

Implementing DNSSEC into Domain Name System probably will not set up higher level of DDoS threats in existing domain resolution system except attacks against DNS software (software DoS). More lines of code responsible for DNSSEC cryptographic functions potentially could be exploited.

According to the tests conducted by NASK (November 2007), average DNSSEC responses are **bigger 3-4 times** than normal DNS traffic. Name Servers Internet links will be more loaded with DNSSEC outbound traffic than they're now with non-DNSSEC. In consequence we need to provide more bandwidth to absorb DDoS traffic. Therefore, one of costs implementing DNSSEC is increasing bandwidth of Name Servers Internet links.

As we know the most important factor in successful DDoS attack is amount of data transferred to target host. Today's most sophisticated attacks called 'reflected DDoS' is using open recursive name servers to reflect spoofed DNS packets to target machine/machines. These DNS packets includes special crafted TXT record with garbage data (about 4KB, determined by some software implementations). Of course forged source addresses isn't DNS problem itself and there's some methods to prevent such attacks like BCP38 but unfortunately it isn't widely used.

Reflected packet size does matter. We know that we can craft same big packets using DNS just like using DNSSEC but using large RRsets in DNSSEC we can omit crafting TXT records and using open recursive name servers as reflectors. The success of 'reflected DDoS' is amplification - relatively small query to big response. Amplification factor using large RRsets from DNSSEC may be smaller then using TXT records but it's still big.

We can talk about DNSSEC DDoS threats in scope of recursive servers. This machines will be responsible for setting chain of trust between them (resolvers) and trust anchor and also validate cryptographically secured DNS packets. More computing resources are needed. Potentially we can drain this resources with many queries. But this is local not global problem (open recursive servers are dangerous and should be separated in local networks).

DDoS against DNS with DNSSEC probably will not be more destructive then present attacks using old not cryptographically secured system. DNSSEC doesn't make DDoS problem worse.

Zbigniew Jasinski
zbigniew.jasinski@nask.pl