DNS Session 5

Additional Topics

Joe Abley
AfNOG 2006, Nairobi, Kenya

Upgrading BIND

Why Upgrade?

- Almost all software has bugs
  - Although BIND 9 is much more conservative than previous versions, it is not immune to software defects
- Better performance
- New features

Where to Find BIND

- http://www.isc.org/sw/bind/
- ftp://ftp.isc.org/isc/bind9/
- Today, the recommended version to run is BIND 9.3.2
  - Maybe 0.01% of people have a reason to run BIND 8 instead of BIND 9
  - Nobody has a reason to run BIND 4

Warning!

- Many operating systems come with BIND built-in
- If you compile your own, you may end up with two copies of BIND on the same server
  - confusing
  - annoying

Securing Nameservers

Host Security

- Your authority servers contain valuable data
- If intruders can change the records in your zones, this could spell trouble
  - phishing
  - denial-of-service
- Long TTLs can make changes hard to back out (why?)

Restricting Recursion

- Why control which clients can perform recursive lookups?
  - cache poisoning
  - server load
  - network load
  - reflection attacks

Separate Recursive and Authority Servers

- Avoid serving stale zones authoritatively
- Avoiding exposing nameservers to cache poisoning attacks is even more important when the potential client population is large, and the answers are marked authoritative

Host Local Zones Locally

- Avoid leaking queries for private zones
- Avoid unnecessary query loads on the root servers, or on the AS112 servers
- Avoid calling ISC complaining that prisoner.iana.org is attacking you on port 53

By the Way...

- Encourage people who run your network to read and understand BCP 38
  - http://www.ietf.org/rfc/rfc2827.txt
- Preventing source spoofing helps reduce the opportunity for many attacks, including Reflection Attacks

Restricting AXFR/IXFR

- People can extract information about you and your customers by reading your zones
  - hosts to try and attack (e.g. ssh brute force attacks)
  - mail servers to exploit (e.g. relay attempts, dictionary attacks)
  - cache poisioning opportunities

Transaction Signatures (TSIG)

- Master and slave servers:
  - share a common secret key
  - agree on the key name
  - have clocks which are approximately in sync (e.g. they both use NTP) (why?)
- The shared information is used to authenticate a client to a server

Zone Transfers

- TSIG is most-commonly used to authenticate slave servers to master servers during zone transfers
  - alternative to using source IP address ACLs
  - better than IP address ACLs (why?)

Secrets, Secrets

- If you don't run the slave servers and the mater servers yourself, you need a way to distribute the secret key to the slave server operator
  - how?
- You also probably want to change the key every now and then (why?)

DNS Security

DNS Insecurity?

- How can you trust answers you get from a cache?
- How can a cache trust the answers it gets from authority servers?
- How do you know that the www.centralbank.go.ke address you obtained is genuine?

DNSSEC

- DNSSEC is a 10+ year effort to introduce security into the DNS
- Secures the data in the DNS, not the transport
- Provides a way for clients to be able to judge the security of data they extract from the DNS

General Concepts

- Public Key Cryptography
- Clients obtain a trusted copy of a public key used to sign the root zone
- Each zone includes a signed copy of the public key of each signed daughter zone
- All resource records in a signed zones are signed by a zone-signing key

Detailed Description

- Ha ha, not here!
- Maybe if you have a spare week!

Questions?