DNS DOS Saldırılarına Karşı Önlem

DNS'ler varsayılan olarak UDP protokolü üzerinden çalışırlar. UDP protokolünde TCP'deki gibi 3 yollu el sıkışma olmadığı için IP spoofing yapmak mümkündür. Yani saldırgan bir DNS sunucusuna kaynak IP'sini farklı göstererek sorgu gönderilebilir.

Peki IP spoofing ile DNS sunucularına yapılan DOS saldırılarını DNS sunucuları nasıl engelleyebilirler? Ya da DNS sunucuları yapılanın bir saldırı olduğunu, yani gelen paketin kaynak IP'sinin sahte olduğunu nasıl anlayabilirler? Bunları DNS sunucuları UDP protokolünün tasarımından kaynaklanan problem nedeniyle yapamazlar. Ne saldırıyı engelleyebilir ne de gelen paketin sahte IP'li olduğunu anlayabilirler. Bunları ancak ISP'ler yapabilir. Çünkü ISP'ler müşterilerinin IP'lerini bilirler ve müşteriden gelen paketin kaynak IP'siyle müşterinin IP'sini kıyaslayıp aynı değilse paketi düşürebilir ki böylece bir saldırı girişimini engellemiş olurlar, aynıysa yoluna devam etmesine izin verebilirler. Yani ISP'ler DNS sunucularını DOS ataklarından kurtarabilirler. Bu teorik olarak iyi bir çözüm gibi dursa da pratikte ISP'lerin bu işi halledecek yazılımlar geliştirmesi maliyetli olabilir: İşlemci kullanımı, bellek kullanımı, vs...

Kaynak:

https://www.youtube.com/watch?v=rbFBU9oMna8