CAMP: Compositional Amplification Attacks against DNS

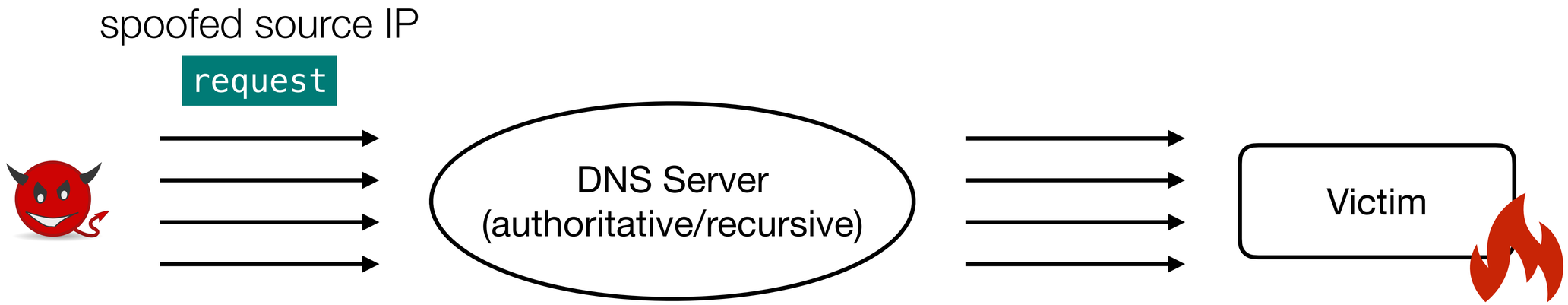
Huayi Duan[1], Marco Bearzi[1], Jodok Vieli[1], David Basin[1],
Adrian Perrig[1], Si Liu[1], and Bernhard Tellenbach[2]

[1]ETH Zürich, [2]Armasuisse

USENIX Security 2024, Philadelphia

Common DNS-related DoS attacks

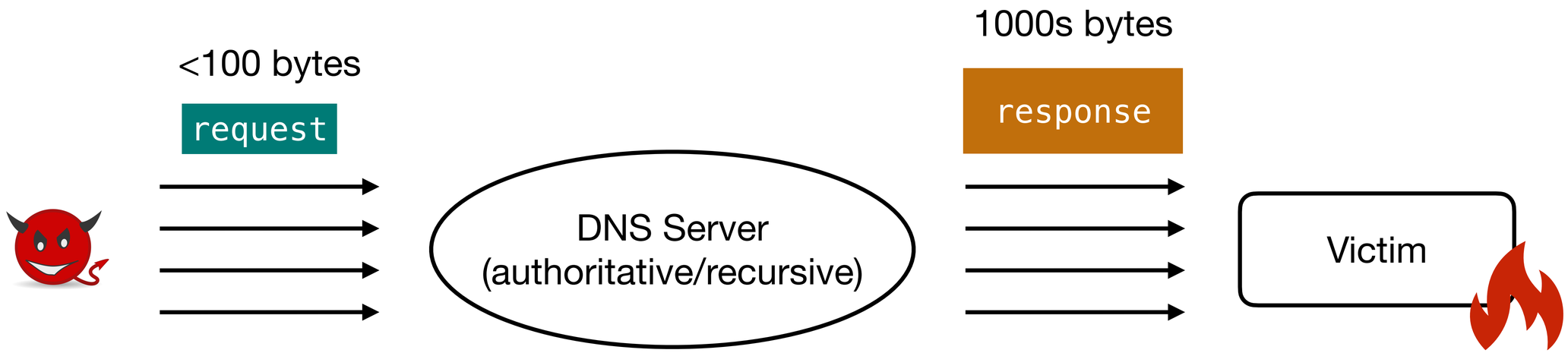
Reflection



Common DNS-related DoS attacks

MAF = 1

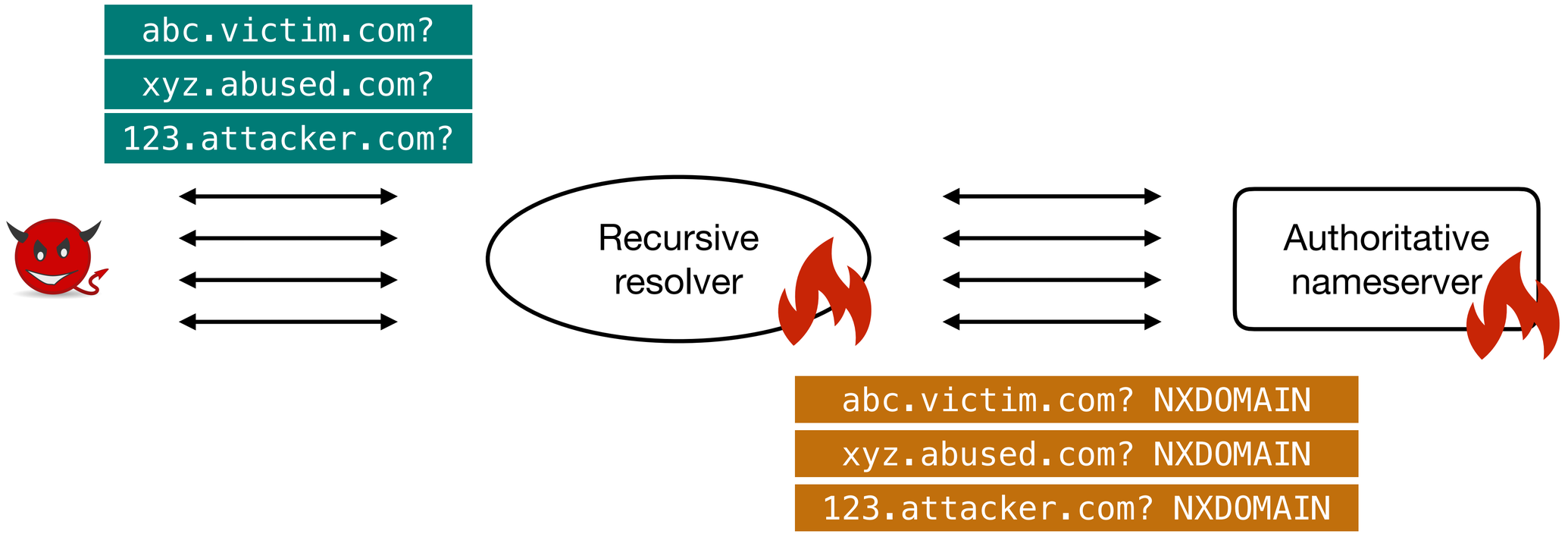
Reflection with ***simple amplification***



Common DNS-related DoS attacks

MAF = 1

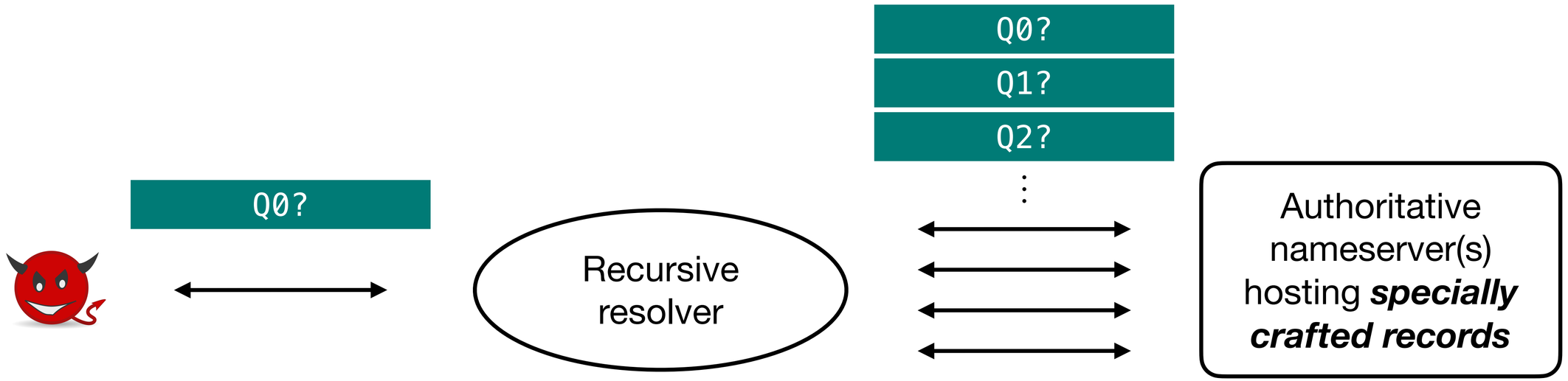
Pseudo-random Subdomain (PRSD) ***without amplification***



Rise of application-layer amplification

MAF > 1

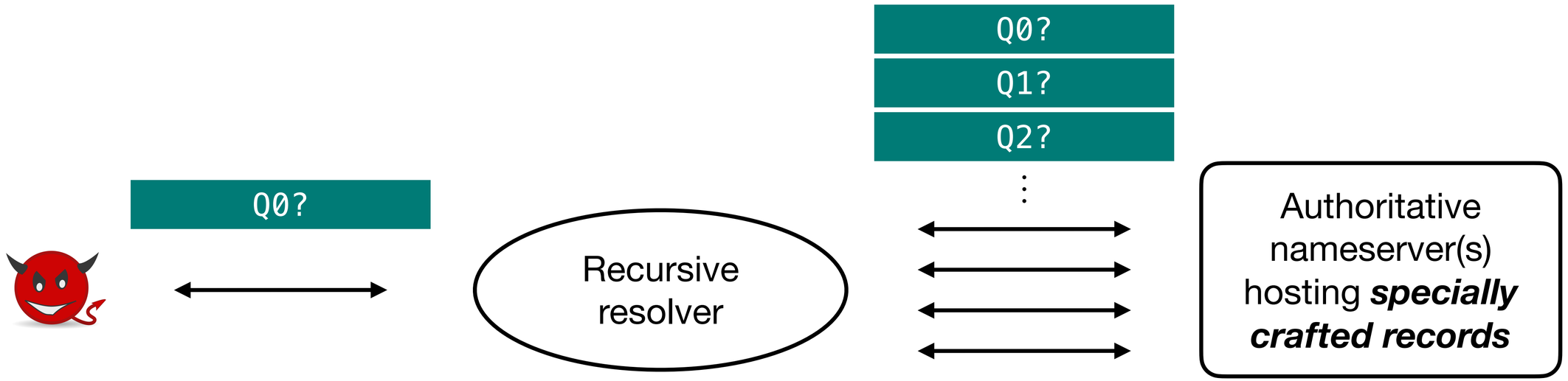
Each ***single client request*** triggers ***excessive resolver queries***



Rise of application-layer amplification

MAF > 1

Each ***single client request*** triggers ***excessive resolver queries***



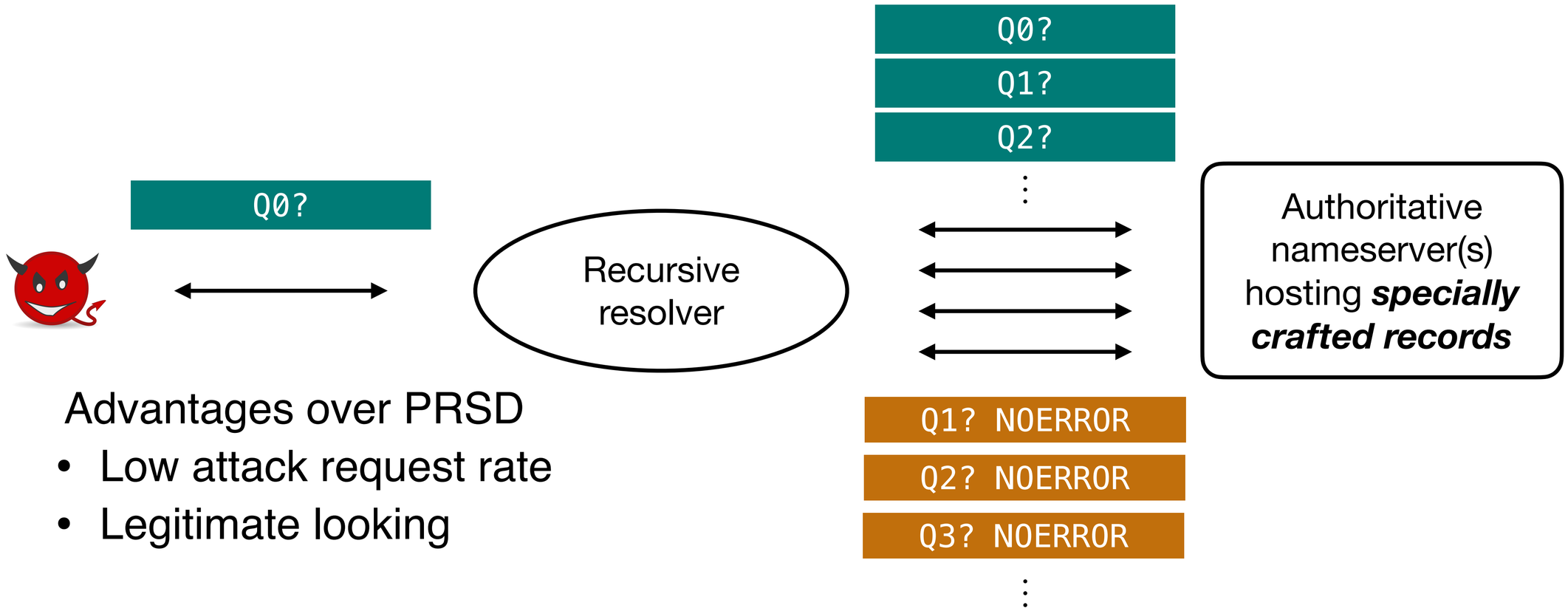
Advantages over PRSD

- Low attack request rate

Rise of application-layer amplification

MAF > 1

Each ***single client request*** triggers ***excessive resolver queries***



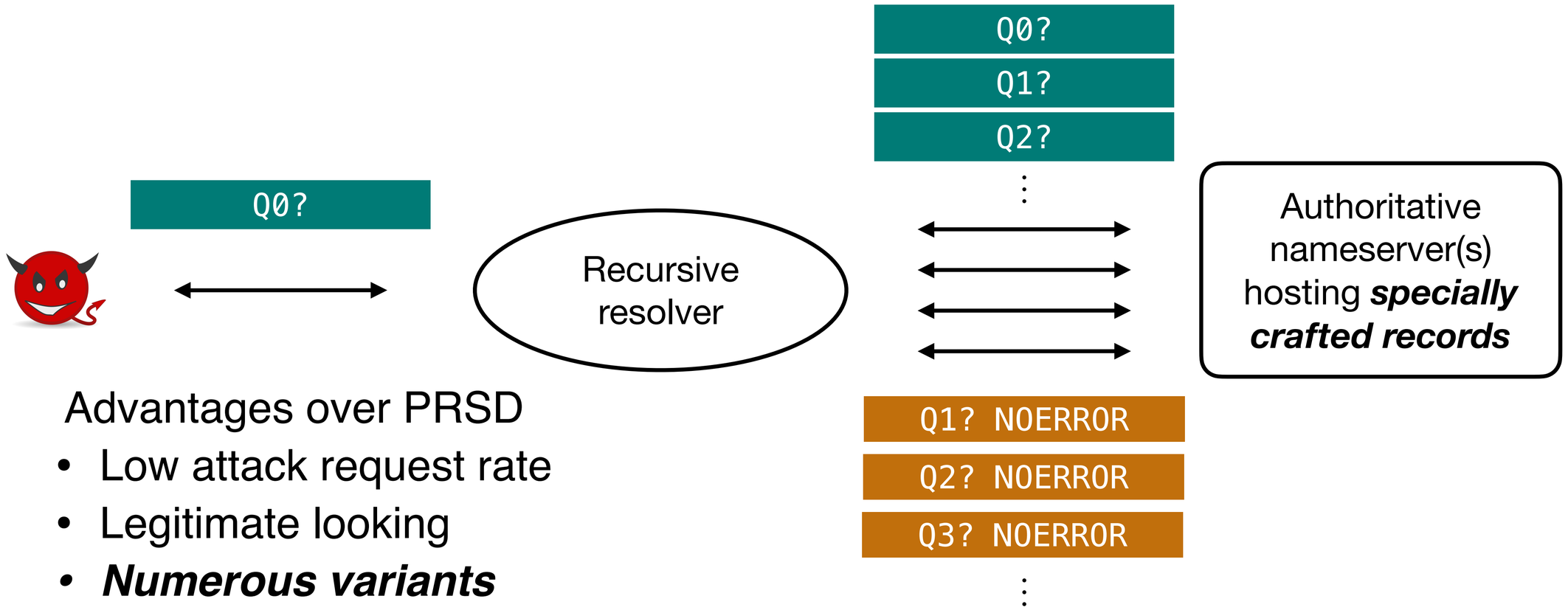
Advantages over PRSD

- Low attack request rate
- Legitimate looking

Rise of application-layer amplification

MAF > 1

Each ***single client request*** triggers ***excessive resolver queries***



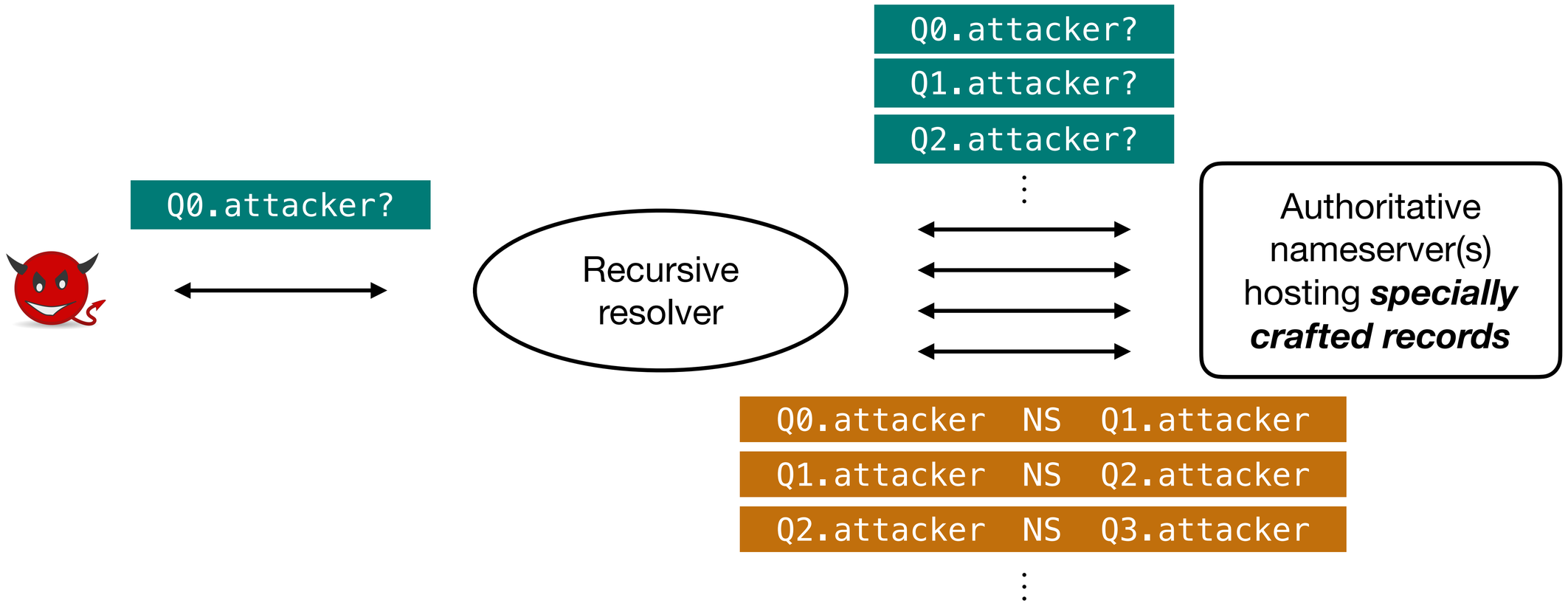
Advantages over PRSD

- Low attack request rate
- Legitimate looking
- ***Numerous variants***

Rise of application-layer amplification

MAF = #NS recursions

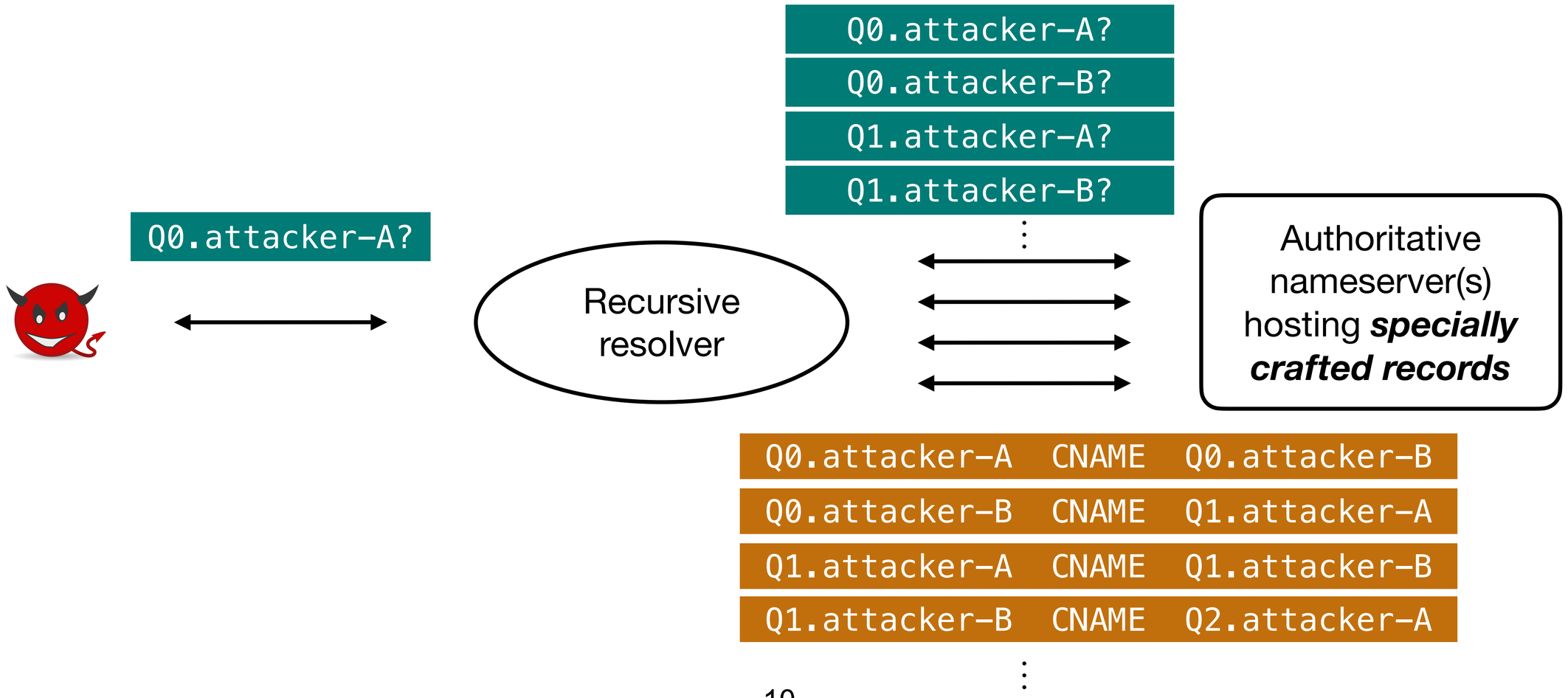
iDNS attack (Maury, 2015): “indefinitely” delegating nameserver



Rise of application-layer amplification

MAF = #Qry rewrites

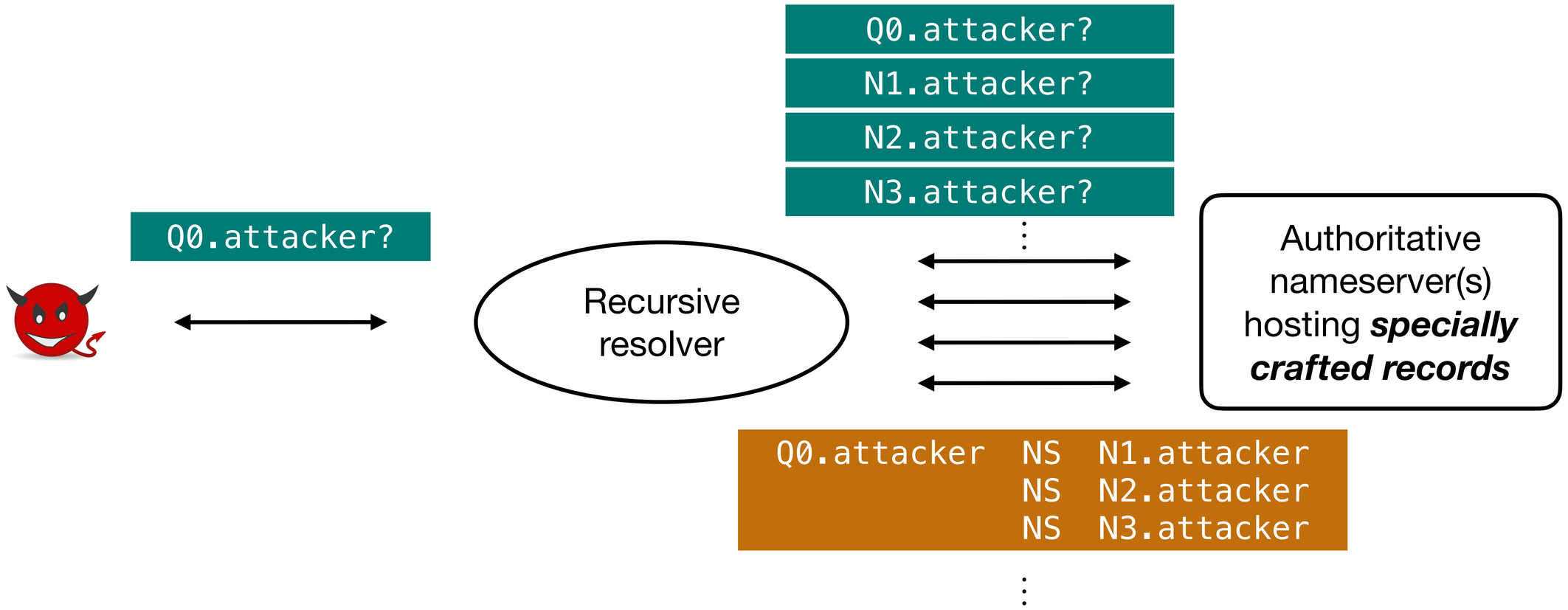
Unchained attack (Bushart and Rossow, 2018): CNAME chain chasing



Rise of application-layer amplification

MAF = #NS fetches

NXNSAttack (Afek et al., 2020): proactive and parallel NS fetching



Rise of application-layer amplification

Questions:

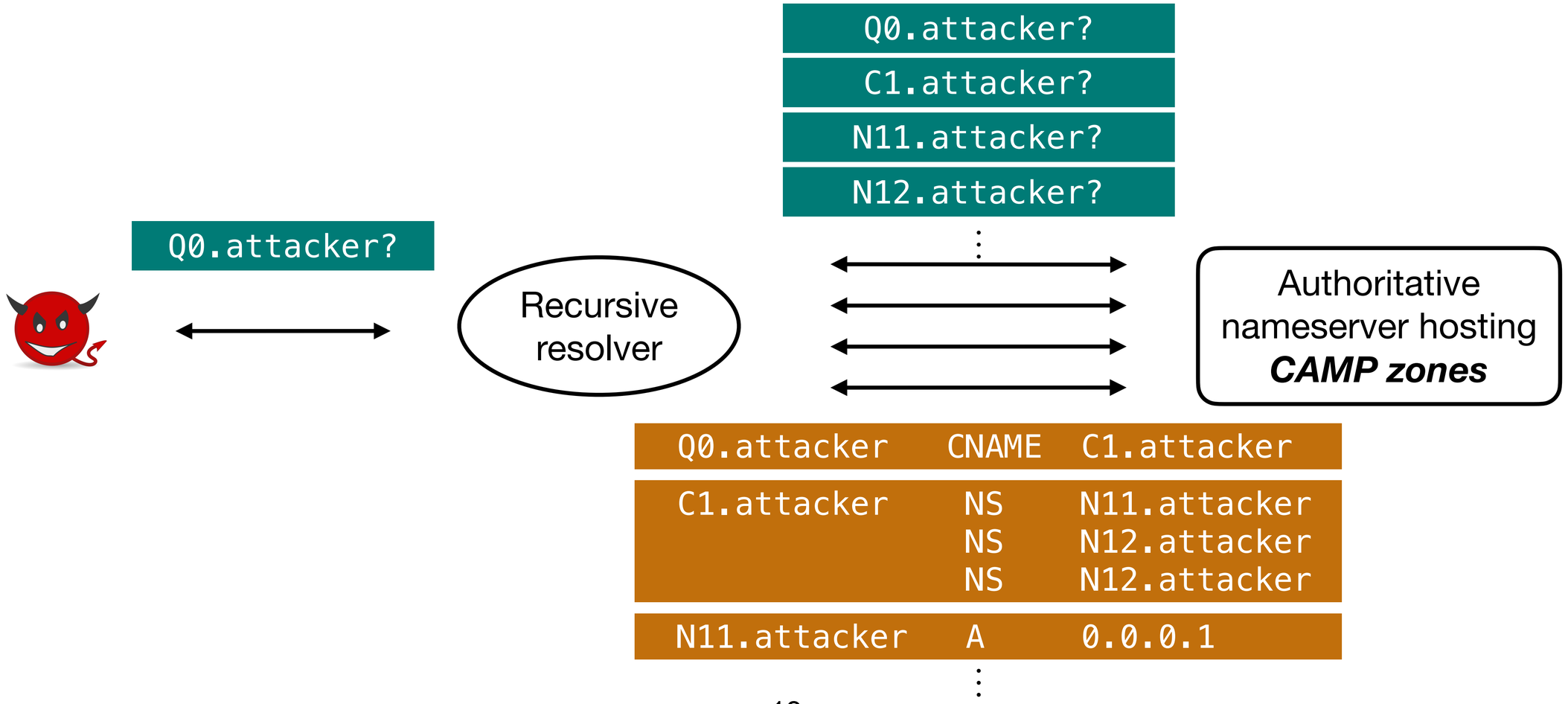
How many more such vulnerabilities are out there?

What is the maximum achievable MAF?

CAMP: compositional amplification attacks

MAF = X*Y

Compose ***amplification primitives*** to produce ***multiplicative effects***

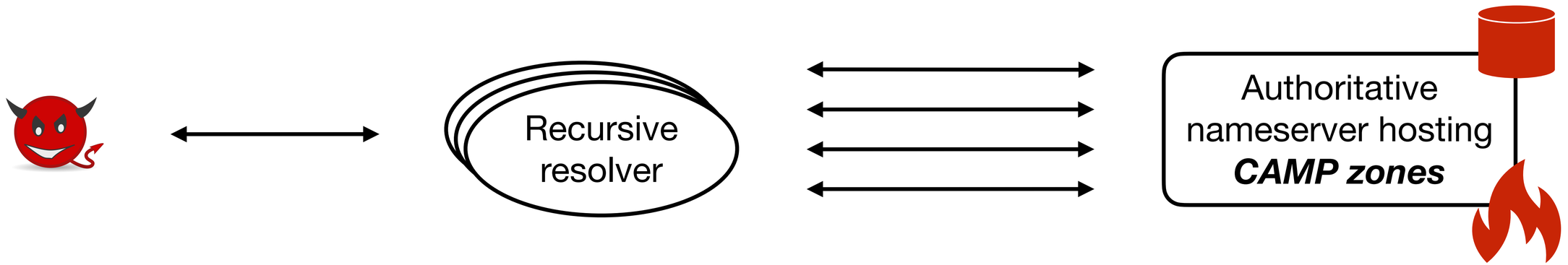


CAMP: compositional amplification attacks

MAF = X*Y

Possible target: nameserver where attacker can set up CAMP zones

Likely victim: public DNS hosting services

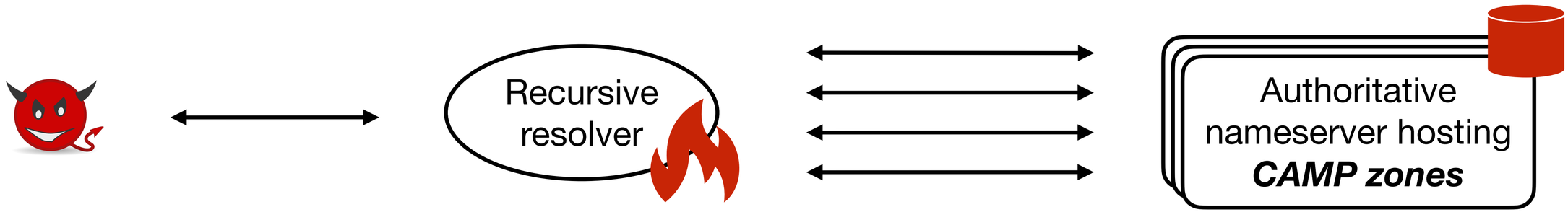


CAMP: compositional amplification attacks

MAF = X*Y

Possible target: resolver accessible to attacker

Major impact on cache-missing requests from normal clients

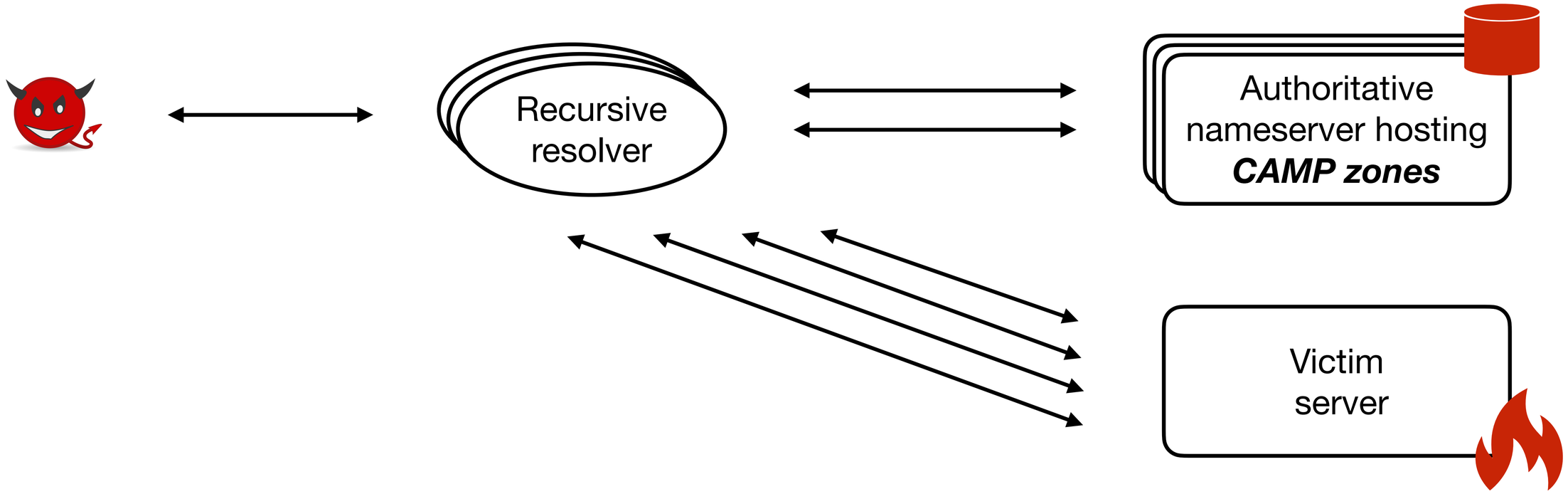


CAMP: compositional amplification attacks

MAF = X*Y

Possible target: arbitrary nameserver

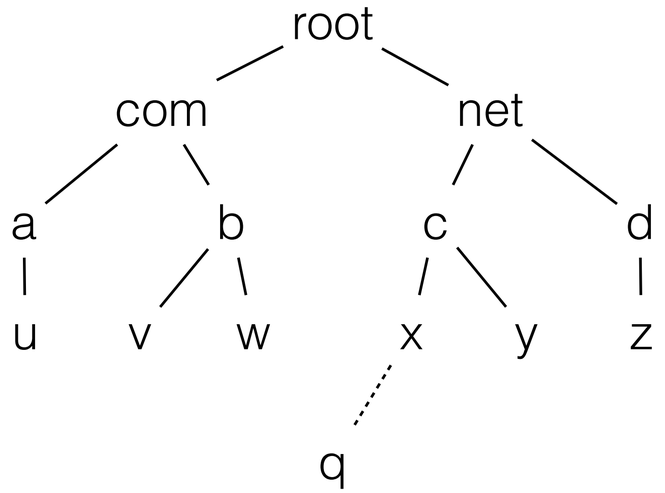
Let NS records in fanout primitives (see later) point to the victim



Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***



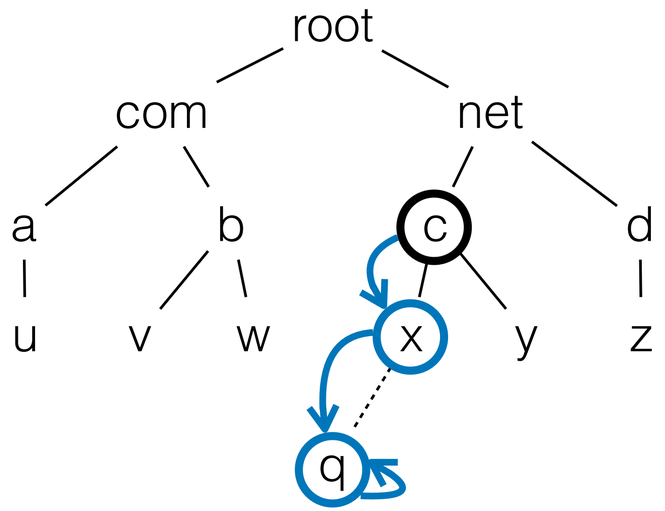
Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

All names on the
same path of DNS hierarchy

Self-probing



Taxonomy of amplification primitives

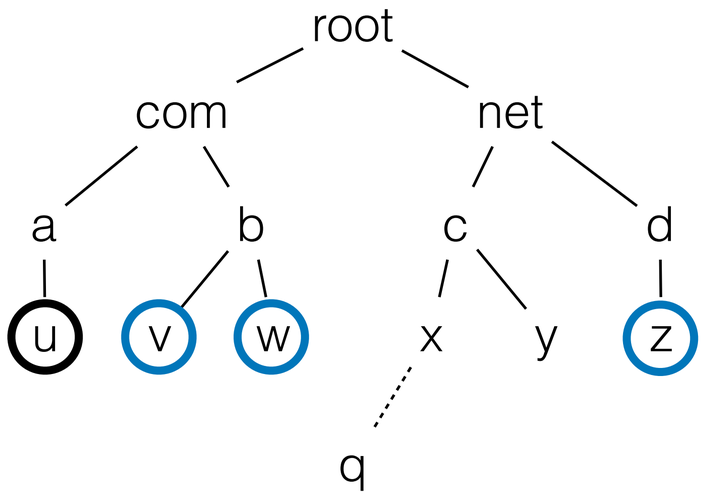
Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

All names on the same path of DNS hierarchy

Self-probing

No pair of names on the same path



Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

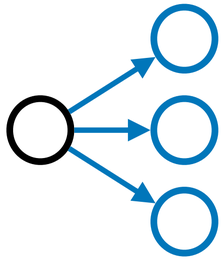
All names on the same path of DNS hierarchy

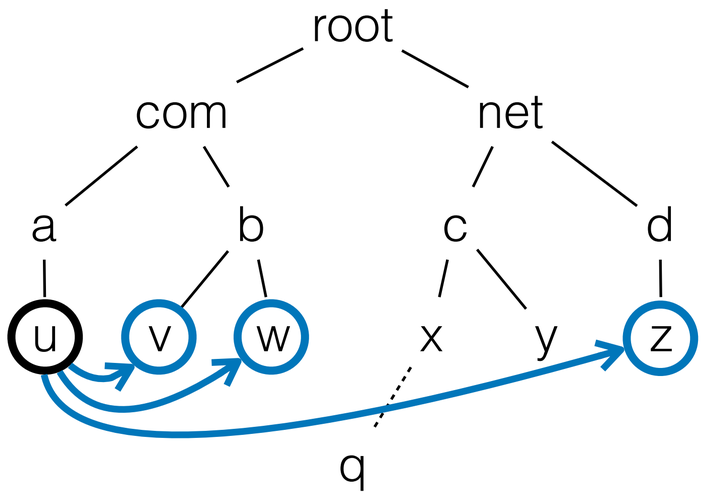
Self-probing

No pair of names on the same path

All derivatives are independently queryable

Fanout





Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

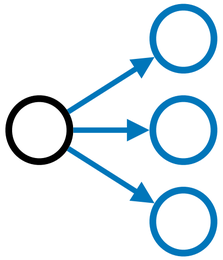
All names on the same path of DNS hierarchy

Self-probing

No pair of names on the same path

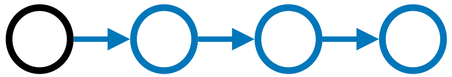
All derivatives are independently queryable

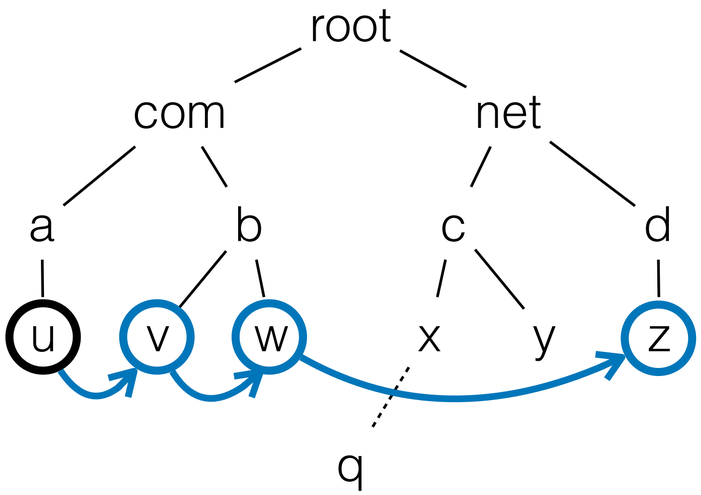
Fanout



Every derivative depends uniquely on another (or the base)

Chaining





Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

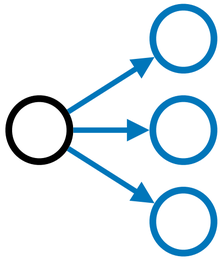
All names on the same path of DNS hierarchy

Self-probing

No pair of names on the same path

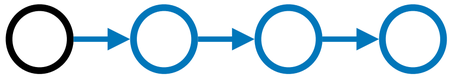
All derivatives are independently queryable

Fanout

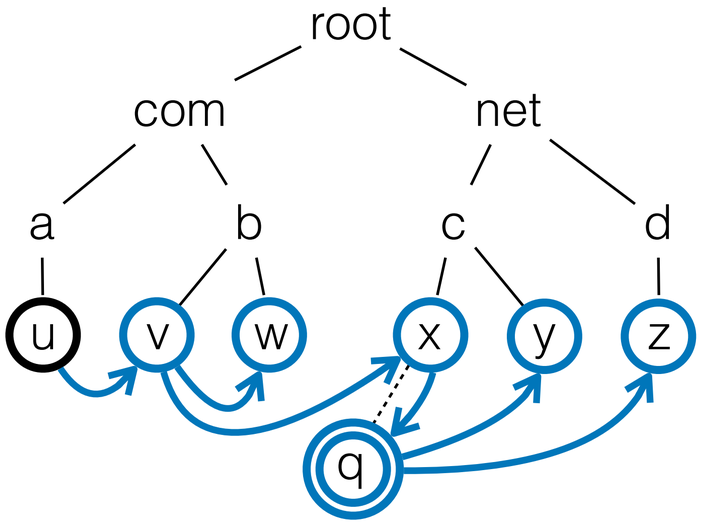


Every derivative depends uniquely on another (or the base)

Chaining



Allow untangling complex resolution!



Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

All names on the same path of DNS hierarchy

Self-probing

Query name minimization (Q.M.)

Dense delegation (D.D.)

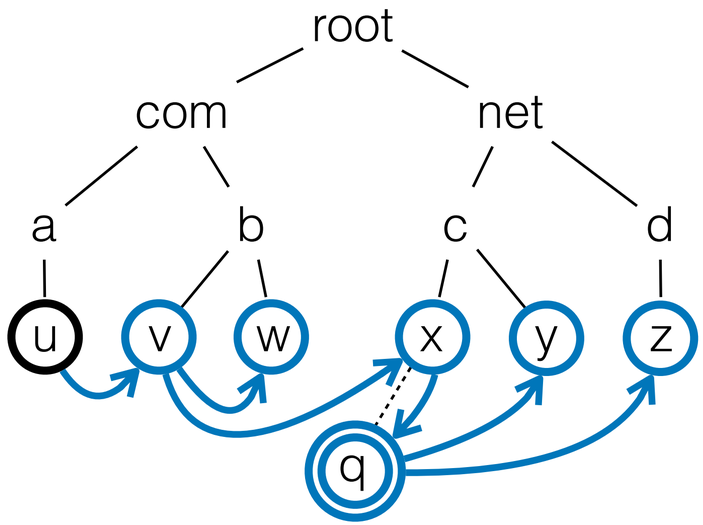
No pair of names on the same path

All derivatives are independently queryable

Fanout

Every derivative depends uniquely on another (or the base)

Chaining



Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

All names on the same path of DNS hierarchy

Self-probing

Query name minimization (Q.M.)

Dense delegation (D.D.)

No pair of names on the same path

All derivatives are independently queryable

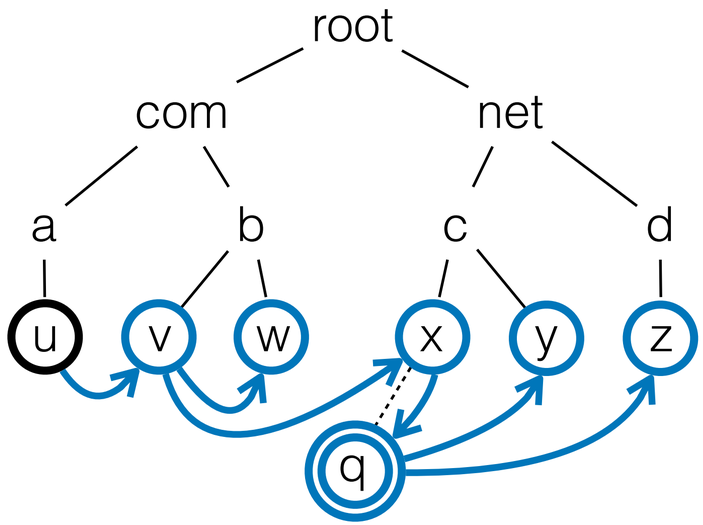
Fanout

Concurrent

Failover (F.O.)

Every derivative depends uniquely on another (or the base)

Chaining



Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

All names on the same path of DNS hierarchy

Self-probing

Query name minimization (Q.M.)

Dense delegation (D.D.)

No pair of names on the same path

All derivatives are independently queryable

Fanout

Concurrent (F.O.)

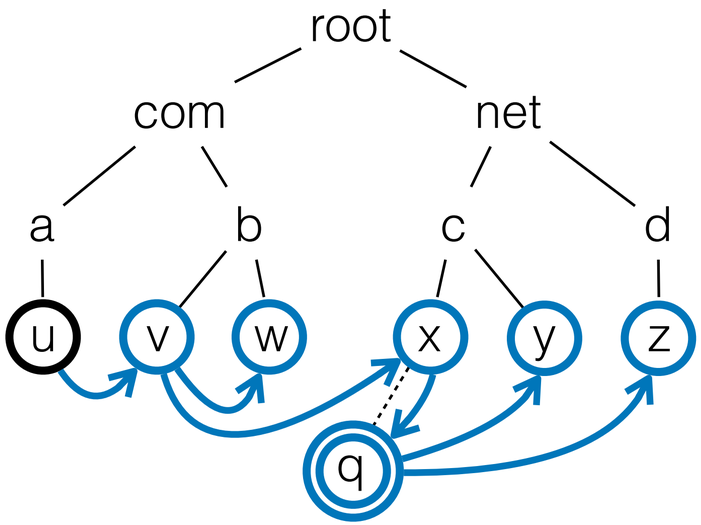
Failover

Every derivative depends uniquely on another (or the base)

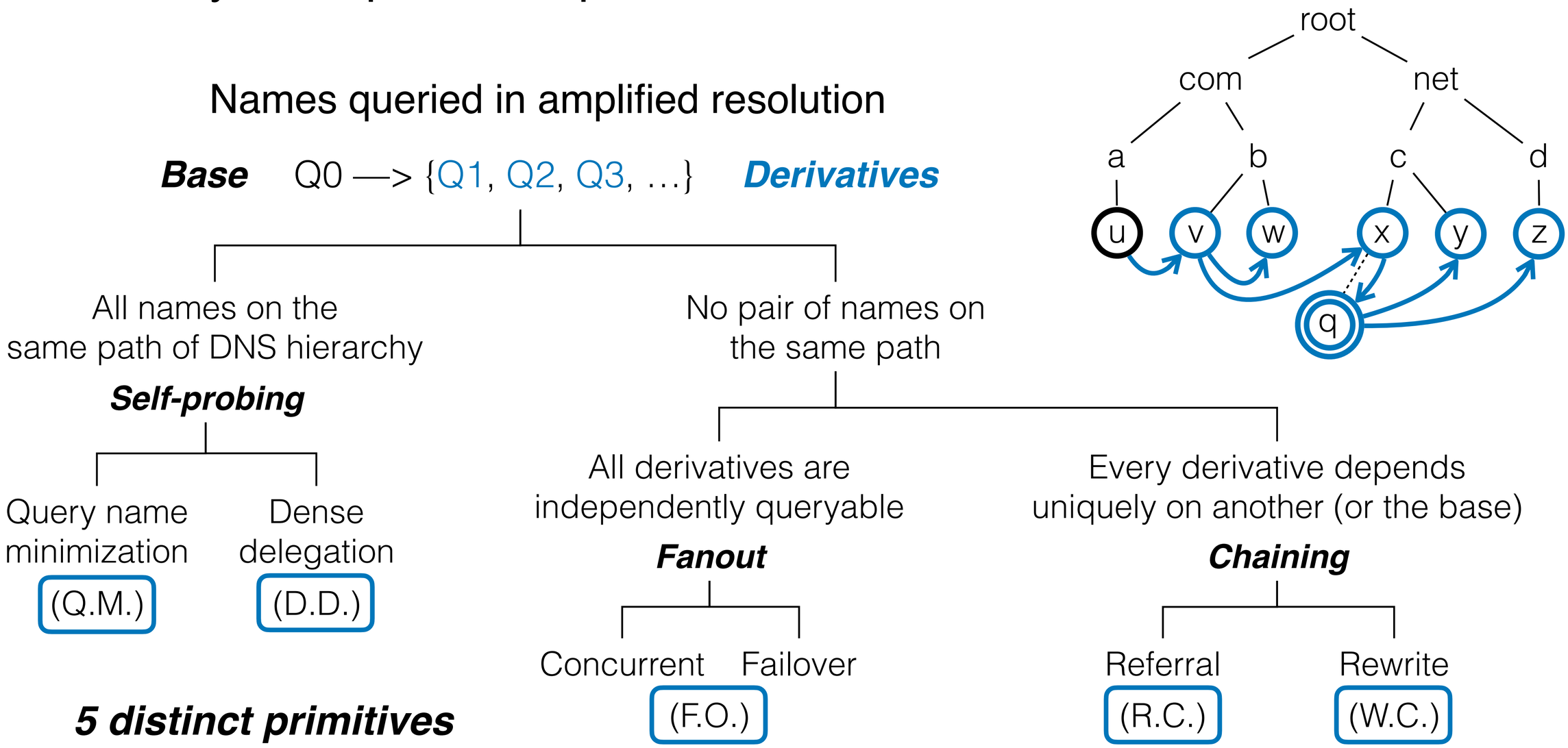
Chaining

Referral (R.C.)

Rewrite (W.C.)



Taxonomy of amplification primitives

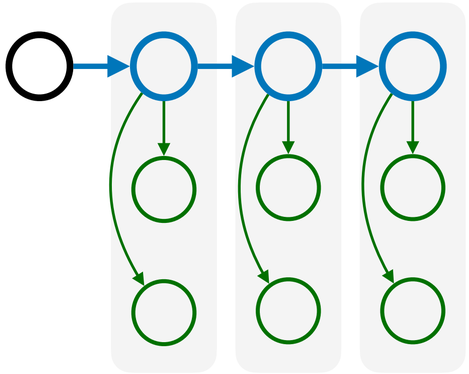


Composability analysis

Observation: one amplification primitive's derivative can be another primitive's base

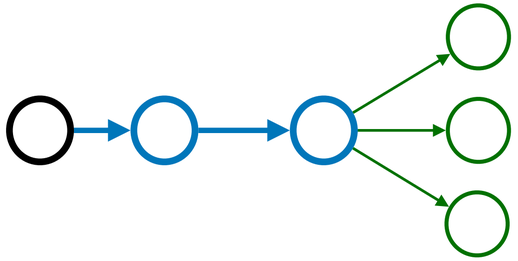
primary ***secondary***

Focus on ***regular multiplicative*** compositions

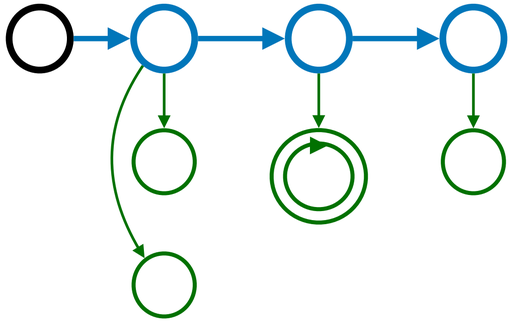


secondaries of same type & size

additive



irregular



Composability analysis

Results: 16 out of 25 conceivable compositions are constructible

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✔	✔	✔	✔	✔
	R.C.	✘	✘	✘	✔	✔
	W.C.	✔	✔	✘	✔	✔
	Q.M.	✘	✘	✘	✘	✘
	D.D.	✔	✔	✔	✔	✔

Composability analysis

Results: 16 out of 25 conceivable compositions are constructible

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✔	✔	✔	✔	✔
	R.C.	✘	✘	✘	✔	✔
	W.C.	✔	✔	✘	✔	✔
	Q.M.	✘	✘	✘	✘	✘
	D.D.	✔	✔	✔	✔	✔

All from ***legitimate DNS features***, only one exception

"The domain name used as the value of an NS record, or part of the value of an MX record ***must not be an alias****."*

RFC2181

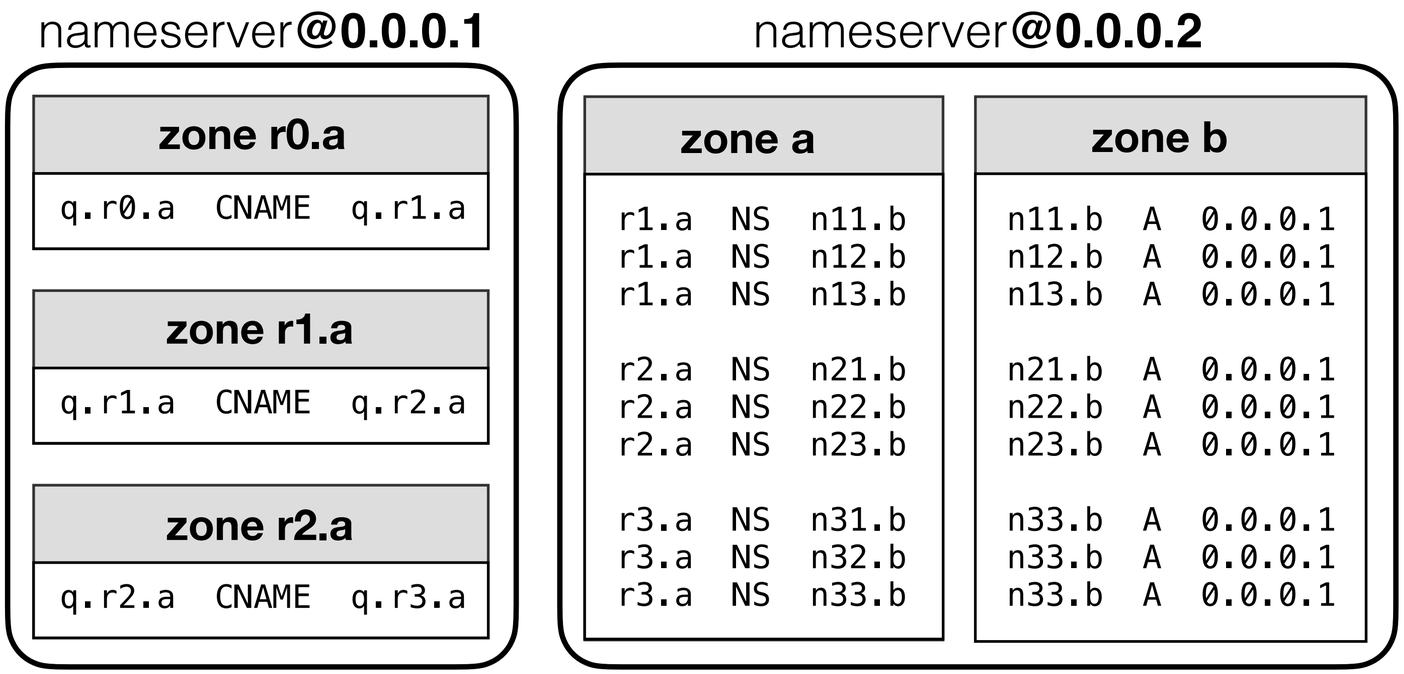
Many implementations are *non-compliant*…

Composability analysis

Static construction with pre-installed zones files

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✔	✔	✔	✔	✔
	R.C.	✘	✘	✘	✔	✔
	W.C.	✔	✔	✘	✔	✔
	Q.M.	✘	✘	✘	✘	✘
	D.D.	✔	✔	✔	✔	✔

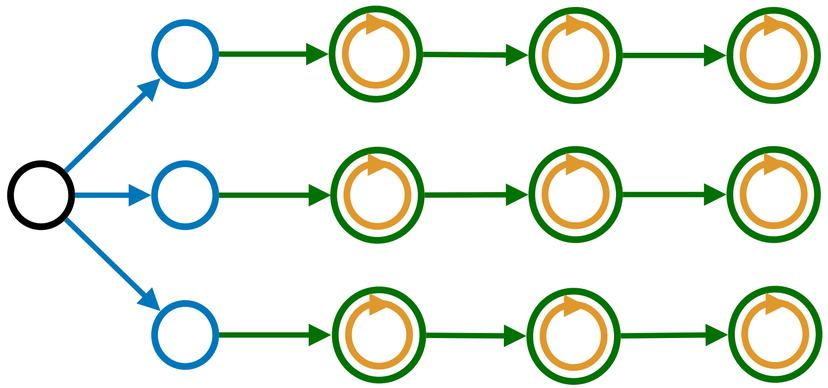
Example: Rewrite Chain X Fanout



Composability analysis

Exponentially many ***multi-dimensional*** (regular or irregular) compositions!

Example: **Fanout** X **Chain** X **Self-probing**



Validation on major DNS implementations

Message amplification factor (MAF)* measured on a controlled local testbed

Primary	F.O.				W.C.			R.C.	D.D.				F.O.	W.C.	D.D.
Secondary	F.O.	R.C.	W.C.	Q.M.	F.O.	R.C.	Q.M.	Q.M.	F.O.	R.C.	W.C.	Q.M.	W.C.	F.O.	W.C.
Tertiary	-	-	-	-	-	-	-	-	-	-	-	-	Q.M.	R.C.	Q.M.
Compo. Index	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
BIND	31	36	21	21	**119**	**136**	82	8	80	50	2	21	26	**731**	2
Unbound	12	17	73	61	28	60	**112**	43	30	67	**241**	**201**	**726**	23	**2400**
PowerDNS	57	57	56	91	24	31	99	98	21	30	53	90	97	11	97

*MAF = #queries received by focal nameserver
<= #queries sent by the amplifying resolver

Resolver Limits	BIND 9.18.4	Unbound 1.16.0	PowerDNS 4.7.3
Concurrent NS queries	5	3	1
Failover NS queries	-	3	9
Total NS queries^	-	6	10
Referral chain length	7	4	15
Rewrite chain length	17	12	12
QMIN iterations	5	10	10
DDLG iterations	>20	>20	>20
Max queries per cli. req.	100	32	60/100

^Resovler queries for IPv6 nameserver disabled

Validation on major DNS implementations

Message amplification factor (MAF)* measured on a controlled local testbed

Primary	F.O.				W.C.			R.C.	D.D.				F.O.	W.C.	D.D.
Secondary	F.O.	R.C.	W.C.	Q.M.	F.O.	R.C.	Q.M.	Q.M.	F.O.	R.C.	W.C.	Q.M.	W.C.	F.O.	W.C.
Tertiary	-	-	-	-	-	-	-	-	-	-	-	-	Q.M.	R.C.	Q.M.
Compo. Index	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
BIND	31	36	21	21	**119**	**136**	82	8	80	50	2	21	26	**731**	2
Unbound	12	17	73	61	28	60	**112**	43	30	67	**241**	**201**	**726**	23	**2400**
PowerDNS	57	57	56	91	24	31	99	98	21	30	53	90	97	11	97

Highlight #1: CAMP can bypass
query limits on individual features

Resolver Limits	BIND 9.18.4	Unbound 1.16.0	PowerDNS 4.7.3
Concurrent NS queries	5	3	1
Failover NS queries	-	3	9
Total NS queries^	-	6	10
Referral chain length	7	4	15
Rewrite chain length	17	12	12
QMIN iterations	5	10	10
DDLG iterations	>20	>20	>20
Max queries per cli. req.	100	32	60/100

*MAF = #queries received by focal nameserver
<= #queries sent by the amplifying resolver

^Resovler queries for IPv6 nameserver disabled

Validation on major DNS implementations

Message amplification factor (MAF)* measured on a controlled local testbed

Primary	F.O.				W.C.			R.C.	D.D.				F.O.	W.C.	D.D.
Secondary	F.O.	R.C.	W.C.	Q.M.	F.O.	R.C.	Q.M.	Q.M.	F.O.	R.C.	W.C.	Q.M.	W.C.	F.O.	W.C.
Tertiary	-	-	-	-	-	-	-	-	-	-	-	-	Q.M.	R.C.	Q.M.
Compo. Index	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
BIND	31	36	21	21	**119**	**136**	82	8	80	50	2	21	26	**731**	2
Unbound	12	17	73	61	28	60	**112**	43	30	67	**241**	**201**	**726**	23	**2400**
PowerDNS	57	57	56	91	24	31	99	98	21	30	53	90	97	11	97

Highlight #2: CAMP can exceed ***global query limit per client request***

Resolver Limits	BIND 9.18.4	Unbound 1.16.0	PowerDNS 4.7.3
Concurrent NS queries	5	3	1
Failover NS queries	-	3	9
Total NS queries^	-	6	10
Referral chain length	7	4	15
Rewrite chain length	17	12	12
QMIN iterations	5	10	10
DDLG iterations	>20	>20	>20
Max queries per cli. req.	100	32	60/100

*MAF = #queries received by focal nameserver
<= #queries sent by the amplifying resolver

^Resovler queries for IPv6 nameserver disabled

Validation on major DNS implementations

Message amplification factor (MAF)* measured on a controlled local testbed

Primary	F.O.				W.C.			R.C.	D.D.				F.O.	W.C.	D.D.
Secondary	F.O.	R.C.	W.C.	Q.M.	F.O.	R.C.	Q.M.	Q.M.	F.O.	R.C.	W.C.	Q.M.	W.C.	F.O.	W.C.
Tertiary	-	-	-	-	-	-	-	-	-	-	-	-	Q.M.	R.C.	Q.M.
Compo. Index	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
BIND	31	36	21	21	**119**	**136**	82	8	80	50	2	21	26	**731**	2
Unbound	12	17	73	61	28	60	**112**	43	30	67	**241**	**201**	**726**	23	**2400**
PowerDNS	57	57	56	91	24	31	99	98	21	30	53	90	97	11	97

Highlight #3: CAMP can ***grow exponentially in #dimensions***

Resolver Limits	BIND 9.18.4	Unbound 1.16.0	PowerDNS 4.7.3
Concurrent NS queries	5	3	1
Failover NS queries	-	3	9
Total NS queries^	-	6	10
Referral chain length	7	4	15
Rewrite chain length	17	12	12
QMIN iterations	5	10	10
DDLG iterations	>20	>20	>20
Max queries per cli. req.	100	32	60/100

*MAF = #queries received by focal nameserver
<= #queries sent by the amplifying resolver

^Resovler queries for IPv6 nameserver disabled

Concluding remarks

First systematic study of application-layer amplification intrinsic to DNS

Analysis framework can incorporate new features, e.g., SVCB record

CAMP can explore the full amplification potential of a resolver

100—1000s of MAFs on real-world resolvers

Amplification can be upper-bounded but not eliminated

Mitigation at protocol-, impl-, and operation-level

Disclosure status

Initially to BIND, Unbound, and PowerDNS, patched with better query limiting

To international DNS entities via Swiss National Cyber Security Centre NCSC

Thank you!
Questions?

Contact: huayi.duan@inf.ethz.ch