ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

TECHNISCHE
UNIVERSITÄT
DARMSTADT

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

ValidaTor: Domain Validation Over Tor

Jens Frieß | Haya Schulmann | Michael Waidner

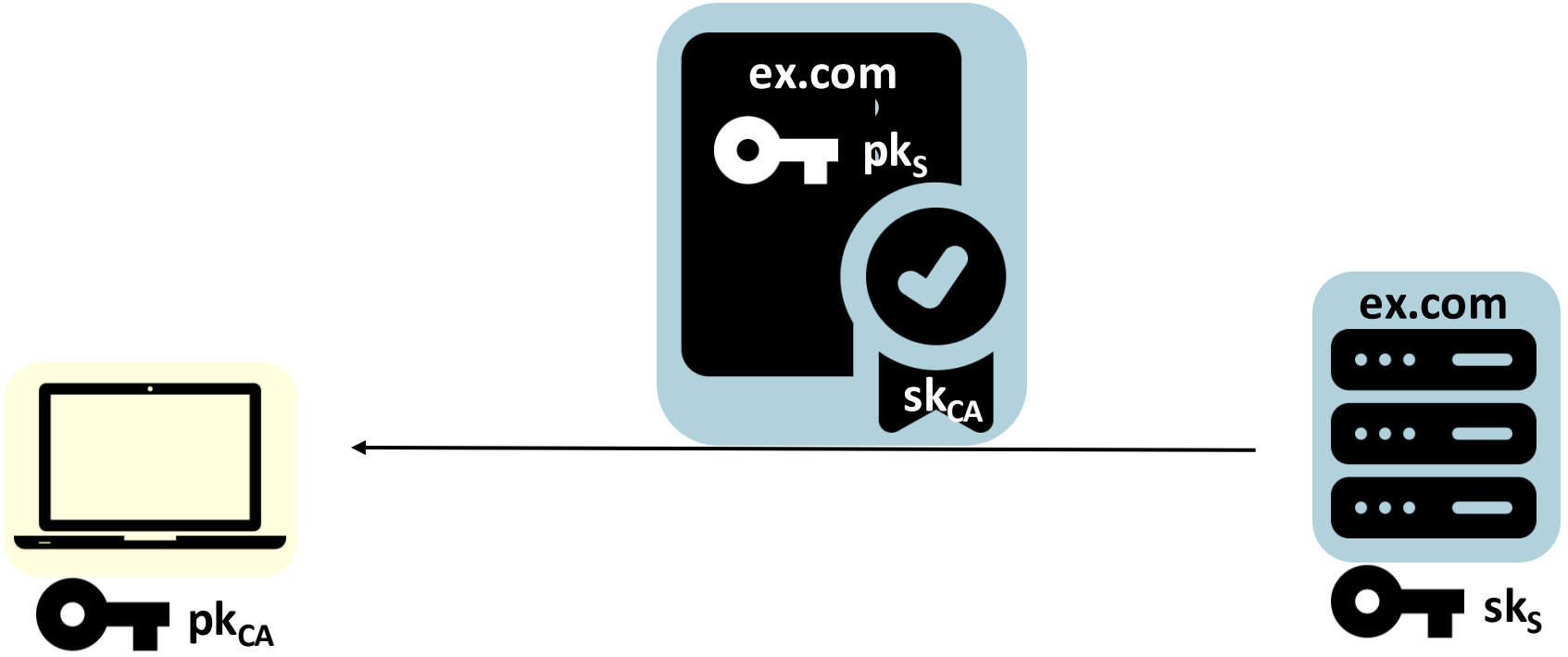
ATHENE | Technische Universität Darmstadt | Goethe-Universität Frankfurt a.M.

NSDI'25
Philadelphia, April 2025

TLS, PKI, Certificates, ...

Public key in TLS certificate used to authenticate server in TLS handshake

TLS, PKI, Certificates, ...

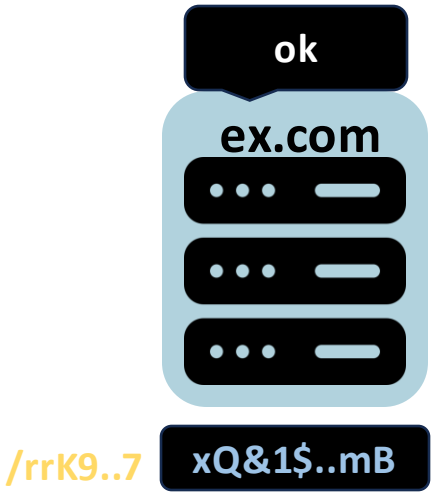


TLS certificate signed by trusted 3rd party: Certificate Authority (CA)

Domain Validation

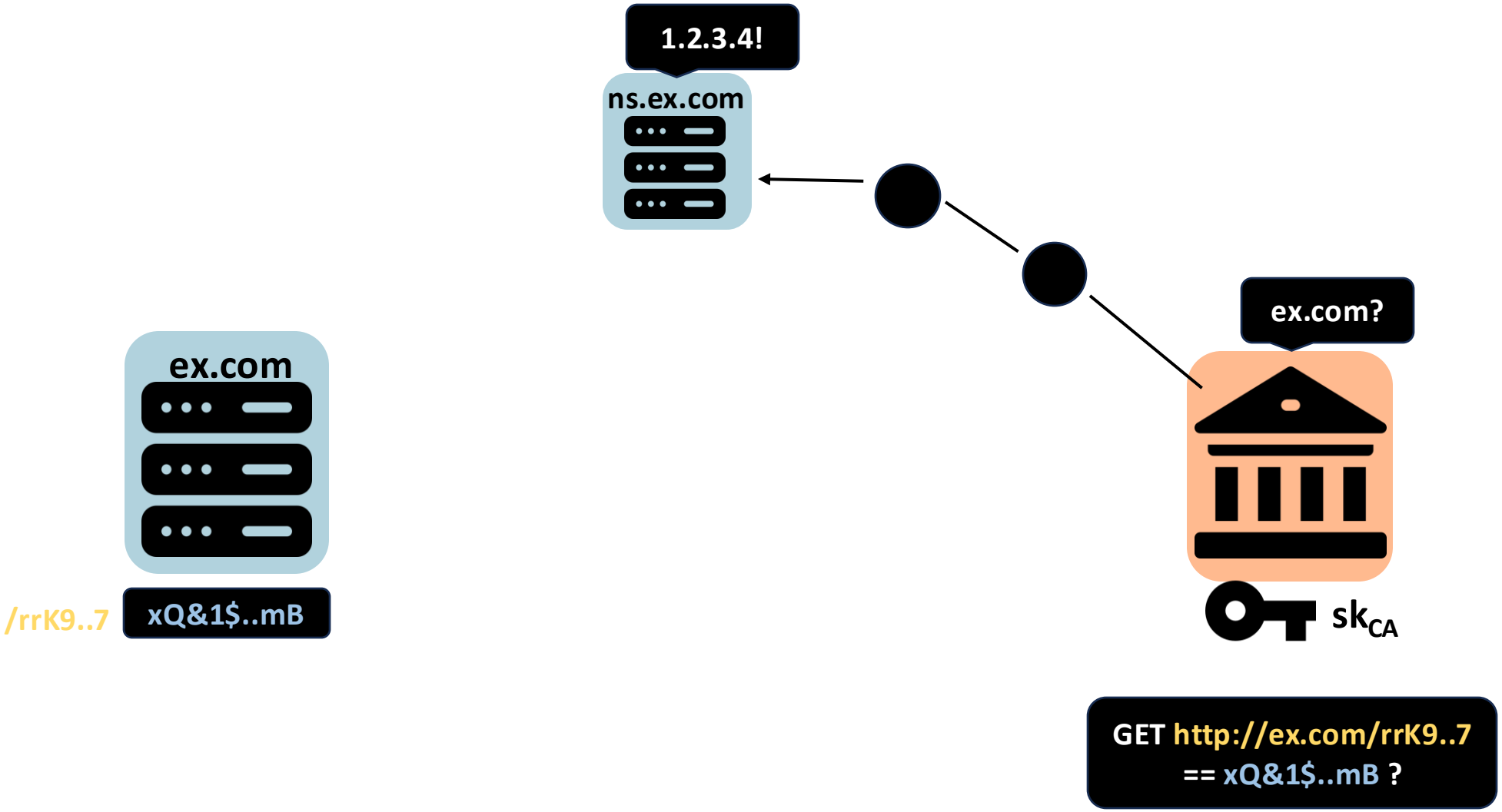
Domain Validation

Domain Validation

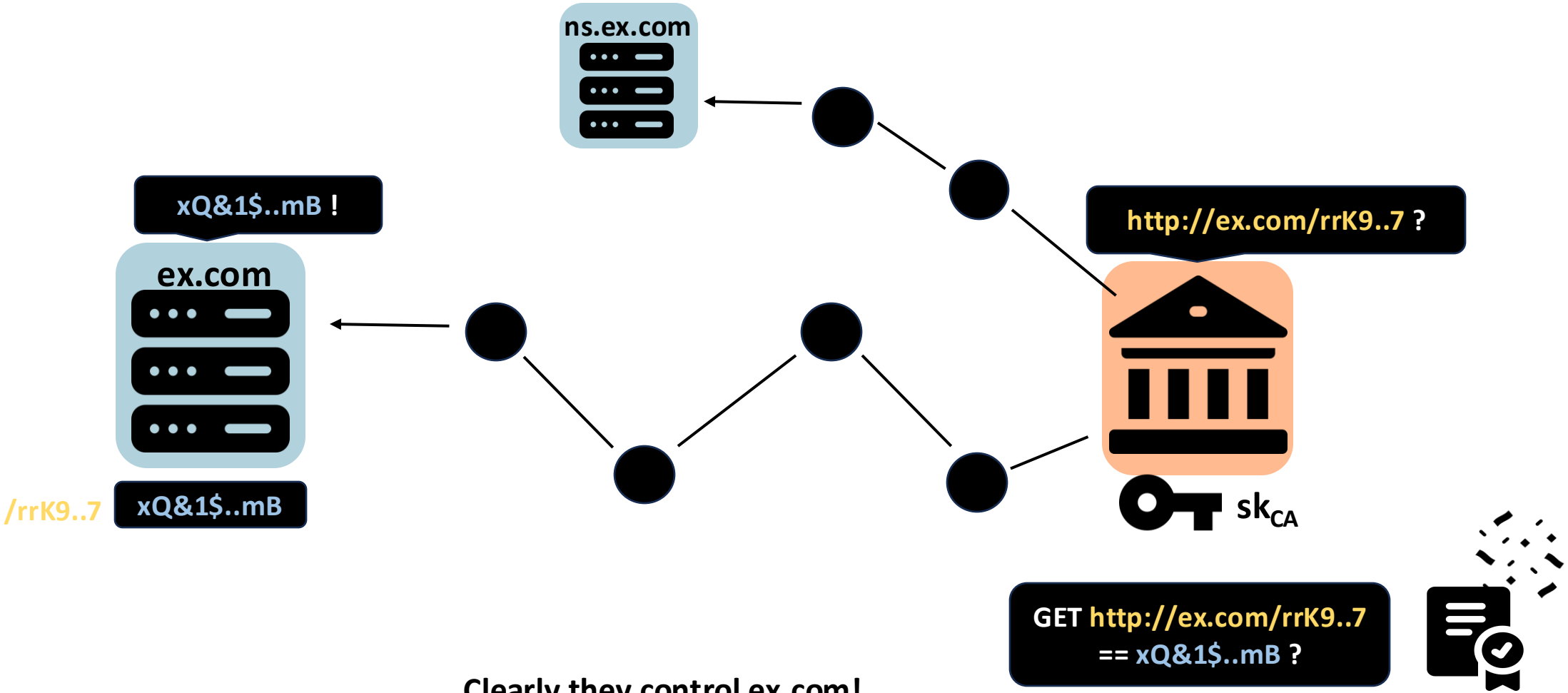


GET http://ex.com/rrK9..7
== xQ&1$..mB ?

Domain Validation



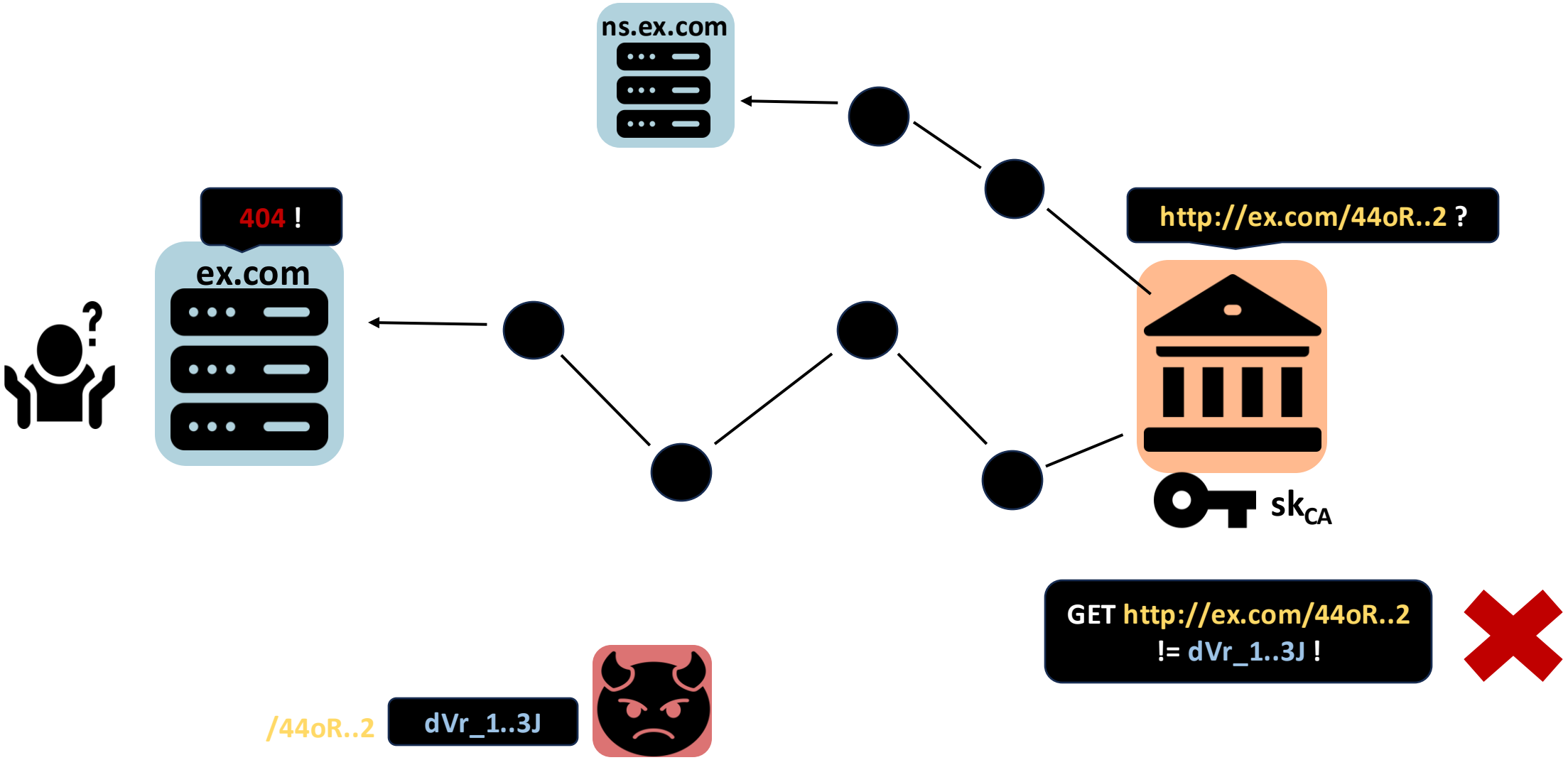
Domain Validation



Clearly they control ex.com!

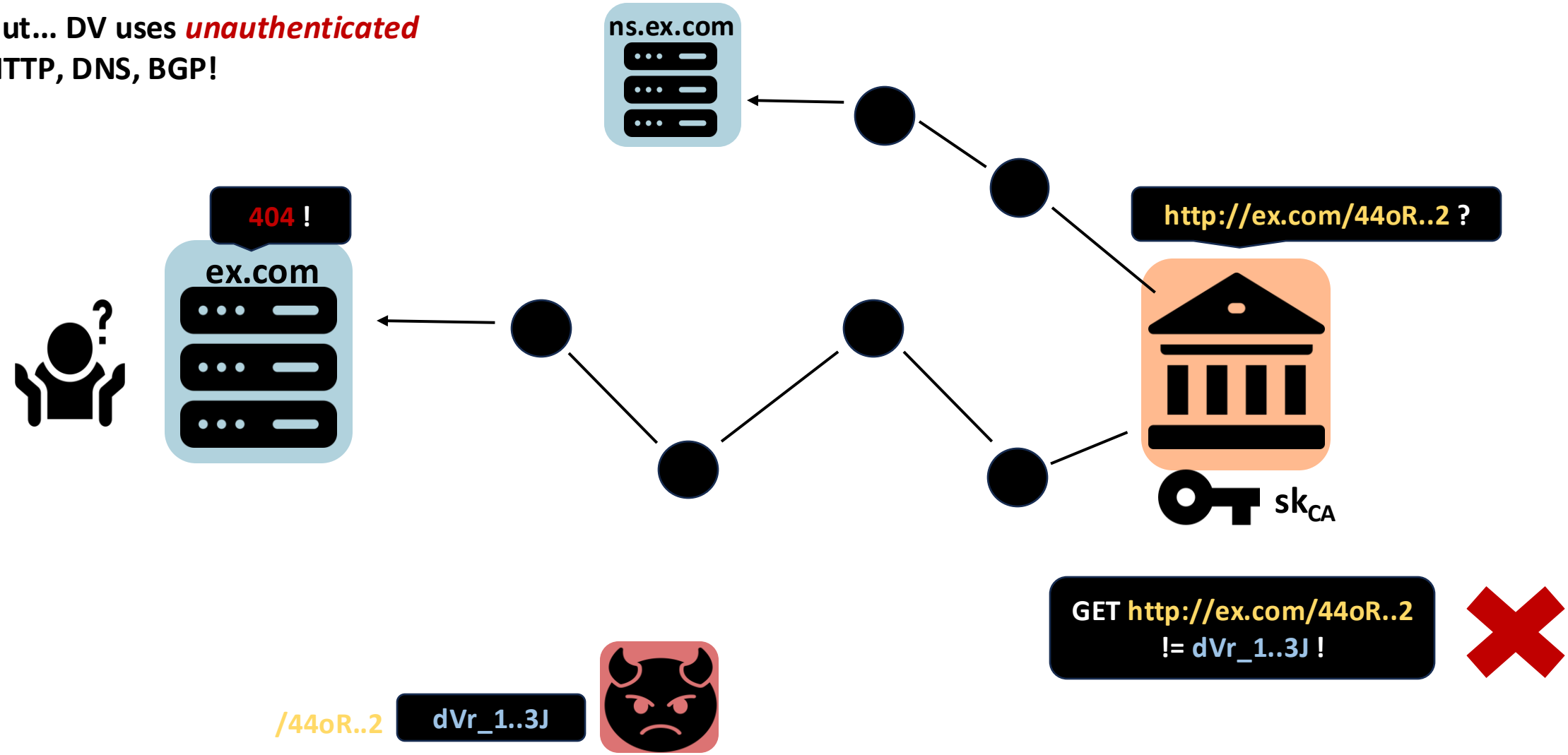
Domain Validation

Domain Validation



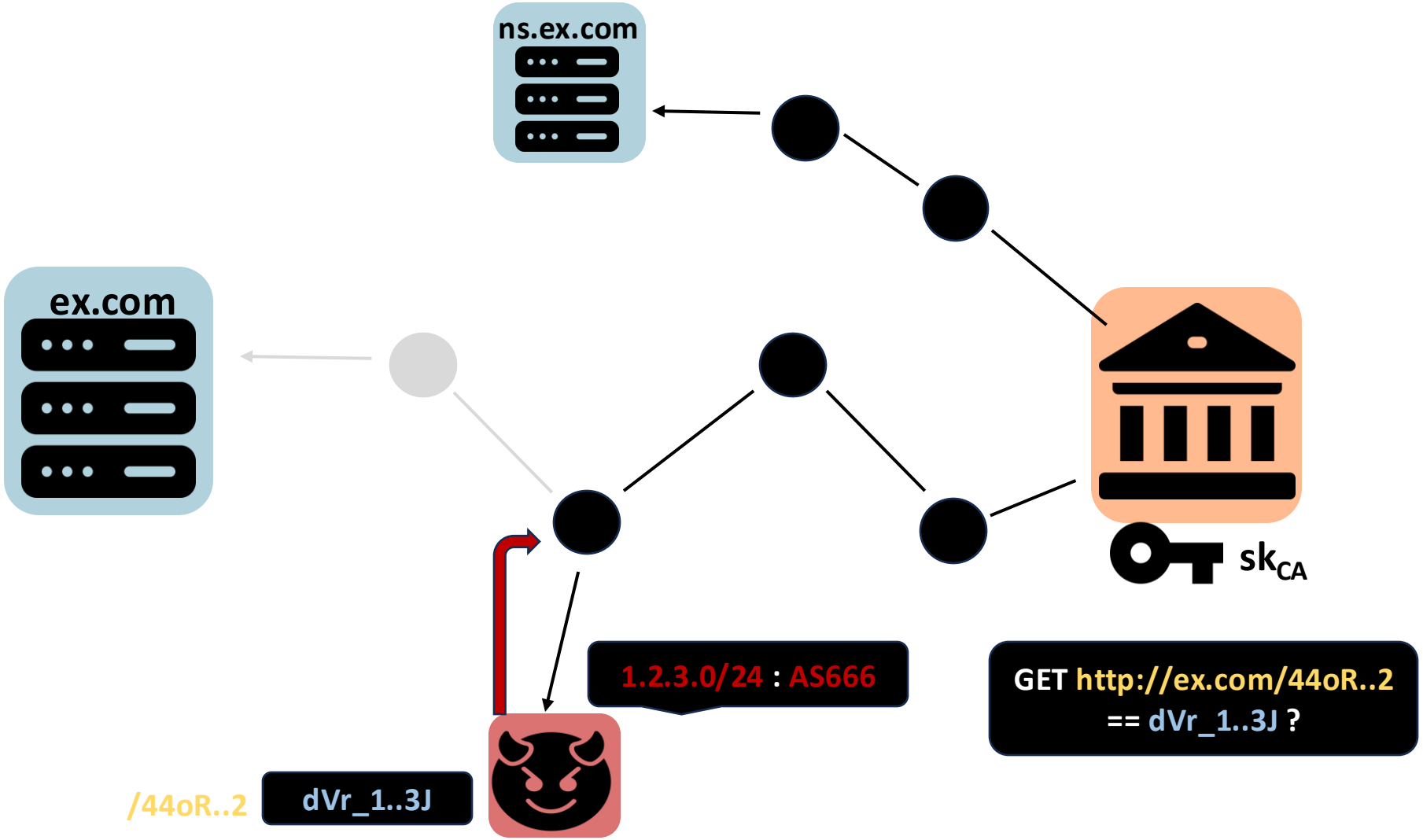
Domain Validation

But… DV uses *unauthenticated*
HTTP, DNS, BGP!



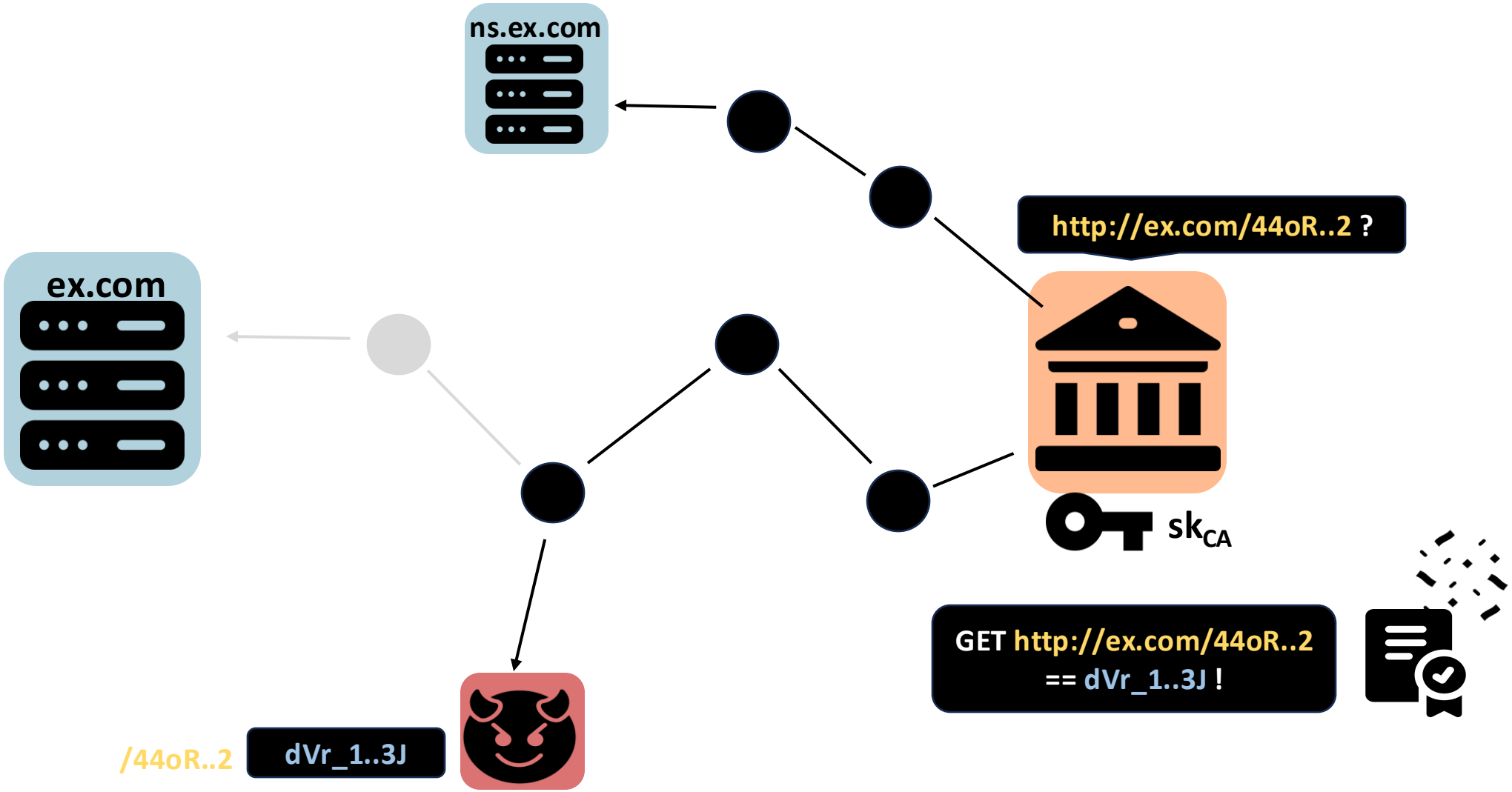
BGP Hijack

HotPETS'17
USENIX SEC'18



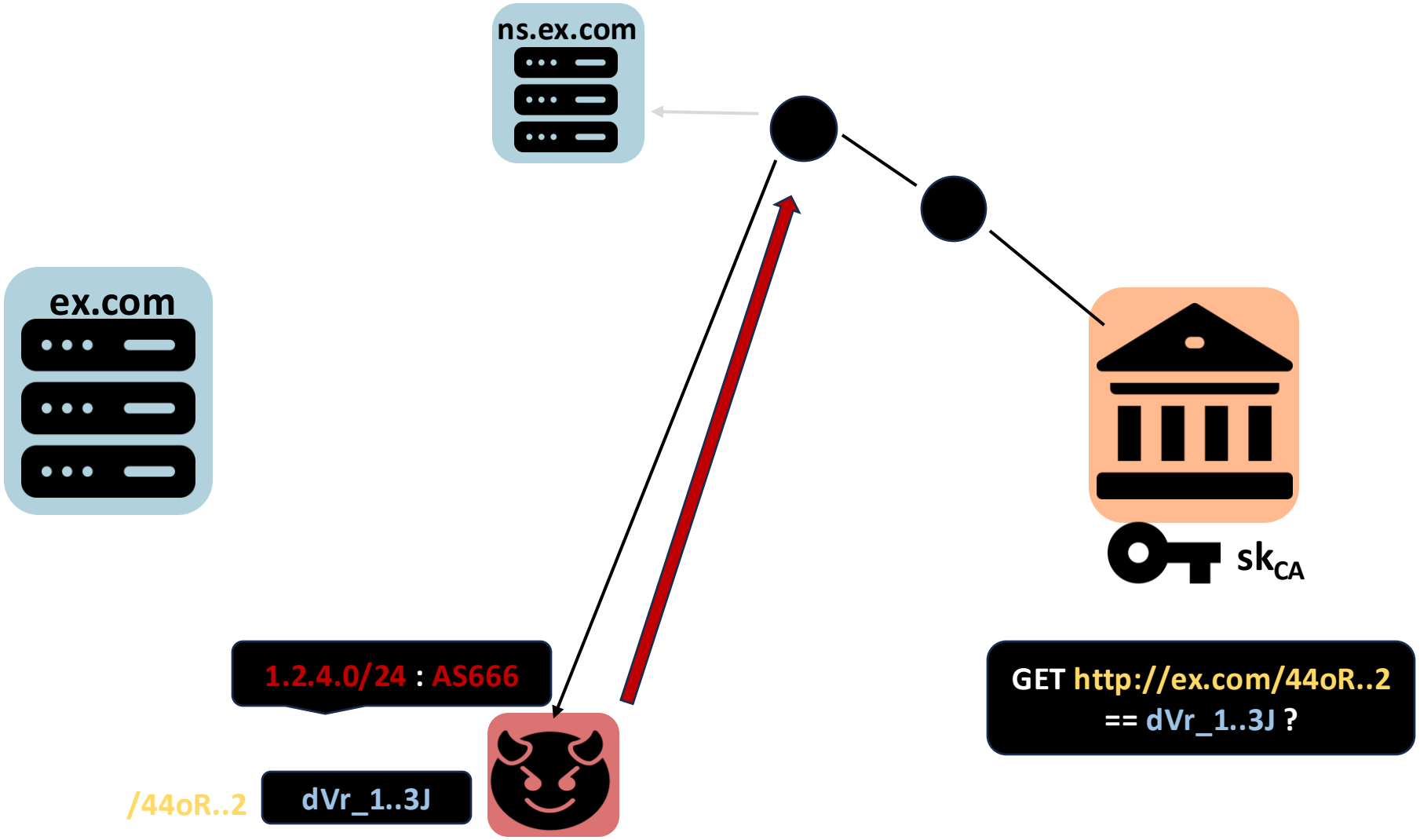
BGP Hijack

HotPETS'17
USENIX SEC'18



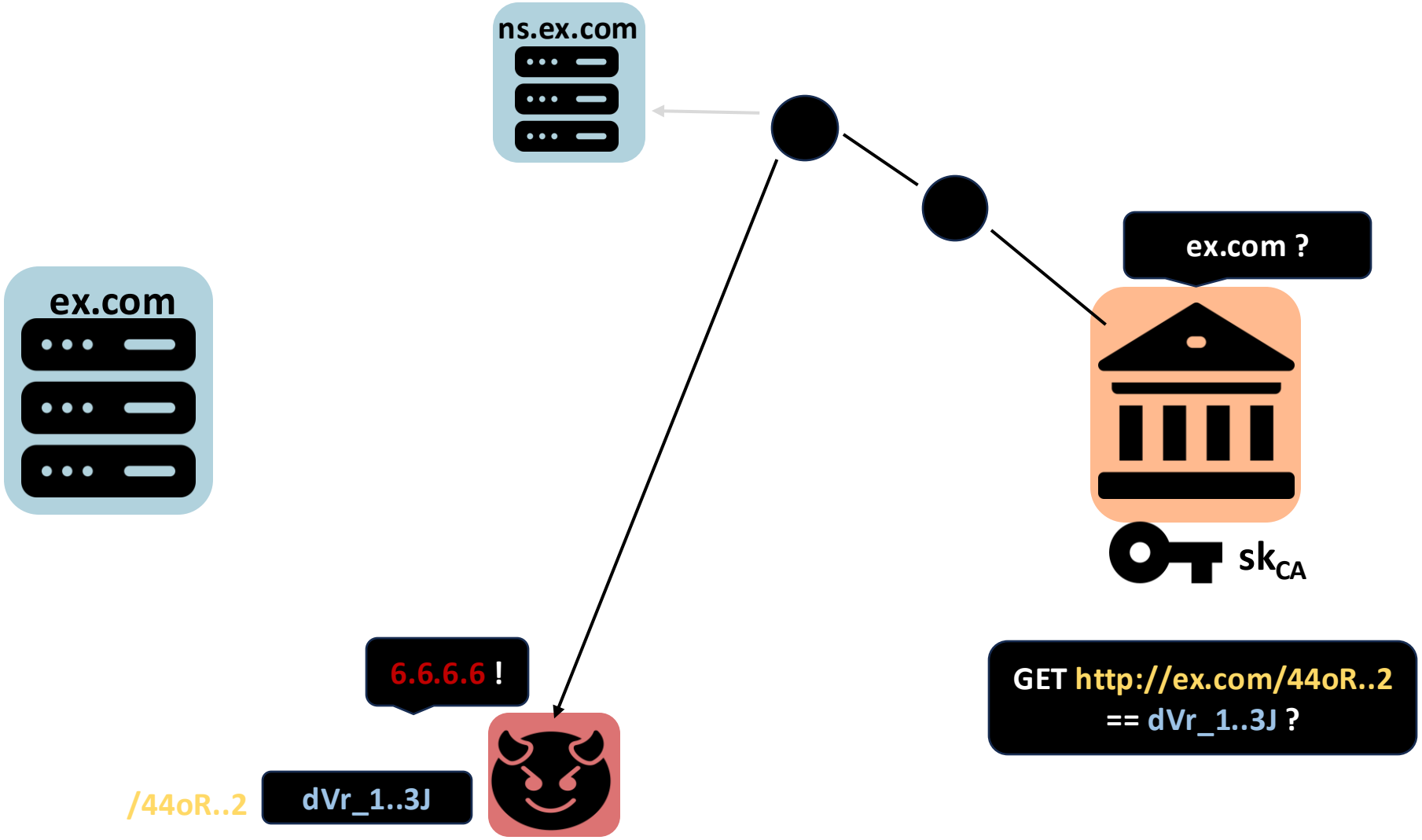
BGP Hijack

HotPETS'17
USENIX SEC'18



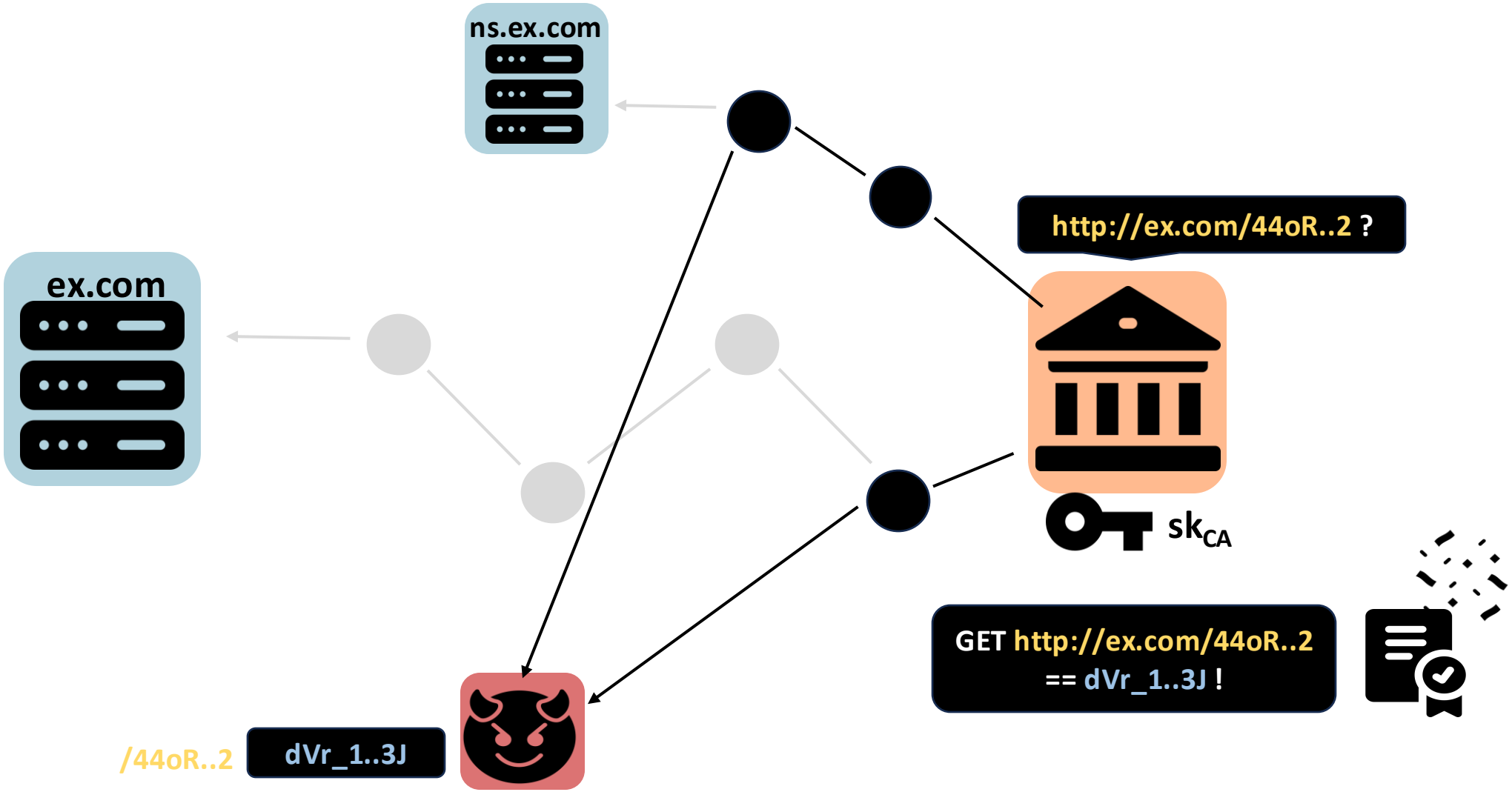
BGP Hijack

HotPETS'17
USENIX SEC'18



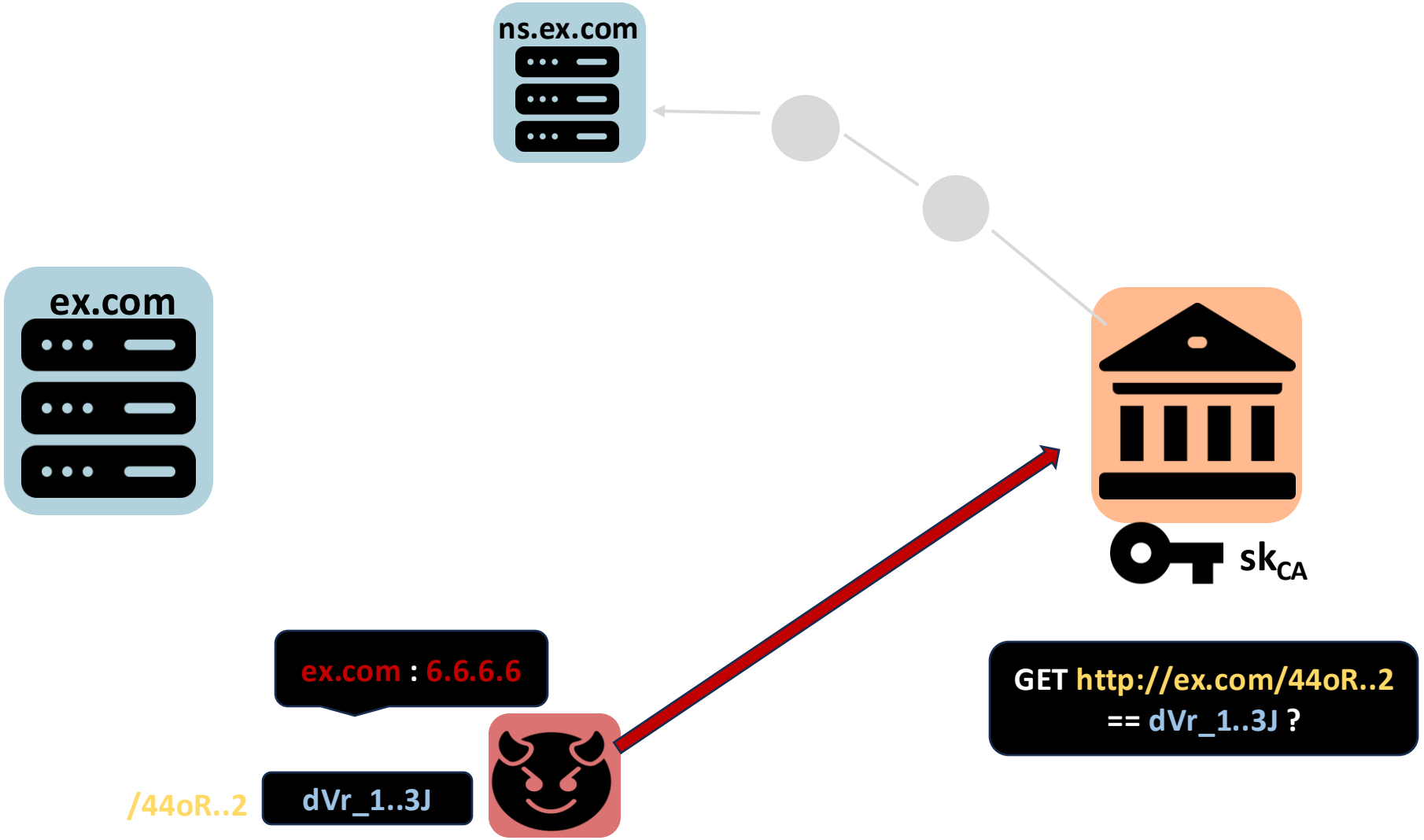
BGP Hijack

HotPETS'17
USENIX SEC'18



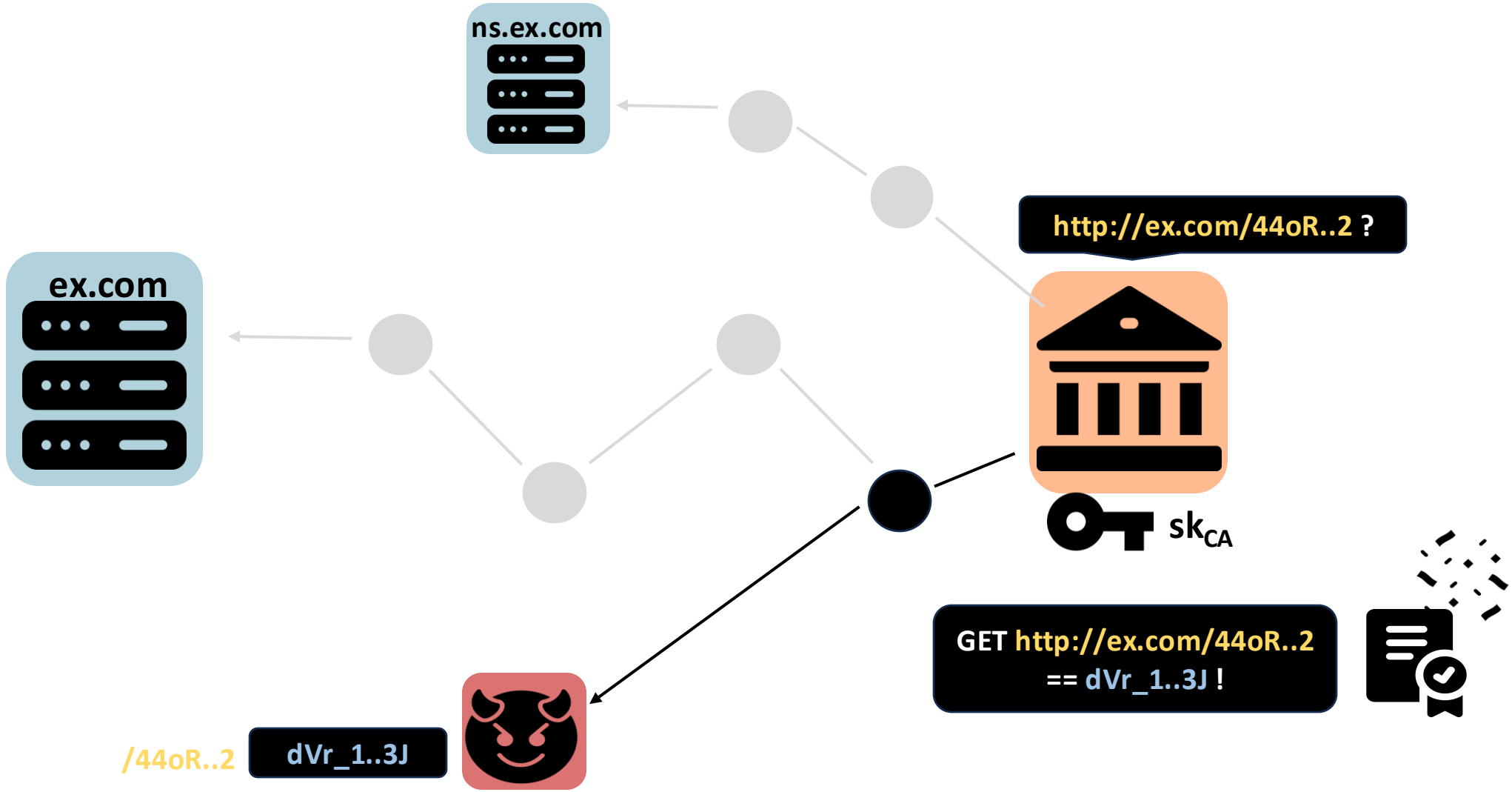
DNS Cache Poisoning

CCS'18

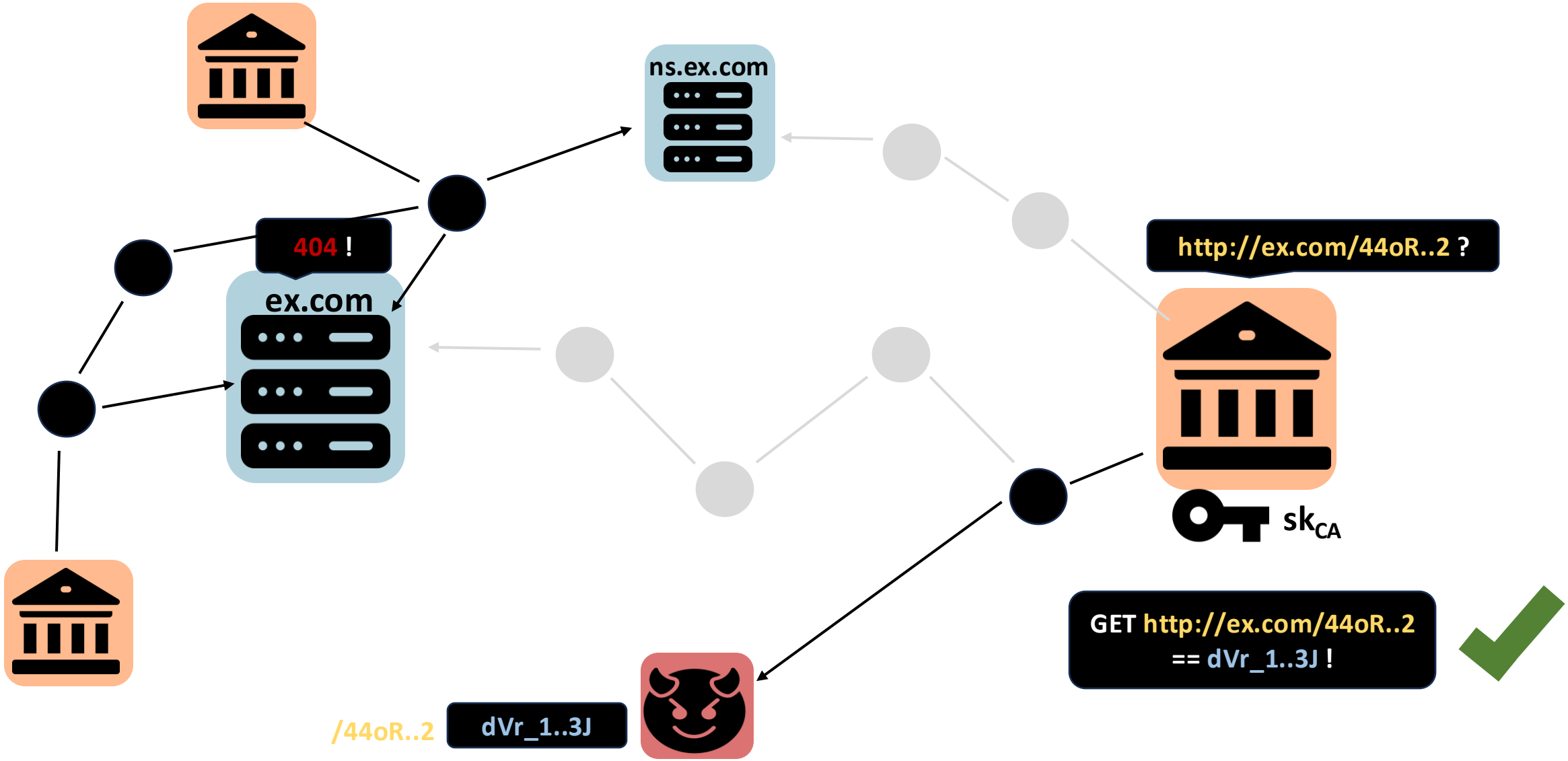


DNS Cache Poisoning

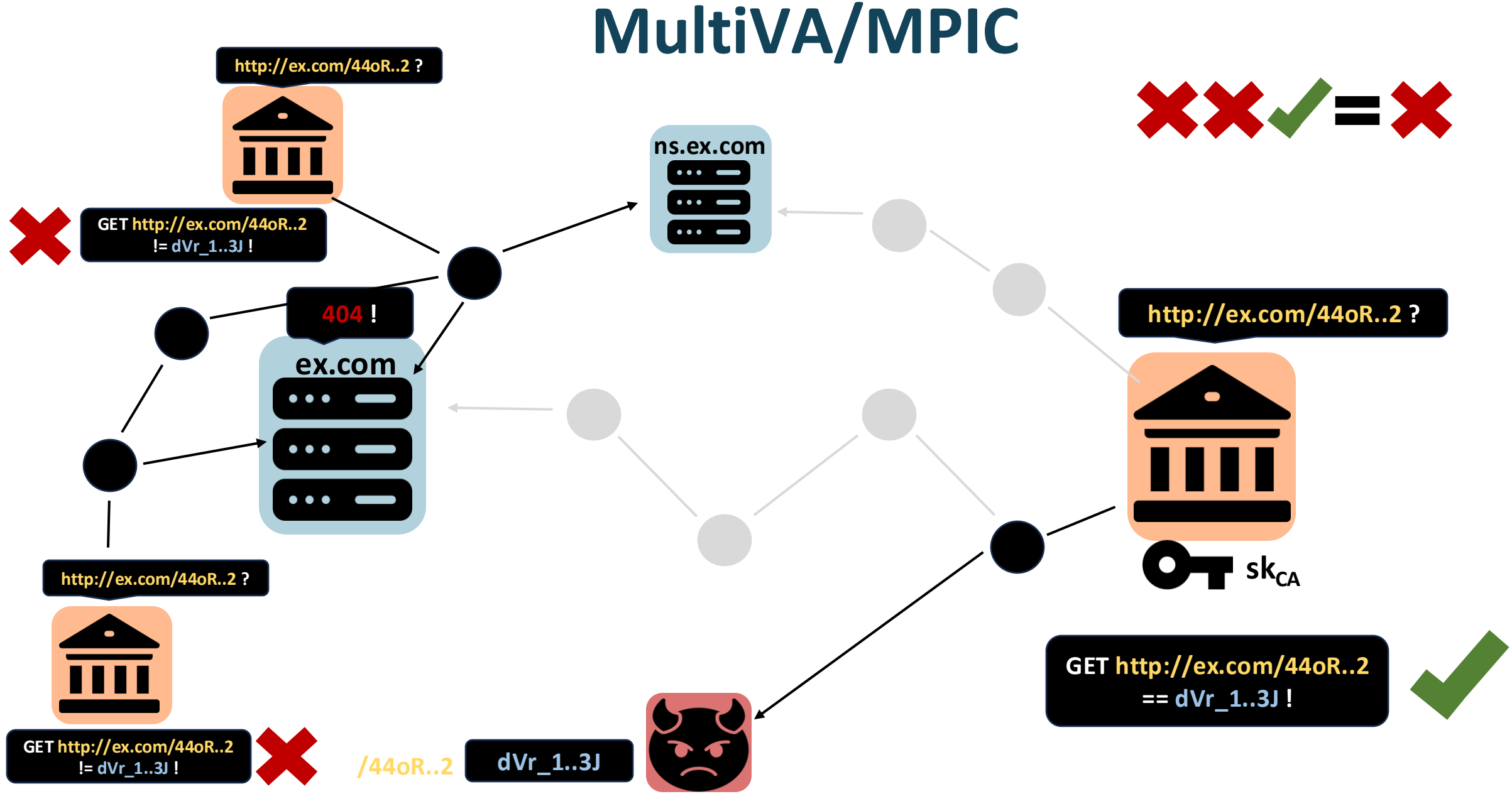
CCS'18



MultiVA/MPIC

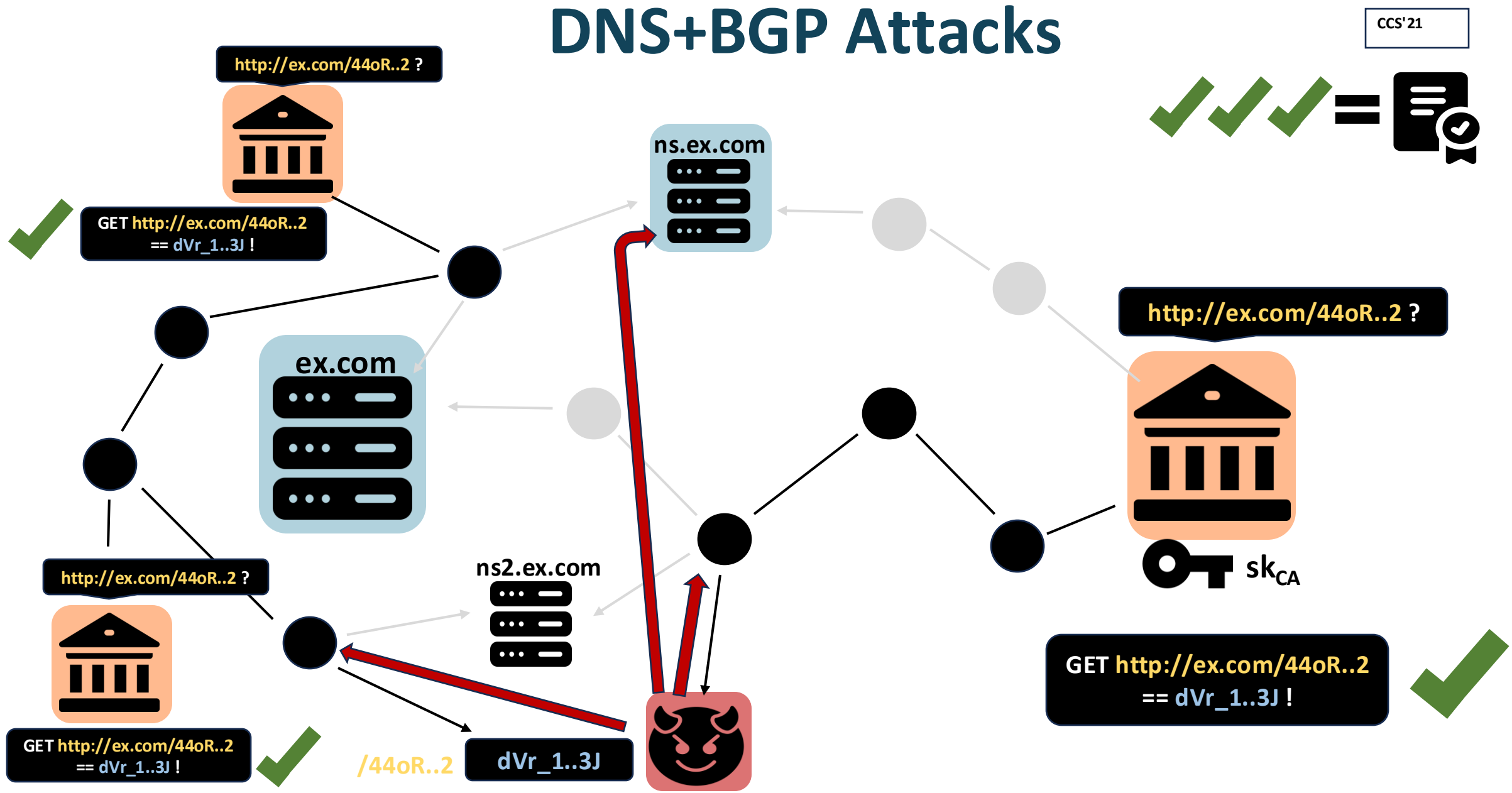


MultiVA/MPIC



DNS+BGP Attacks

CCS'21



Validators should be

a) distributed

b) *unpredictable*

Randomized Distributed DV

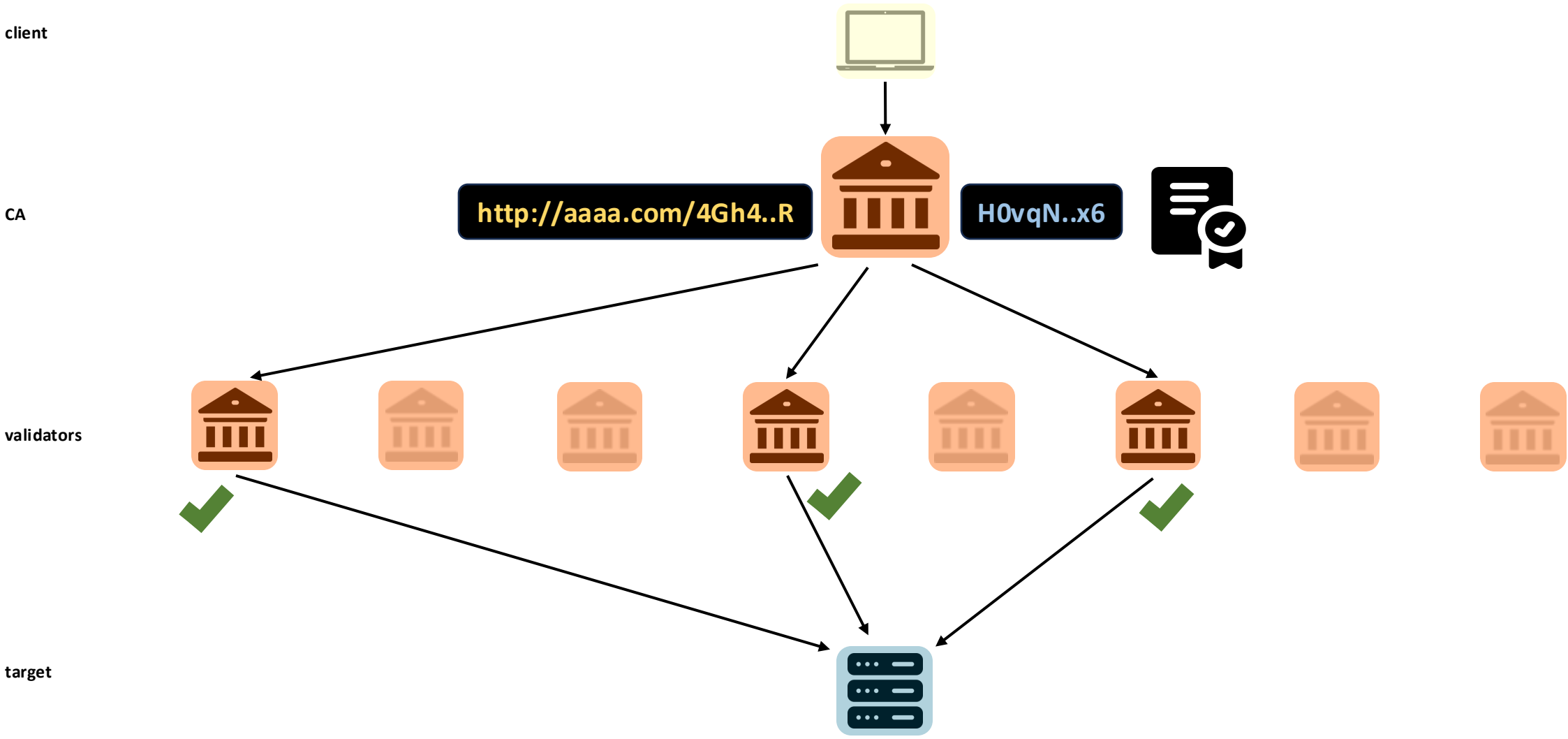
client

CA

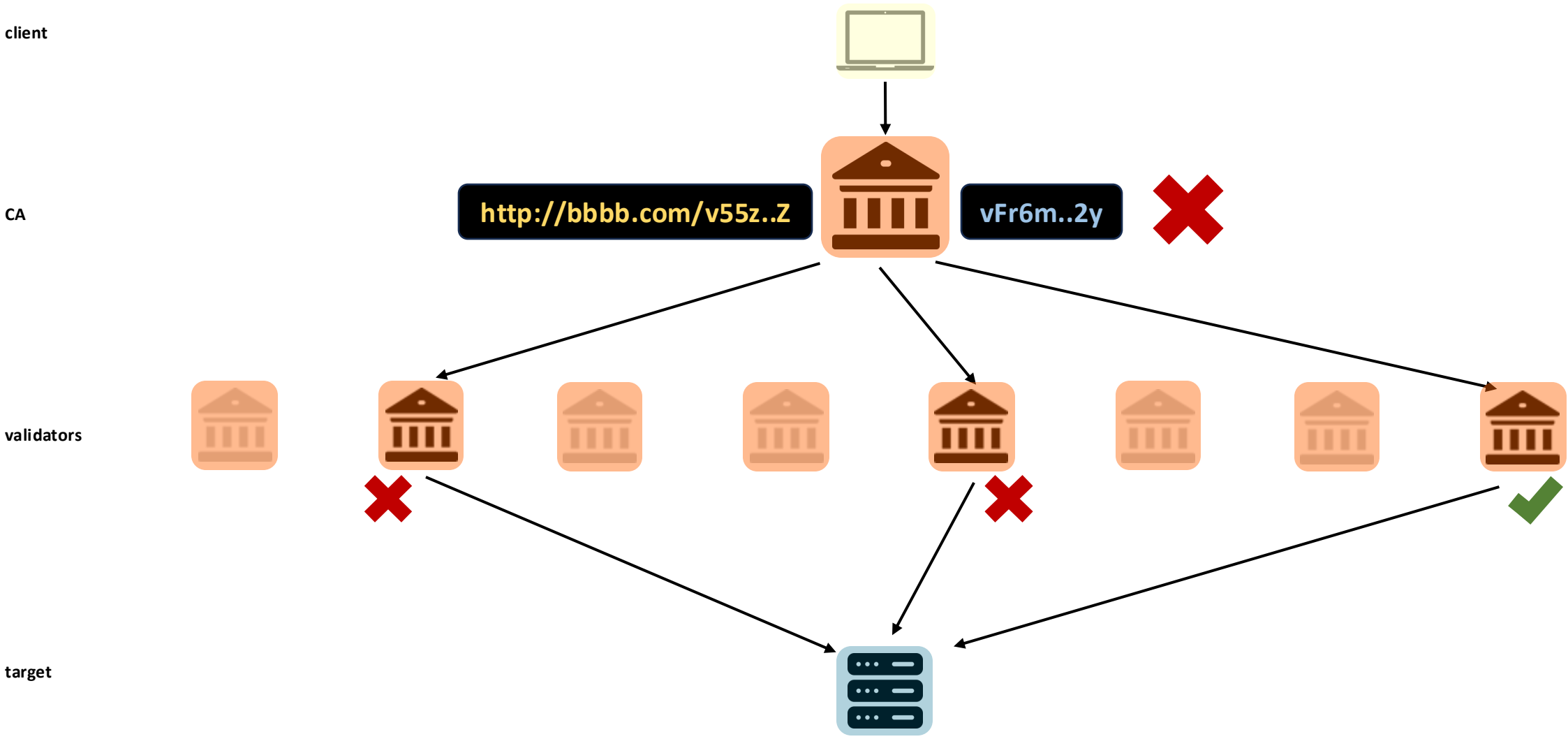
validators

target

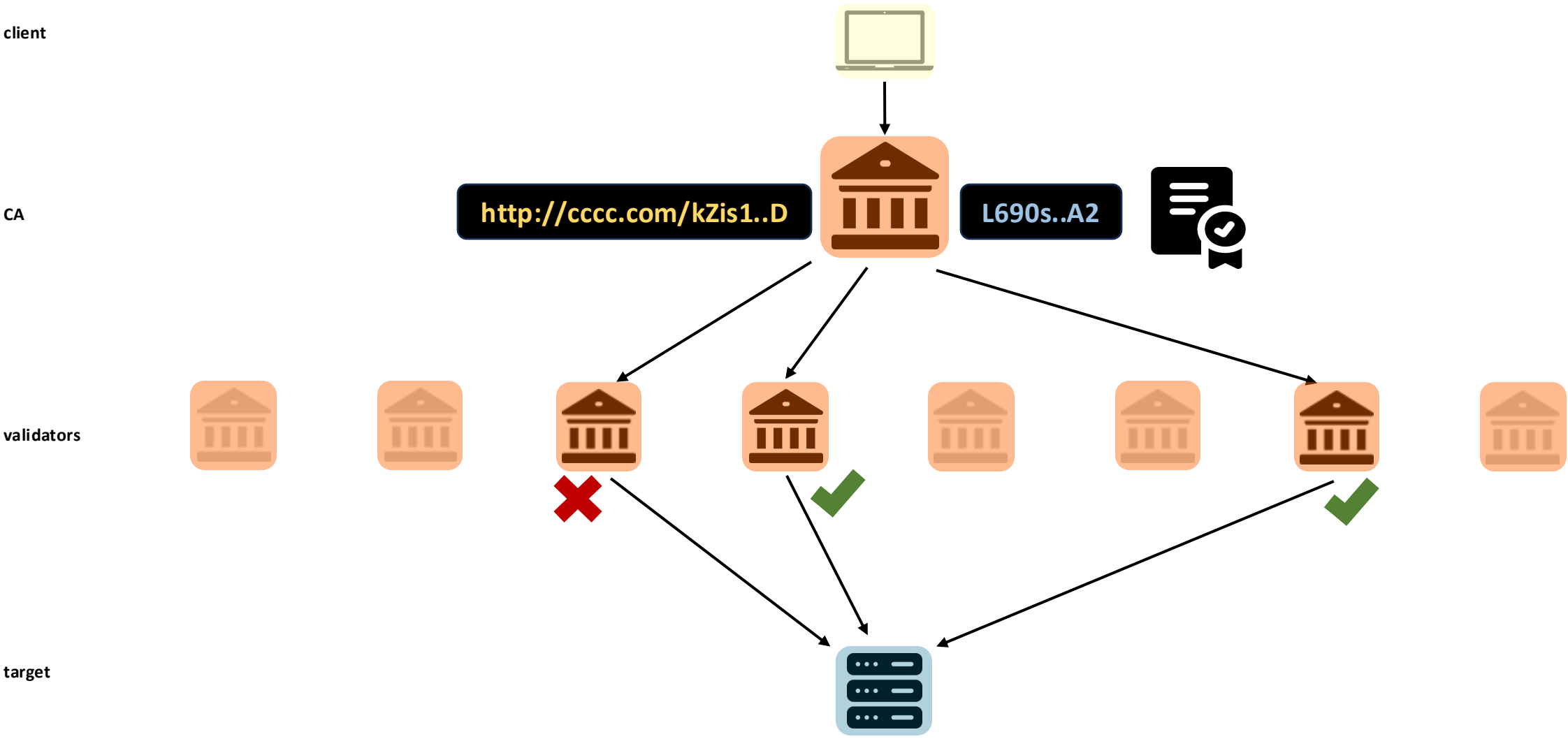
Randomized Distributed DV



Randomized Distributed DV



Randomized Distributed DV

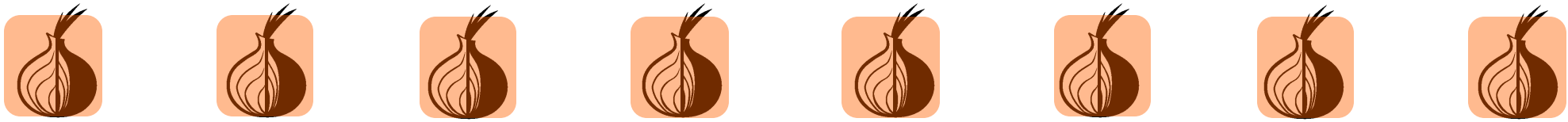


Randomized Distributed DV over Tor

client

CA

validators



target

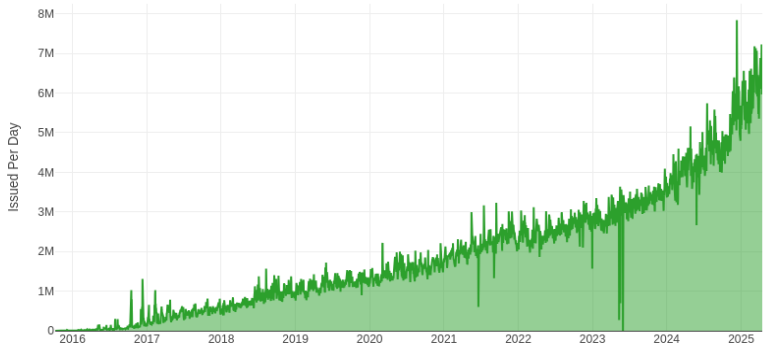
Why ?

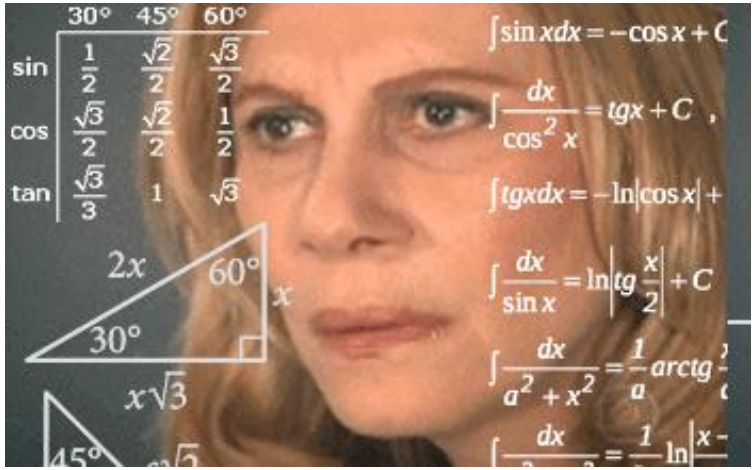
" In **2019** Let's Encrypt **will** secure a massive portion of the Web with a budget of only **$3.6M**. "

Here's how our 2017 budget breaks down:

Expense	Cost
Staffing	$2.06M USD
Hardware/Software	$0.20M USD
Hosting/Auditing	$0.30M USD
Legal/Administrative	$0.35M USD
Total	$2.91M USD

Let's Encrypt Certificates Issued Per Day





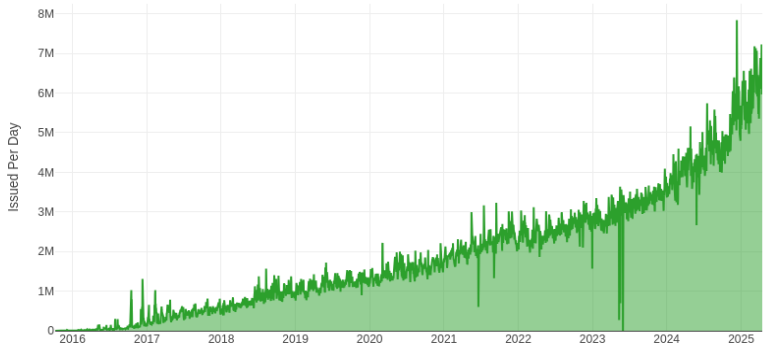
Why ?

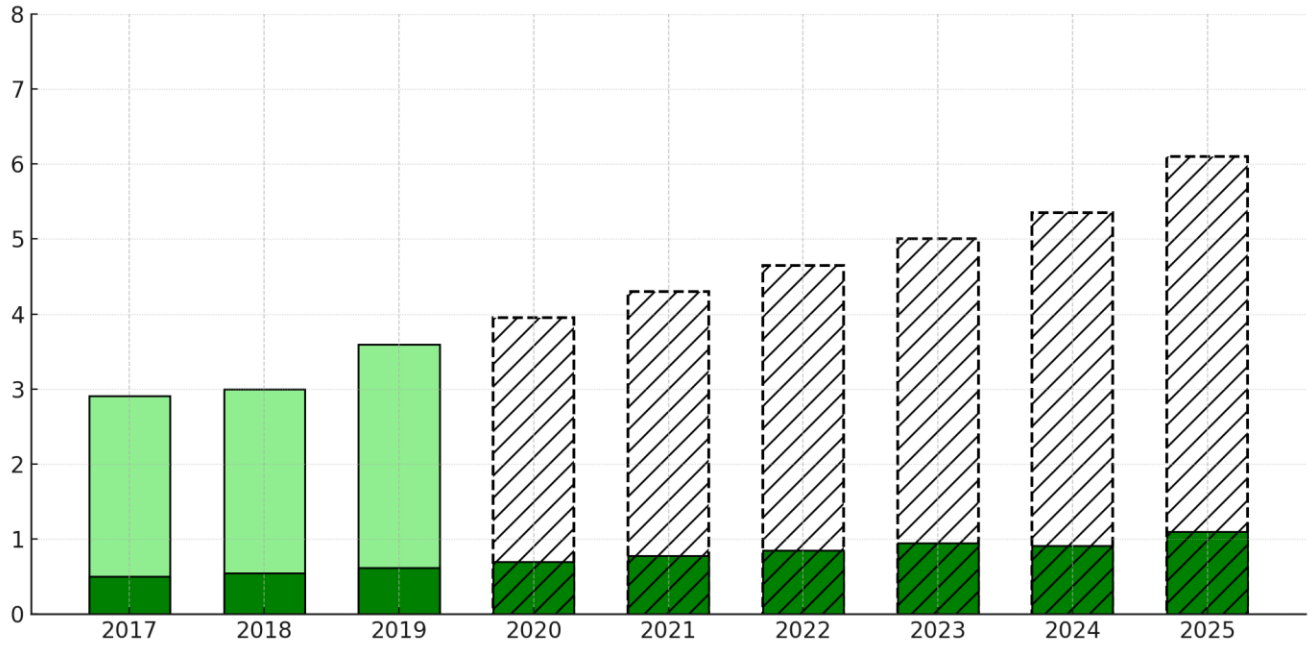
" In **2019** Let's Encrypt **will** secure a massive portion of the Web with a budget of only **$3.6M**. "

Here's how our 2017 budget breaks down:

Expense	Cost
Staffing	$2.06M USD
Hardware/Software	$0.20M USD
Hosting/Auditing	$0.30M USD
Legal/Administrative	$0.35M USD
Total	$2.91M USD

Let's Encrypt Certificates Issued Per Day





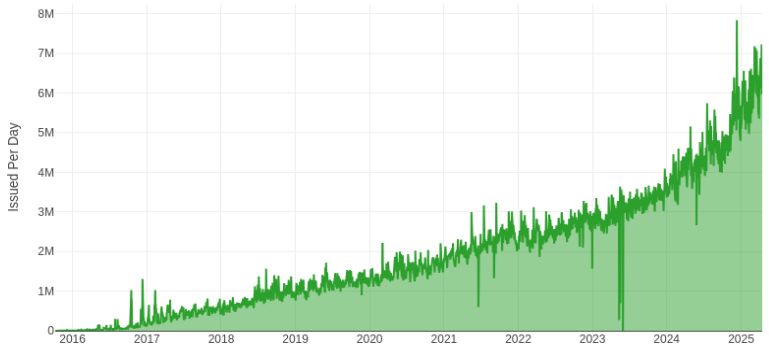
Why ?

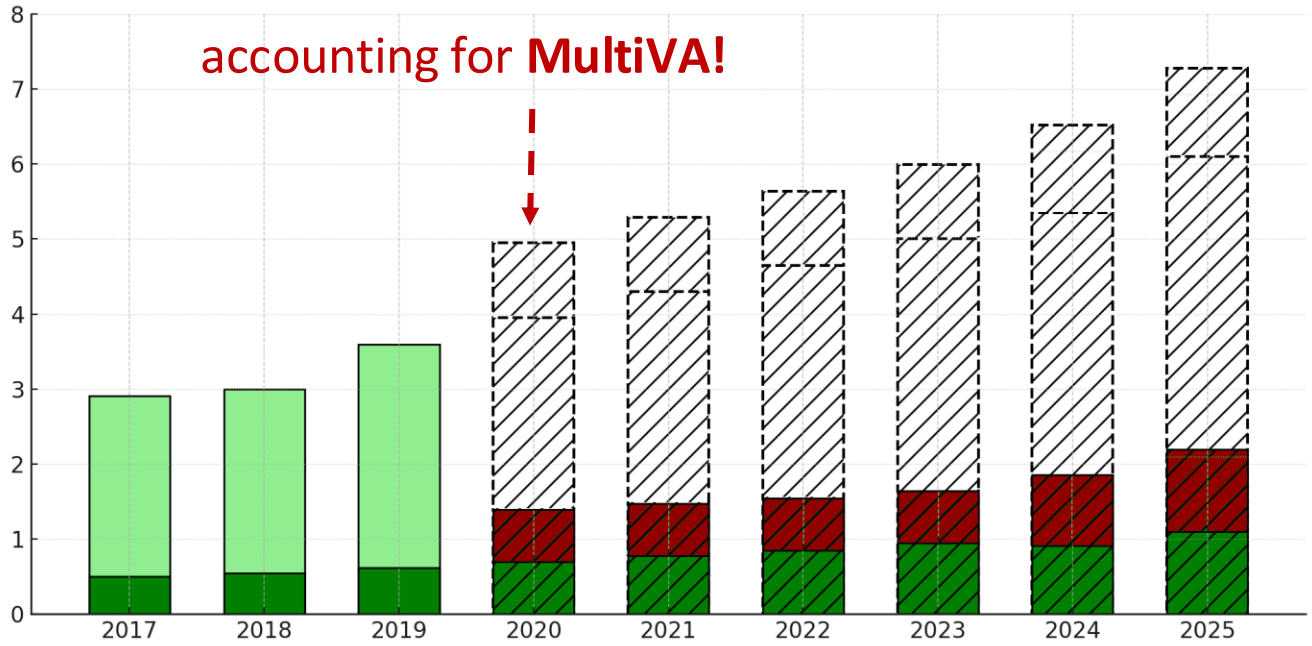
" In **2019** Let's Encrypt **will** secure a massive portion of the Web with a budget of only **$3.6M**. "

Here's how our 2017 budget breaks down:

Expense	Cost
Staffing	$2.06M USD
Hardware/Software	$0.20M USD
Hosting/Auditing	$0.30M USD
Legal/Administrative	$0.35M USD
Total	$2.91M USD

Let's Encrypt Certificates Issued Per Day





Why  ?

cloud?

Microsoft Azure aws

dedicated volunteer networks?

RIPE Atlas NLNOG RING

public VPNs?

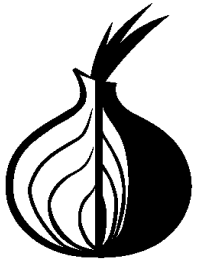
ExpressVPN NordVPN

residential proxies?

bright data smartproxy oxylabs

other anonymity networks?

NYM I2P



Free

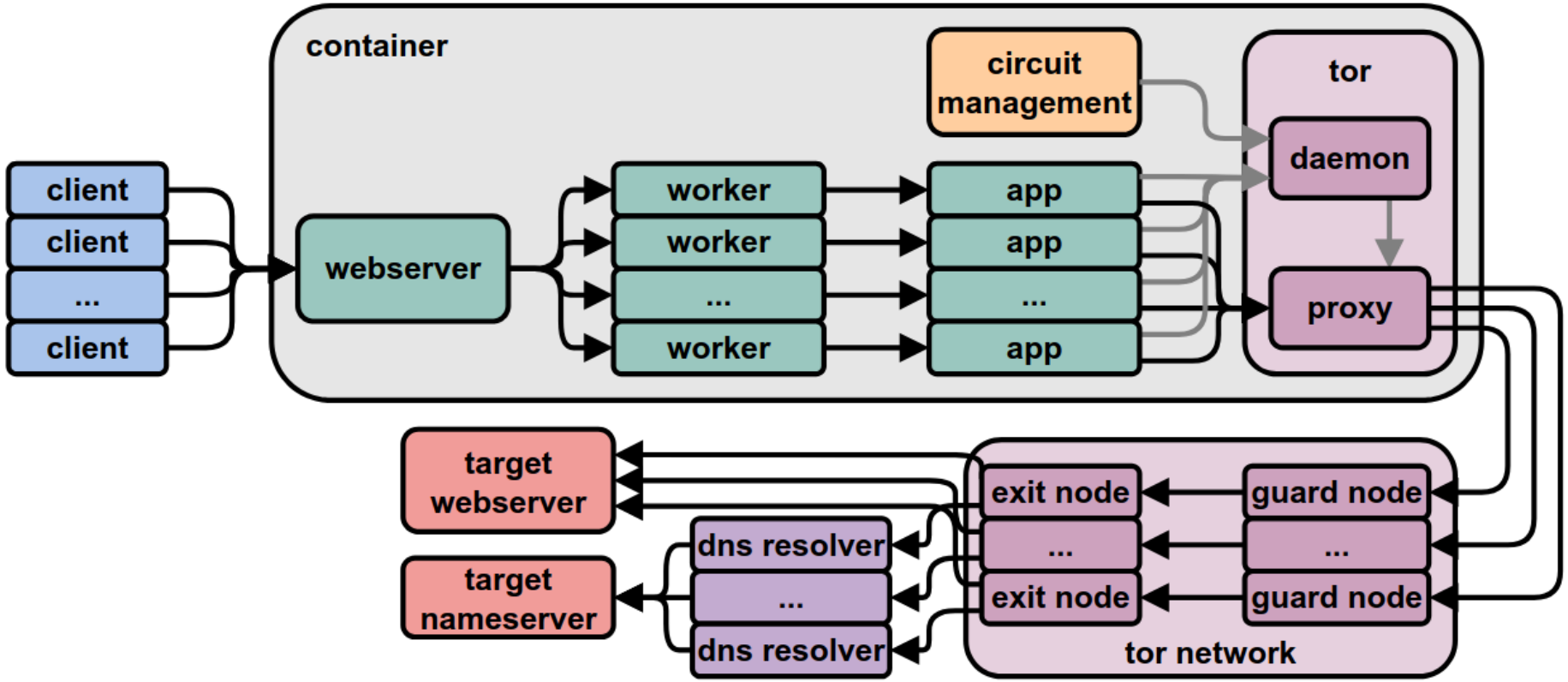
High Capacity

Many Nodes

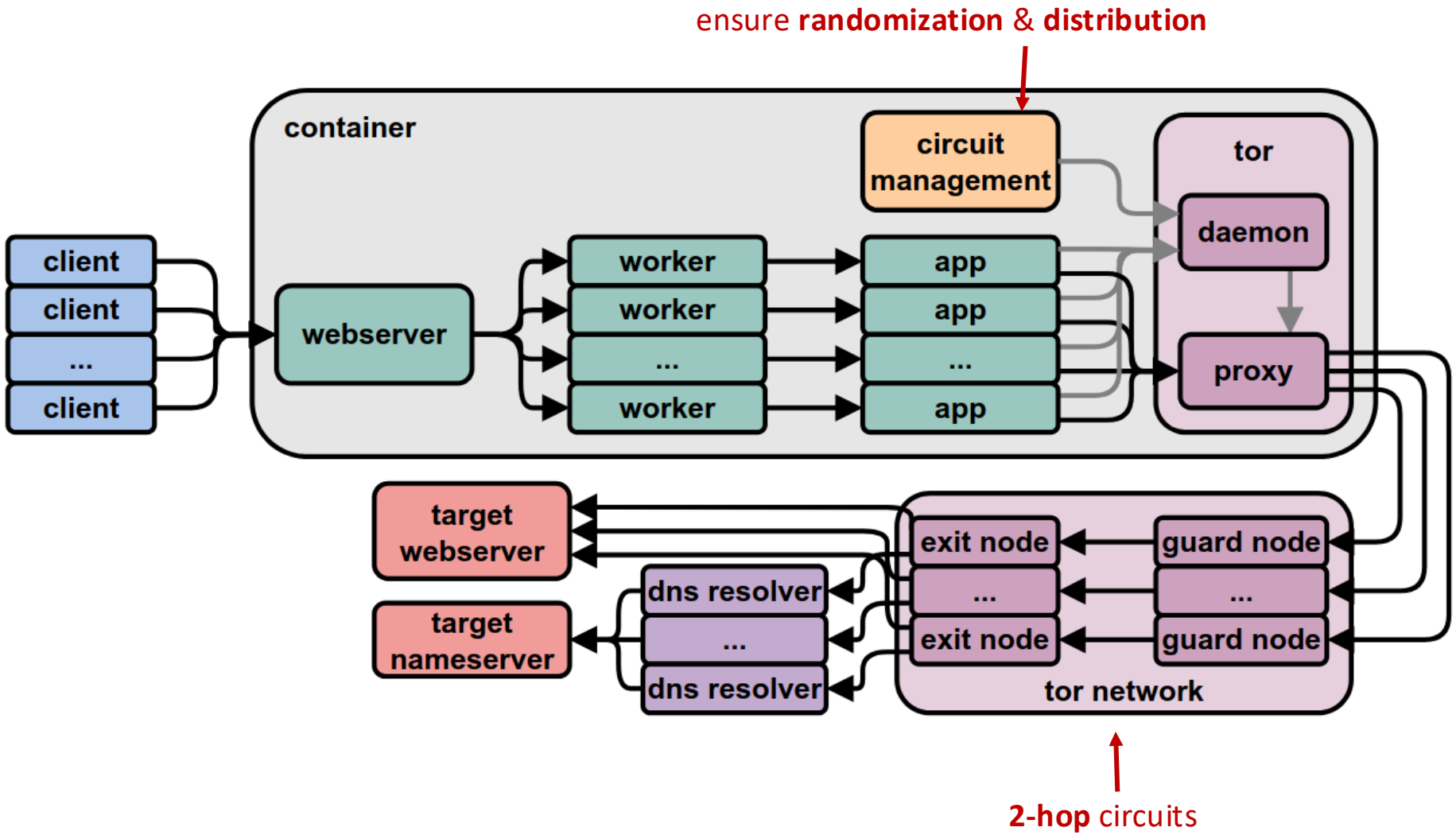
Monitored

Easy to Study

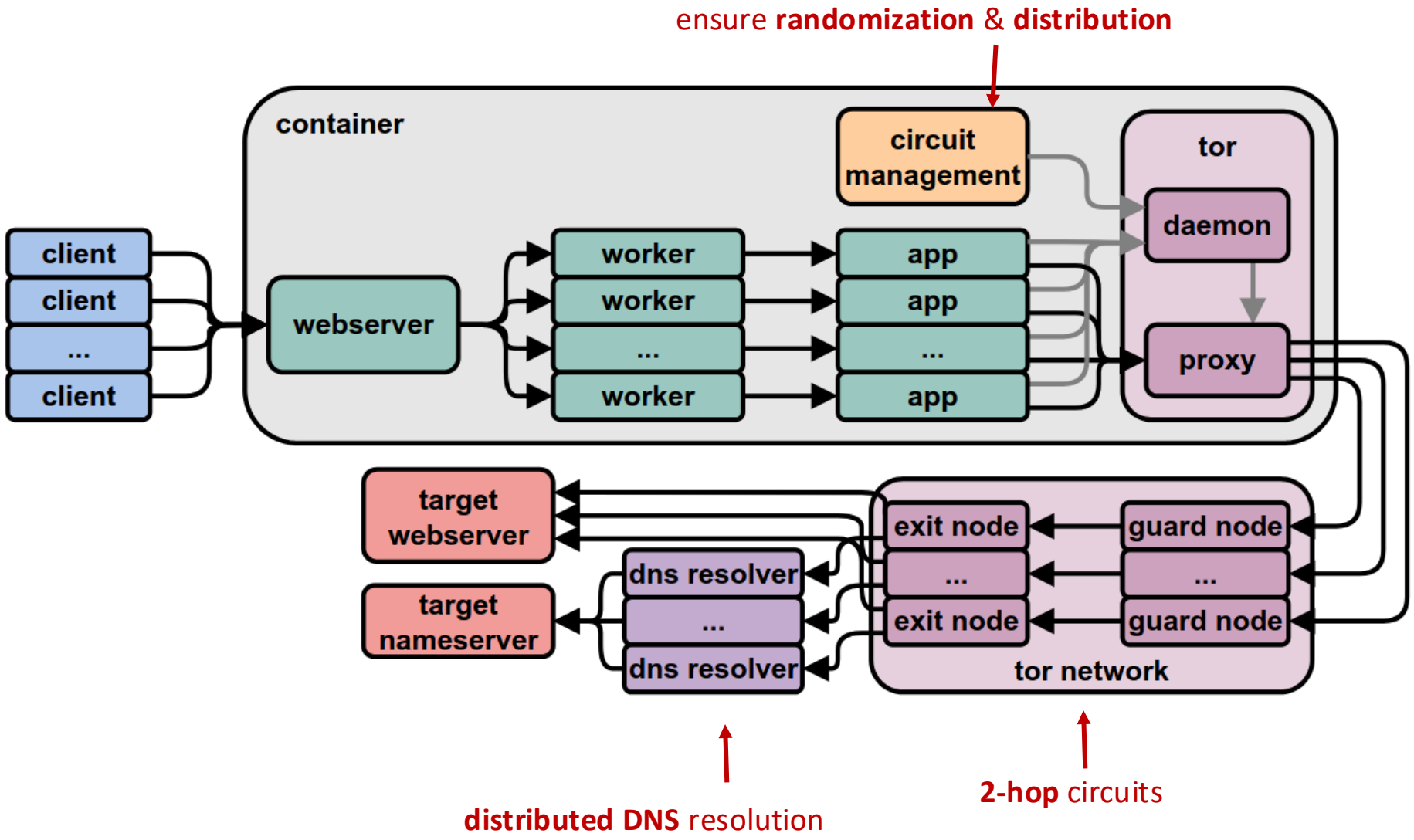
Setup – PoC Docker Container



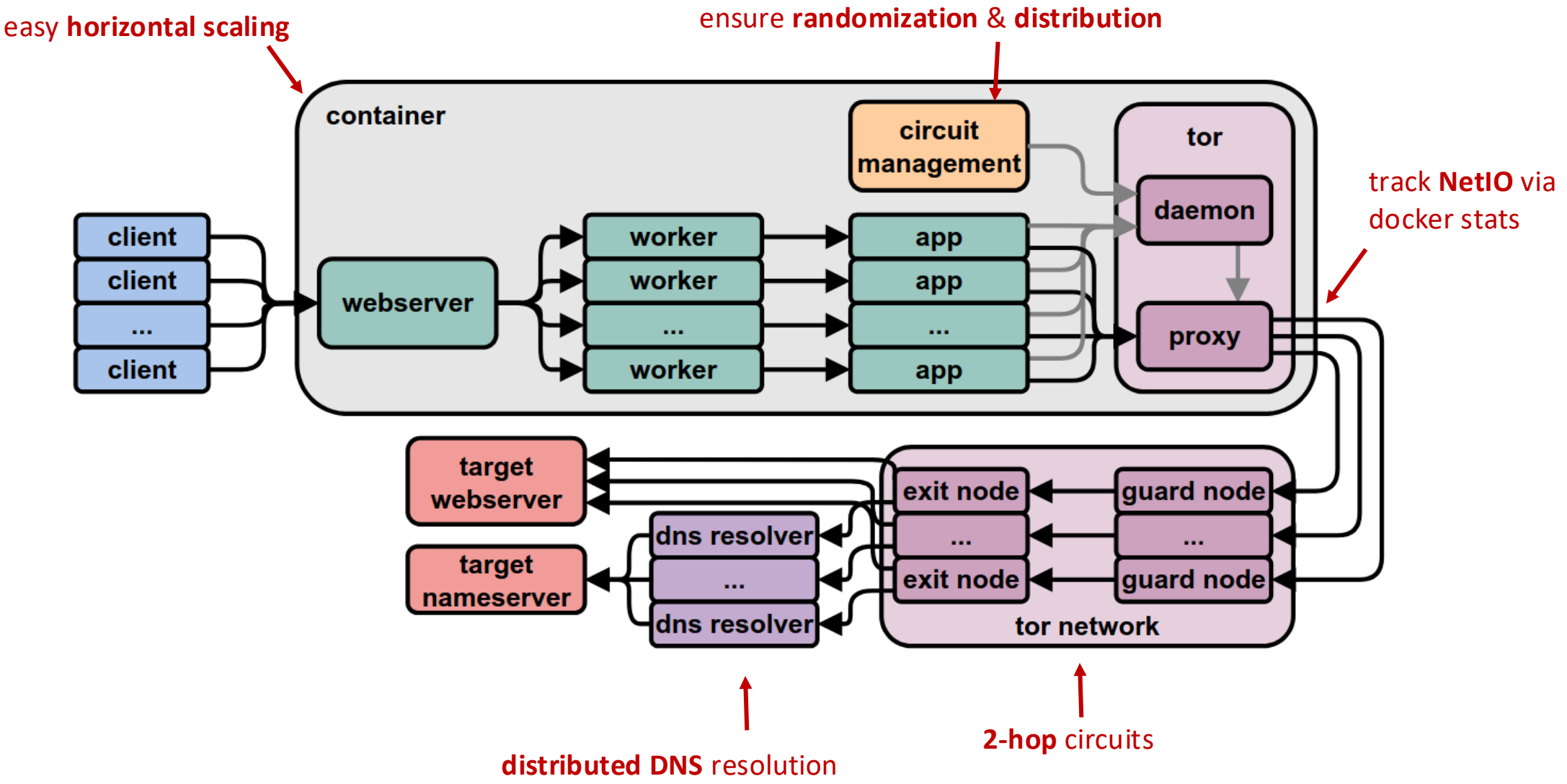
Setup – PoC Docker Container



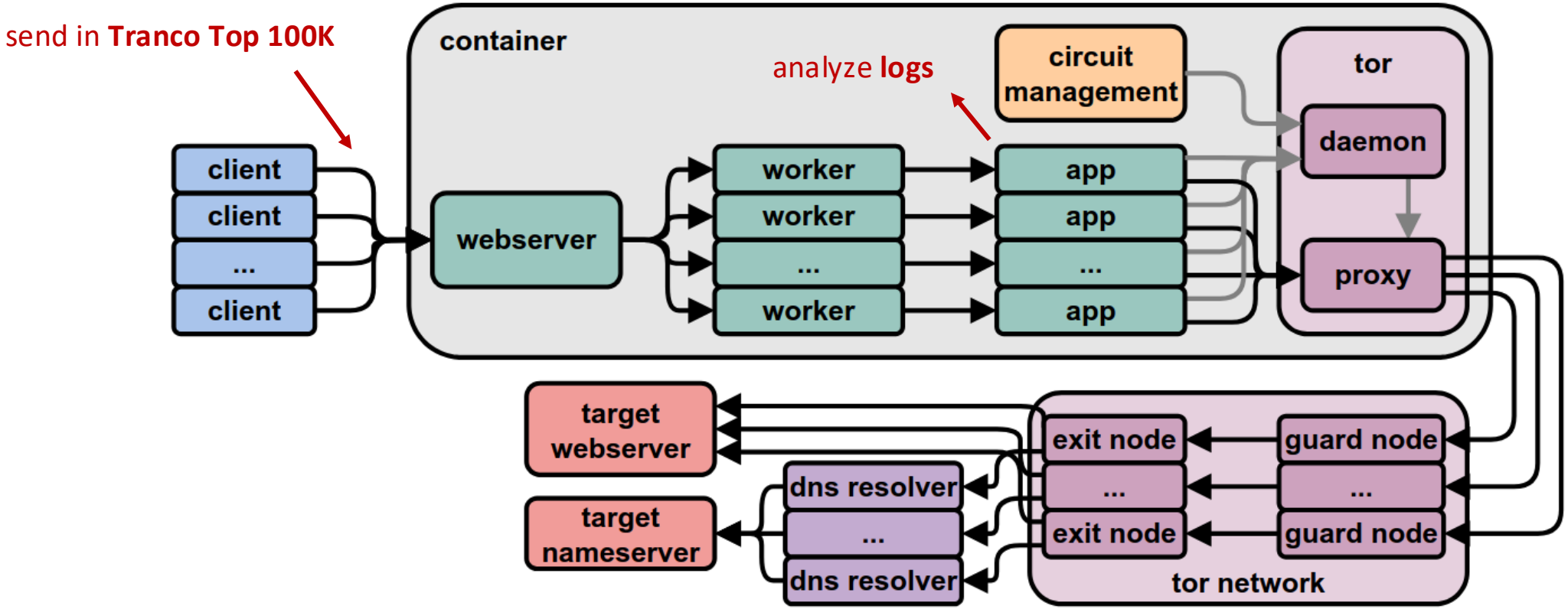
Setup – PoC Docker Container



Setup – PoC Docker Container



Setup – PoC Docker Container



Path Diversity

In the **absence** of **targeted attacks** on validators,
what is the **remaining attack surface**?

Path Diversity

In the **absence** of **targeted attacks** on validators,
what is the **remaining attack surface**?

Path Overlap

What is the relative
pair-wise overlap in AS paths for a
given validation?

Path Diversity

In the **absence** of **targeted attacks** on validators,
what is the **remaining attack surface**?

Path Overlap

What is the relative
pair-wise overlap in AS paths for a
given validation?

On-Path ASes

What **percentage of validators** can a
given AS intercept?

Path Diversity

In the **absence** of **targeted attacks** on validators,
what is the **remaining attack surface**?

Path Overlap

What is the relative
pair-wise overlap in AS paths for a
given validation?

On-Path ASes

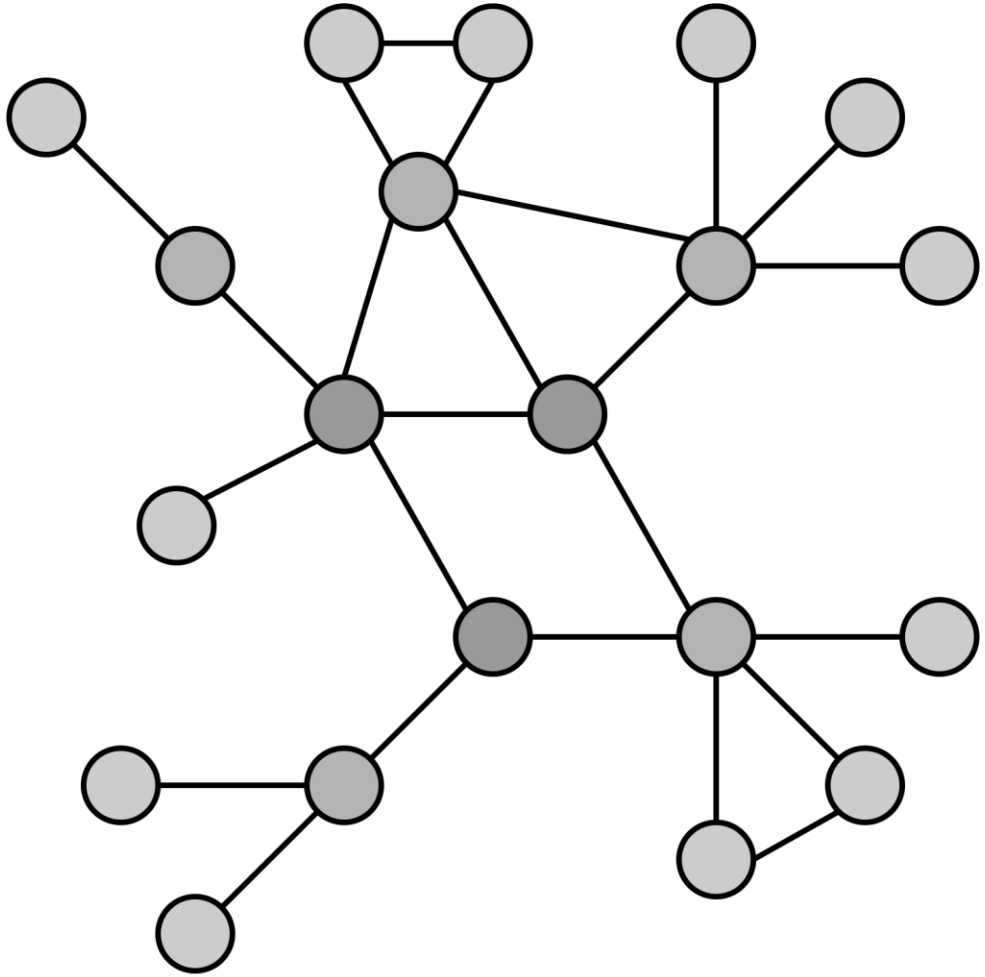
What **percentage of validators** can a
given AS intercept?

What percentage of ASes can
intercept 100% of validators?

Routing Simulation

Reconstruct BGP network from

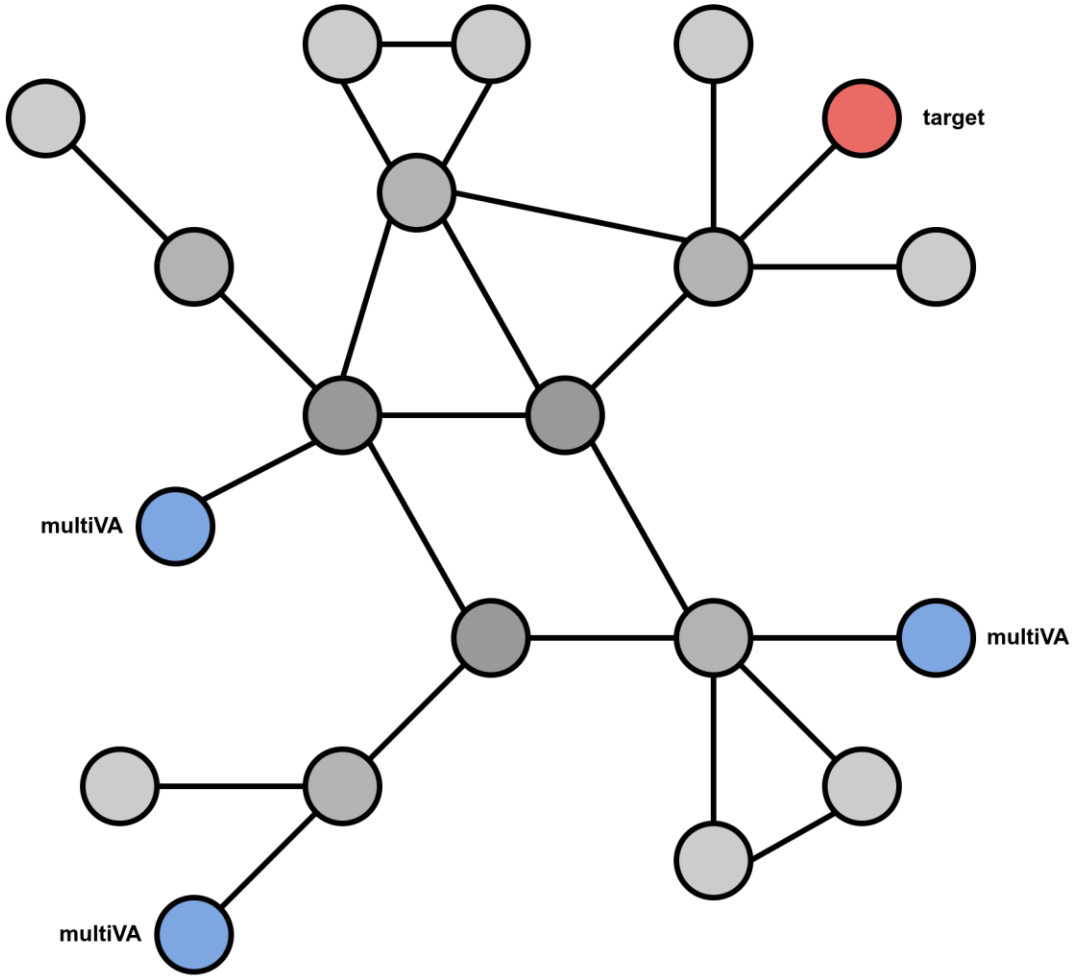
BGP collector data:
RIPE RIS
RouteViews.org
+
CAIDA AS Relationships



Routing Simulation

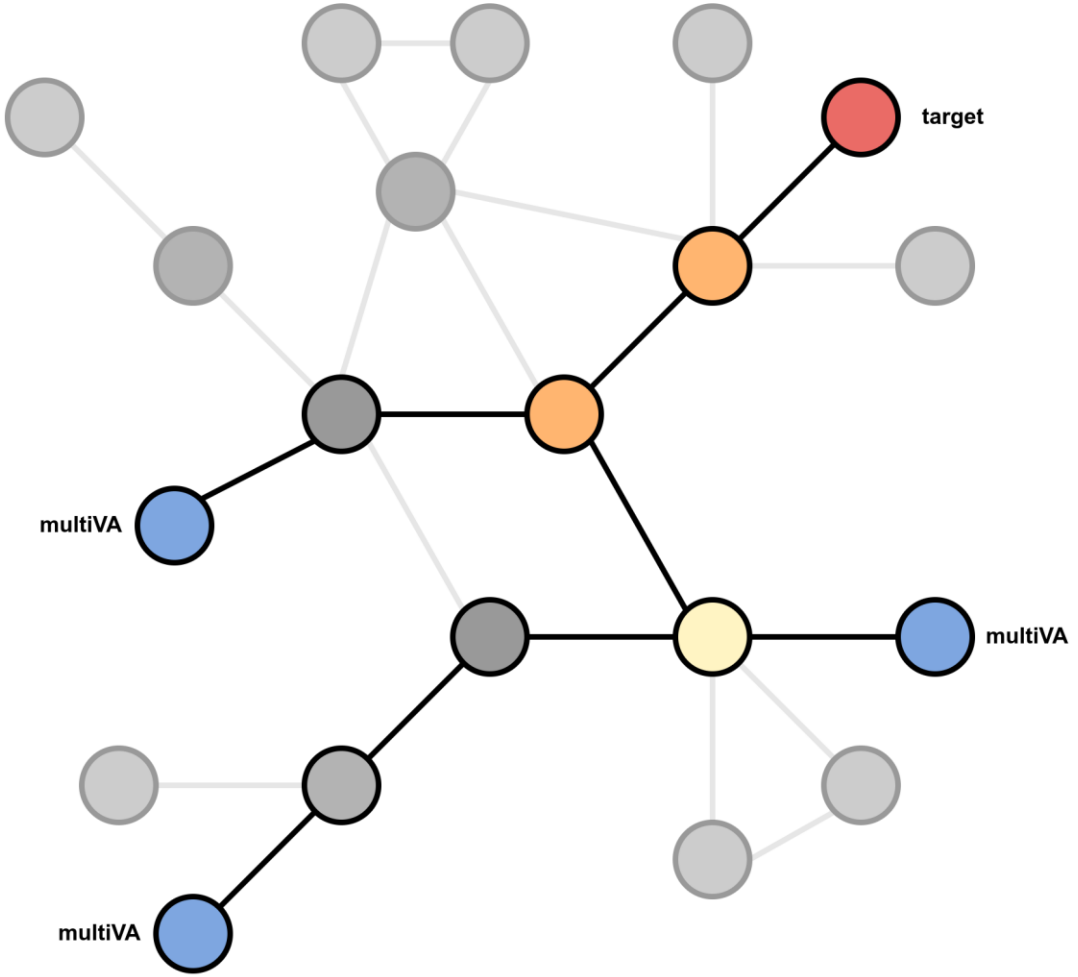
Determine **AS** from recorded **IP** address

for **target** domains and **validators**



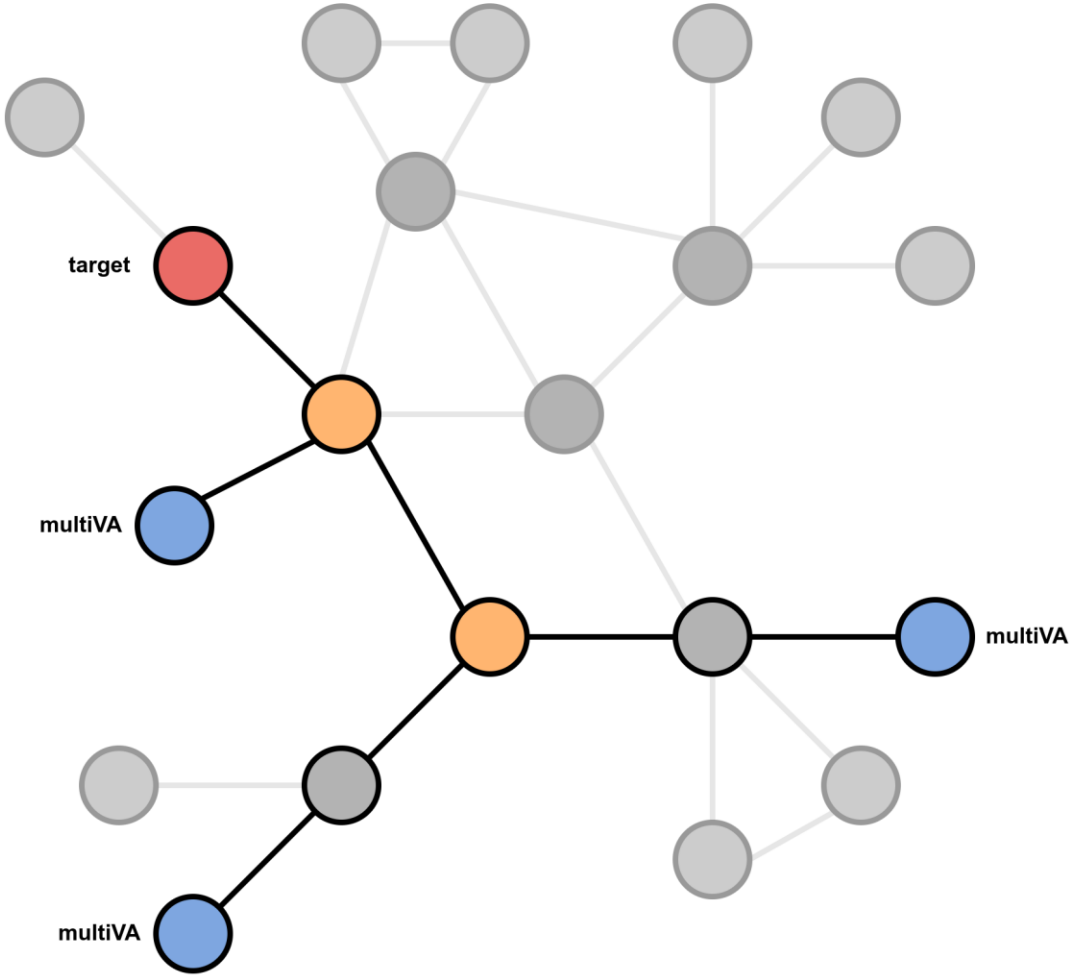
Routing Simulation

Simulate **paths** of validation traffic
for various targets



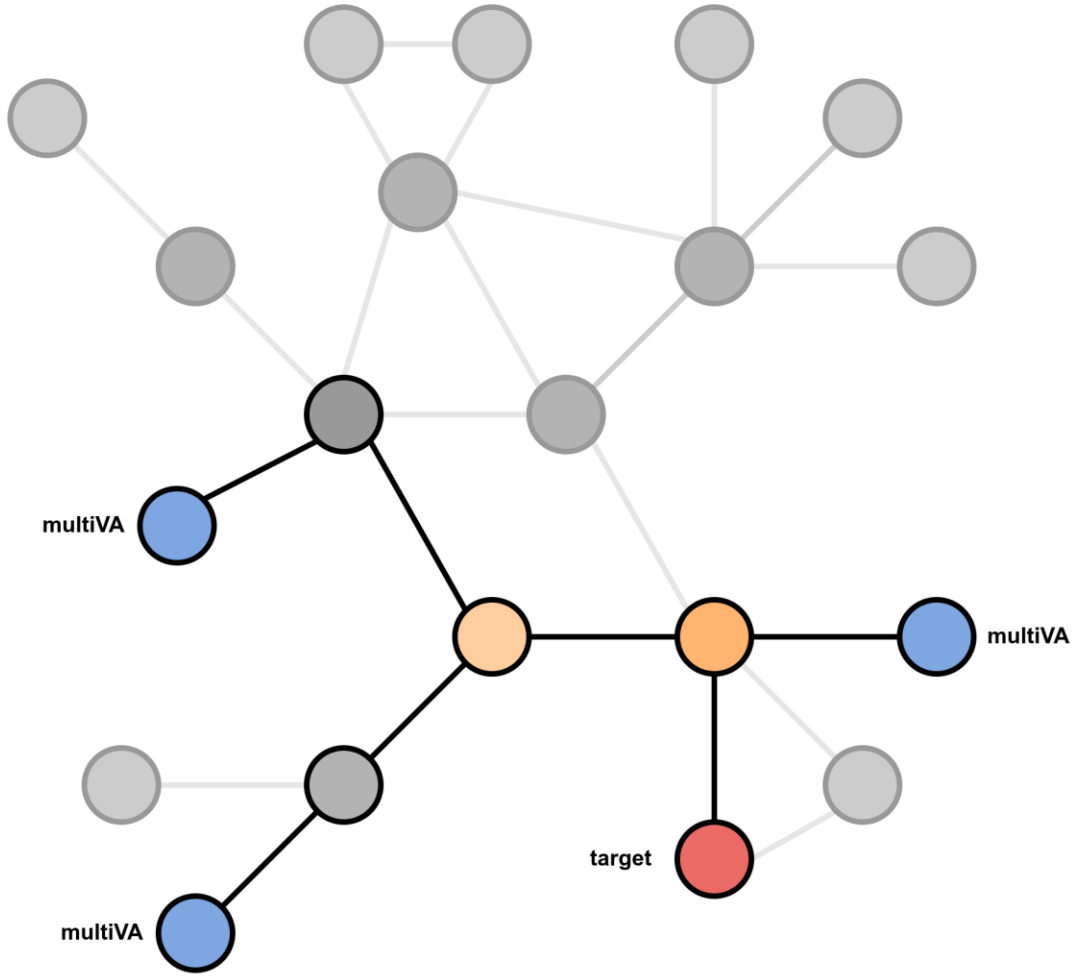
Routing Simulation

Simulate **paths** of validation traffic
for various targets

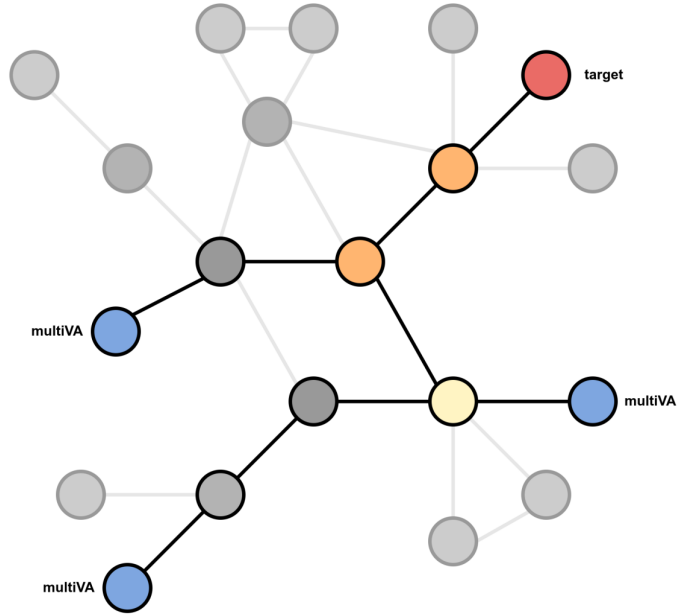


Routing Simulation

Simulate **paths** of validation traffic
for various targets

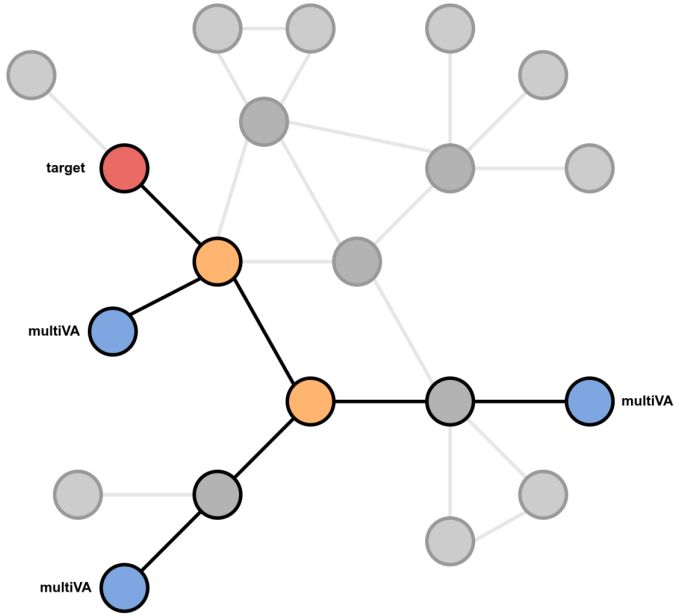


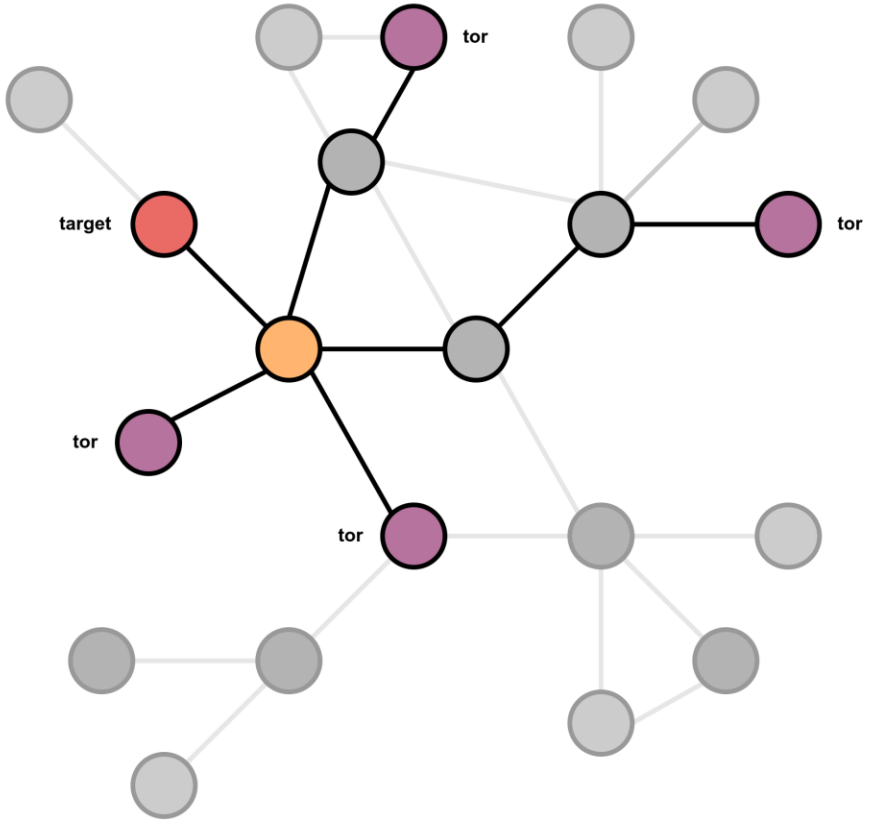
Comparison



path overlap	**0.48**	**0.43**
100% intercept	**2**	**1**

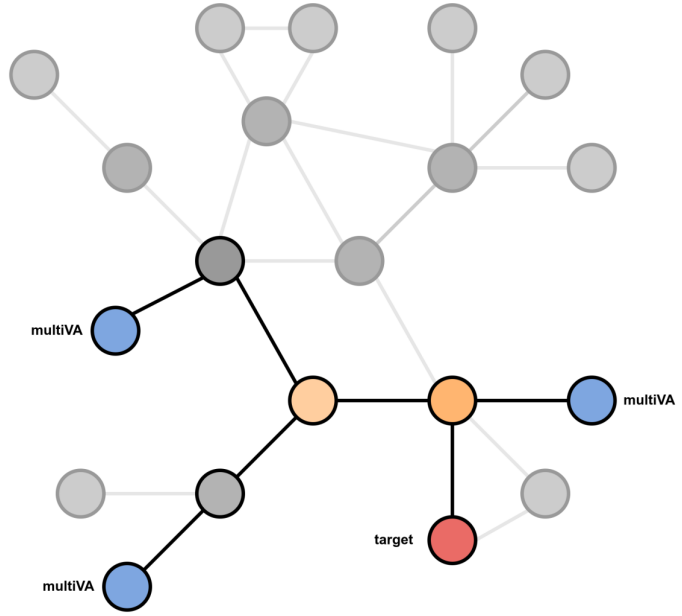
Comparison

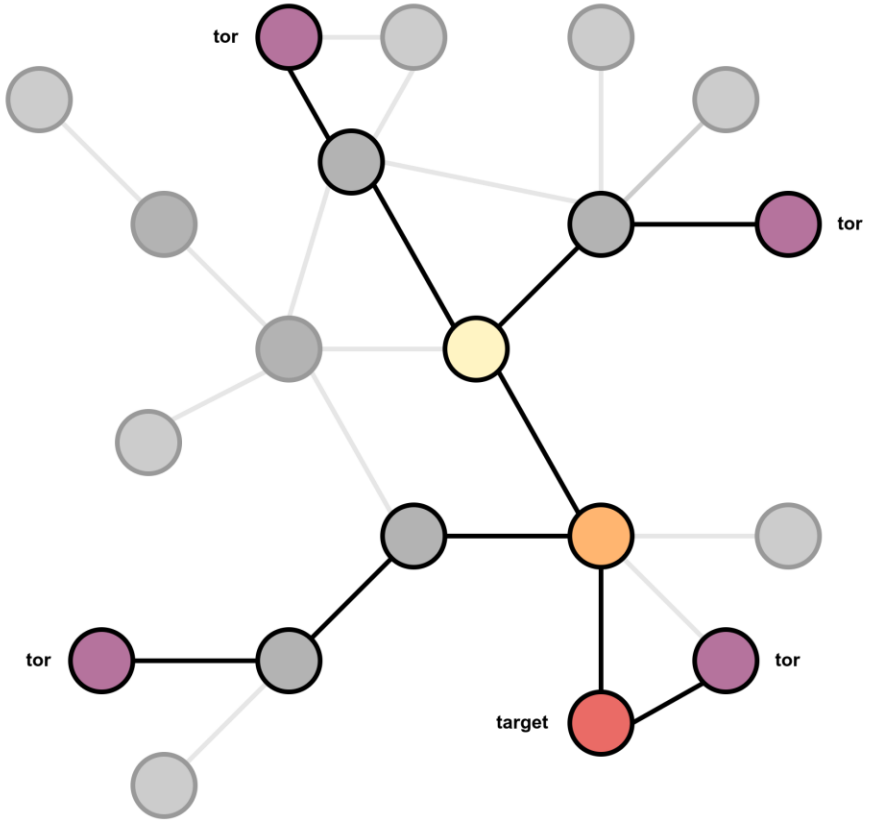




path overlap	**0.61**	**0.48**
100% intercept	**1**	**1**

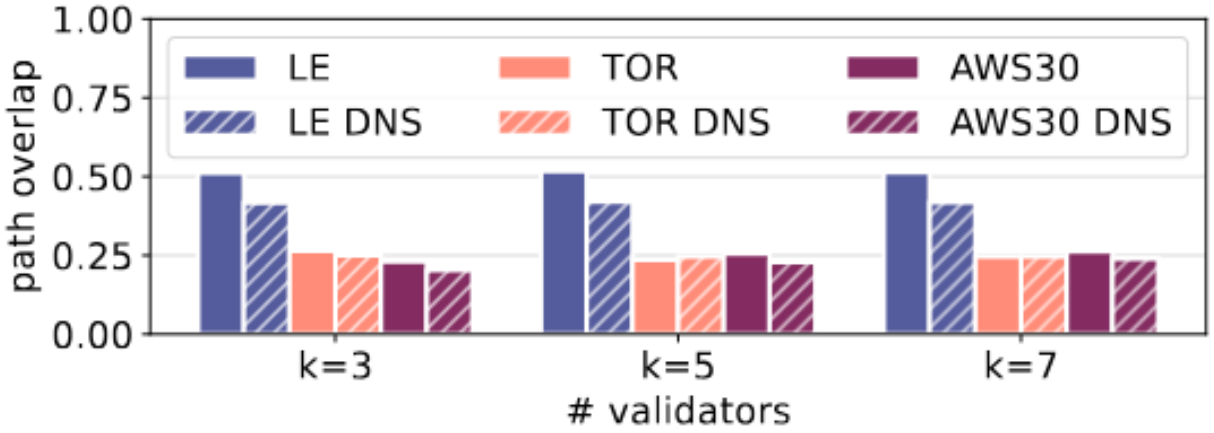
Comparison



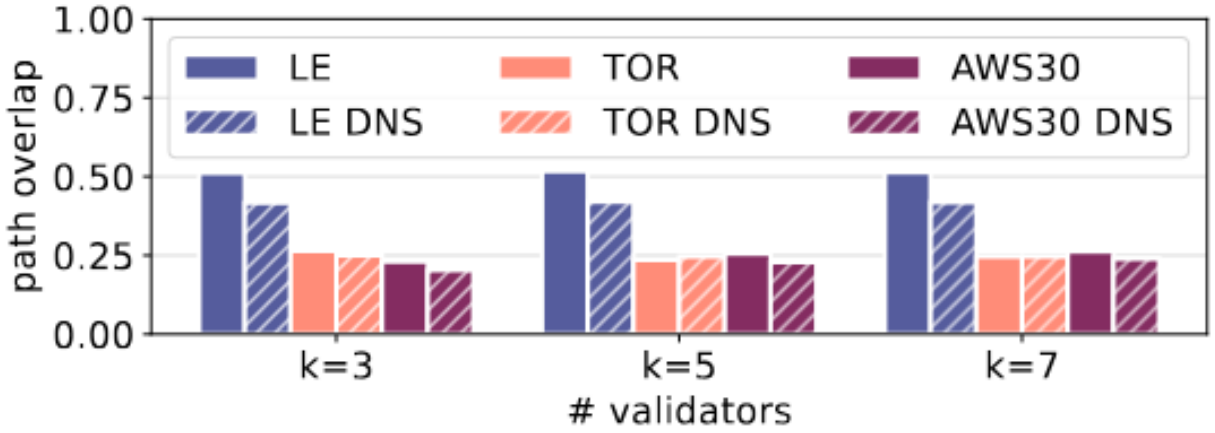


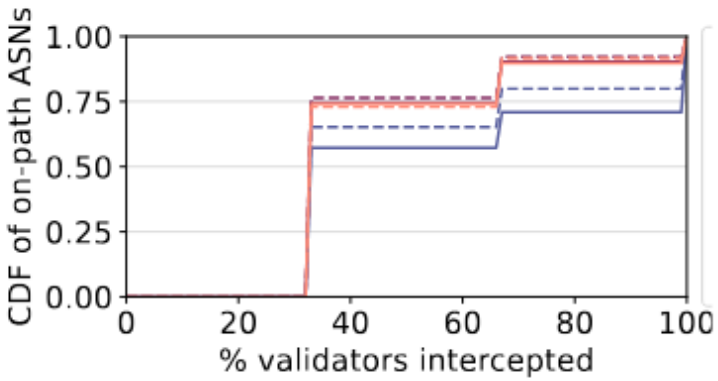
path overlap	**0.39**	**0.15**
100% intercept	**1**	**0**

Results

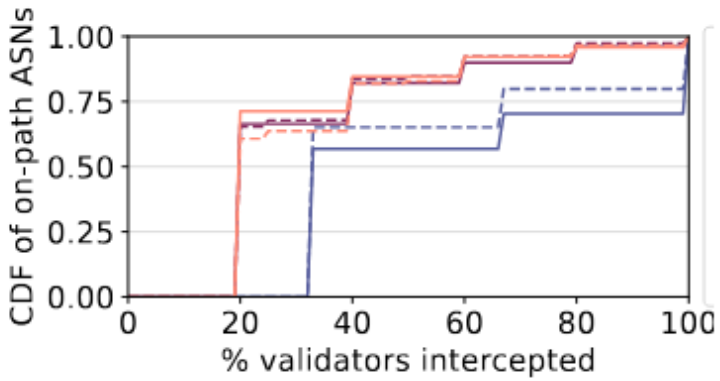

1.00
0.75
0.50
0.25
0.00
path overlap
LE
LE DNS
TOR
TOR DNS
AWS30
AWS30 DNS
k=3
k=5
k=7
# validators

Results

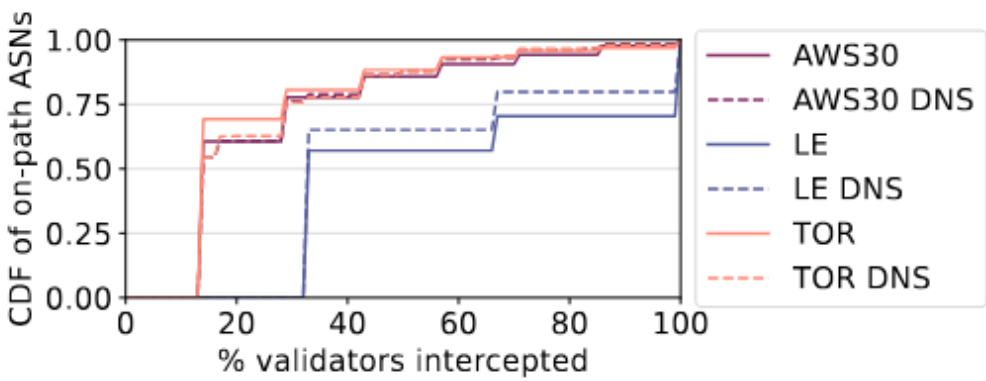




k=3

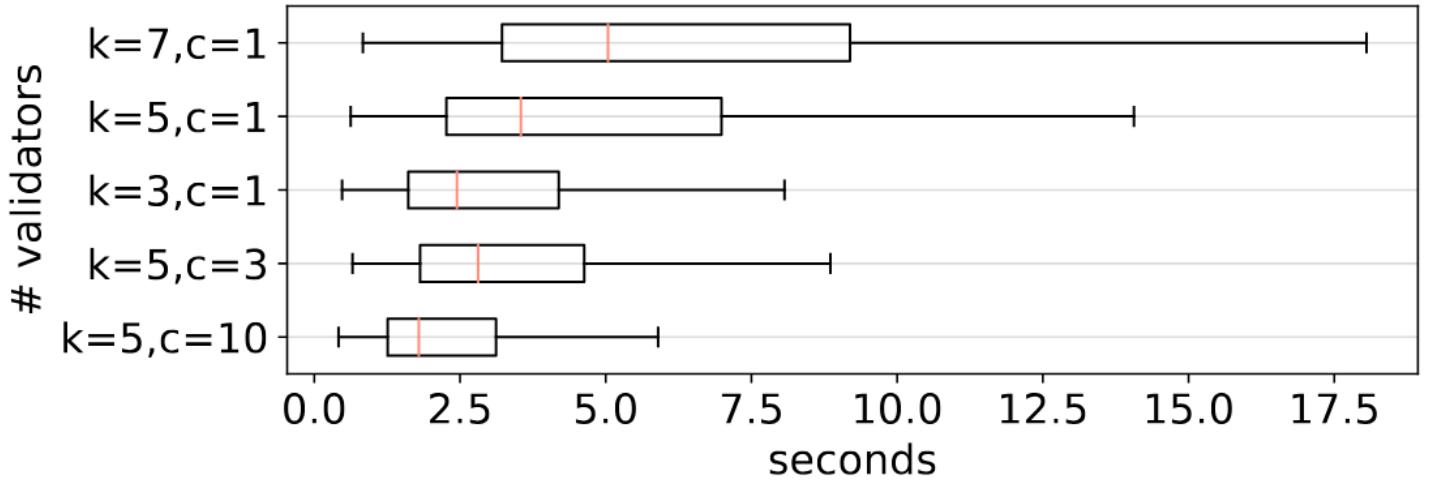


k=5



k=7

Performance?



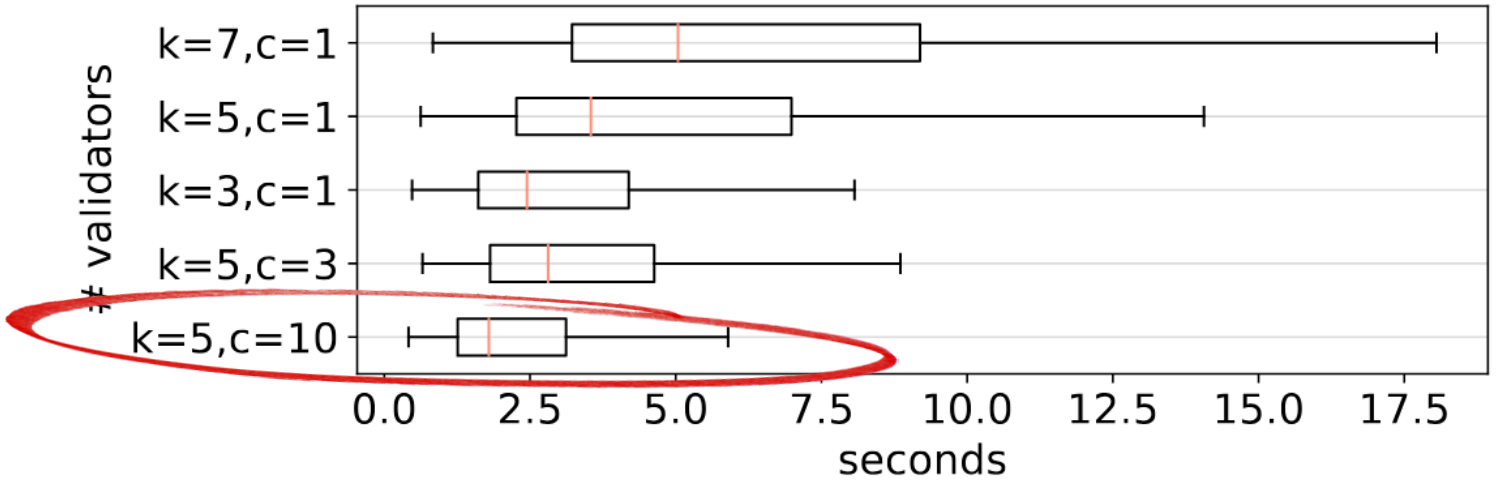
containers	k	validations / s
1	3	2.7
1	5	2.1
1	7	1.6

containers	k	validations / s
3	5	6.5
10	5	11.9

Table 1: Validation throughput.

on Tranco Top 100K

Performance?



containers	k	validations / s
1	3	2.7
1	5	2.1
1	7	1.6

containers	k	validations / s
3	5	6.5
10	5	11.9

Table 1: Validation throughput.

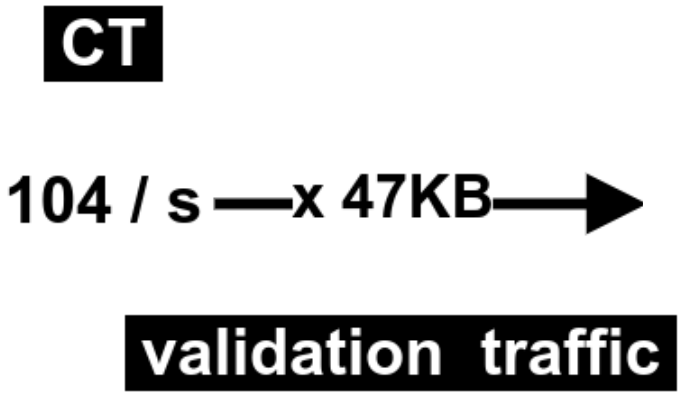
on Tranco Top 100K

But what about the load on Tor?

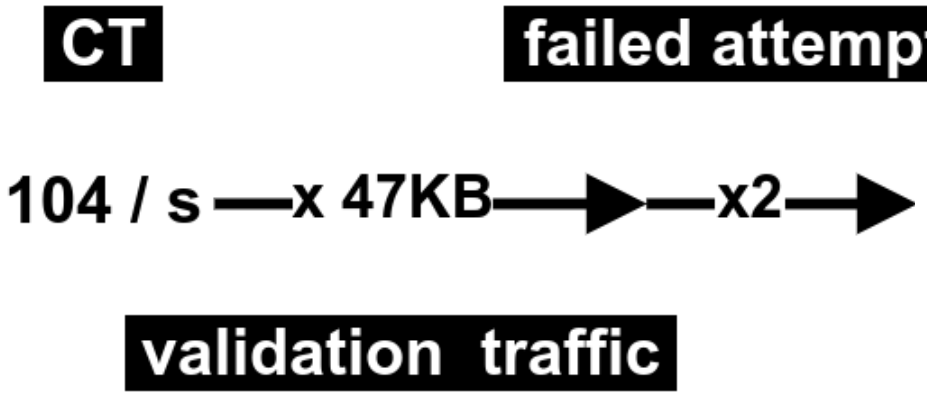
CT

104 / s

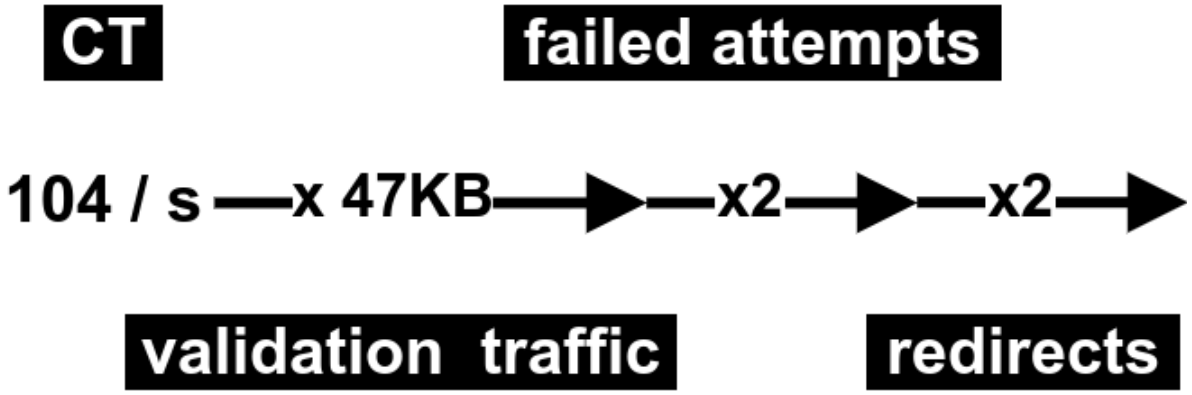
But what about the load on Tor?



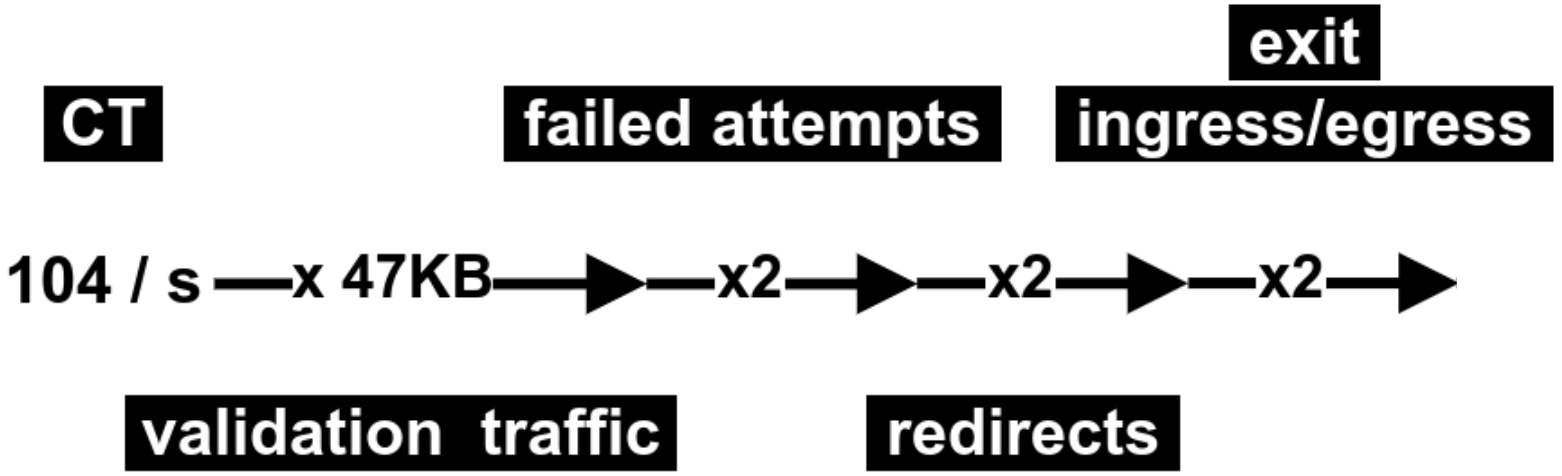
But what about the load on Tor?



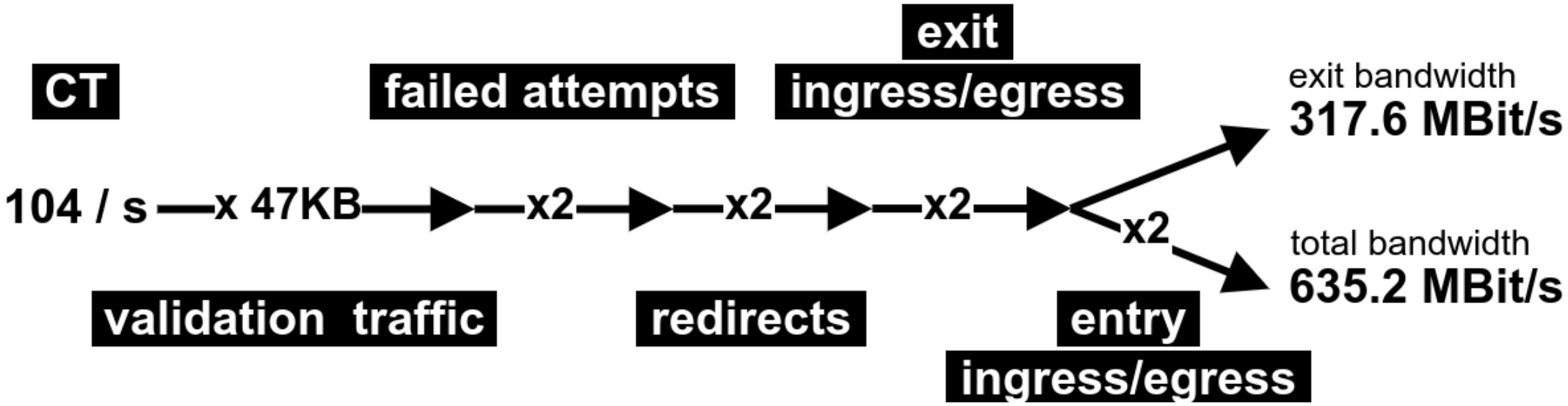
But what about the load on Tor?



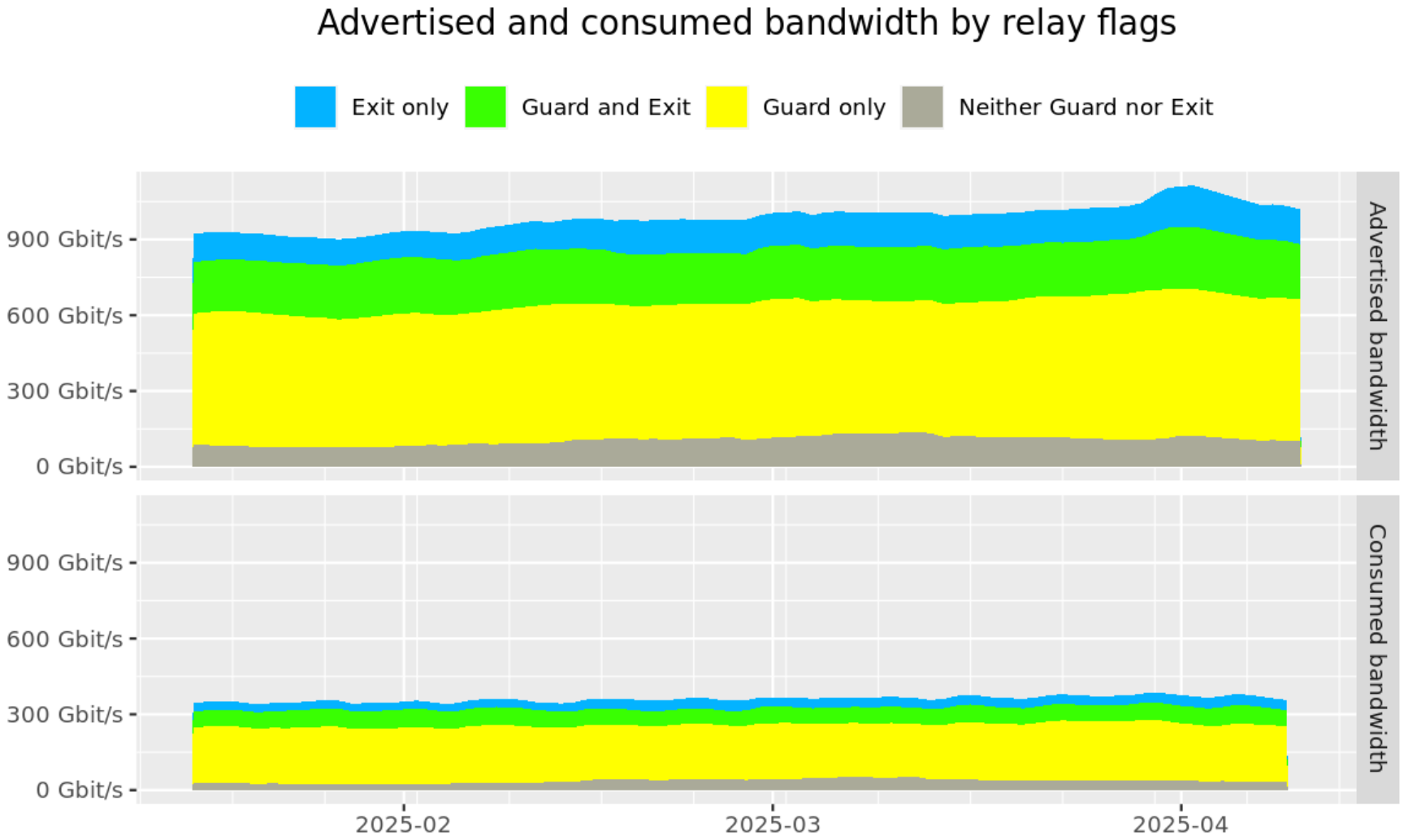
But what about the load on Tor?



But what about the load on Tor?



But what about the load on Tor?

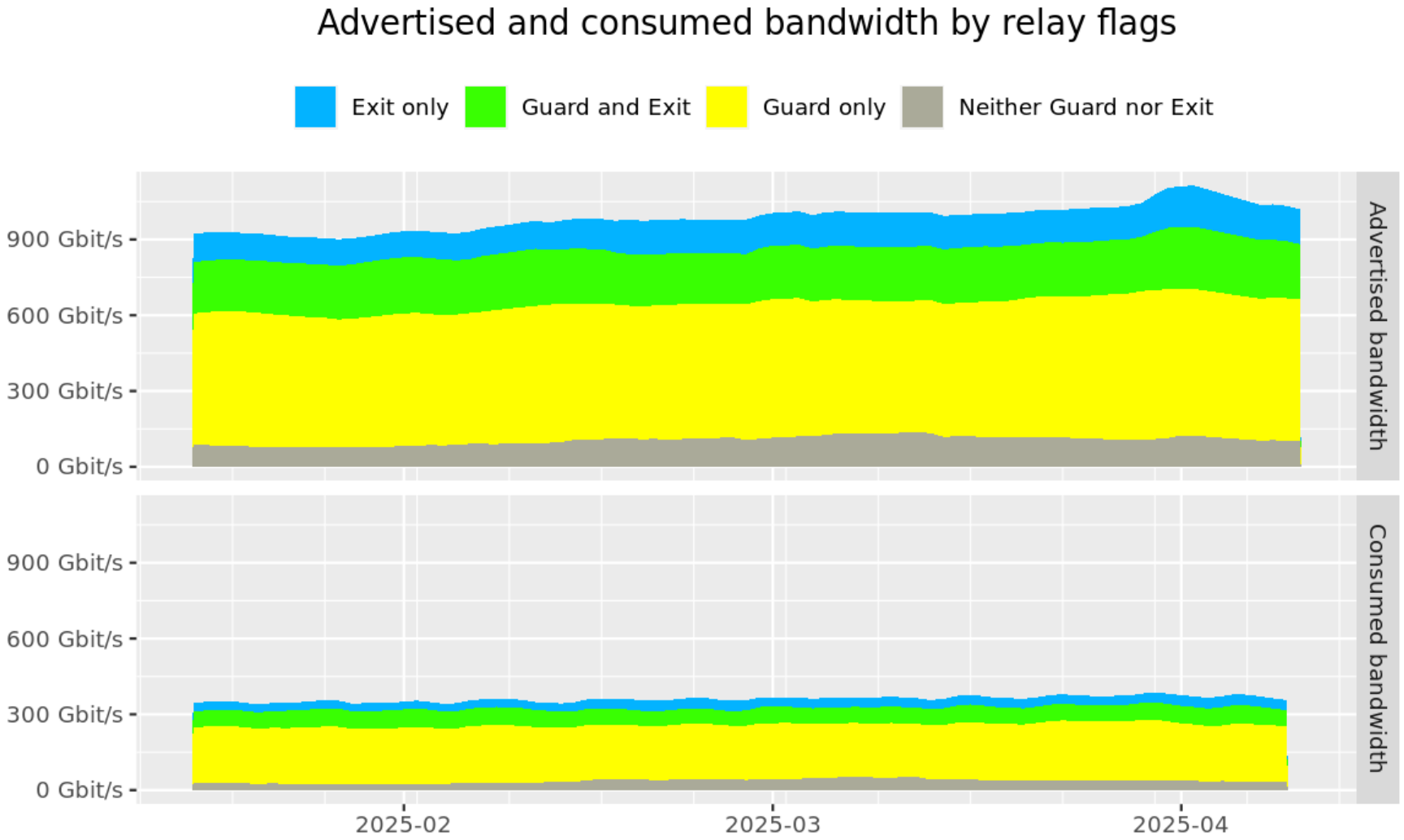


exit bandwidth
317.6 MBit/s

total bandwidth
635.2 MBit/s

The Tor Project - https://metrics.torproject.org/

But what about the load on Tor?



The Tor Project - https://metrics.torproject.org/

0.15% exit bandwidth **317.6 MBit/s**

0.11% total bandwidth **635.2 MBit/s**

of *remaining* available bandwidth

What about malicious nodes?

probability of fraudulent validation ***p*** with:

***M* malicious** nodes
out of ***N* total** nodes
using ***k*-out-of-*n*** validation

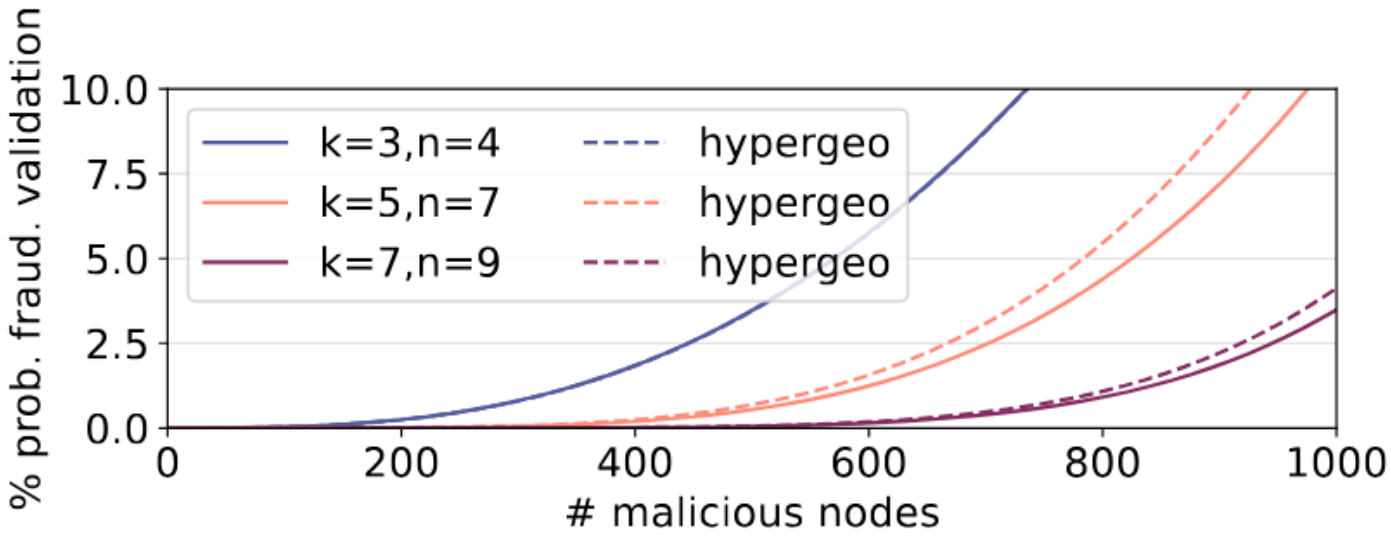
$$p(M,N,n,k) = \sum_{j=k-(n-k)}^{k} \binom{k}{j} \left(\frac{M}{N}\right)^{k} \left(1 - \frac{M}{N}\right)^{k-j}$$

What about malicious nodes?

probability of fraudulent validation ***p*** with:

***M* malicious** nodes
out of ***N* total** nodes
using ***k*-out-of-*n*** validation

$$p(M,N,n,k) = \sum_{j=k-(n-k)}^{k} \binom{k}{j} \left(\frac{M}{N}\right)^k \left(1-\frac{M}{N}\right)^{k-j}$$



What about malicious nodes?

Thousands of Tor exit nodes attacked cryptocurrency users over the past year

For more than 16 months, a threat actor has been seen adding malicious servers to the Tor network in order to intercept traffic and perform SSL stripping attacks on users accessing cryptocurrency-related sites.

...

This most recent attack was spotted within a day after it increased the Tor network's exit capacity from around its daily 1,500 exit relays to more than 2,500, a spike that nobody could ignore inside the Tor Project.

What about malicious nodes?

Thousands of Tor exit nodes attacked cryptocurrency users over the past year

For more than 16 months, a threat actor has been seen adding malicious servers to the Tor network in order to intercept traffic and perform SSL stripping attacks on users accessing cryptocurrency-related sites.

...

This most recent attack was spotted within a day after it increased the Tor network's exit capacity from around its daily 1,500 exit relays to more than 2,500, a spike that nobody could ignore inside the Tor Project.

$$p(1000, 2500, \mathbf{4}, \mathbf{3}) = \sum_{j=k-(n-k)}^{k} \binom{k}{j} \left(\frac{M}{N}\right)^{k} \left(1 - \frac{M}{N}\right)^{k-j} = \mathbf{17.9\%}$$

What about malicious nodes?

Thousands of Tor exit nodes attacked cryptocurrency users over the past year

For more than 16 months, a threat actor has been seen adding malicious servers to the Tor network in order to intercept traffic and perform SSL stripping attacks on users accessing cryptocurrency-related sites.

...

This most recent attack was spotted within a day after it increased the Tor network's exit capacity from around its daily 1,500 exit relays to more than 2,500, a spike that nobody could ignore inside the Tor Project.

$$p(1000, 2500, \mathbf{7}, \mathbf{5}) = \sum_{j=k-(n-k)}^{k} \binom{k}{j} \left(\frac{M}{N}\right)^{k} \left(1 - \frac{M}{N}\right)^{k-j} = \mathbf{7.8\%}$$

What about malicious nodes?

Thousands of Tor exit nodes attacked cryptocurrency users over the past year

For more than 16 months, a threat actor has been seen adding malicious servers to the Tor network in order to intercept traffic and perform SSL stripping attacks on users accessing cryptocurrency-related sites.

...

This most recent attack was spotted within a day after it increased the Tor network's exit capacity from around its daily 1,500 exit relays to more than 2,500, a spike that nobody could ignore inside the Tor Project.

$$p(1000, 2500, \mathbf{9}, \mathbf{7}) = \sum_{j=k-(n-k)}^{k} \binom{k}{j} \left(\frac{M}{N}\right)^{k} \left(1 - \frac{M}{N}\right)^{k-j} = 2.1\%$$

What about malicious nodes?

Thousands of Tor exit nodes attacked cryptocurrency users over the past year

For more than 16 months, a threat actor has been seen adding malicious servers to the Tor network in order to intercept traffic and perform SSL stripping attacks on users accessing cryptocurrency-related sites.

...

This most recent attack was spotted within a day after it increased the Tor network's exit capacity from around its daily 1,500 exit relays to more than 2,500, a spike that nobody could ignore inside the Tor Project.

$$p(1000, 2500, \mathbf{11}, \mathbf{9}) = \sum_{j=k-(n-k)}^{k} \binom{k}{j} \left(\frac{M}{N}\right)^k \left(1 - \frac{M}{N}\right)^{k-j} = \mathbf{0.5\%}$$

What about malicious nodes?

Thousands of Tor exit nodes attacked cryptocurrency users over the past year

For more than 16 months, a threat actor has been seen adding malicious servers to the Tor network in order to intercept traffic and perform SSL stripping attacks on users accessing cryptocurrency-related sites.

...

This most recent attack was spotted within a day after it increased the Tor network's exit capacity from around its daily 1,500 exit relays to more than 2,500, a spike that nobody could ignore inside the Tor Project.

$$p(1000, \mathbf{3293}, 11, 9) = \sum_{j=k-(n-k)}^{k} \binom{k}{j} \left(\frac{M}{N}\right)^{k} \left(1 - \frac{M}{N}\right)^{k-j} = \mathbf{0.05\%}$$

Thank you!

jens.friess@athene-center.de

github.com/jenfrie/tova

Extra Slides

Why  ?

Why ?

cloud?

Why ?

" In **2019** Let's Encrypt **will** secure a massive portion of the Web with a budget of only **$3.6M**. "

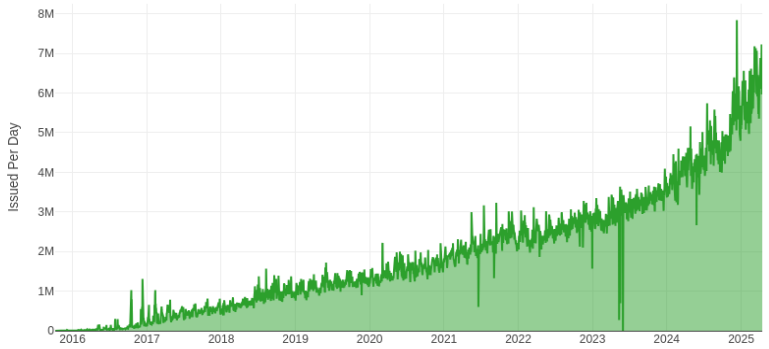
Here's how our 2017 budget breaks down:

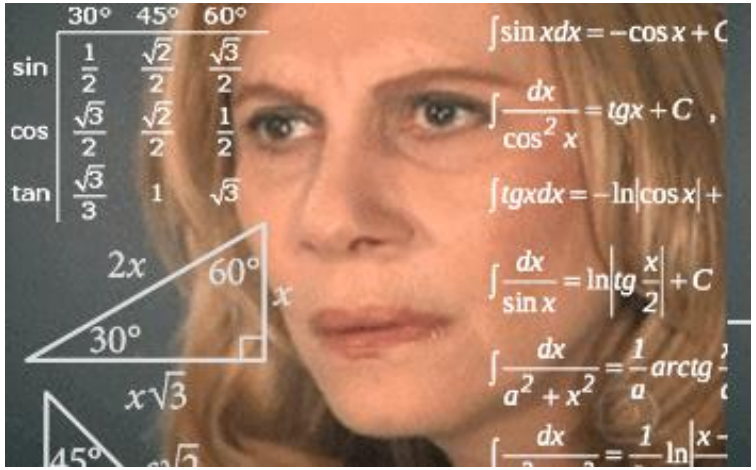
Expense	Cost
Staffing	$2.06M USD
Hardware/Software	$0.20M USD
Hosting/Auditing	$0.30M USD
Legal/Administrative	$0.35M USD
Total	$2.91M USD

cloud?

Microsoft Azure aws

Let's Encrypt Certificates Issued Per Day





Why ?

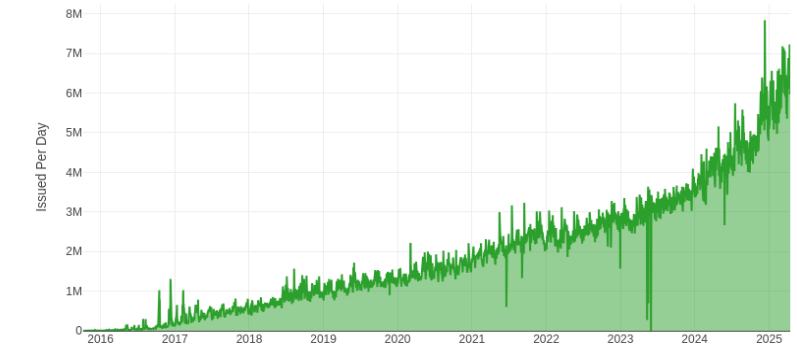
" In **2019** Let's Encrypt **will** secure a massive portion of the Web with a budget of only **$3.6M**. "

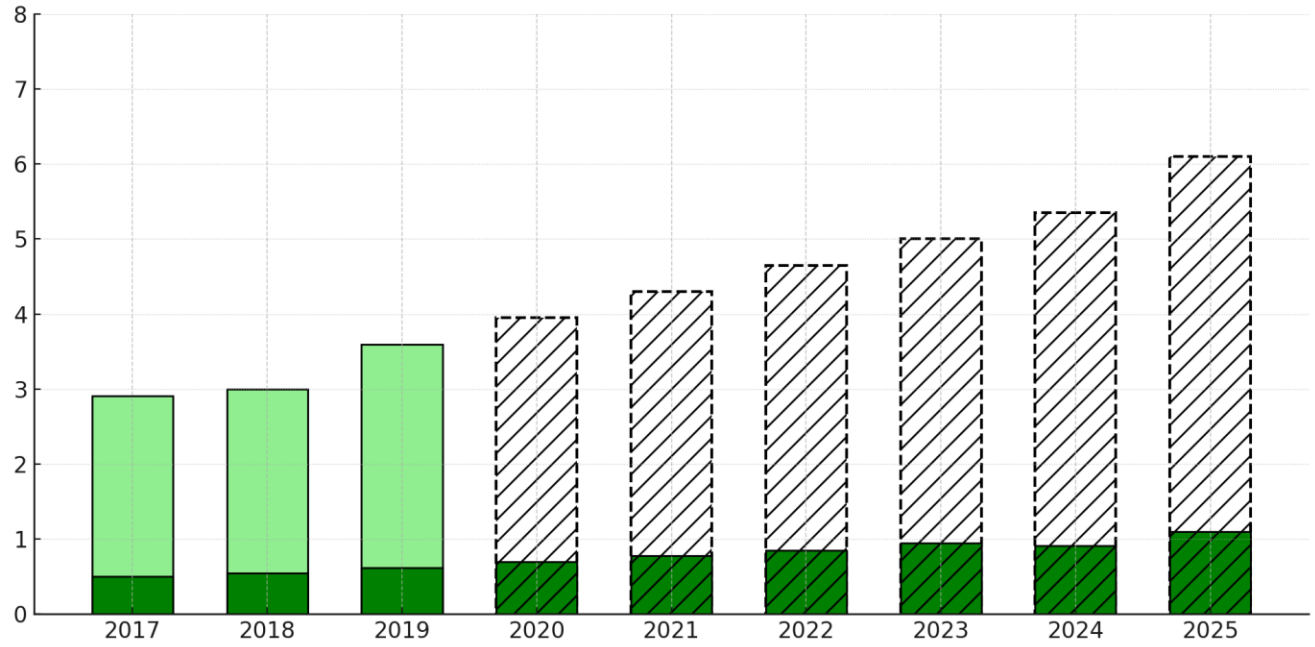
Here's how our 2017 budget breaks down:

Expense	Cost
Staffing	$2.06M USD
Hardware/Software	$0.20M USD
Hosting/Auditing	$0.30M USD
Legal/Administrative	$0.35M USD
Total	$2.91M USD

cloud?

Microsoft Azure aws





Why ?

" In **2019** Let's Encrypt **will** secure a massive portion of the Web with a budget of only **$3.6M**. "

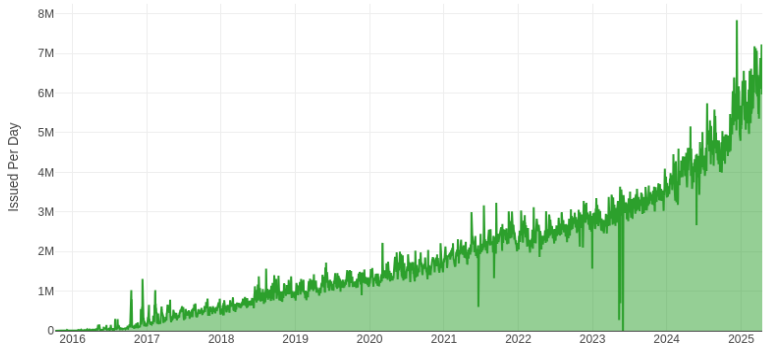
Here's how our 2017 budget breaks down:

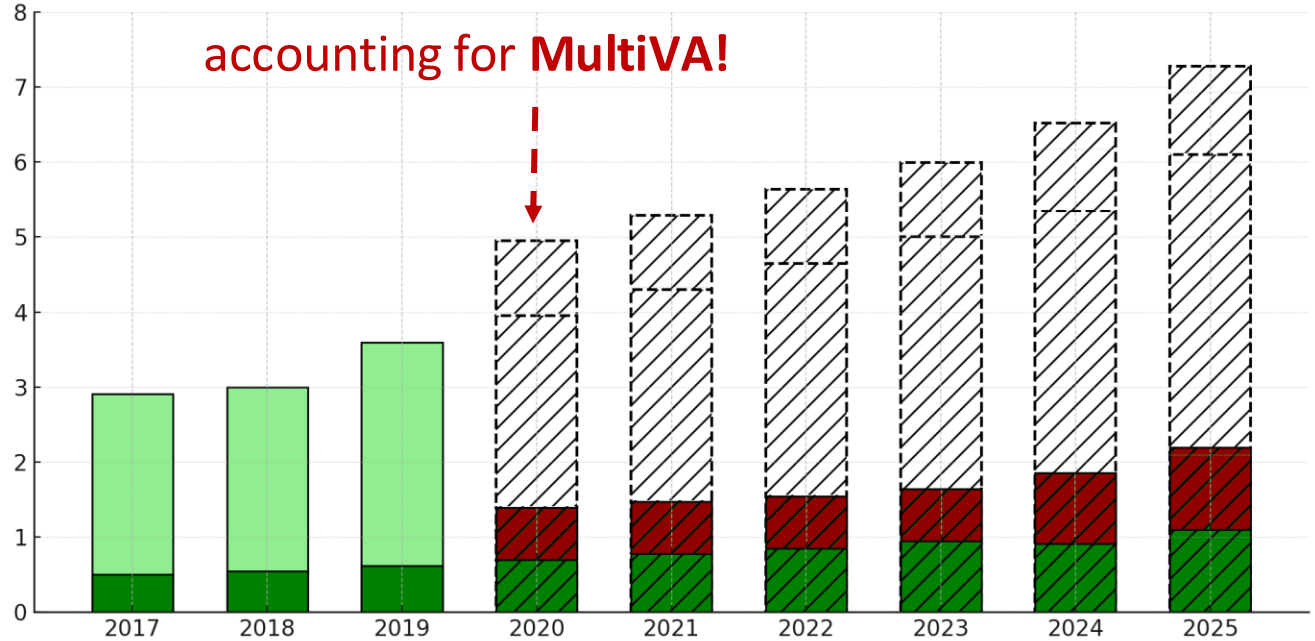
Expense	Cost
Staffing	$2.06M USD
Hardware/Software	$0.20M USD
Hosting/Auditing	$0.30M USD
Legal/Administrative	$0.35M USD
Total	$2.91M USD

cloud?

Microsoft Azure aws

Let's Encrypt Certificates Issued Per Day





Why ?

cloud?

Microsoft Azure

aws

residential proxies?

bright data

smartproxy

oxylabs

Why ?

cloud?

Microsoft Azure aws

$0.42/GB x ~317 MBit/s

= ~$4.2M/year

residential proxies?

bright data smartproxy

oxylabs

Why ?

cloud?

Microsoft Azure aws

public VPNs?

ExpressVPN NordVPN

residential proxies?

bright data smartproxy

oxylabs

~$100/year, "unlimited bandwidth"…
… but 1.1TB/h likely violates ToS

Why ?

cloud?

Microsoft Azure aws

public VPNs?

ExpressVPN NordVPN

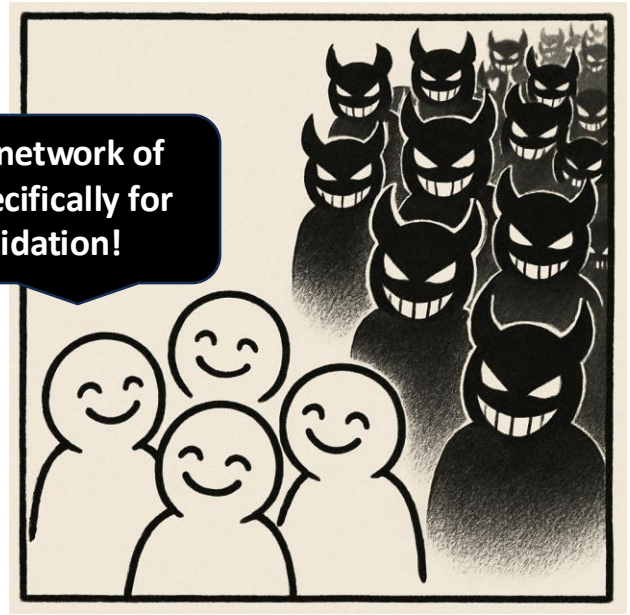
residential proxies?

bright data smartproxy oxylabs

other anonymity networks?

NYM I2P

fewer proxies, lower capacity, pricier



Why Tor?

cloud?

Microsoft Azure aws

dedicated volunteer networks?

RIPE Atlas NLNOG RING

public VPNs?

ExpressVPN NordVPN

residential proxies?

bright data smartproxy oxylabs

other anonymity networks?

NYM I2P

Why ?

cloud?

Microsoft Azure aws

dedicated volunteer networks?

RIPE Atlas NLNOG RING

public VPNs?

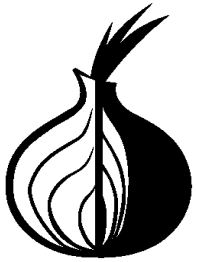
ExpressVPN NordVPN

residential proxies?

bright data smartproxy oxylabs

other anonymity networks?

NYM I2P



Free

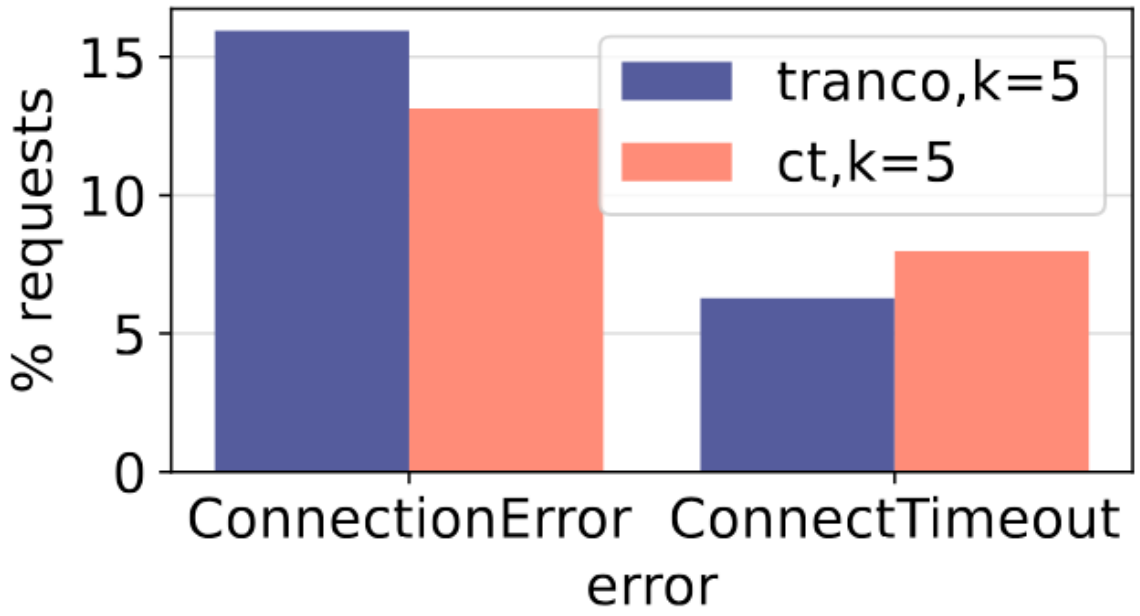
High Capacity

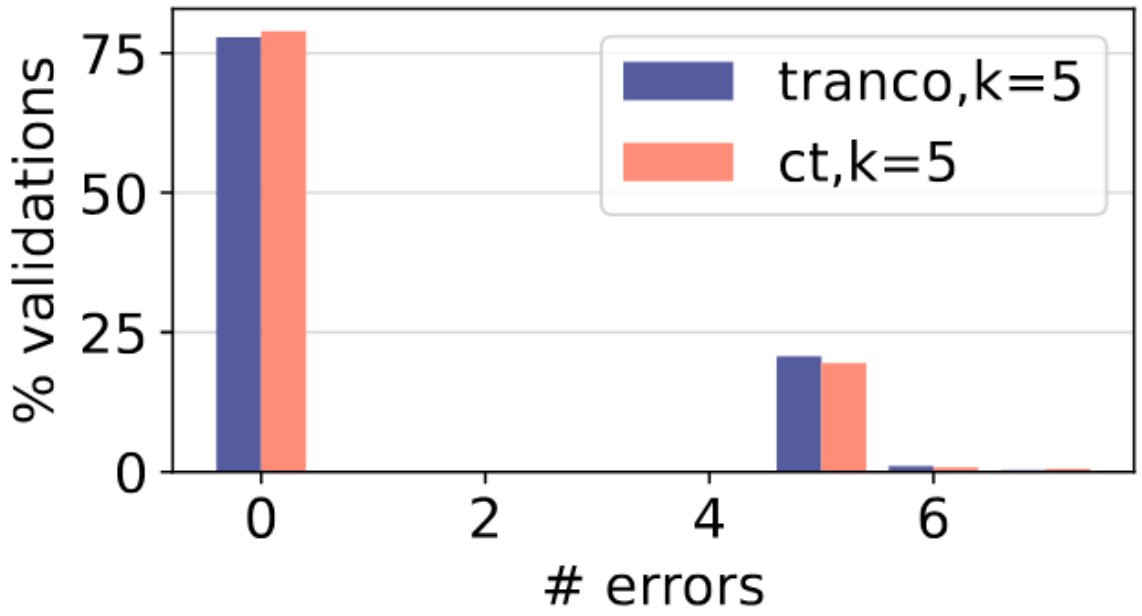
Many Nodes

Monitored

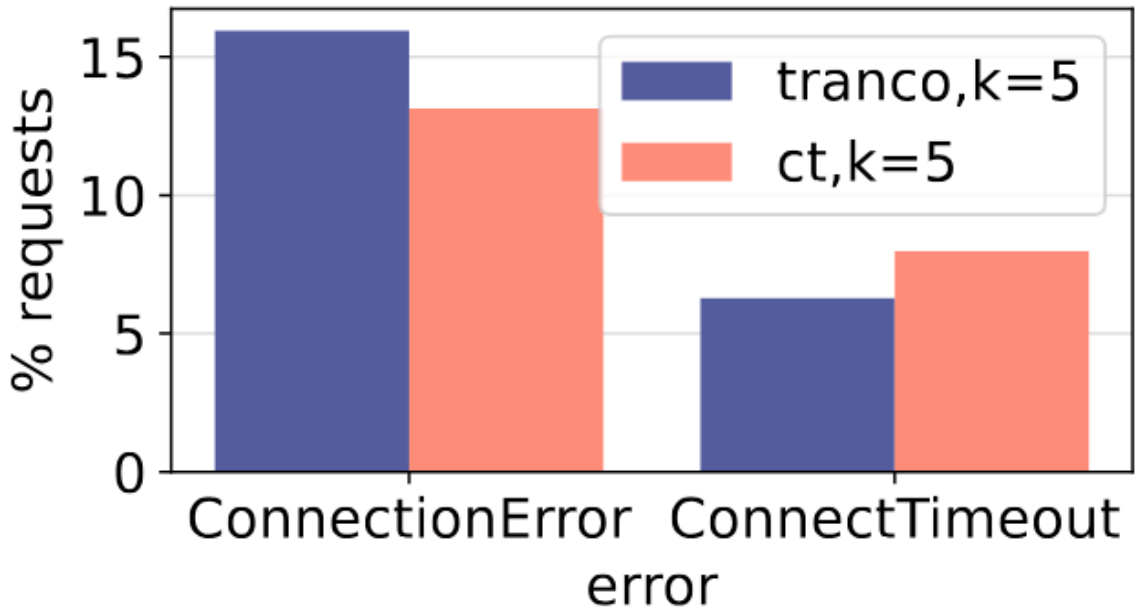
Easy to Study

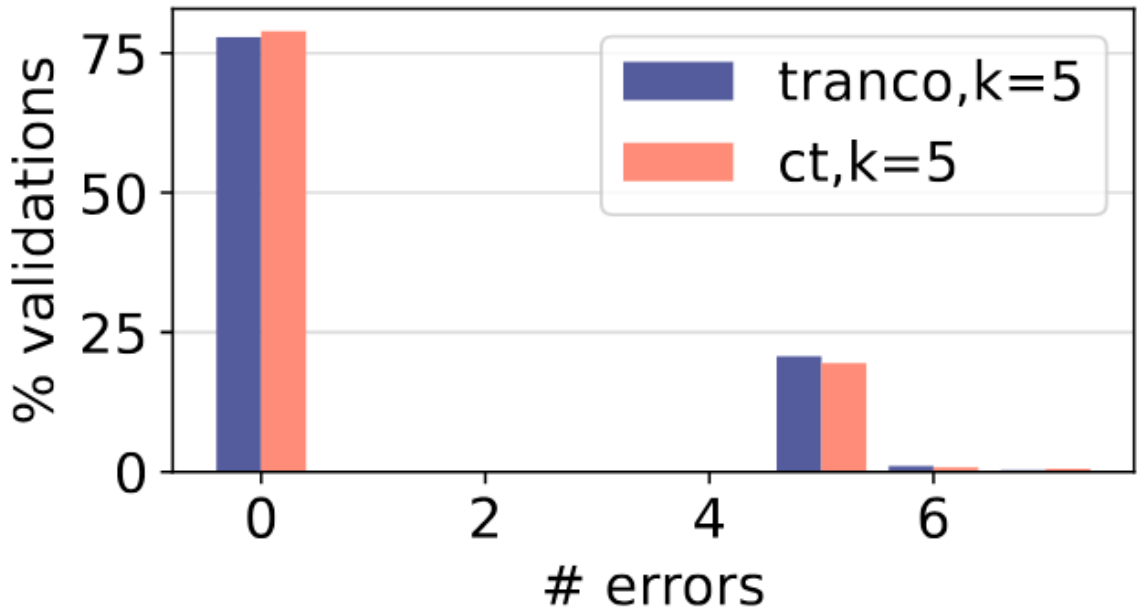
But what about networks blocking Tor?





But what about networks blocking Tor?

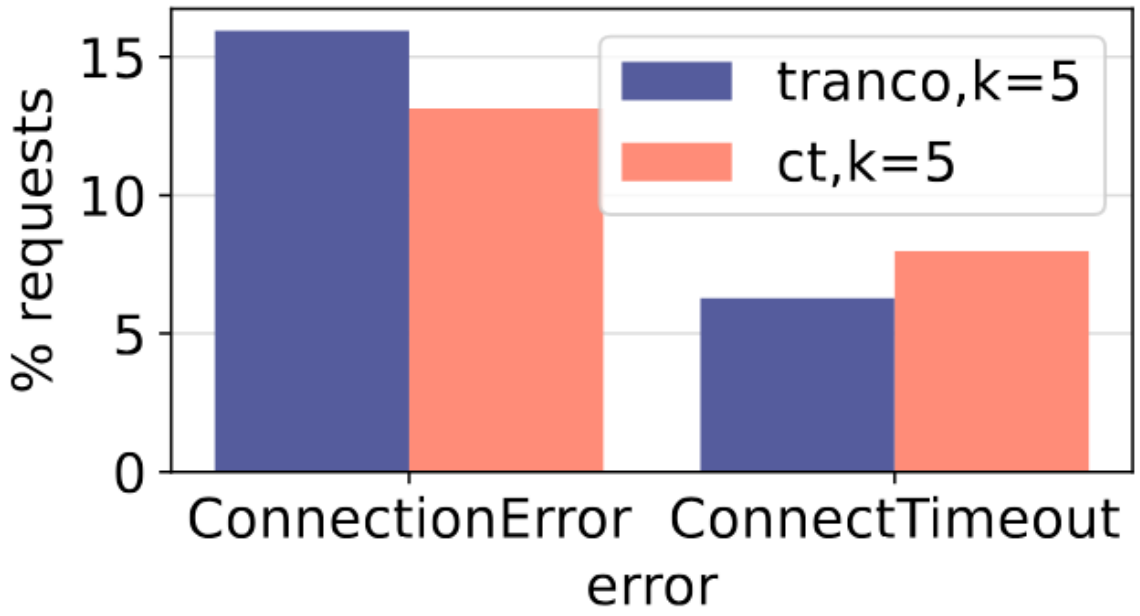


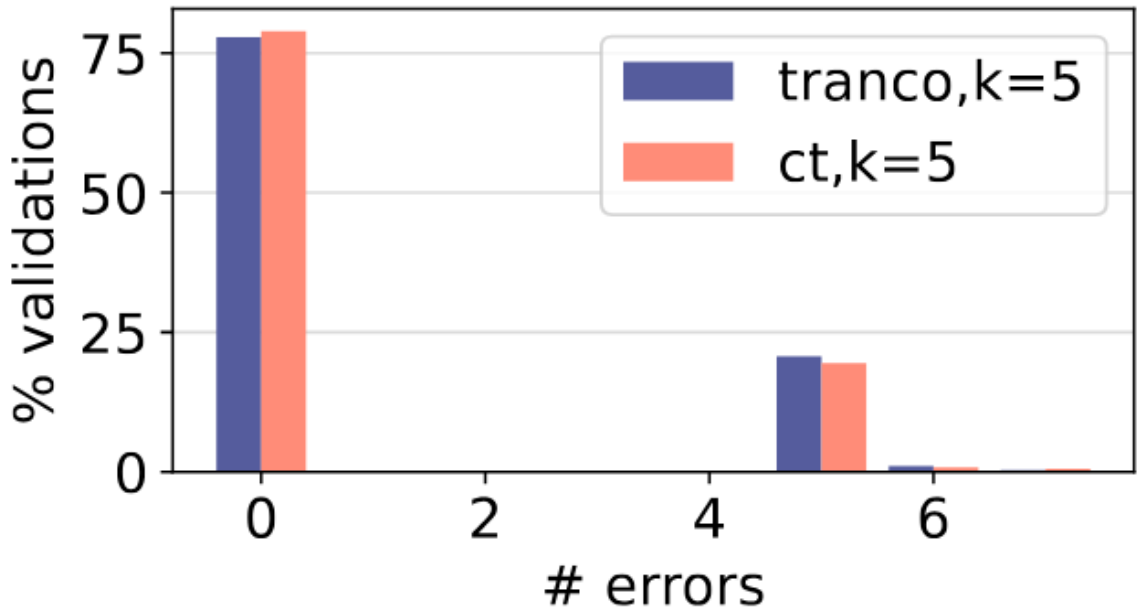


Only **~1.3%** of traversed ASes
consistenly implicated in **failed requests**

Only **~0.2%** are **transit** ASes

But what about networks blocking Tor?





Only **~1.3%** of traversed ASes
consistenly implicated in **failed requests**

Only **~0.2%** are **transit** ASes

Virtually **no "partial"** failures

If Tor is **blocked**, then by the **target** server

How many nodes for a cloud deployment?

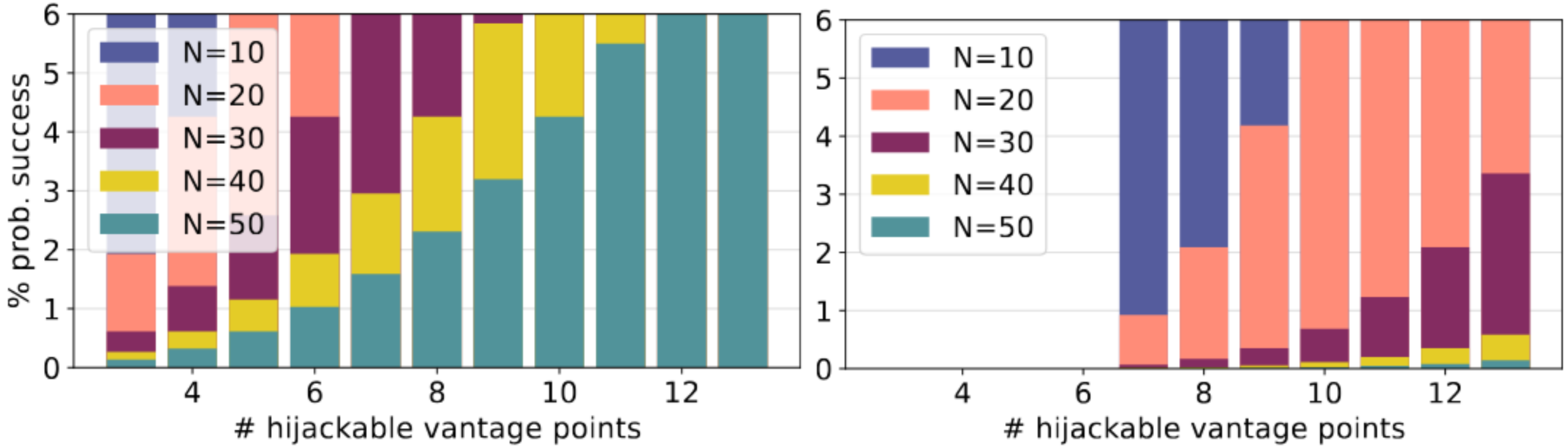


Figure 8: Probability of fraudulent validation by hijacking cloud vantage points, using $k = 3$ (left) and $k = 7$ (right) validators.