DNS SECURITY

13.1 Security Overview

DNS Security is a huge and complex topic. It is made worse by the fact that almost all the documentation dives right in and you fail to see the forest for all the d@!mned trees.

The critical point is to first understand what you want to secure - or rather what threat level you want to secure against. This will be very different if you run a root server vs running a modest in-house DNS serving a couple of low volume web sites.

The term DNSSEC is thrown around as a blanket term in a lot of documentation. This greatly over simplifies the range of security solutions that are available. There are at least three types of DNS security, two of which are - relatively - painless and what is increasing just called DNSSEC which is - relatively - painful.

Security is always an injudicious blend of real threat and paranoia - but remember just because you are naturally paranoid does not mean that **they** are not after you!

▲

13.1.1 Security Threats

In order to be able to assess the potential threats and the possible counter-measures it is first and foremost necessary to understand the normal data flows in a DNS system. Diagram 1-3 below shows this flow.

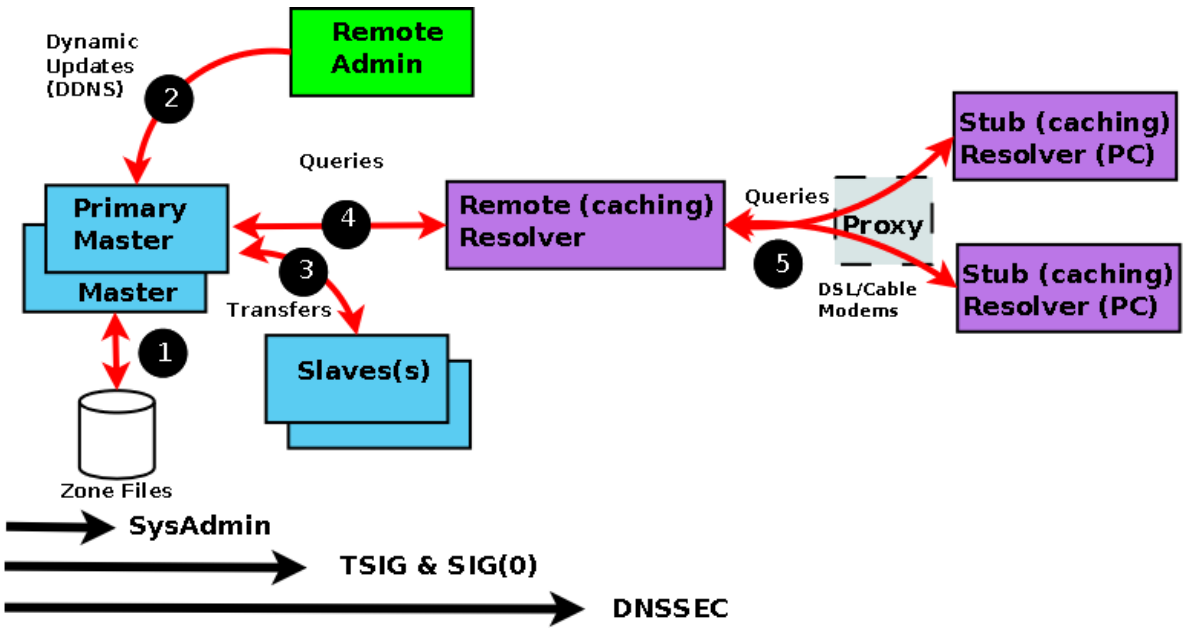

Diagram 1-3 DNS Data Flow

Every data flow (each RED line above) is a potential source of threat!. Using the numbers from the above diagram here is what can happen at each flow:

Number	Area	Threat
(1)	Zone Files	File Corruption (malicious or accidental). Reading private zone files, configuration files and logs to expose **hidden** devices. Local threat. Mitigated by good System Administration practices.
(2)	Zone Transfers	IP address spoofing (impersonating update source), DDoS attacks (persistent requests for transfer). Server to Server threat. Mitigated by either IP address limits or cryptographic solutions using TSIG (shared secret MAC).
(3)	Dynamic Updates	Unauthorized Updates, malicious updates, IP address spoofing (impersonating update source). Server to Server Threat. Mitigated by either IP address limits or cryptographic solutions using either TSIG (symmetric-like MAC)or SIG(0) (an asymmetric).
(4)	Remote Queries	Cache Poisoning/Pollution by IP spoofing, data interception or a subverted Master or Slave. DDoS attacks based on Open Resolvers and other configuration errors. Zombied or virus compromised PC or server. Server to Client threat. Mitigated by either IP address limits or cryptographic solutions using DNSSEC (asymmetric cryptography).
(5)	Resolver Queries	Data interception, Poisoned/Polluted Cache, subverted Master or Slave, local IP spoofing. Increasingly remote devices use a DNS proxy which can either be compromised, badly configured or poorly implemented. Remote Client-Client threat. Mitigated by end-to-end cryptographic solutions using DNSSEC (asymmetric cryptography).

The first phase of getting a handle on the problem is to figure (audit) what threats are applicable and how seriously they are rated, or determining if they even apply. As an example: if Dynamic Updates are not permitted (BIND's default mode) - there is no Dynamic Update threat. Finally, in this section a warning: **the further you go from the Master the more complicated the solution and implementation**. Unless there is a very good reason for not doing so, it is always recommend that you start from the Master and work out. It would be a little disappointing, after implementing a complex DNSSEC solution, to discover that zone files are all world-readable or that zone transfers are accepted from any source.

Source : http://www.zytrax.com/books/dns/ch13/