Review “Kaminsky”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name：

Friedl, S. (2008). An illustrated guide to the kaminsky dns vulnerability. *Unixwiz. net Tech Tips, August*.

Contribution:

In this paper covers mechanism behind DNS both at high level and at packet structure level. It also describes vulnerabilities which introduces cache poisoning attack for DNS. At the end, the author gives out some suggestions on mitigation against cache poisoning. Kaminsky identifies by flooding the recursive server with lots of answers and the right combination could be sent a few seconds. This paper also states that the two identifiers the attacker needs to guess are not random.

Motivation:

DNS is not secure. This paper states that DNS has vulnerability in following process: (1) computer sends a query to a DNS server; (2) DNS server replies answers back to the computer; (3) if the answer appears to match the query, the computer completely trusts that it is correct. This leads to a vulnerability in DNS, as multiple ways exist to make traffic on the Internet can be intercepted and rerouted, or impersonated.

For performance consideration, DNS servers usually store results cache for speeding up lookups. In case of cache is poisoned, wrong answers to queries are stored, wrong queries results will be replied to who request for ip addresses.

Related works:

This paper firstly reviews terminologies for DNS, and how DNS works. Then introduces how cache is involved in this process. And it reviews previous works on how poisoning cache might impact the result.

Methodology:

Cache is used to improve performance of lookups in DNS servers. Cache poisoning attack works as: (1) a computer sends out query and waits for an answer to return; (2) if the query computer t has gets a packets with several attributes in the answer match the question it asked, it claims it has got answer of ip address for domain name requested; (3) if a DNS server with wrong answers replies faster than the right one, the computer assume the wrong answer is the correct ip address for domain name requested.

The matched field includes: (1) it got reply from same IP address it was sent from; (2) it got reply from same port number is was sent from; (3) query result matches the query asked; (4) unique transaction number matches what was sent.

Results:

Cache poisoning works as first good answer wins.

Take away:

We should introduce security to the DNS by: (1) upgrading the DNS server with patches for security, like SSL; (2) turning off open recursive name servers, as the attack does not work if attacker can not send question packets to name servers; (3) make randomised transaction numbers for query ID.