Contribution ID : **13** Type : **Standard Presentation**

Measures against cache poisoning attacks using IP fragmentation in DNS

Monday, 13 May 2019 12:00 (30)

Researchers proposed DNS cache poisoning attacks using IP fragmentation.
This talk reports them and proposes feasible and adequate measures at full-service resolvers against these attacks.
To protect resolvers from these attacks, avoid fragmentation (limit requestor's UDP payload size to 1220/1232), drop fragmented UDP DNS responses and use TCP at resolver side.
And more, it will report current status of fragmentation and EDNS0 payload size.
It is time to consider to avoid IP Fragmentation (and path MTU discovery) in DNS. It is not good that DNS is the biggest user of IP fragmentation.

(draft-fujiwara-dnsop-fragment-attack)

Summary

Talk Duration

30 Minutes

Primary author(s) : FUJIWARA, Kazunori (Japan Registry Services Co., Ltd)

Presenter(s) : FUJIWARA, Kazunori (Japan Registry Services Co., Ltd)

Track Classification : Public Workshop