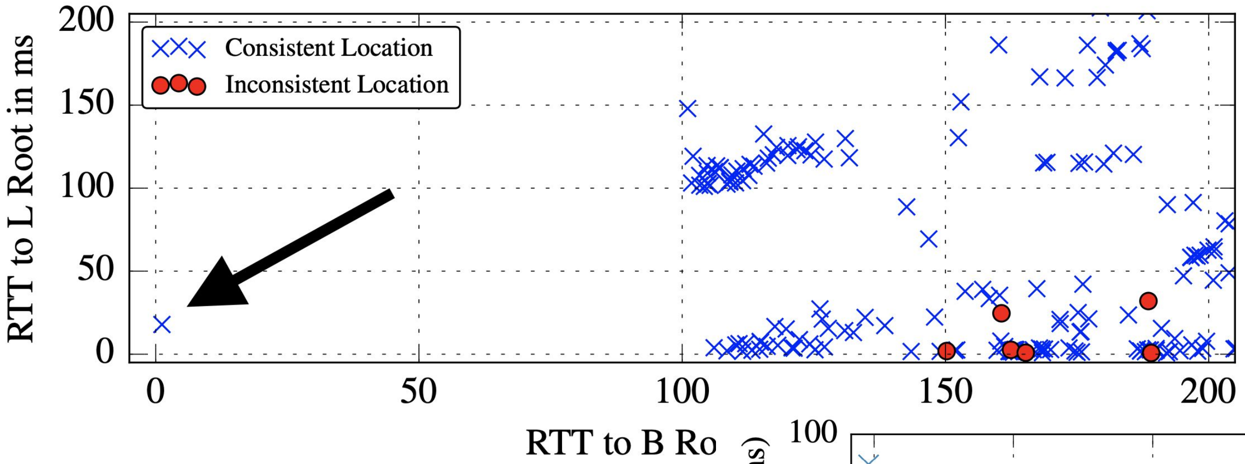
Vantage point & dataset collection

DNS, ping & traceroute requests to the Unicast-B Root

Measurements	Dates	Manipulation
RIPE Atlas		
ping	July 6–13, 2014	root mirrors
HOSTNAME.BIND	July 22, 2014	proxies & root mirrors
traceroutes	July 6, 2014	proxies & root mirrors
BGP		
RIPE RIS	July 6–13, 2014	root mirrors
RouteViews	July 7, 2014	root mirrors

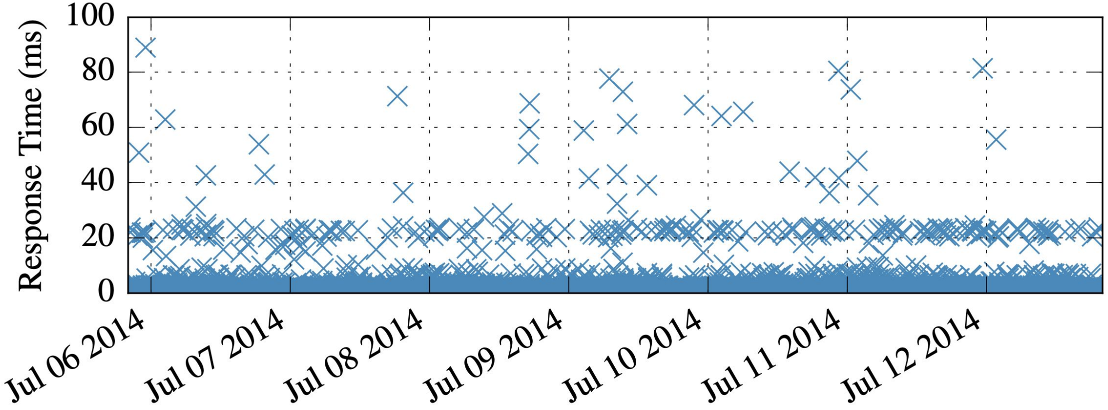
Table 1: Data sources used to investigate possible manipulation.

D. Root Manipulation - Unauthorized Root



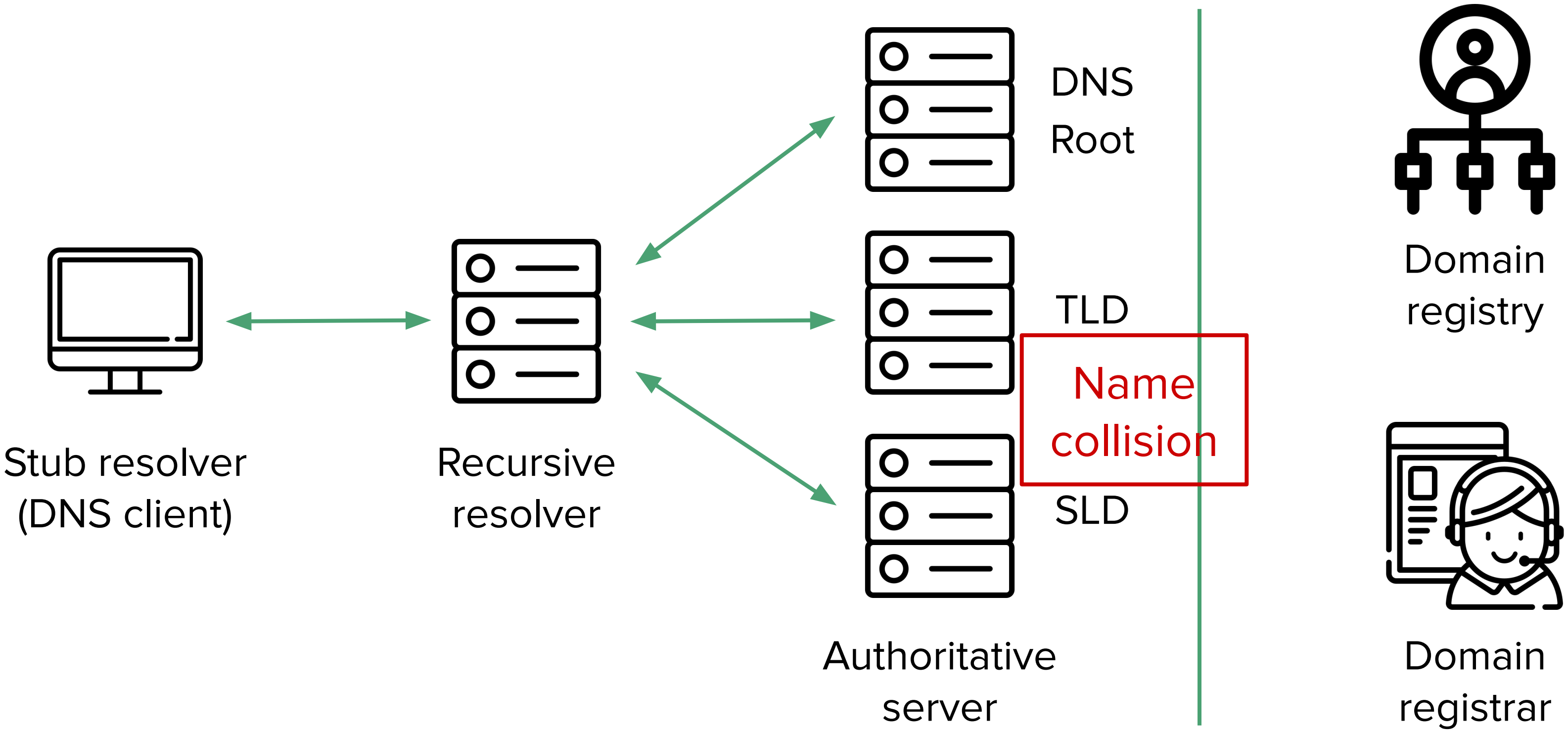
Consistently short RTT.

Traceroutes are in the same ASN.



An unauthorized root mirror in CERNET

DNS Infrastructure



E. Name Collision - New gTLD

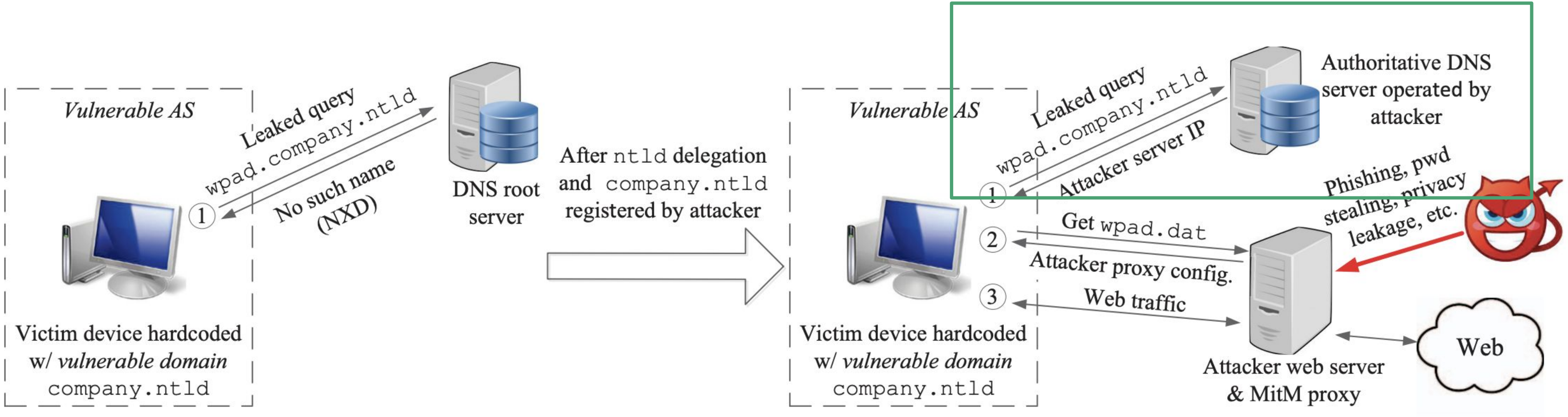
MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era

Qi Alfred Chen, Eric Osterweil[†], Matthew Thomas[†], Z. Morley Mao
University of Michigan, [†]Verisign Labs
alfchen@umich.edu, {eosterweil, mthomas}@verisign.com, zmao@umich.edu

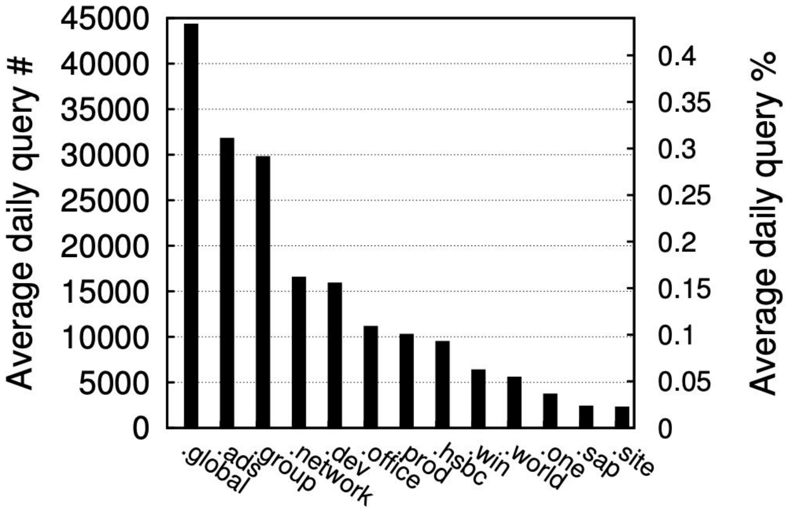
E. Name Collision - New gTLD

Threat model

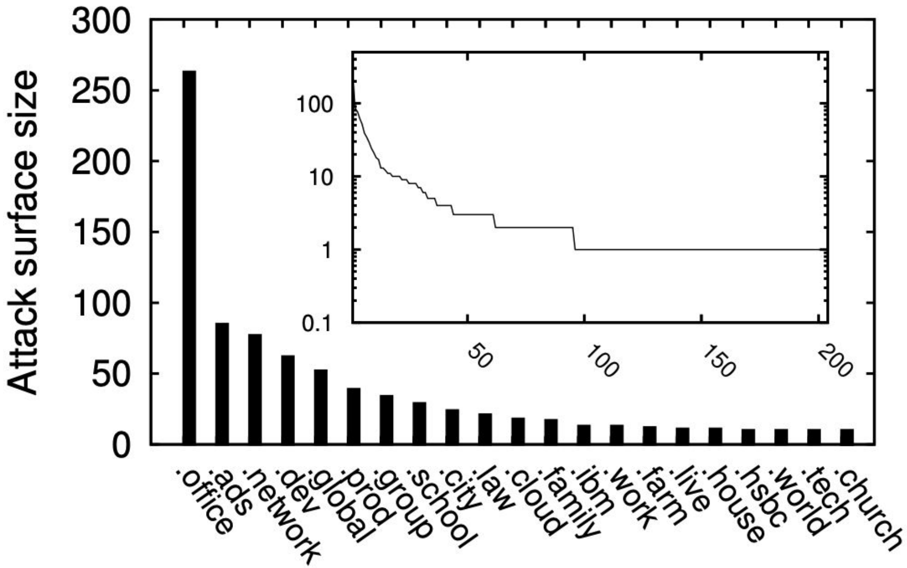
Name collision caused by new gTLD



E. Name Collision - New gTLD



Popular delegated new gTLDs in NXD WPAD queries



New gTLDs ranked by attack surface size

Potential attack surface is opening.

E. Name Collision - New gTLD

Client-side Name Collision Vulnerability in the New gTLD Era: A Systematic Study

Qi Alfred Chen, Matthew Thomas[†], Eric Osterweil[†], Yulong Cao, Jie You, Z. Morley Mao
University of Michigan, †Verisign Labs
alfchen@umich.edu,{mthomas,eosterweil}@verisign.com,{yulongc,jieyou,zmao}@umich.edu

E. Name Collision - New gTLD

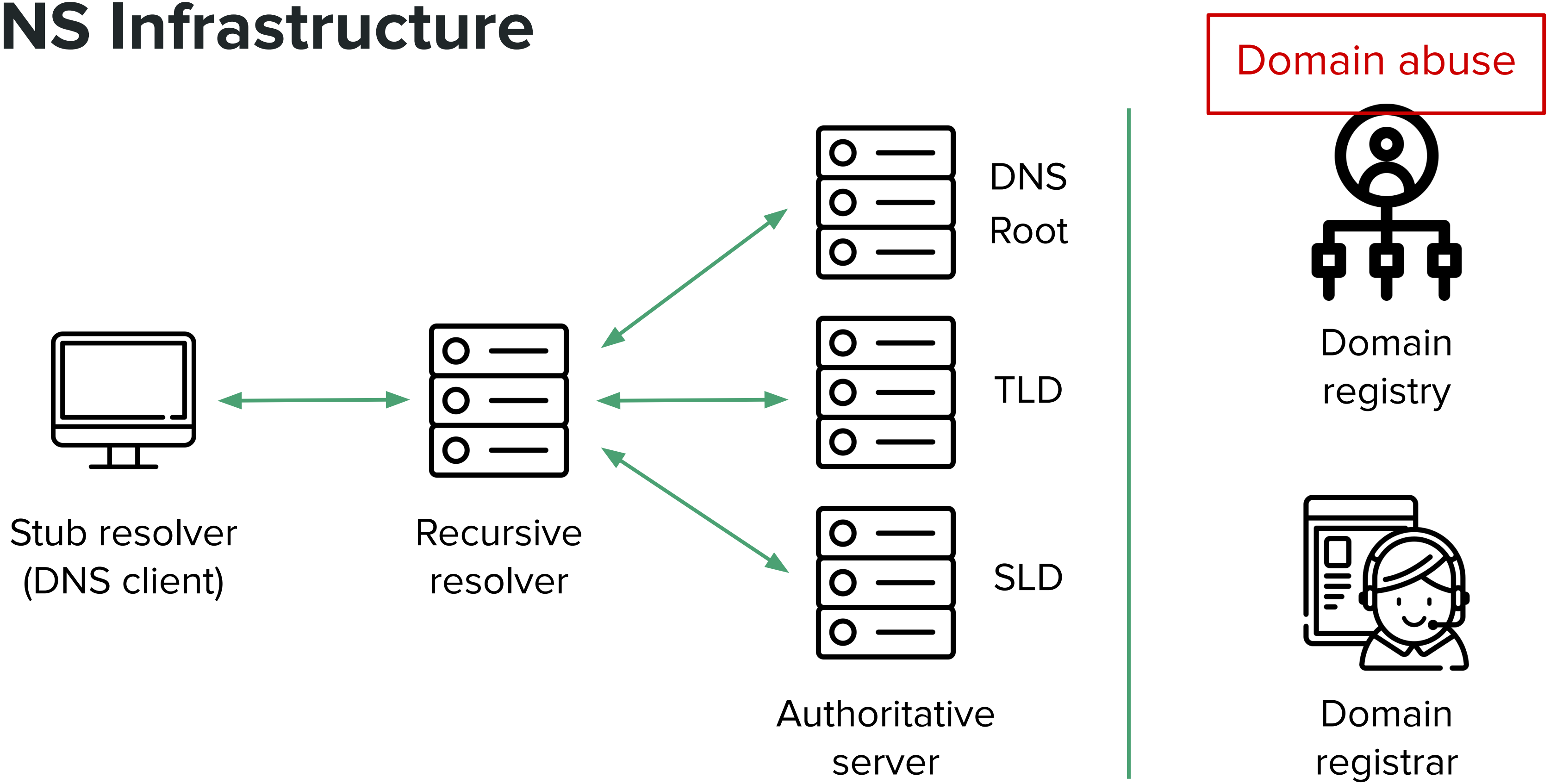
Other vulnerable services except for WPAD

Exposed service functionality	Exposed service name	Potential security implications
Proxy/tunnel config.	wpad① (N), isatap② (N), proxy② (N)	MitM attack
Time config.	ntp③	Time shifting attack
Software activation	vlmcs② (N)	DoS
Directory service (help a client locate a server of the requested service)	ns*① (N), alt*① (N), lb① (N), db① (N), dns-sd①, dr① (N), tracker② (N), dns-llq⑤, dns-update⑤	Server spoofing, service info. leakage
Web service	www*① (N), api① (N), static① (N), cf① (N), share① (N), http②, https③	Web-based phishing attack, malicious script execution

E. Name Collision - Recommendations

Level	Remediation strategy	Effectiveness	Deploy #
New gTLD registry	Scrutinize the registration of the union set of highly-vulnerable domains	97.4%	494
Victim AS	Filter the intersection set of highly-vulnerable domains	36.4%	11305
	Filter AS-specific highly-vulnerable domains	97.4%	
	Filter responses w/ public IP	Not evaluated	
End user	Disable WPAD service (if not used in internal networks)	Not evaluated	> 6.6 million
	Update OS, no hardcoding	~100.0% (in theory)	
	Filter device-level leaks		

DNS Infrastructure



F. Domain Abuse

F. Domain Abuse

What can you do with youtube.com?

Type	Example	Paper
Typosquatting	youtu**eb**.com	[NDSS ’15]
Bitsquatting	youtub**u**.com	[WWW ’13]
Combosquatting	youtube**-videos**.com	[CCS ’17]
Levelsquatting	youtube.com**.youtube-service.com**	[SecureComm ’19]
Homograph attack	y**0**utube.com	[USENIX ’06] [DSN ’18]

F. Domain Abuse - Typosquatting

youtube.com -> youtu**eb**.com

Seven Months' Worth of Mistakes:
A Longitudinal Study of Typosquatting Abuse

Pieter Agten*, Wouter Joosen*, Frank Piessens* and Nick Nikiforakis†
* iMinds-DistriNet, KU Leuven,
{firstname}.{lastname}@cs.kuleuven.be
† Department of Computer Science, Stony Brook University,
nick@cs.stonybrook.edu

F. Domain Abuse - Typosquatting

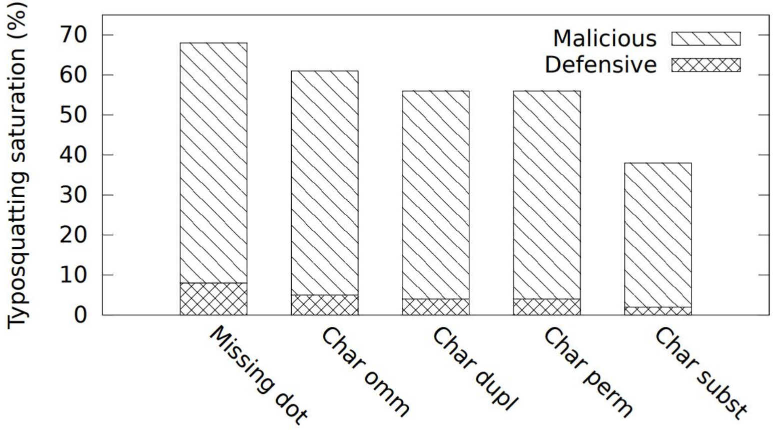
Dataset collection

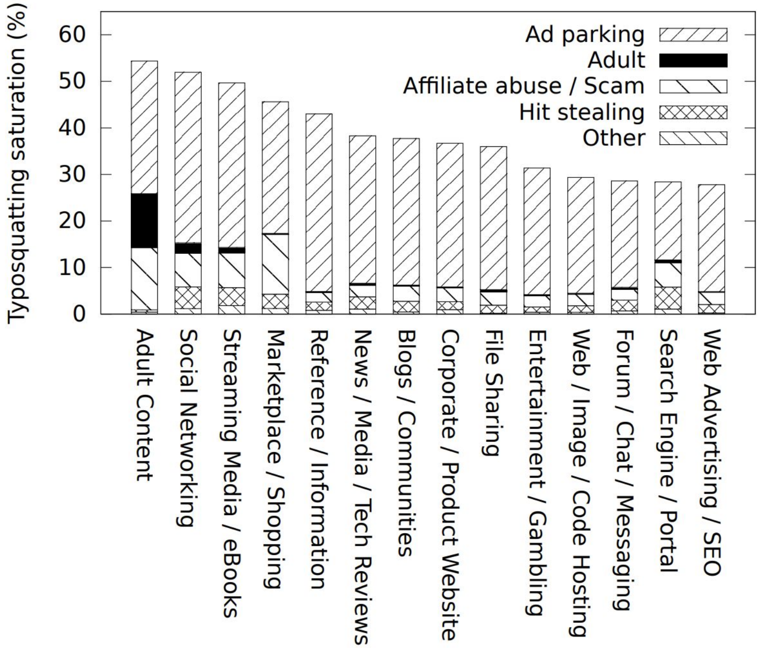
Typosquatting domains

F. Domain Abuse - Typosquatting

Malicious contents are hosting on the domains.

Ad parking	Pages that have no content other than showing advertisements
Adult content	Pages showing adult/pornographic content
Affiliate abuse	Pages taking advantage of an affiliate program offered by ano
For sale	Pages that have no content other than being advertised as for
Hit stealing	Pages redirecting to a legitimate domain without abusing an a
Scam	Pages persuading the user to enter personal information or to





F. Domain Abuse - Bitsquatting

youtube.com -> youtub**u**.com

Bitsquatting: Exploiting Bit-flips for Fun, or Profit?

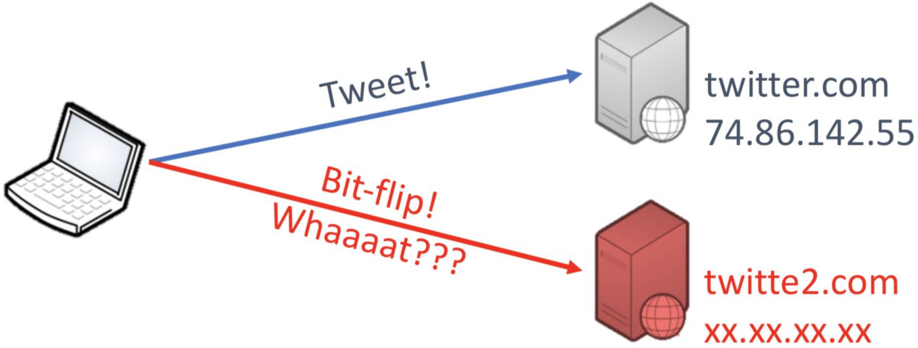
Nick Nikiforakis, Steven Van Acker, Wannes Meert[†], Lieven Desmet, Frank Piessens, Wouter Joosen

iMinds-DistriNet / [†]DTAI, KU Leuven, 3001 Leuven, Belgium
firstname.lastname@cs.kuleuven.be

F. Domain Abuse - Bitsquatting

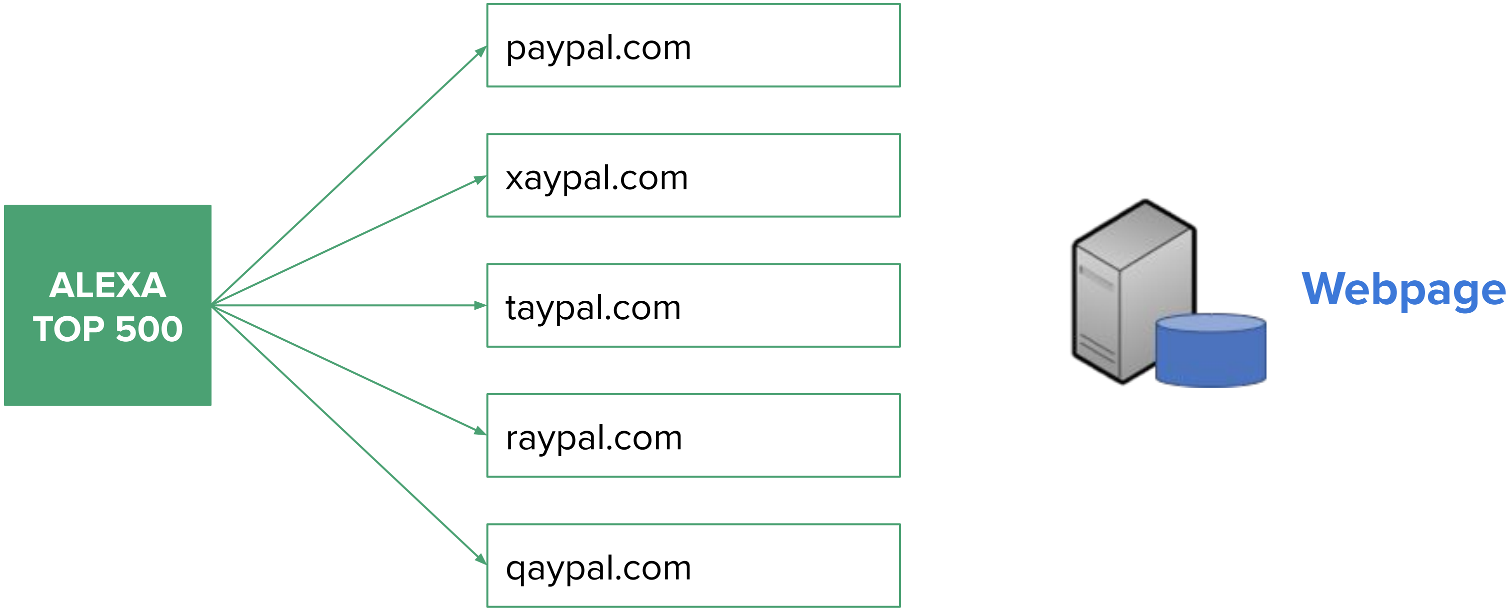
youtube.com -> youtub**u**.com

- Bitsquatting
  - Caused by random bit-flip errors.
  - 1 of every $10^7 – 10^8$ DNS resolutions suffers from an error.



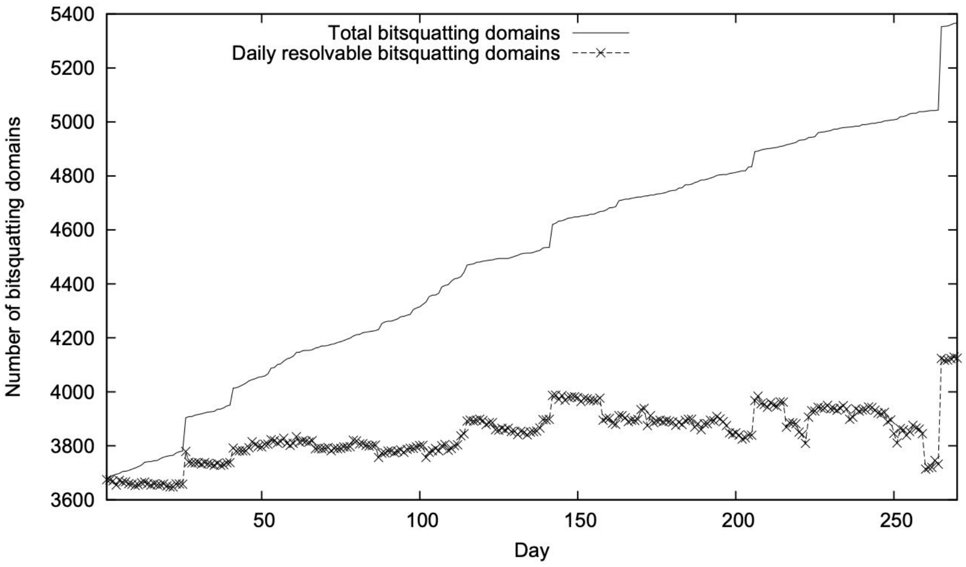
F. Domain Abuse - Bitsquatting

Dataset collection



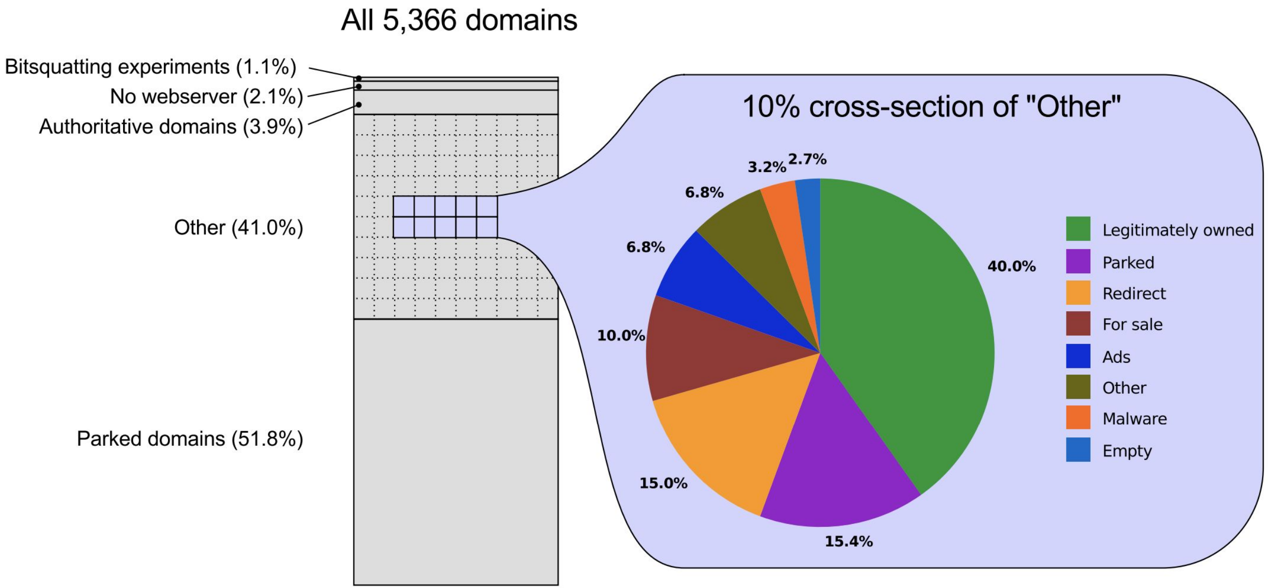
Bitsquatting domains

F. Domain Abuse - Bitsquatting



Growing number of bitsquatting domains (5.3K in total)

F. Domain Abuse - Bitsquatting



F. Domain Abuse - Combosquatting

youtube.com -> youtube-**videos**.com

Session C2: World Wide Web of Wickedness CCS'17, October 30-November 3, 2017, Dallas, TX, USA

Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse

Panagiotis Kintis
Georgia Institute of Technology
kintis@gatech.edu

Najmeh Miramirkhani
Stony Brook University
nmiramirkhani@cs.stonybrook.edu

Charles Lever
Georgia Institute of Technology
chazlever@gatech.edu

Yizheng Chen
Georgia Institute of Technology
yzchen@gatech.edu

Roza Romero-Gómez
Georgia Institute of Technology
rgomez30@gatech.edu

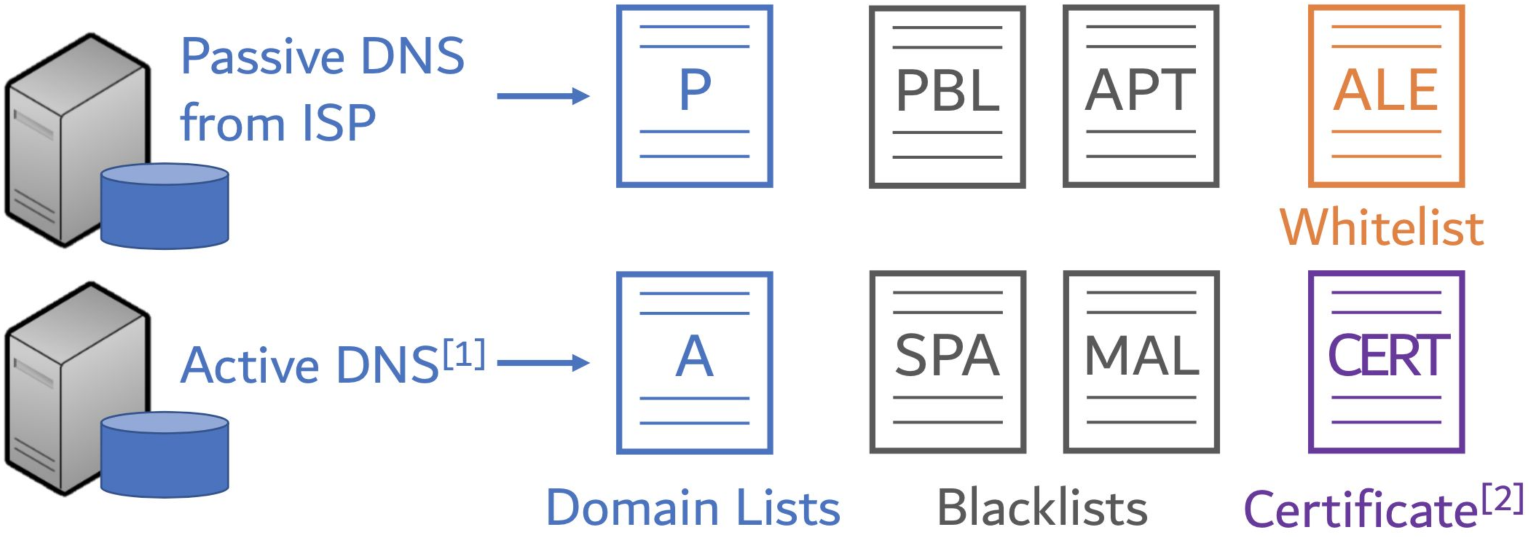
Nikolaos Pitropakis
London South Bank University
pitropan@lsbu.ac.uk

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

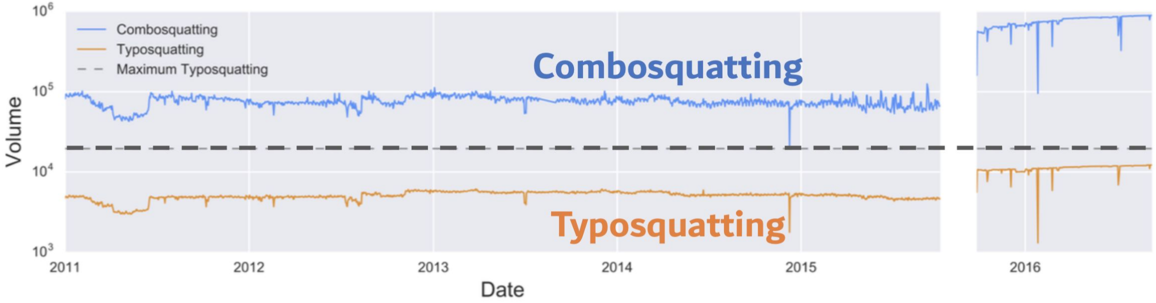
Manos Antonakakis
Georgia Institute of Technology
manos@gatech.edu

F. Domain Abuse - Combosquatting

Dataset collection



F. Domain Abuse - Combosquatting



Combosquatting is way more popular.

2 orders of magnitude more domains.

The domains are already being used in malicious businesses.

Trademark	#Phishing	Example
Facebook	56	facebook123[.]cf
icloud	48	icloudaccountuser[.]com
Amazon	7	secure5-amazon[.]com
Google	8	drivegoogle[.]ga
PayPal	8	paypal-updates[.]ml
Instagram	7	wvwinstagram[.]com
Baidu	4	baidullhk[.]com

F. Domain Abuse - Levelsquatting

youtube.com -> youtube.com.**youtube-service**.com

TL;DR Hazard: A Comprehensive Study of Levelsquatting Scams

Kun Du[1], Hao Yang[1], Zhou Li[2], Haixin Duan[3(✉)], Shuang Hao[4], Baojun Liu[1], Yuxiao Ye[1,5], Mingxuan Liu[1], Xiaodong Su[6], Guang Liu[7], Zhifeng Geng[8], Zaifeng Zhang[9], and Jinjin Liang[9]

F. Domain Abuse - Levelsquatting

F. Domain Abuse - Levelsquatting

No.	Type	Count	Percentage
1	Porn	348,233	42.59%
2	Lottery	281,425	34.42%
3	Phishing	137,388	16.80%
4	Blackhat SEO	40,316	4.93%
5	Malware delivery	2,893	0.35%
6	Others	7,426	0.91%
Total	-	817,681	100%

Fig. 5: Levelsquatting FQDN categories.

No.	Type	Count	Percentage
1	Fake web portal	45,783	33.32%
2	Fake finance	41,322	30.08%
3	Fake advertisement	29,925	21.78%
4	Fake search engine	13,331	9.70%
5	Fake domain Parking	1,937	1.41%
Total	-	132,298	96.30%

Fig. 6: Phishing FQDN sub-categories.

817K levelsquatting domains detected.

Flawed browser implementations found.

Mobile (Resolution: 720x1280)	
Browser Version	**Address Bar**
Firefox 64.0.2	mails.tsinghua.
Chrome 71.0.3578.99	tsinghua.edu.cn.locale.rebornplasticsurgery.com
Opera 49.2.2361	mails.tsinghua.edu.cn.locale.rebornplasticsurgery.com
Safari with WebKit 605.1.15	mails.tsinghua.edu.cn.locale.rebornplasticsur
UCBrowser 12.2.6.1133	清华邮箱 Search

Fig. 9: Address bar of mobile browsers.

F. Domain Abuse - Homograph Attack

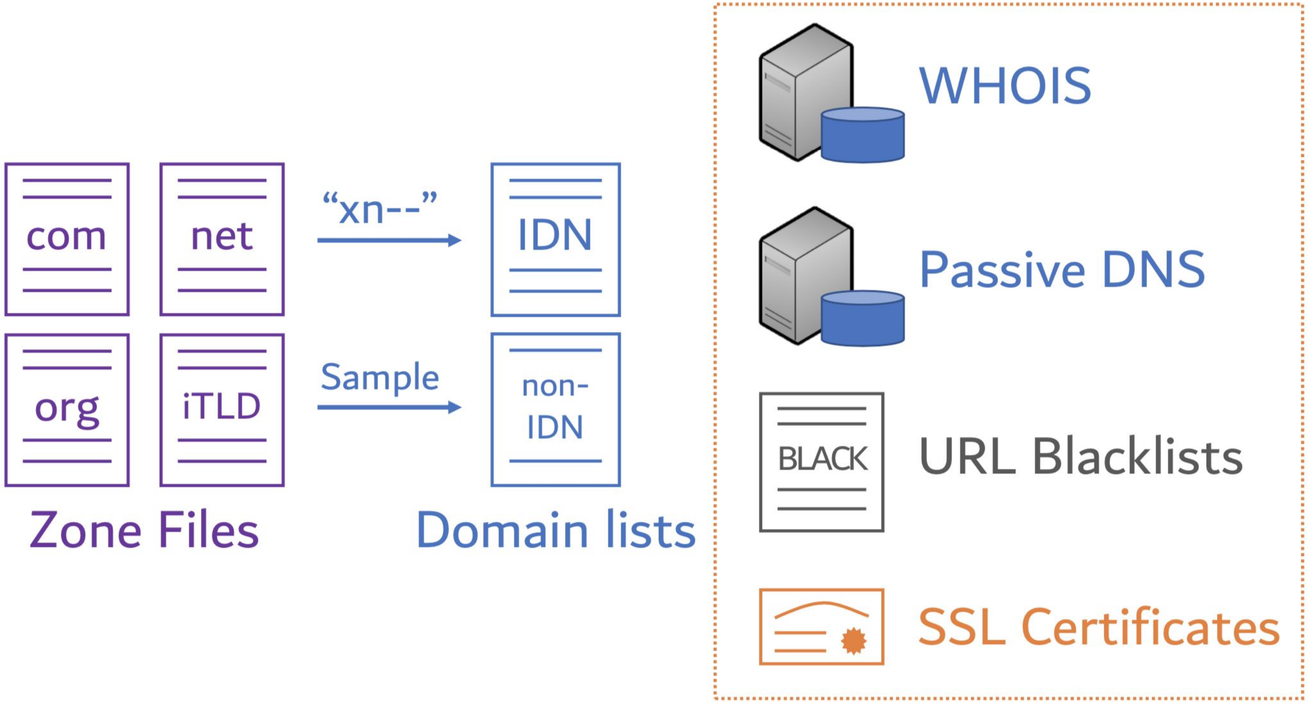
youtube.com -> youtub**ê**.com

> **A Reexamination of Internationalized Domain Names: the Good, the Bad and the Ugly**
>
> Baojun Liu*, Chaoyi Lu*, Zhou Li†, Ying Liu*✉, Haixin Duan*, Shuang Hao‡ and Zaifeng Zhang§
> * Tsinghua University, † IEEE Member, ‡ University of Texas at Dallas, § Netlab of 360

faceboọk.com	faċebook.com	faceḅook.com	faceboôk.com
facebọọk.com	fácebook.com	fâcêbook.com	facebooĸ.com
facebóók.com	fạcẹḅook.com	fącebook.com	facebỏok.com

F. Domain Abuse - Homograph Attack

Dataset collection



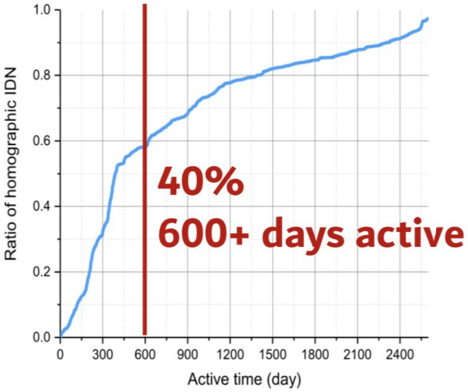
F. Domain Abuse - Homograph Attack

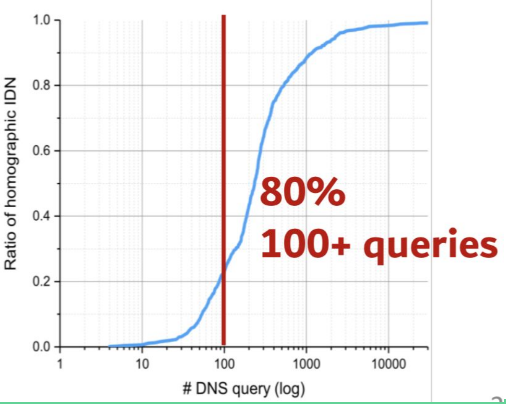
TABLE XIII: Top 10 brand domains ordered by homographic IDNs

Domain	Alexa	# IDN	Rate	Protective Registrations
google.com	1	121	8.0%	19
facebook.com	3	98	6.5%	0
amazon.com	11	55	3.6%	14
icloud.com	372	42	2.8%	0
youtube.com	2	41	2.7%	0
apple.com	55	39	2.6%	0
sex.com	537	36	2.4%	0
go.com	391	29	1.9%	0
ea.com	742	28	1.8%	0
twitter.com	13	25	1.6%	5
Total		**514**	**33.9%**	**38**

1,516 homographic IDNs detected.

The domains are visited very often.





F. Domain Abuse - Homograph Attack

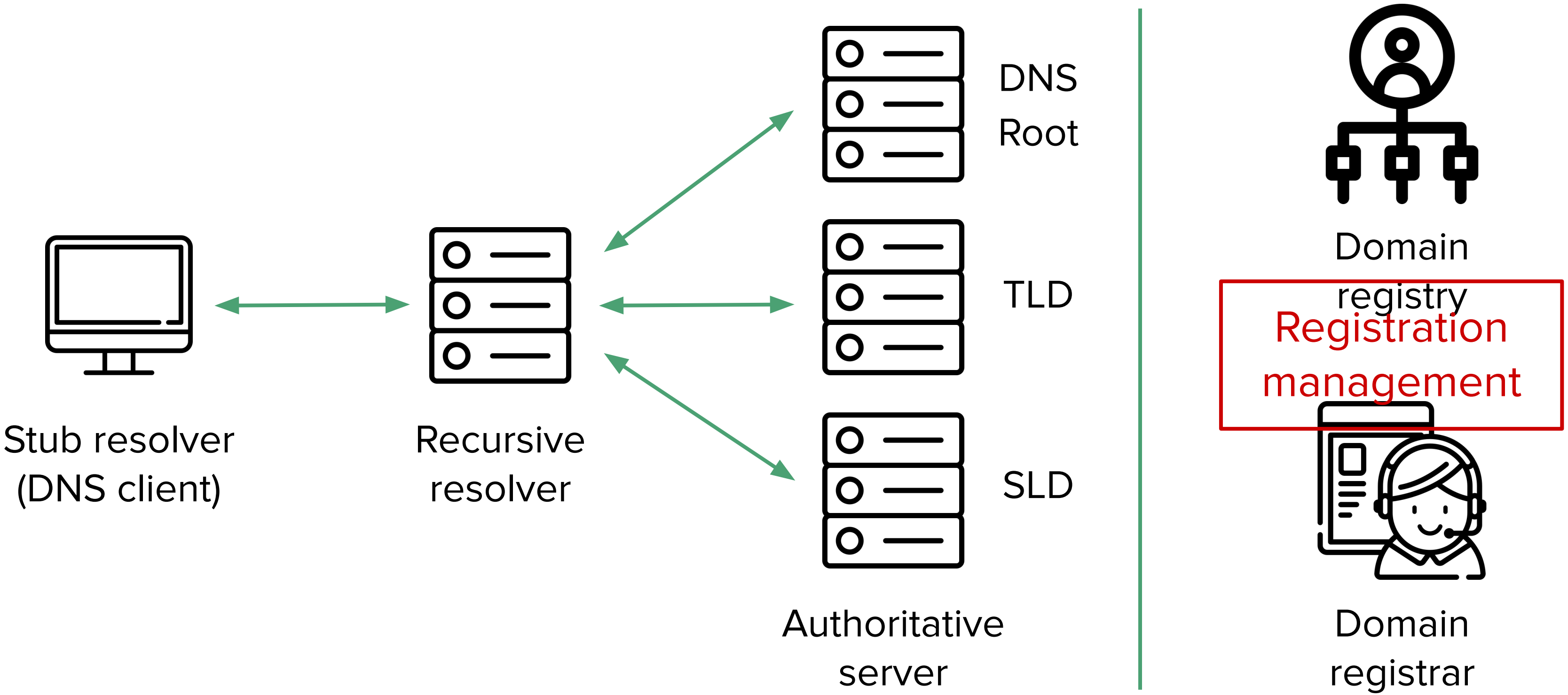
Platform / Browser	PC		
	Ver.	iTLD IDN Supported	Homograph Attack
Chrome	62.0		
Firefox	57.0	Need prefix	Bypassed
Opera	49.0		Bypassed
Safari	11.0		
IE	11.0		
QQ	9.7		
Baidu	8.7		Bypassed
Qihoo 360	9.1		
Sogou	7.1		Vulnerable
Liebao	6.5		Bypassed

Flawed browser display.

F. Domain Abuse - Recommendations

Type	Recommendation
Typosquatting	Registration check; defensive registrations
Bitsquatting	Registration check; use ECC-enabled RAM
Combosquatting	Registration check; stop using combosquatting domains for benign services
Levelsquatting	Registration check; browser fix
Homograph attack	Registration check; browser fix; user education

DNS Infrastructure



F. Domain Registration Management

Risky BIZness: Risks Derived from Registrar Name Management

Gautam Akiwate
UC San Diego
gakiwate@cs.ucsd.edu

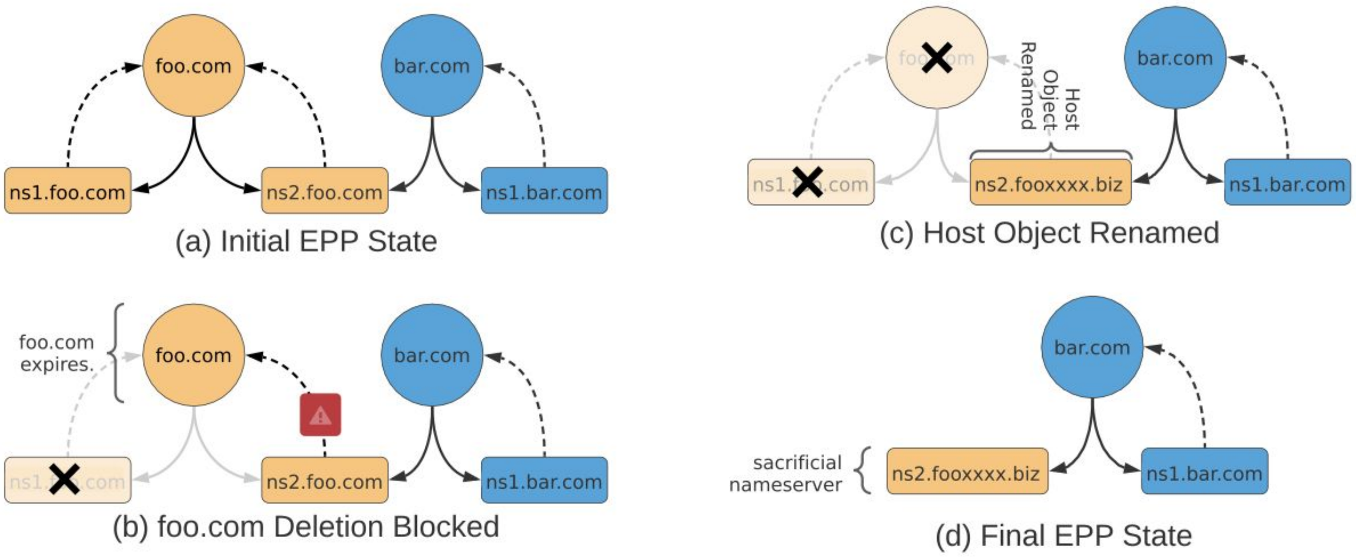
Stefan Savage
UC San Diego
savage@cs.ucsd.edu

Geoffrey M. Voelker
UC San Diego
voelker@cs.ucsd.edu

KC Claffy
CAIDA/UC San Diego
kc@caida.org

F. Domain Registration Management

What's the problem?



F. Domain Registration Management

How many domains might have been hijacked through this?

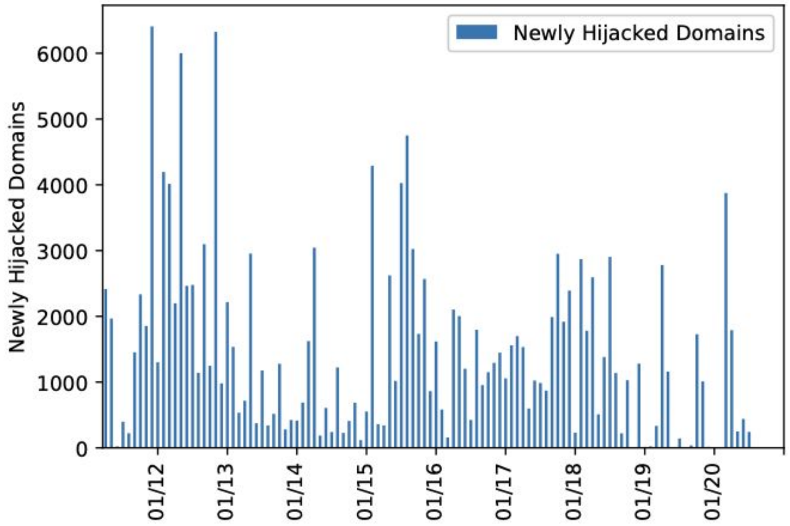


Figure 4: New hijacked domains per month from April 2011 to September 2020.

HAPPY MEASURING!