

Asia Pacific Network Information Centre

APNIC

Reverse DNS, TSIG and DNSSEC

Champika Wijayatunga <champika@apnic.net>


03 July 2008

Port Vila, Vanuatu
PACNOG 4

Asia Pacific Network Information Centre

APNIC


Reverse DNS



APNIC
Asia Pacific Network Information Centre

Overview

- Principles
- Creating reverse zones
- Setting up nameservers
- Reverse delegation procedures



APNIC
Asia Pacific Network Information Centre

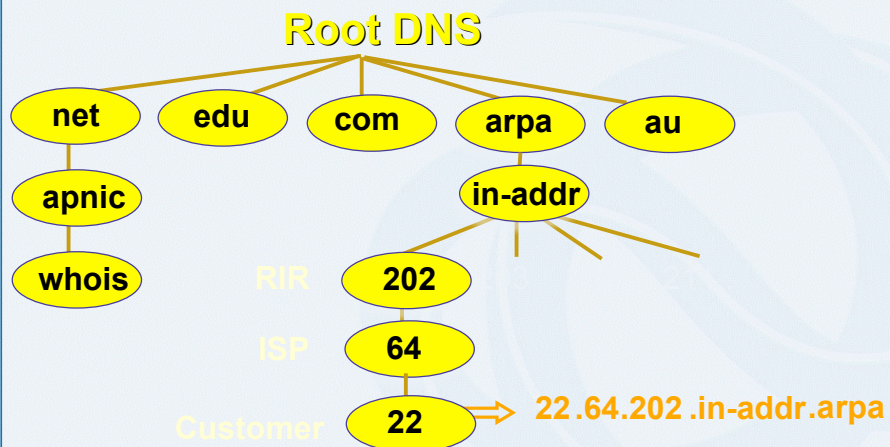
What is 'Reverse DNS'?

- 'Forward DNS' maps names to numbers
 - svc00.apnic.net -> 202.12.28.131
- 'Reverse DNS' maps numbers to names
 - 202.12.28.131 -> svc00.apnic.net

Reverse DNS - why bother?

- Service denial
 - That only allow access when fully reverse delegated
eg. anonymous ftp
- Diagnostics
 - Assisting in trace routes etc
- SPAM identifications
- Registration responsibilities

Principles – DNS tree




Creating reverse zones

- Same as creating a forward zone file
 - SOA and initial NS records are the same as normal zone
 - Main difference
 - need to create additional PTR records
- Can use BIND or other DNS software to create and manage reverse zones
 - Details can be different

Creating reverse zones - contd

- Files involved
 - Zone files
 - Forward zone file
 - e.g. db.domain.net
 - Reverse zone file
 - e.g. db.192.168.254
 - Config files
 - <named.conf>
 - Other
 - Hints files etc.
 - Root.hints



APNIC
 Asia Pacific Network Information Centre

Start of Authority (SOA) record

```

<domain.name.>      CLASS  SOA      <hostname.domain.name.>
<mailbox.domain.name> (
                                <serial-number>
                                <refresh>
                                <retry>
                                <expire>
                                <negative-caching> )
          
```

253.253.192.in-addr.arpa.


APNIC
 Asia Pacific Network Information Centre

Pointer (PTR) records

- Create pointer (PTR) records for each IP address

```
131.28.12.202.in-addr.arpa. IN PTR svc00.apnic.net.
```

| | | | |
|-----|----|-----|------------------|
| 131 | IN | PTR | svc00.apnic.net. |
|-----|----|-----|------------------|

A reverse zone example

```
$ORIGIN 1.168.192.in-addr.arpa.
@      3600  IN SOA test.company.org. (
                                sys\.admin.company.org.
                                2002021301      ; serial
                                1h                ; refresh
                                30M              ; retry
                                1W              ; expiry
                                3600 )          ; neg. answ. ttl

      NS      ns.company.org.
      NS      ns2.company.org.

1      PTR     gw.company.org.
      PTR     router.company.org.

2      PTR     ns.company.org.
;auto generate: 65 PTR host65.company.org
$GENERATE 65-127 $ PTR host$.company.org.
```

Setting up the primary nameserver

- Add an entry specifying the primary server to the *named.conf* file

```
zone "<domain-name>" in {
    type master;
    file "<path-name>"; };

```

- - Ex: 28.12.202.in-addr.arpa.
- <type master>
 - Define the name server as the primary
- <path-name>
 - location of the file that contains the zone records

Setting up the secondary nameserver

- Add an entry specifying the primary server to the **named.conf** file

```
zone "<domain-name>" in {  
    type slave;  
    file "<path-name>";  
    Masters { <IP address> ; }; };
```

- <type slave> defines the name server as the secondary
- <ip address> is the IP address of the primary name server
- <domain-name> is same as before
- <path-name> is where the back-up file is

Reverse delegation requirements

- /24 Delegations
 - Address blocks should be assigned/allocated
 - At least two name servers
- /16 Delegations
 - Same as /24 delegations
 - APNIC delegates entire zone to member
 - Recommend APNIC secondary zone
- < /24 Delegations
 - Read "classless in-addr.arpa delegation"



APNIC & ISPs responsibilities

- APNIC
 - Manage reverse delegations of address block distributed by APNIC
 - Process organisations requests for reverse delegations of network allocations
- Organisations
 - Be familiar with APNIC procedures
 - Ensure that addresses are reverse-mapped
 - Maintain nameservers for allocations
 - Minimise pollution of DNS

Reverse delegation procedures

- Upon allocation, member is asked if they want /24 place holder domain objects with member maintainer
 - Gives member direct control
- Standard APNIC database object,
 - can be updated through myAPNIC, Online form or via email.
- Nameserver/domain set up verified before being submitted to the database.
- Protection by maintainer object
 - (current auths: CRYPT-PW, PGP).
- Zone file updated 2-hourly

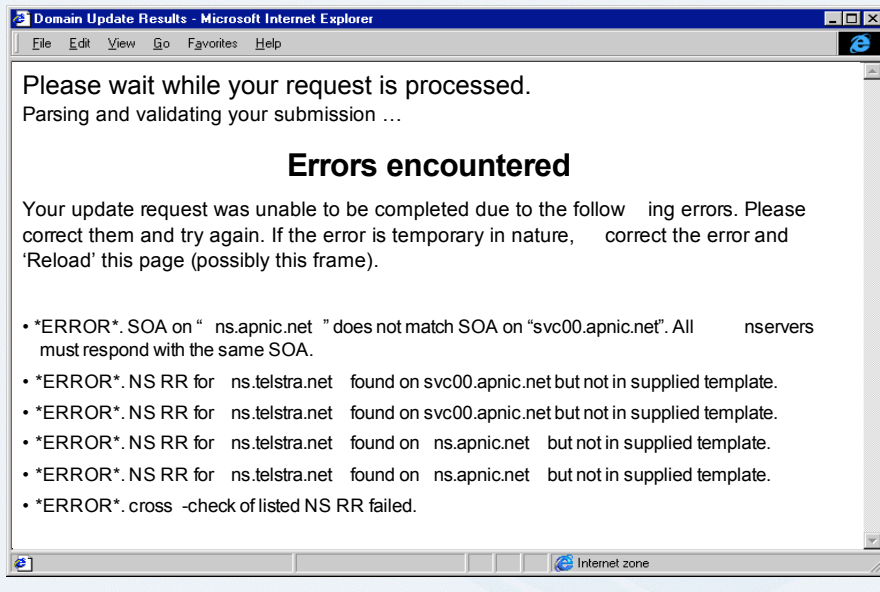
Reverse delegation procedures

- Use MyAPNIC to create 'domain' objects
 - Highly recommended
- Or use the web form
 - <http://www.apnic.net/db/domain.html>
- On-line form interface
 - Real time feedback
 - Gives errors, warnings in zone configuration
 - serial number of zone consistent across nameservers
 - nameservers listed in zone consistent

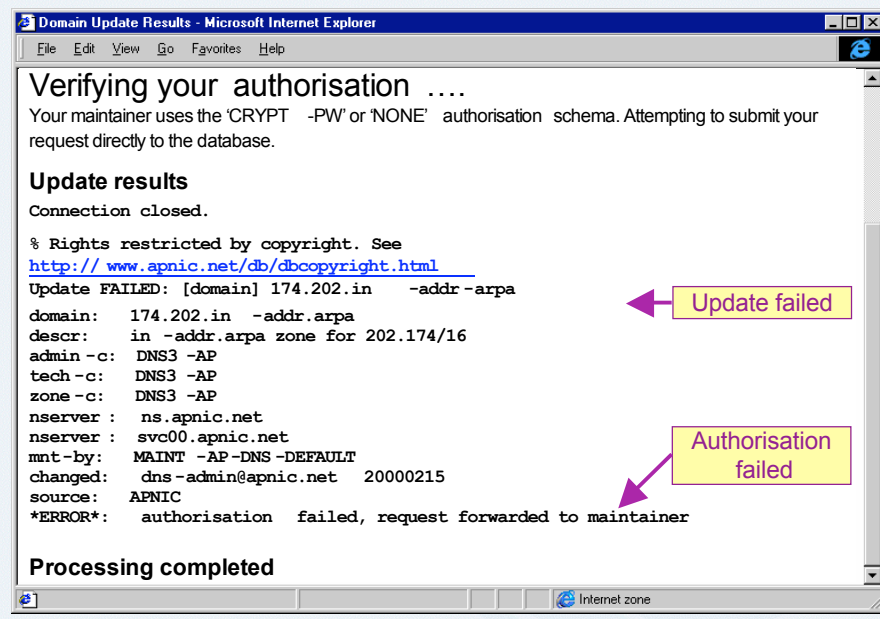
Evaluation procedures

- Parser checks for
 - 'whois' database
 - IP address range is assigned or allocated
 - Must be in APNIC database
 - Maintainer object
 - Mandatory field of domain object
 - Nic-handles
 - zone-c, tech-c, admin-c

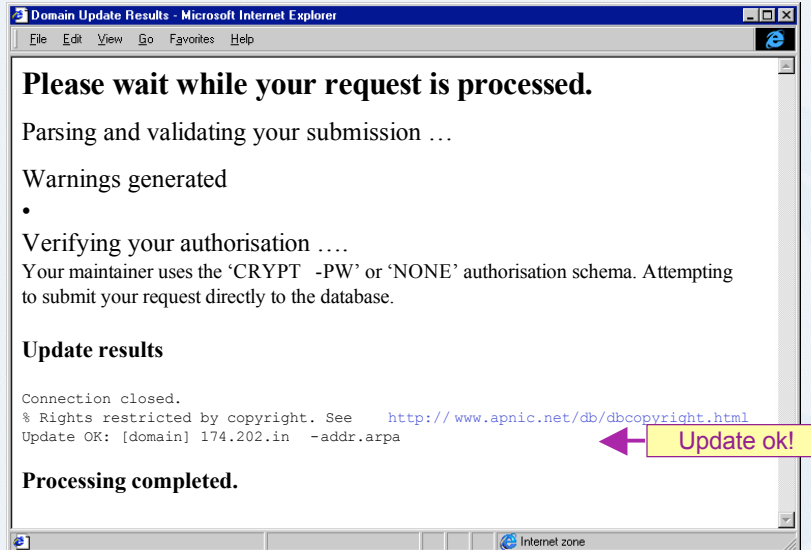
Online errors (also via email)



Request submission error



Successful update



Creation of domain objects

- If you opt to create the domain objects yourself
 - Either you can use MyAPNIC
 - Or use web/email templates
- Using web/email templates will result in initial errors
 - As the /8 is hierarchically maintained by MAINT-AP-DNS
 - Contact <helpdesk@apnic.net>

Whois domain object

domain: 28.12.202.in-addr.arpa
descr: in-addr.arpa zone for 28.12.202.in-addr.arpa
admin-c: DNS3-AP
tech-c: DNS3-AP
zone-c: DNS3-AP
nserver: ns.telstra.net
nserver: rs.arin.net
nserver: ns.myapnic.net
nserver: svc00.apnic.net
nserver: ns.apnic.net
mnt-by: MAINT-APNIC-AP
mnt-lower: MAINT-DNS-AP
changed: inaddr@apnic.net 19990810
source: APNIC


Reverse Zone

Contacts


Name
ServersMaintainers
(protection)


Removing lame delegations

- Objective
 - To repair or remove persistently lame DNS delegations
- DNS delegations are lame if:
 - Some or all of the registered DNS nameservers are unreachable or badly configured
- APNIC commenced formal implementation of the lame DNS reverse delegation procedures


**APNIC**
Asia Pacific Network Information Centre

Questions ?



**APNIC**
Asia Pacific Network Information Centre

TSIG



What is TSIG - Transaction Signature?

- A mechanism for protecting a message from a primary to secondary and vice versa
- A keyed-hash is applied (like a digital signature) so recipient can verify message
 - DNS question or answer
 - & the timestamp
- Based on a shared secret - both sender and receiver are configured with it

What is TSIG - Transaction Signature?

- TSIG (RFC 2845)
 - authorizing dynamic updates & zone transfers
 - authentication of caching forwarders
- Used in server configuration, not in zone file

Names and Secrets

- TSIG name
 - A name is given to the key, the name is what is transmitted in the message (so receiver knows what key the sender used)
- TSIG secret value
 - A value determined during key generation
 - Usually seen in Base64 encoding

Using TSIG to protect AXFR

- Deriving a secret

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

e.g.

```
> dnssec-keygen -a HMAC-MD5 -b 128 -n HOST
  ns1-ns2.pcx.net
```

This will generate the key

```
> Kns1-ns2.pcx.net.+157+15921
```



```
> ls
➤ Kns1-ns2.pcx.net.+157+15921.key
➤ Kns1-ns2.pcx.net.+157+15921.private
```

Using TSIG to protect AXFR

- Configuring the key
 - in named.conf file, same syntax as for rndc
 - `key { algorithm ...; secret ...; }`
- Making use of the key
 - in named.conf file
 - `server x { key ...; }`
 - where 'x' is an IP number of the other server

Configuration Example – named.conf

Primary server 10.33.40.46


```
key ns1-ns2.pcx.net {
    algorithm hmac-md5;
    secret "APlaceToBe";
};
server 10.33.50.35 {
    keys {ns1-ns2.pcx.net};
};
zone "my.zone.test." {
    type master;
    file "db.myzone";
    allow-transfer {
        key ns1-ns2.pcx.net ;};
};
```

Secondary server 10.33.50.35

```
key ns1-ns2.pcx.net {
    algorithm hmac-md5;
    secret "APlaceToBe";
};
server 10.33.40.46 {
    keys {ns1-ns2.pcx.net};
};
zone "my.zone.test." {
    type slave;
    file "myzone.backup";
    masters {10.33.40.46};
    allow-transfer {
        key ns1-ns2.pcx.net};
};
```

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";
```

Asia Pacific Network Information Centre

TIME!!!


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




Asia Pacific Network Information Centre

Other uses of TSIG

- TSIG was designed for other purposes as well
 - Protecting sensitive stub resolvers
 - This has proven hard to accomplish
 - Dynamic Update
 - Discussed later, securing this relies on TSIG

**APNIC**
Asia Pacific Network Information Centre

Questions ?

**APNIC**
Asia Pacific Network Information Centre

DNSSEC

Background

- The original DNS protocol wasn't designed with security in mind
- It has very few built-in security mechanism
- As the Internet grew wilder & woolier, IETF realized this would be a problem
 - For example DNS spoofing was too easy
- DNSSEC and TSIG were developed to help address this problem

Why DNSSEC?

- DNS is not secure
 - Applications depend on DNS
 - Known vulnerabilities
- DNSSEC protects against data spoofing and corruption

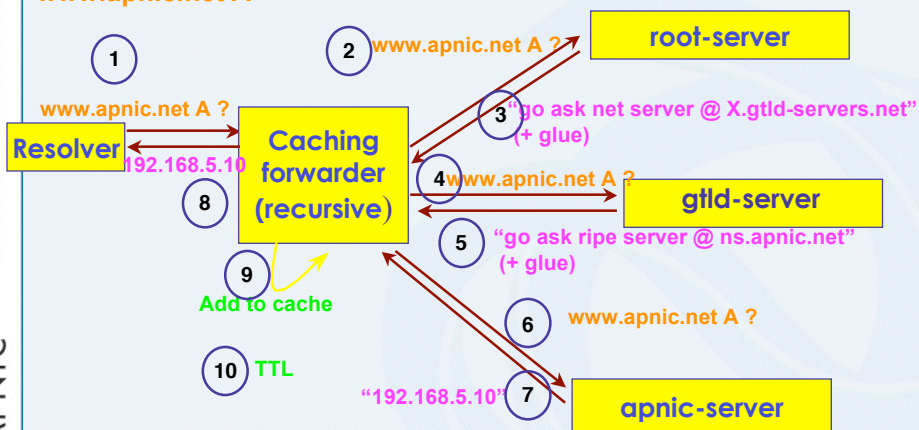
Overview

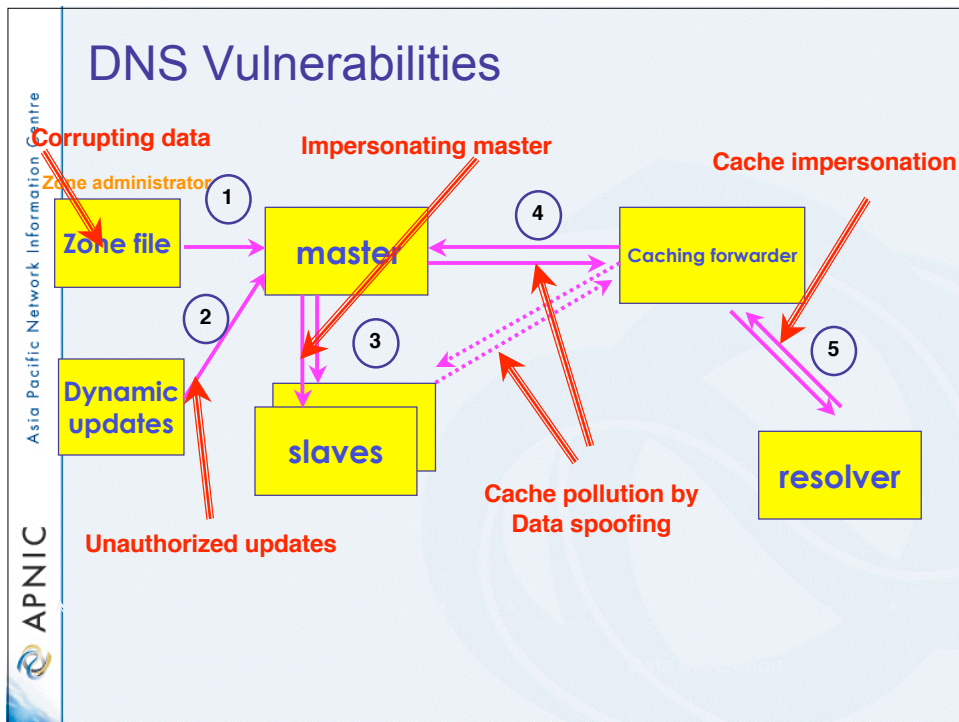
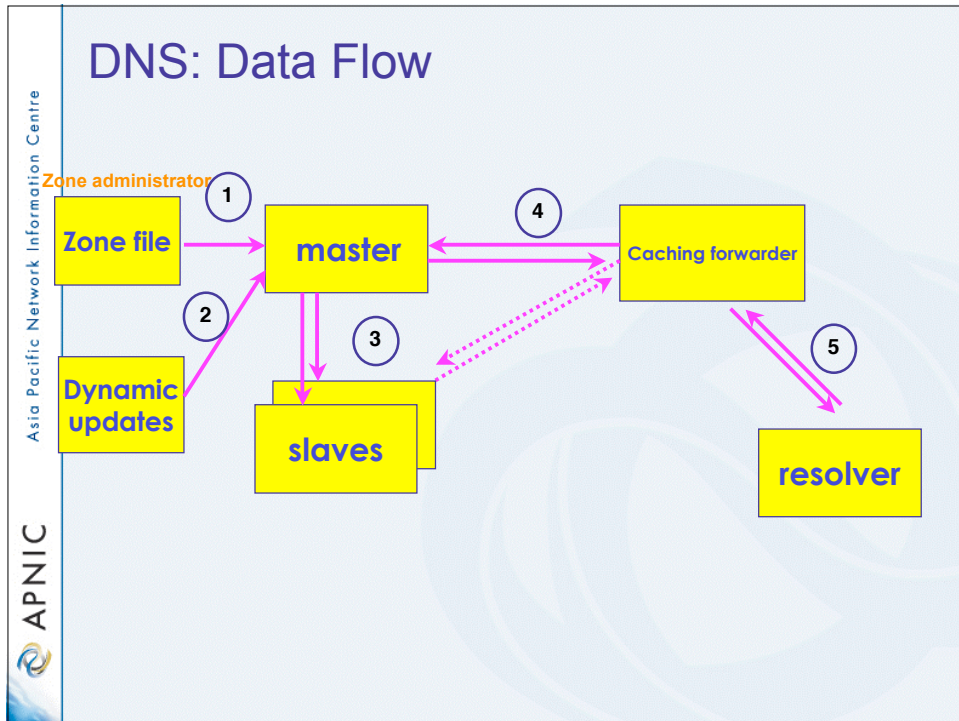
- Introduction
- DNSSEC mechanisms
 - To authenticate servers (TSIG)
 - To establish authenticity and integrity of data
 - Quick overview
 - New RRs
 - Using public key cryptography to sign a single zone
 - Delegating signing authority ; building chains of trust
 - Key exchange and rollovers
- Conclusions

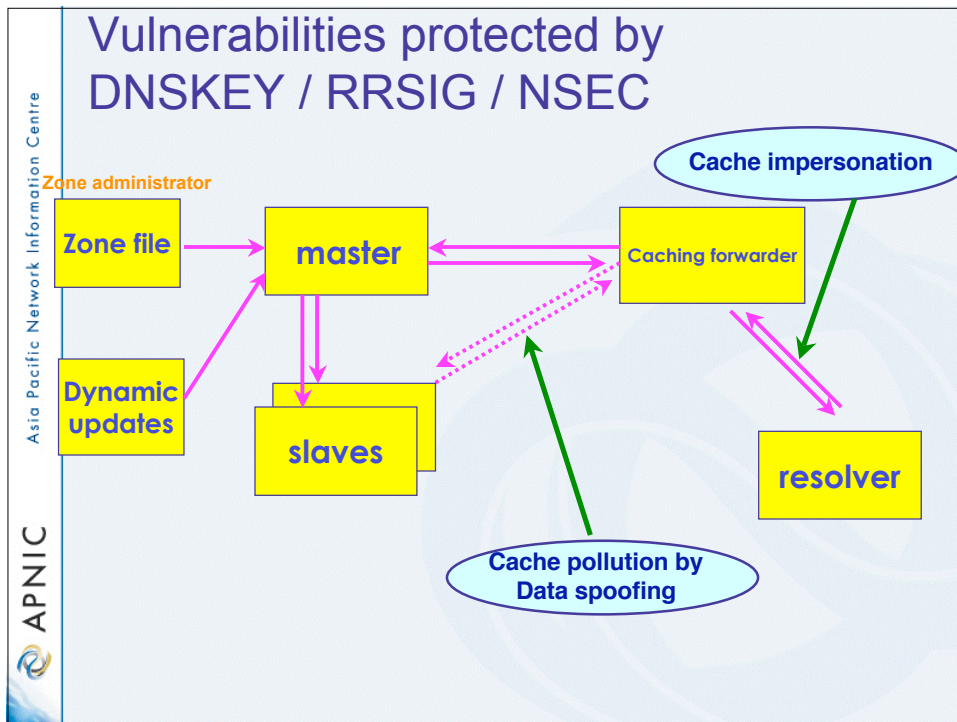
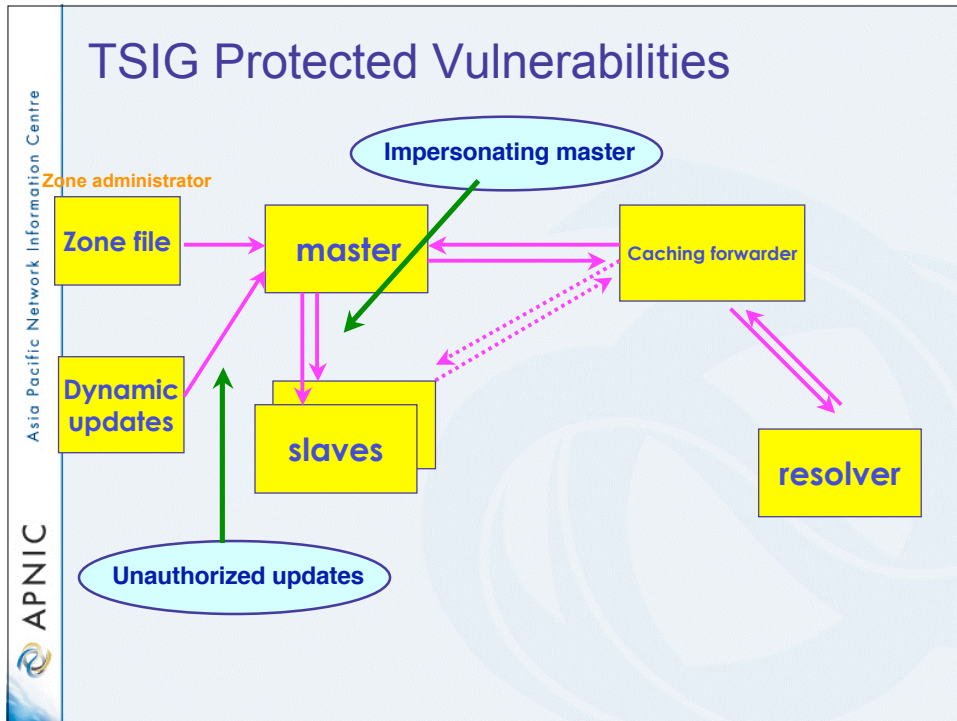
Reminder: DNS Resolving

Question:

www.apnic.net A







Difference Between TSIG and DNSSEC

- TSIG secures transaction
 - Making sure DNS messages come from the right place and aren't modified in transit
- DNSSEC secures (signs) zone data
 - Making sure resource records are those signed by the administrator of the zone
- Only endpoints that share a key can use TSIG to verify DNS messages
- Any endpoints that support DNSSEC can use it to verify signed zone data

Enable dnssec

- In the named.conf,

```
Options {  
    directory "..."  
    dnssec-enable yes;  
};
```

Create key pairs

- To create ZSK
 - > `dnssec-keygen -a rsasha1 -b 1024 -n zone champika.net`
- To create KSK
 - > `dnssec-keygen -a rsasha1 -b 1400 -f KSK -n zone champika.net`

What will be created?

- After key generations (ZSK & KSK) you will see 2 files have been created
 - Files with *.key* and *.private* extensions
 - *.key* file contains your public key where as *.private* file contains your private key

Publishing your public key

- Using \$INCLUDE you can call the public key (DNSKEY RR) inside the zone file
 - \$INCLUDE /path/Kchampika.net.+005+57163.key ; ZSK
 - \$INCLUDE /path/Kchampika.net.+005+40485.key ; KSK
- You can also manually enter the DNSKEY RR in the zone file

Signing the zone


- > dnssec-signzone -o champika.net -t -k
Kchampika.net.+005+57163 db.champika.net
Kchampika.net.+005+40485
- Once you sign the zone a file with a .signed extension will be created
 - db.champika.net.signed

Signed Zone

- Observe the signed zone file
- Resource Records
 - DNSKEY
 - RRSIG
 - NSEC
- Difference in the file size
 - *db.champika.net* Vs *db.champika.net.signed*

Updates to the config file

- Modify the zone statement
- Replace the previous zone file with the signed zone file




APNIC
Asia Pacific Network Information Centre

Testing the server

- Ask a dnssec enabled question from the server and see whether the answer contains dnssec-enabled data
 - Basically the answers are signed

➤ `dig @localhost www.champika.net +dnssec +multiline`



APNIC
Asia Pacific Network Information Centre

Questions ?