draft-fujiwara-dnsop-poisoning-measures-00

Kazunori Fujiwara, JPRS
fujiwara@jprs.co.jp
IETF 90 dnsop WG, July 2014

Forged response cache poisoning

- Bernhard Muller, Improved DNS spoofing using node re-delegation, July 2008
- Wikipedia DNS spoofing
  - http://en.wikipedia.org/wiki/DNS_spoofing

> Redirect the target domain's nameserver
>
> The first variant of DNS cache poisoning involves redirecting the nameserver of the attacker's domain to the nameserver of the target domain, then assigning that nameserver an IP address specified by the attacker.

- Dan Kaminsky, "DNS 2008 and the new (old) nature of critical infrastructure", July 2008
- RFC 3833 Threat Analysis of the Domain Name System (DNS)
  - 2.2. ID guessing and query prediction
- Birthday attacks

2. Detection

- Attacks hardly success by one time trial
- Victim full resolver receives many unmatched responses
- They contain what attacker want to inject
- However, forget responses may be too much
  - Log aggregation is important
- Important data is
  - Query source address of random queries
  - Base domain name of random queries
  - Authority and Additional section of forged responses

3.Measures to forged response attacks

- Use TCP as a DNS transport
  - each TCP packet has 32bit sequence number
  - the attacker need to inject at least two packets
    - SYN and first DATA
- Issues
  - Increased response time
  - Performance (both full resolver and authoritative)

4. Possible solution

- Combination of the detection and the use of TCP transport
  - Detect attacked domain names
  - Change attacked domain name queries to use TCP transport
- This idea may be well known and some products may implement it already
  - They may have patents
- Encryption of DNS traffic is a good countermeasure, however, both resolvers and authoritatives need to be changed

Missed to write -00

- When you detect poisoning
  1. Flush the poisoned RRSet
  2. Resolve the poisoned RRSet
  3. Compare the poisoned RRSet with other full resolvers
     - Your other full resolvers
     - Or, public DNS (for example, Google)
  - Because cache flush may cause another poisoning
- Other measures
  - DNS cookies
  - Nonce prefix (Google Public DNS)
  - harden-referral-path (unbound)
  - Assign many IP addresses to full-resolvers

Question and request

- May I gather measures ?
- Is this draft useful ?
- If it is useful, I need co-authors