Restricting Zone Transfers
Rationale

- This is a policy issue
- People have different opinions
- Some people think it’s a good idea to restrict zone transfers to particular slaves
- In case you think that, this is how you do it
Authorising Zone Transfers

- Two ways to authorise zone transfers from a master server:
  1. using a shared secret (password)
  2. by source IP address
Shared Secret

- TSIG
  - easy to configure
  - need to agree a password with the people who operate your slave servers
  - we are going to talk about this later
IP Address

• Checking the source address is a weak way to authenticate anything, but sometimes it’s better than nothing

• why is it weak?
ACLs for Zone Transfers

zone "joe.lk" {
    type master;
    file "master/joe.lk";
    allow-transfer {
        199.212.90.7;
        203.97.2.226;
    };
};
Manual Zone Transfer

[jabley@buffoon]% dig @193.0.2.74 np.ws.isc.org axfr

; DiG 8.3 @193.0.2.74 np.ws.isc.org axfr
; (1 server found)
$ORIGIN np.ws.isc.org.
@                       30M IN SOA      ns1 hostmaster (2004061901 ; serial
                                 1H ; refresh
                                 15M ; retry
                                 4W ; expiry
                                 5M ) ; minimum

30M IN NS       ns1.gh.ws.isc.org.
30M IN NS       ns1
ns1
30M IN A        193.0.2.74
@                       30M IN SOA      ns1 hostmaster (2004061901 ; serial
                                 1H ; refresh
                                 15M ; retry
                                 4W ; expiry
                                 5M ) ; minimum

;; Received 1 answer (5 records).
;; FROM: buffoon.automagic.org to SERVER: 193.0.2.74
;; WHEN: Sun Jun 20 04:03:27 2004
[jabley@buffoon]%
Exercise

• Restrict zone transfers for XX.ws.isc.org to just the server(s) which are slaves

• Try to do zone transfers from other peoples’ servers, and see whether they work