An analysis of the DNS cache poisoning attack

Executive summary

The Domain Name System (DNS) is essential to the overall functioning of the Internet. Potential attackers are also aware of this and therefore try to find weaknesses and ways to attack this system. Since DNS has existed, several attacks have occurred; the latest known functional is the variant of DNS cache poisoning attack discovered by Dan Kaminsky in the summer of 2008. The attack affects recursive caching name servers (NS), whose basic function is to translate a domain name to an IP address. The recommended way of protection was update to a newer version of recursive NS, which already used randomly generated source ports for their DNS queries, whereby the threat of attack was significantly reduced. But it was not clear how long it would take to attack this 'fixed' recursive NS and under what conditions it would occur.

The document proposes a method for calculating the time requirements of a successful attack with the given probability and applies it to several attack scenarios which were tested in real network conditions using freely available implementation of a DNS cache poisoning attack.

In the case of randomly generated source ports of a recursive NS, an attack is far more complicated, but it is still possible. Overall attack time can differ significantly depending on the attack conditions, such as the bandwidth of the attacker, recursive or authoritative NS; response time of the recursive NS, the number of authoritative NS and other factors as described in the 'Appendix no. 1'. However, we can deduce from the results of the implemented attacks[i] that in a certain situations an attack can be successful within several days. Therefore, DNSSEC[ii] technology, which provides data integrity and the certainty that they have been provided by the correct source, should be implemented as a reliable solution against DNS cache poisoning attacks.

[i] Measured attack times are given in Appendix 2.

[ii] For more information, visit http://www.nic.cz/dnssec/ and http://www.dnssec.net/

Appendix 1 - Factors influencing a DNS cache poisoning attack

Limiting factors of a DNS cache poisoning attack		
Name	Impact	Description
Spoofed source address detection	An attack is not possible	The router between the attacker and the recursive NS blocks packets with a fake source address
Recursive and authoritative NS with DNSSEC	An attack is not possible	DNS Security Extensions protect against DNS cache poisoning attacks
Recursive NS with query filtering	Restricts an attack from permitted networks	The NS accepts recursive queries only from the list of permitted networks
Random ID and source ports	Reduces the effectiveness of an attack	A recursive NS uses randomly generated ID and source ports for its queries
More authoritative NS for the domain	Reduces the effectiveness of an attack	Each new authoritative NS reduces the probability of guessing the source address
IPv6 address on an authoritative and recursive NS	Reduces the effectiveness of an attack	IPv6 address on an authoritative and recursive NS reduces the probability of correctly guessing the response source address of the authoritative NS
Fast response time / high-capacity bandwidth of an authoritative NS	Reduces the effectiveness of an attack	Fast response times reduce a window of opportunity. Sufficient bandwidth makes DDoS attacks on an authoritative NS more difficult.
Insufficient router performance	Reduces the effectiveness of an attack	Insufficient router performance causes loss of attacker’s traffic
Insufficient bandwidth of the attacker or recursive NS connection	Reduces the effectiveness of an attack	Line congestions between the attacker and the recursive NS causes traffic loss
Server or network monitoring	Blocking an attack	Monitoring can recognise increased data flow or load on system resources
Supporting factors of a DNS cache poisoning attack		
DDoS against the authoritative NS	Increases the effectiveness of an attack	The DDoS attack delays or suppresses the response of an authoritative NS and thereby extends the window of opportunity for fake traffic and reduces attack overhead
Recursive NS behind address translation	Increases the effectiveness of an attack	NAT can degrade the source port randomness of a recursive NS
Significant difference in the response time of authoritative NS	Increases the effectiveness of an attack	A recursive NS prefers an authoritative NS with better response time; if the attacker does the same, there will be a better chance of guessing the source address of the fake response

Appendix 2 - Results of attacks and their probabilities

Attack on a recursive NS with a pseudo-randomly generated source port				
Test	Generated traffic of fake responses	Window of opportunity ms	Delivered fake responses per window of opportunity	Duration of the attack (corresponding probability)
1.	85.31 Mbps	45.491	3 820	25 hours 40 minutes (59%)
2.	64.08 Mbps	18.501	1 171	93 hours 41 minutes (88%)
3.	14.34 Mbps	102.241	1 466	64 hours 3 minutes (32%)
4.	14.80 Mbps	684.982	10 139	25 hours 0 minutes (15%)
5.	14.80 Mbps	597.701	8 845	95 hours 52 minutes (45%)
6.	14.15 Mbps	650.851	9 207	50 hours 41 minutes (26%)
7.	14.47 Mbps	504.132	7 293	248 hours 30 minutes (78%)

Based on the results of these final seven attacks we can say that the calculated time requirements for a successful attack are higher than will be actually necessary.