Multi-operator DNSSEC signing system

Kris Shrishak

TU Darmstadt

ICANN69

Based on work published at ESORICS'20
with Anders Dalskov, Marcel Keller, Claudio Orlandi and Haya Shulman

Outline

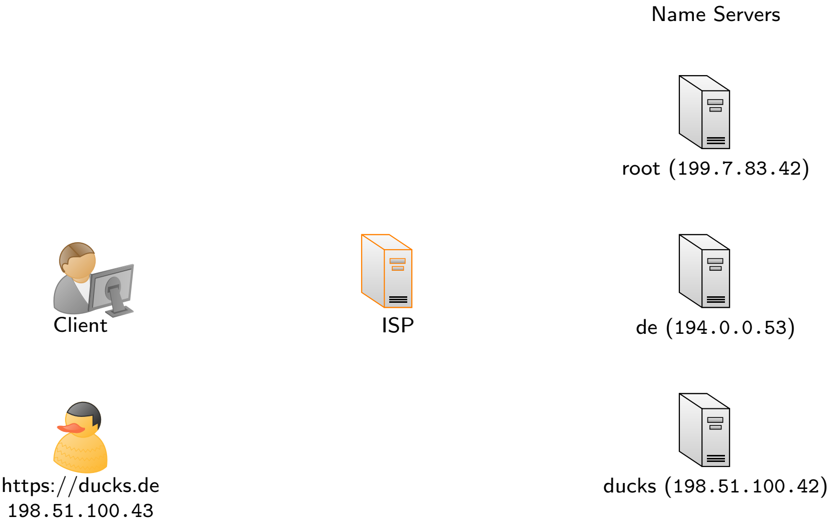
DNS

DNSSEC

Multi-operator DNSSEC signing system

DNS resolution

DNS is a protocol for mapping names to addresses



Name Servers

root (199.7.83.42)

Client

ISP

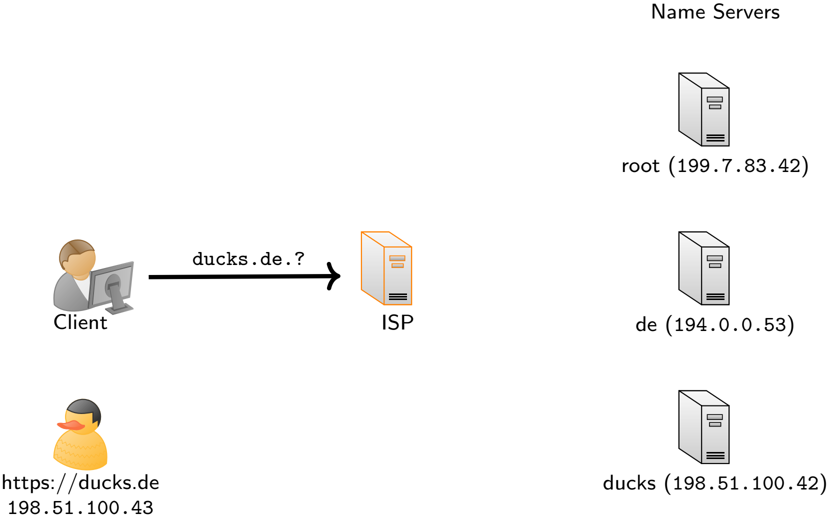
de (194.0.0.53)

https://ducks.de
198.51.100.43

ducks (198.51.100.42)

DNS resolution

Recursive query to the ISP



Name Servers

root (199.7.83.42)

de (194.0.0.53)

ducks (198.51.100.42)

Client

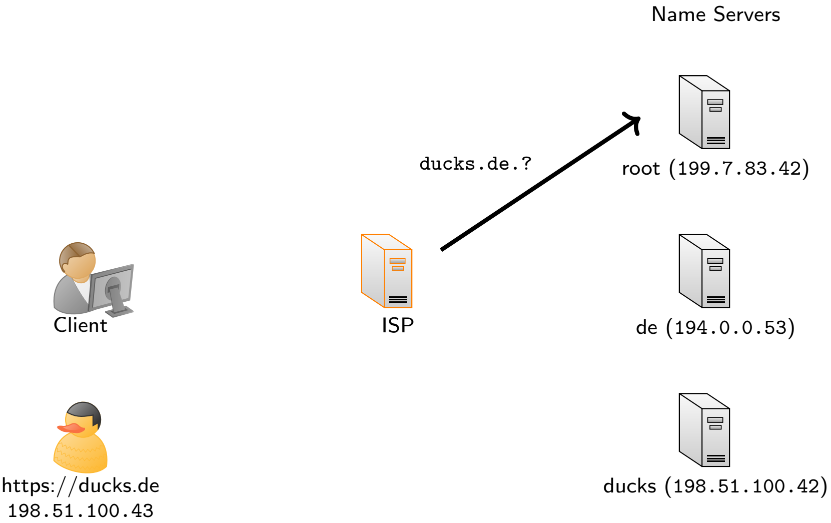
ducks.de.?

ISP

https://ducks.de
198.51.100.43

DNS resolution

Iterative query to the root NS



Name Servers

ducks.de.?

root (199.7.83.42)

Client

ISP

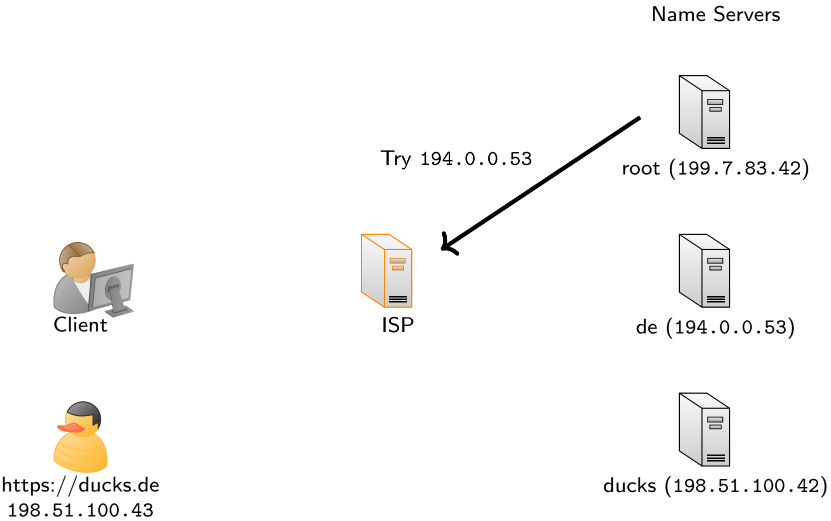
de (194.0.0.53)

https://ducks.de
198.51.100.43

ducks (198.51.100.42)

DNS resolution

Iterative query to the root NS



Name Servers

Try 194.0.0.53

root (199.7.83.42)

Client

ISP

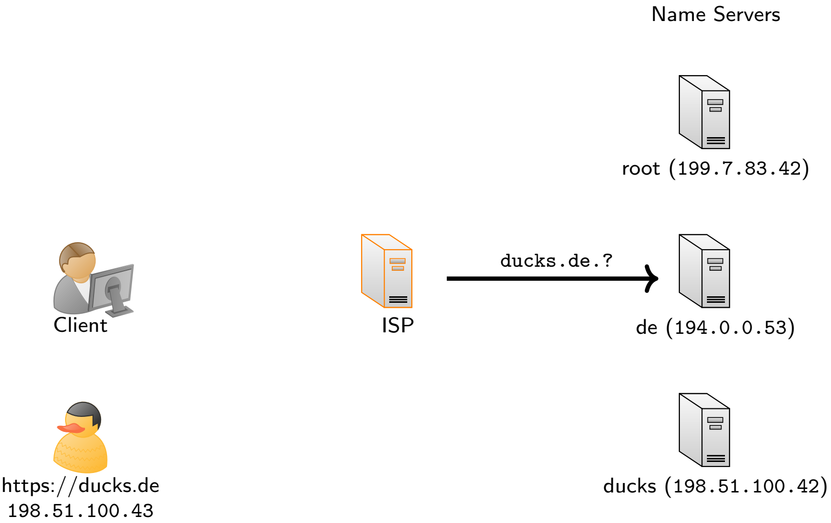
de (194.0.0.53)

https://ducks.de
198.51.100.43

ducks (198.51.100.42)

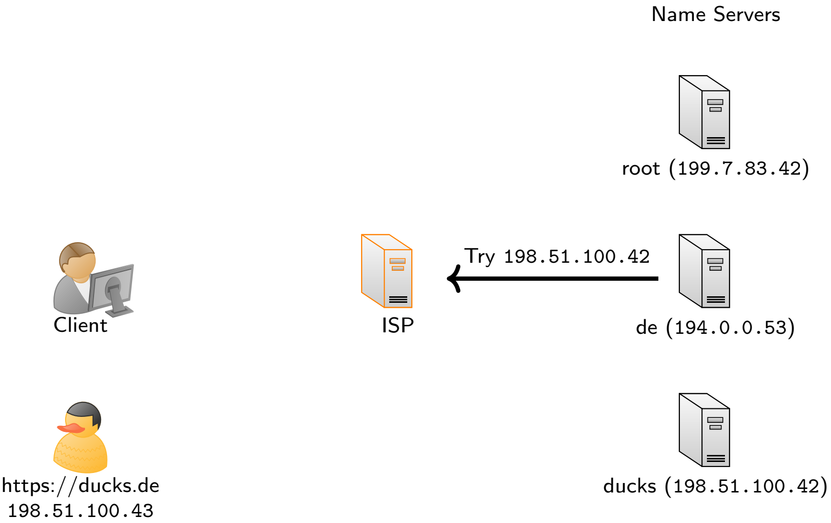
DNS resolution

Iterative query to the de NS



DNS resolution

Iterative query to the de NS



Name Servers

root (199.7.83.42)

Try 198.51.100.42

Client

ISP

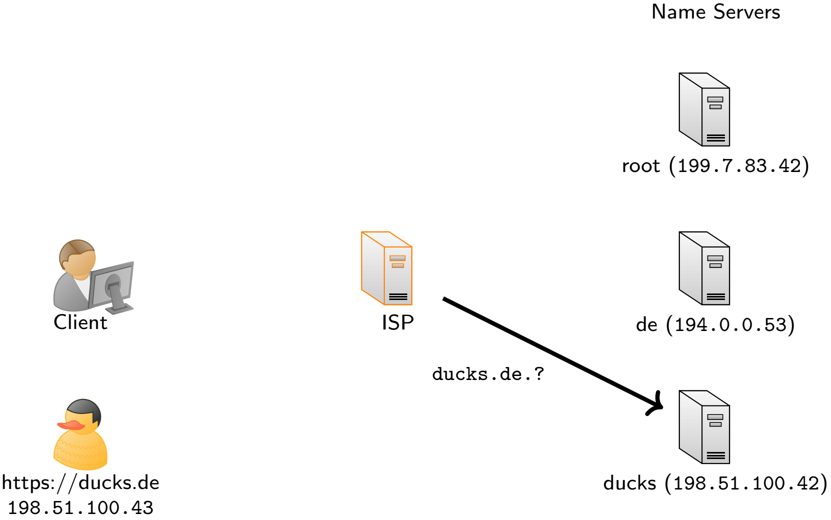
de (194.0.0.53)

https://ducks.de
198.51.100.43

ducks (198.51.100.42)

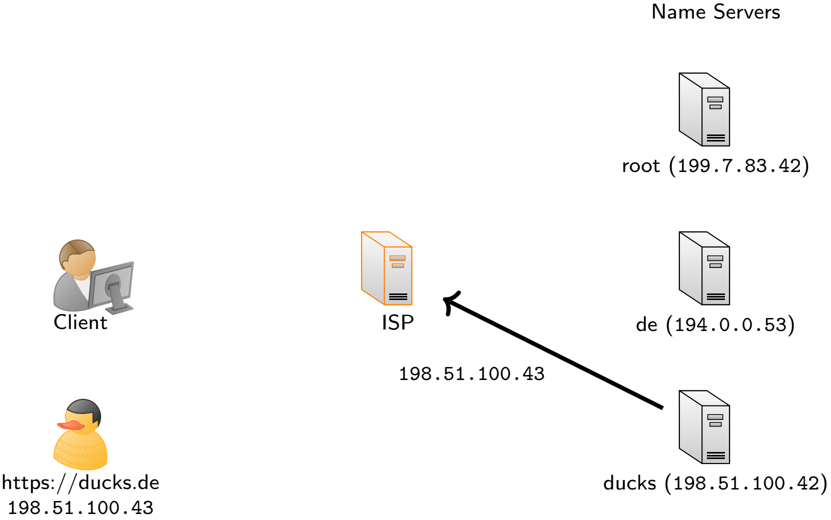
DNS resolution

Iterative query to the ducks NS



DNS resolution

Iterative query to the ducks NS



Name Servers

root (199.7.83.42)

Client

ISP

de (194.0.0.53)

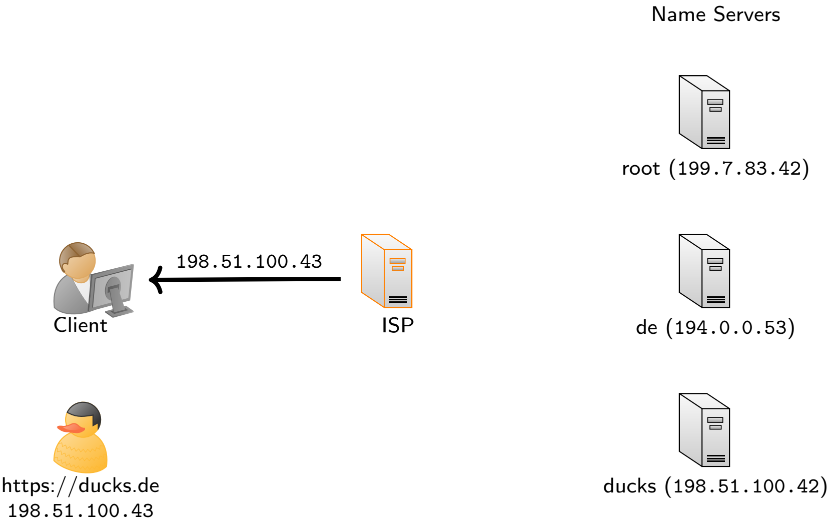
198.51.100.43

https://ducks.de
198.51.100.43

ducks (198.51.100.42)

DNS resolution

ISP responds to the recursive query



Name Servers

root (199.7.83.42)

de (194.0.0.53)

ducks (198.51.100.42)

198.51.100.43

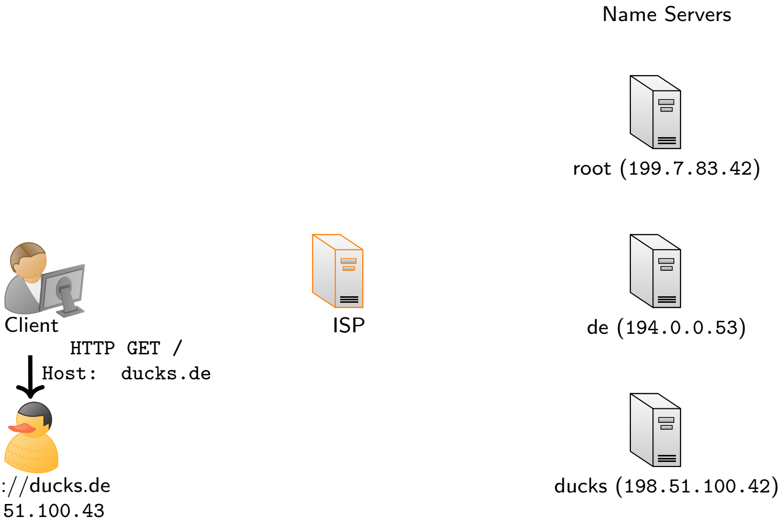
Client

ISP

https://ducks.de
198.51.100.43

DNS resolution

HTTP request



Name Servers

root (199.7.83.42)

Client

ISP

de (194.0.0.53)

HTTP GET /
Host: ducks.de

https://ducks.de
198.51.100.43

ducks (198.51.100.42)

DNS Insecurity

Poisoning/Spoofing is possible

DNS Insecurity

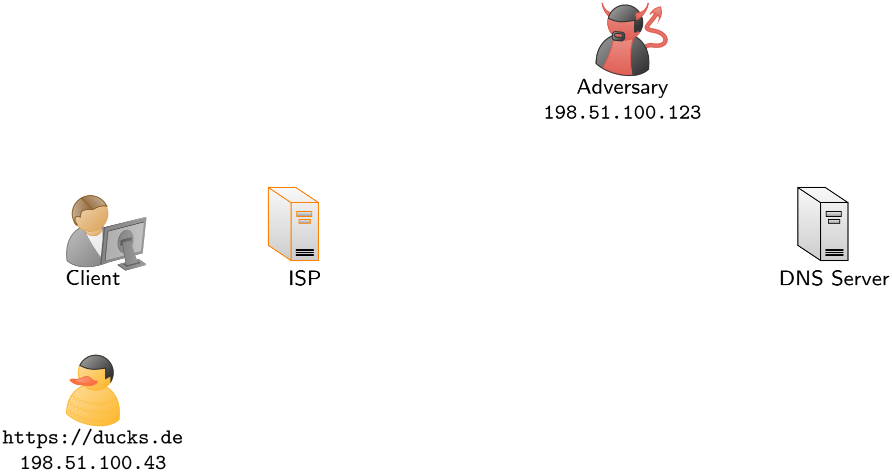
Poisoning/Spoofing is possible

First answer is accepted

DNS Insecurity

Poisoning/Spoofing is possible

First answer is accepted



Adversary
198.51.100.123

Client

ISP

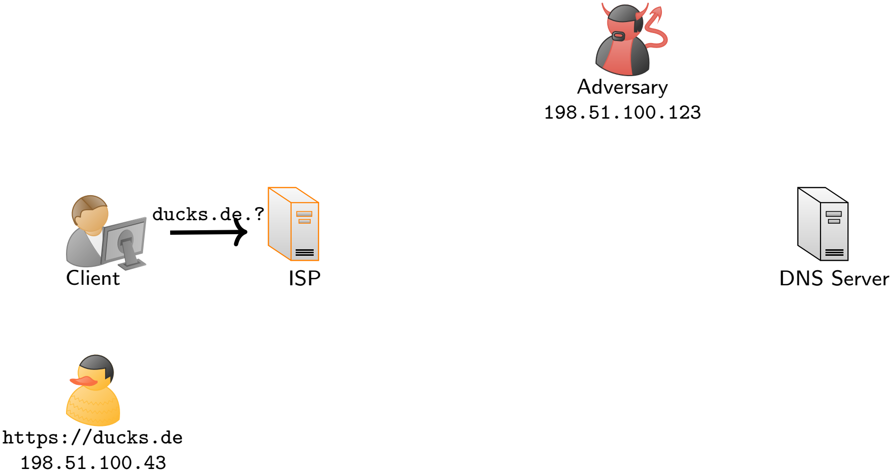
DNS Server

https://ducks.de
198.51.100.43

DNS Insecurity

Poisoning/Spoofing is possible

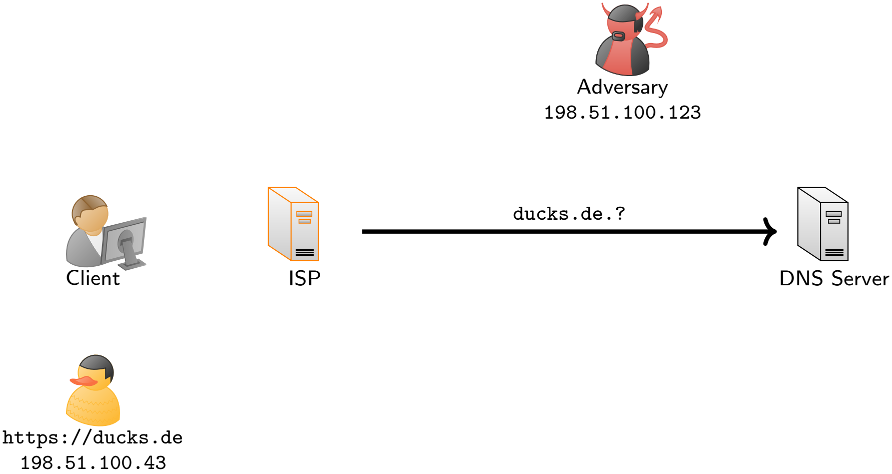
First answer is accepted



DNS Insecurity

Poisoning/Spoofing is possible

First answer is accepted



Adversary
198.51.100.123

ducks.de.?

Client

ISP

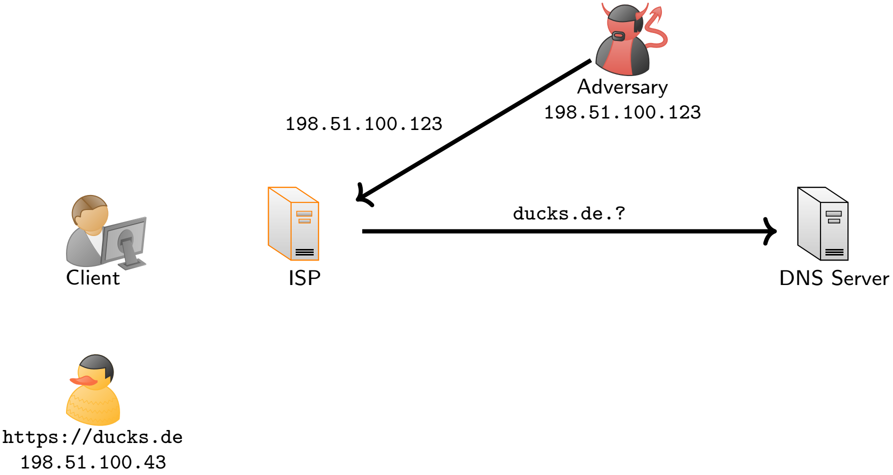
DNS Server

https://ducks.de
198.51.100.43

DNS Insecurity

Poisoning/Spoofing is possible

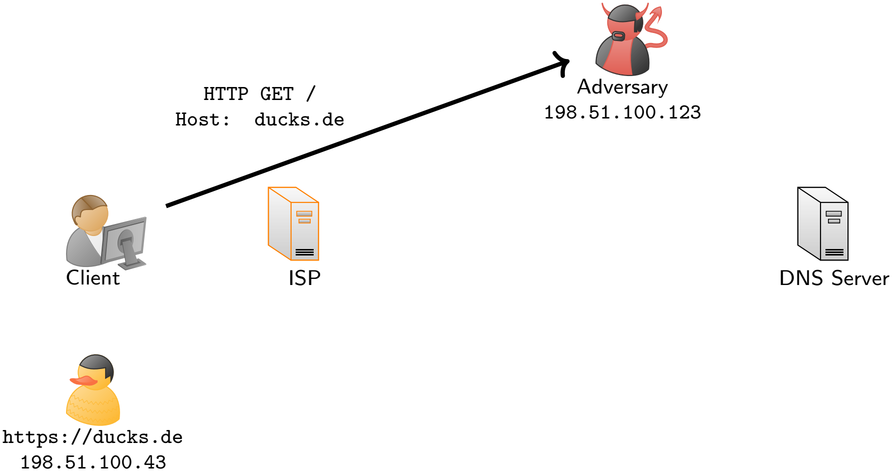
First answer is accepted



DNS Insecurity

Poisoning/Spoofing is possible

First answer is accepted



Outline

DNS

DNSSEC

Multi-operator DNSSEC signing system

DNSSEC

DNSSEC fixes this problem

DNSSEC

DNSSEC fixes this problem

- Data integrity: data was not changed in transit

DNSSEC

DNSSEC fixes this problem

- Data integrity: data was not changed in transit
- Origin authentication: data originated from the owner

DNSSEC

DNSSEC digitally signs the records stored at the name server.

DNSSEC

DNSSEC digitally signs the records stored at the name server.

Root key is hard coded in DNS applications

DNSSEC

DNSSEC digitally signs the records stored at the name server.

Root key is hard coded in DNS applications

Basically certificates for DNS

DNSSEC deployment issues

DNS operation is outsourced to DNS operators, who also handle the signing keys

DNSSEC deployment issues

DNS operation is outsourced to DNS operators, who also handle the signing keys

Studies [1][2] have found that

[1] A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX '17)

[2] One Key to Sign Them All Considered Vulnurable: Evaluation of DNSSEC in the Internet (NSDI '17)

DNSSEC deployment issues

DNS operation is outsourced to DNS operators, who also handle the signing keys

Studies [1][2] have found that

- Some operators use the same key for all domains

[1] A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX ’17)

[2] One Key to Sign Them All Considered Vulnurable: Evaluation of DNSSEC in the Internet (NSDI ’17)

DNSSEC deployment issues

DNS operation is outsourced to DNS operators, who also handle the signing keys

Studies [1][2] have found that

- Some operators use the same key for all domains
  - E.g., one key shared by $> 132\,000$ domains

[1] A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX '17)

[2] One Key to Sign Them All Considered Vulnurable: Evaluation of DNSSEC in the Internet (NSDI '17)

DNSSEC deployment issues

DNS operation is outsourced to DNS operators, who also handle the signing keys

Studies [1][2] have found that

- Some operators use the same key for all domains
  - E.g., one key shared by $> 132\,000$ domains
- Default is 1024-bit RSA

[1] A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX '17)

[2] One Key to Sign Them All Considered Vulnurable: Evaluation of DNSSEC in the Internet (NSDI '17)

DNSSEC deployment issues

DNS operation is outsourced to DNS operators, who also handle the signing keys

Studies [1][2] have found that

- Some operators use the same key for all domains
  - E.g., one key shared by $> 132\,000$ domains
- Default is 1024-bit RSA
  - Most keys 1024-bit, with $\sim$10K domains use 512-bit RSA

[1] A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX '17)

[2] One Key to Sign Them All Considered Vulnurable: Evaluation of DNSSEC in the Internet (NSDI '17)

DNSSEC in practice

DNSSEC

DNSSEC in practice

DNSSEC

- Should use ECDSA instead of RSA

DNSSEC in practice

DNSSEC

- Should use ECDSA instead of RSA
  - Shorter signatures at better/same security
  - Reduces the chance of packet fragmentation[1]

[1] RFC6781 recommends 1024-bit RSA for this reason

DNSSEC in practice

DNSSEC

- Should use ECDSA instead of RSA
  - Shorter signatures at better/same security
  - Reduces the chance of packet fragmentation[1]
- Support multiple DNS operators

[1] RFC6781 recommends 1024-bit RSA for this reason

DNSSEC in practice

DNSSEC

- Should use ECDSA instead of RSA
  - Shorter signatures at better/same security
  - Reduces the chance of packet fragmentation[1]

- Support multiple DNS operators
  - provides DDoS protection[2]
  - better availability

[1] RFC6781 recommends 1024-bit RSA for this reason

[2] E.g., attacks on Dyn and NS1 in 2016

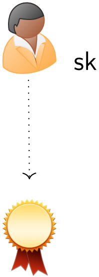
Outline

DNS

DNSSEC

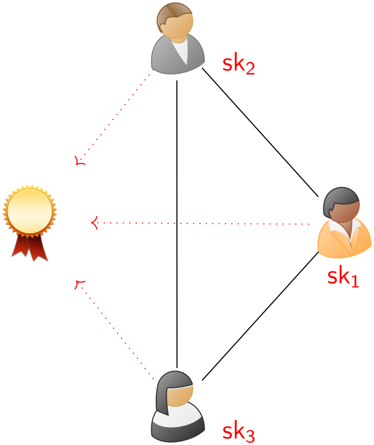
Multi-operator DNSSEC signing system

Traditional Signatures



Threshold Signatures

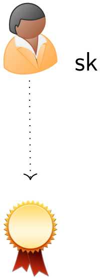
$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$



MPC

Threshold Signatures

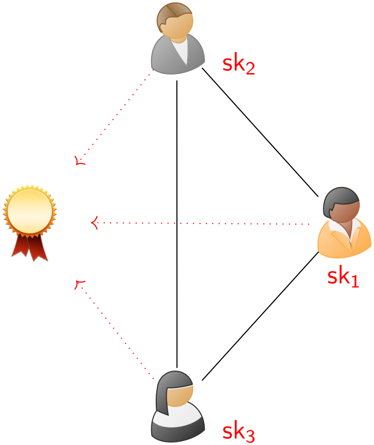
Traditional Signatures



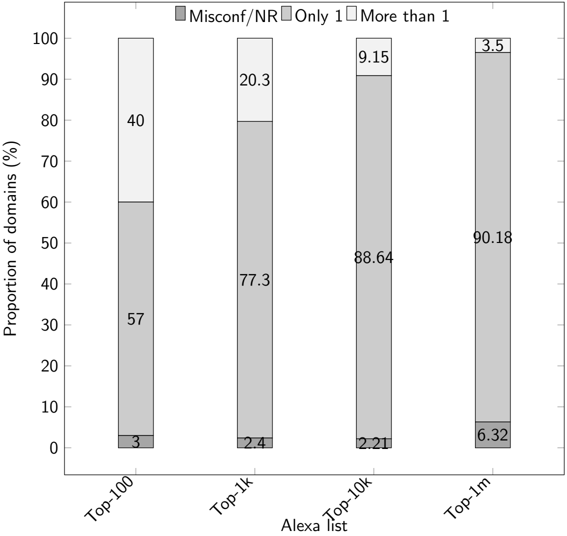
Indistinguishable

Threshold Signatures

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$



Measurement



Threshold signatures for DNSSEC

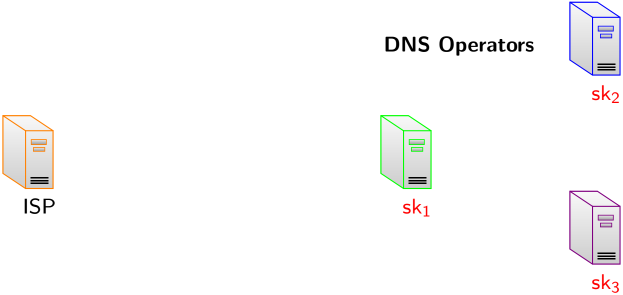
Zone signing with Threshold ECDSA

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$

Threshold signatures for DNSSEC

Zone signing with Threshold ECDSA

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$

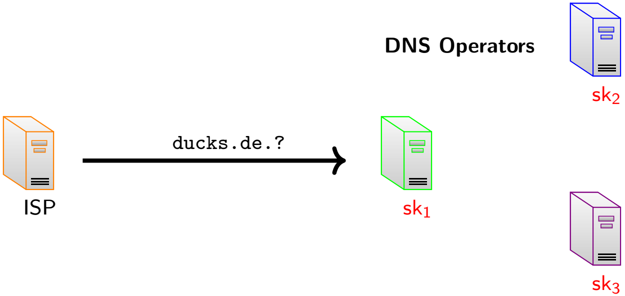


DNS Operators

Threshold signatures for DNSSEC

Zone signing with Threshold ECDSA

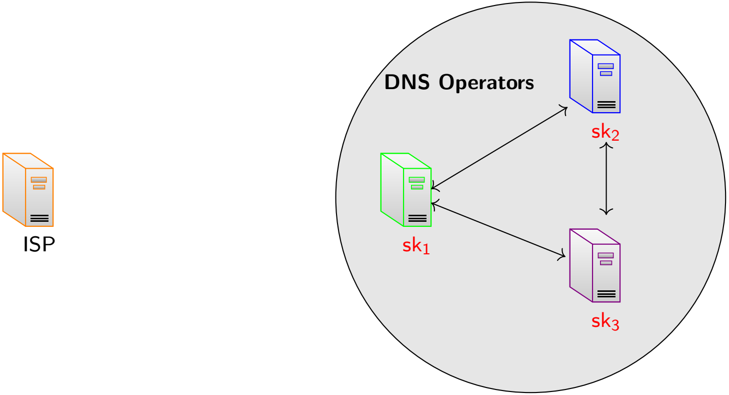
$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$



Threshold signatures for DNSSEC

Zone signing with Threshold ECDSA

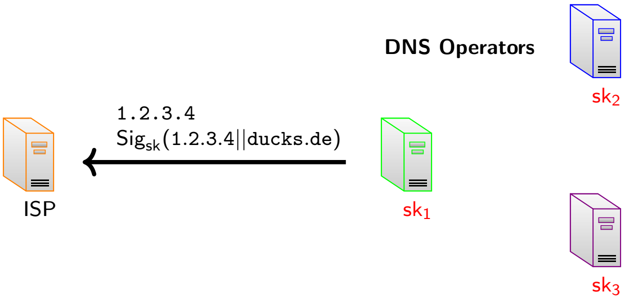
$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$



Threshold signatures for DNSSEC

Zone signing with Threshold ECDSA

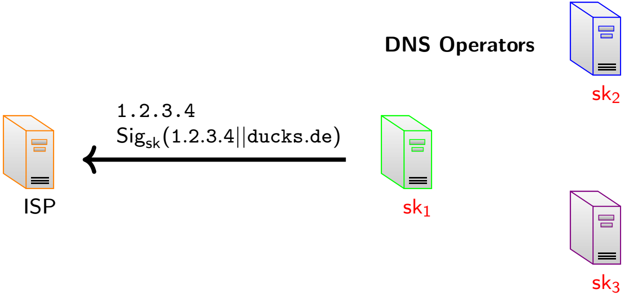
$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$



Threshold signatures for DNSSEC

Zone signing with Threshold ECDSA

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3\} \leftarrow \mathit{Share}(\mathsf{sk})$



Threshold signing should not be much more expensive than regular DNSSEC

ECDSA

$$s = k^{-1}(H(M) + \mathsf{sk} \cdot r_x)$$

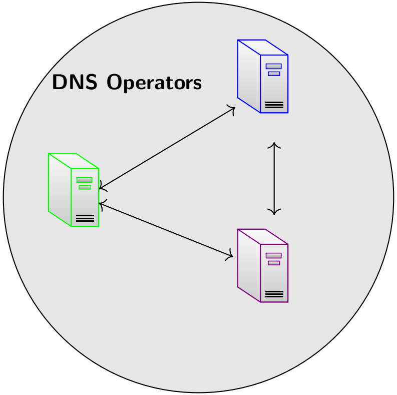
ECDSA

$$s = k^{-1}(H(M) + \mathsf{sk} \cdot r_x)$$

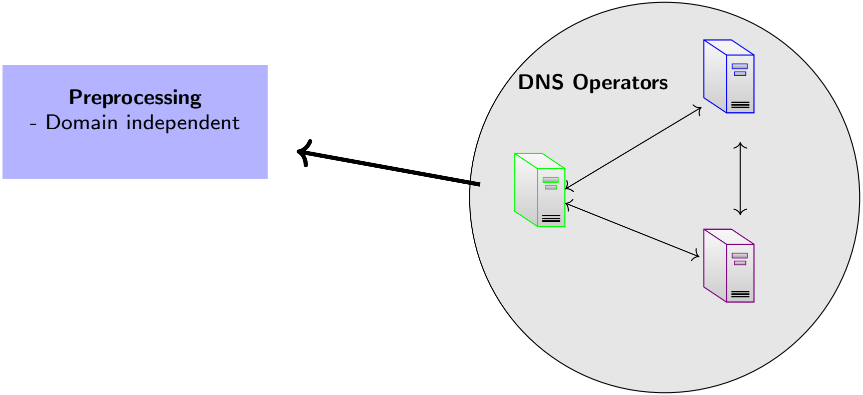
Threshold ECDSA

$$s = H(M)[k^{-1}] + [\mathsf{sk} \cdot k^{-1}] \cdot r_x$$

Threshold Signature in 3 phases



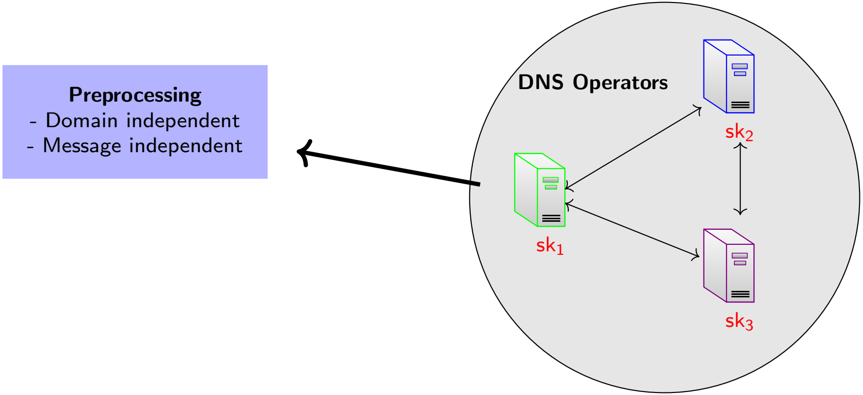
Threshold Signature in 3 phases



Preprocessing
- Domain independent

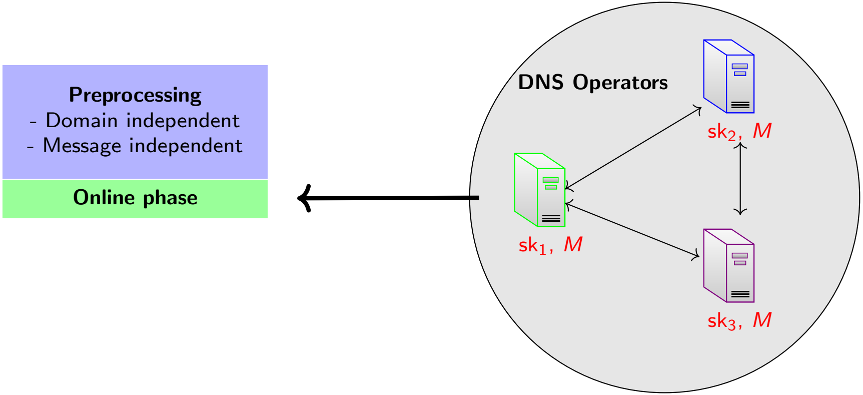
DNS Operators

Threshold Signature in 3 phases



Preprocessing
- Domain independent
- Message independent

Threshold Signature in 3 phases



Preprocessing
- Domain independent
- Message independent

Online phase

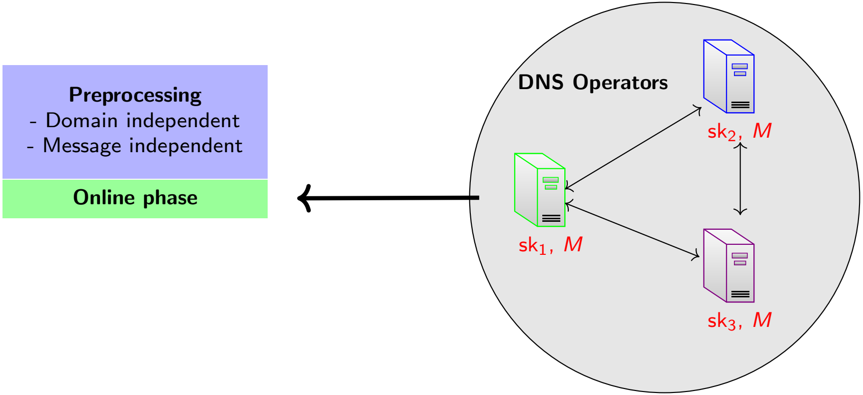
DNS Operators

$\mathsf{sk}_1,\ M$

$\mathsf{sk}_2,\ M$

$\mathsf{sk}_3,\ M$

Threshold Signature in 3 phases



Preprocessing
- Domain independent
- Message independent

Online phase

DNS Operators

$\mathsf{sk}_1,\ M$

$\mathsf{sk}_2,\ M$

$\mathsf{sk}_3,\ M$

Full paper: `ia.cr/2019/889`