# ยินดีต้อนรับสู่

# CYBER SECURITY WORKSHOP

## DNS Resilience

Bangkok
8-9 May 2019

The material in these slides is based on Karst Koymans' CIA course material, see: https://www.os3.nl/2020-2021/courses/cia/start

# Required!

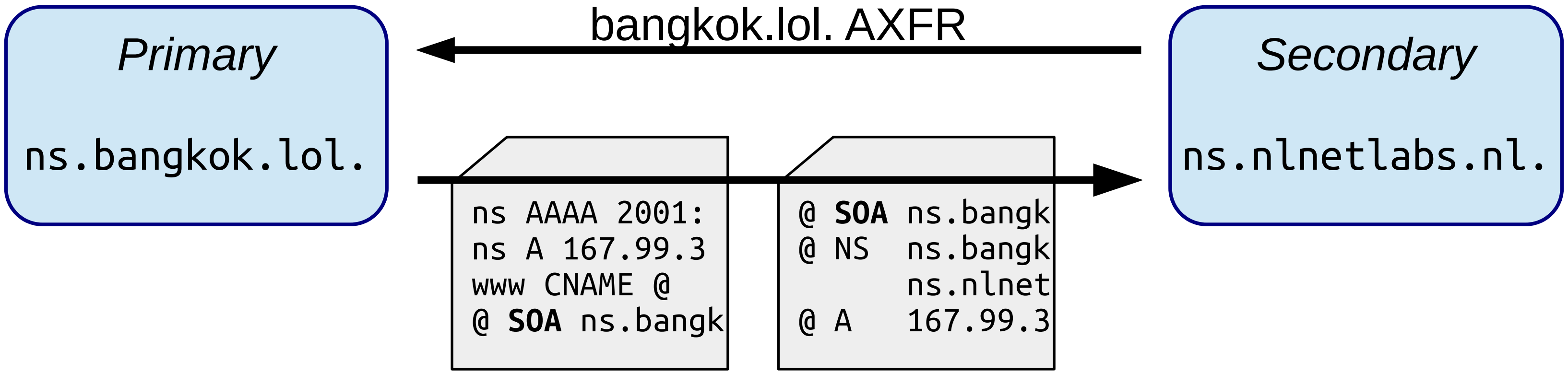
- RFC2182:

  “The DNS requires that multiple servers exist for every zone”

- Why?
  - Resilience
  - Spread the Load
- How?

# Zone transfers

- Pull
  - When Secondary starts without data
  - Query Type `AXFR` (Authoritative Transfer)

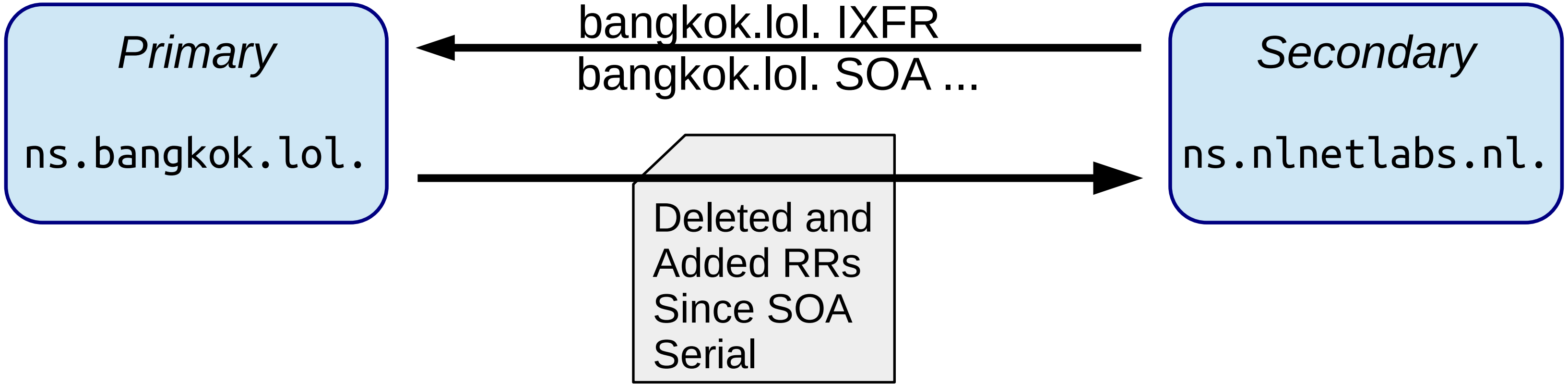


```
ns AAAA 2001:
ns A 167.99.3
www CNAME @
@ SOA ns.bangk
```

```
@ SOA ns.bangk
@ NS  ns.bangk
      ns.nlnet
@ A   167.99.3
```

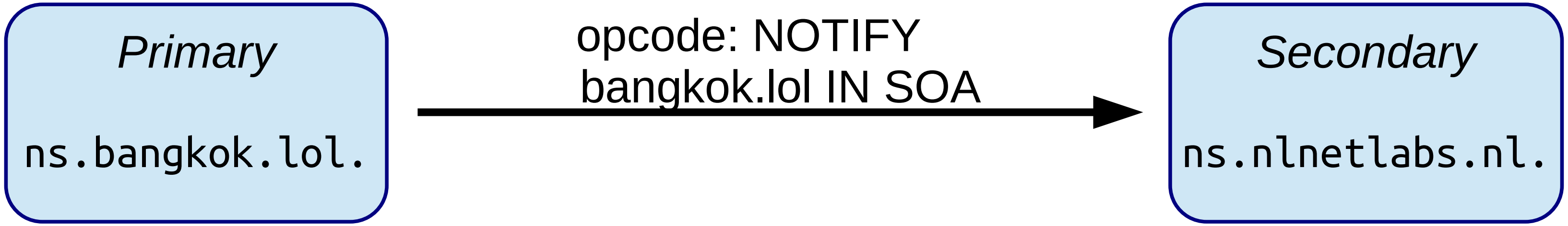
# Zone transfers

- Pull
  - When data changed
    - Slave checks after SOA refresh time
  - Query Type `IXFR` (Incremental Transfer)
    - Include known SOA in authority section



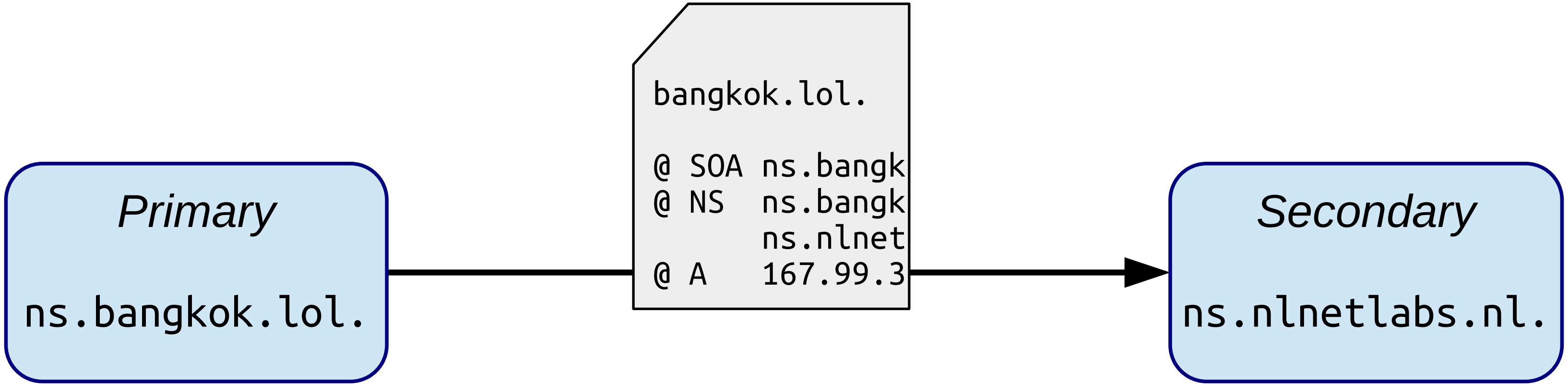
# Zone transfers

- Push
  - Special opcode (4) NOTIFY
- Slave behaves as if SOA refresh timed out



# Zone transfers

- Zone transfers are often limited to slave servers
  - DNS data: public or semipublic?
  - IP level ACL… safe enough?

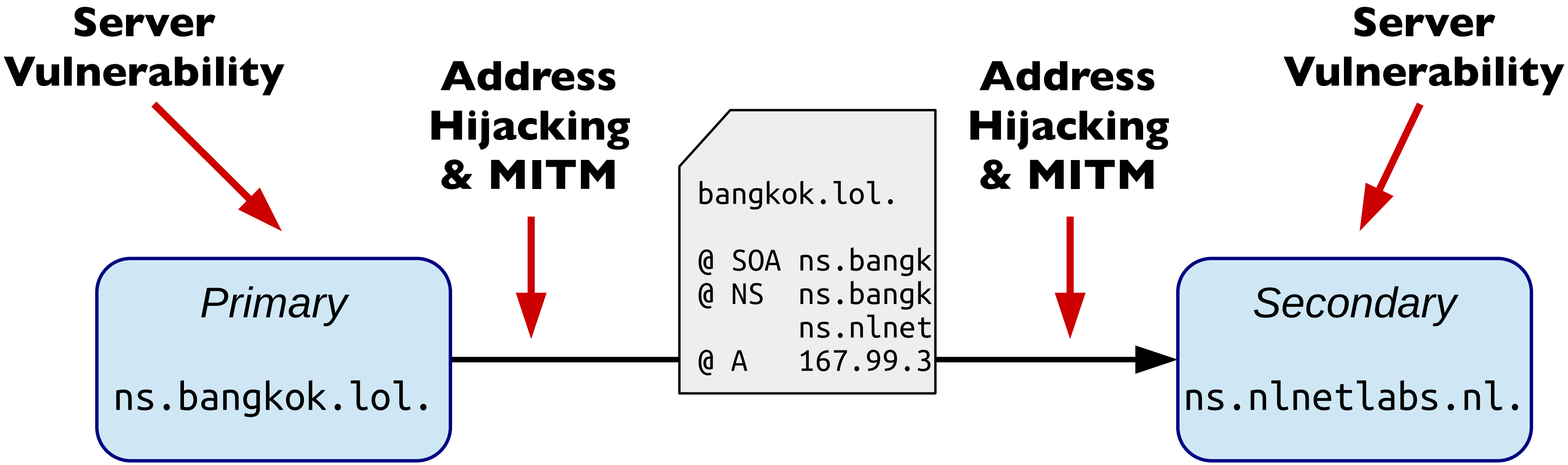


```
bangkok.lol.

@ SOA ns.bangk
@ NS  ns.bangk
      ns.nlnet
@ A   167.99.3
```

# Zone transfers

- Zone transfers are often limited to secondaries
  - DNS data: public or semipublic?
  - IP level ACL… safe enough?

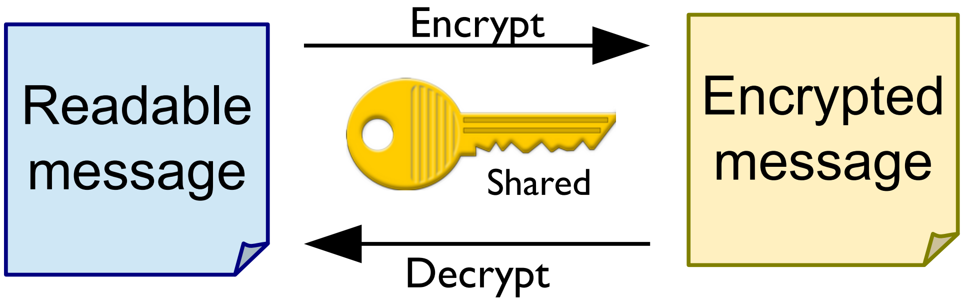


```
bangkok.lol.

@ SOA ns.bangk
@ NS  ns.bangk
      ns.nlnet
@ A   167.99.3
```

# Transaction Signature: TSIG

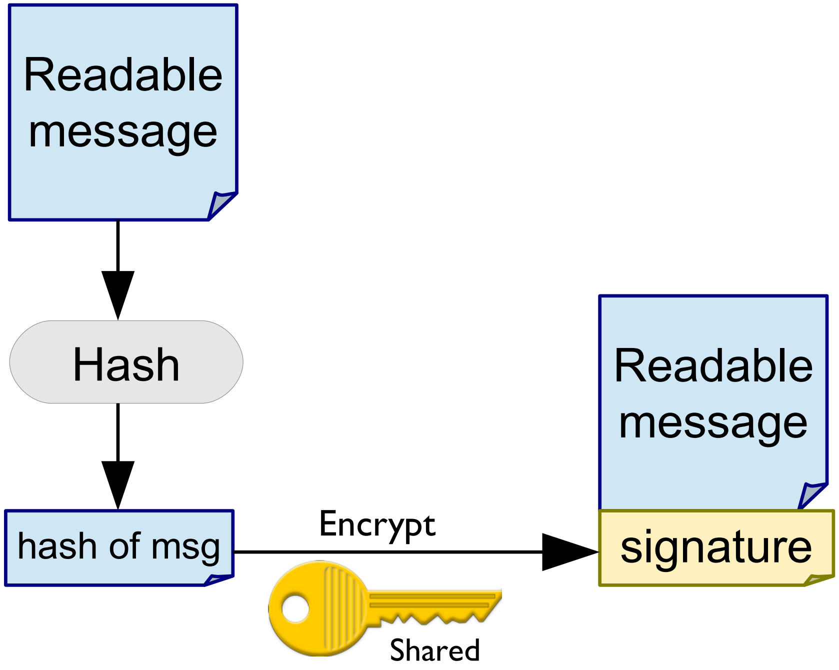
- TSIG (RFC2845)
- Shared secret



- Symmetric encryption

# Transaction security with TSIG

- Hash based Message Authentication Code (HMAC)



Readable message

Hash

hash of msg

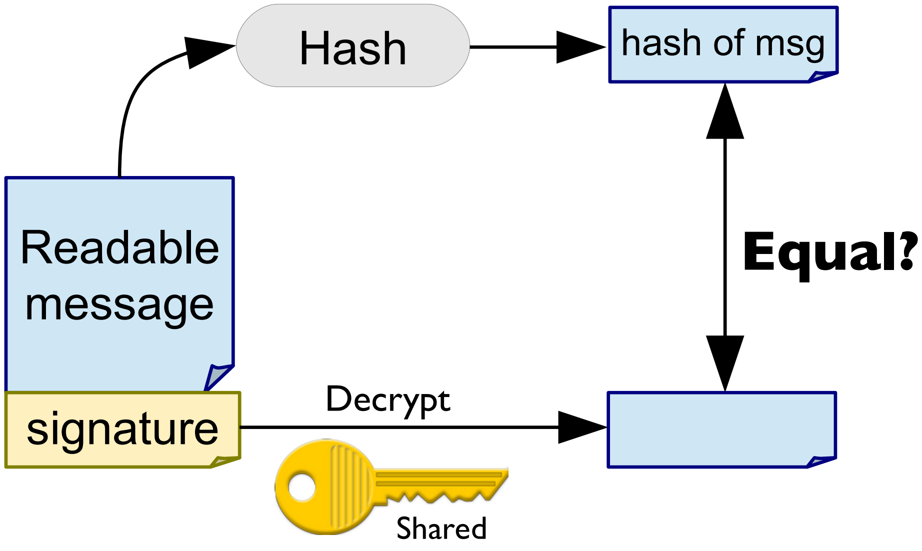
Encrypt

Shared

Readable message

signature

- Create signature



Hash

hash of msg

Readable message

signature

Decrypt

Shared

Equal?

- Verify signature

# Transaction security with TSIG

- TSIG (RFC2845)
- Shared secret
  - Communicated out of band
  - Secret in configuration, **NOT** in zone data!
- Hash based Message Authentication Code (HMAC)
  - Provides mutual Authenticity & Integrity
  - Does not provide confidentiality

# Lab time!

- Hands on: http://bangkok.lol/
- 4. Setup a redundant authoritative name server for your domain

Photo by Alex Kondratiev on Unsplash