DNS/DNSSEC Workshop

In conjunction with LKNOG8

13-16 August 2024

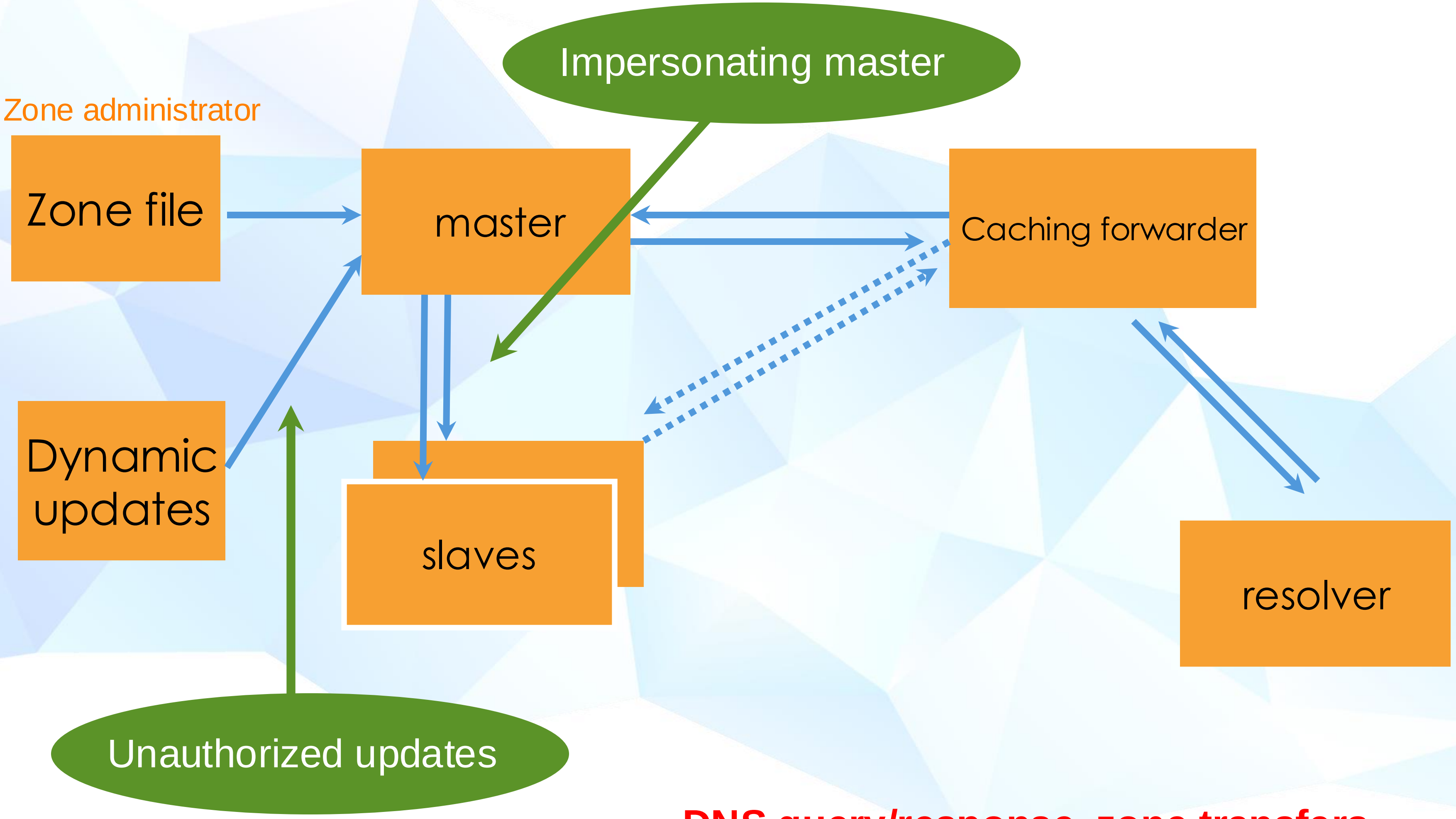
ICANN

Introductions – Trainers

Champika Wijayatunga - *ICANN*
Sampath Hennayake – *LK Domain Registry*
Chamara Disanayake - *NSBM*
Pasan Ravinatha – *University of Moratuwa*

Transaction Signatures

Transactions - Protected Vulnerabilities



DNS query/response, zone transfers, Dynamic updates

TSIG steps

1. Generate secret
2. Communicate secret
3. Configure servers
4. Test

TSIG – Generating a Secret

- dnssec-keygen
  - A simple tool to generate keys
  - Used here to generate TSIG keys

```
dnssec-keygen -a <algorithm> -b <bits> -n
 host <name of the key>
```

TSIG – Generating a Secret

- Example

```
   > dnssec-keygen –a HMAC-SHA256 –b 256 –n HOST ns1-ns2.example.com

   This will generate the key
     Kns1-ns2.example.com.+157+15921

   >ls
 Kns1-ns2.example.com.+157+15921.key
 Kns1-ns2.example.com.+157+15921.private
```

TSIG – Configuring Servers

- Configuring the key

```
key { algorithm ...; secret ...;}
```

- Making use of the key

```
server x { key ...; }
```

where x is the IP address of the other server

Configuration Example – named.conf

Primary server 192.168.1.100

```
key ns1-ns2.example.com {
    algorithm hmac-sha256;
    secret "APlaceToBe";
};
server 192.168.1.200 {
    keys {ns1-ns2.example.com;};
};
zone ”example.com." {
    type master;
    file “db.example.com”;
    allow-transfer {
    key ns1-ns2.example.com ;};
};
```

Secondary server 192.168.1.200

```
key ns1-ns2.example.com {
    algorithm hmac-sha256;
    secret "APlaceToBe";
};
server 192.168.1.100 {
  keys {ns1-ns2.example.com;};
};
zone ”example.com" {
    type slave;
    file “db.example.com.bak”;
    masters {192.168.1.100;};
};
```

You can save this in a file and refer to it in the named.conf using ‘include’ statement:

```
include “/var/named/master/tsig-key-ns1-ns2”;
```

TSIG Testing - Time

- TSIG is time sensitive
- Message protection expires in 5 minutes
  - Make sure time is synchronized
  - For testing, set the time
  - In operations, (secure) NTP is needed

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann