IETF93
22 July 2015
Prague
DNSSD WG

mDNS/DNSSD Threat Analysis

draft-rafiee-dnssd-mdns-threatmodel-03

Author:
Hosnieh Rafiee
Ietf{at}rozanak.com

Threat Analysis Current Status

- Draft draft-rafiee-dnssd-mdns-threatmodel-03 posted on 30 May

Applied comments received during the discussion with WG chairs and discussion on the mailinglist

The updates includes:

  - Removed any attacks that can be applicable and generalized for cases other than mDNS. e.g. virus
  - Improved the sections related to scope of attacks
    - e.g. service configuration which result in exposing the information to unwanted scope

Next Update

- New discussion on the mailinglist regarding amplification attack and mixing unicast DNS and mDNS
  - **Subsection under privacy section:**
    - Mixing unicast and multicast DNS: unicast queries from non-local link that is answered by the multicast DNS service and leaks information
      - Why a service need to request something from a unicast DNS? How a unicast DNS knows the IP address of the service? Why a service receives the unicast DNS request from other network if the recursive DNS server is not in the same network?
  - **Subsection under DoS:**
    - DNS amplification attack on a service that is the result of the IP address of a service known to an attacker.
  - **Subsection under Protection mechanism**
    - Protection against DNS amplification attack
      - Response Rate Limit (RRLs) both on service and unicast DNS
      - Proper authentication mechanism in the unicast DNS

Summary of Attacks

- DoS attack (DNS amplification, gateway or proxy amplification, spoofing → DoS)
- Interoperation of unicast DNS and mDNS
  - Malicious update, exposing mDNS to unwanted scope, rogue service with different character set that is not detectable by human)
- Information leakage to unwanted scope that lead to DoS or privacy issues
  - Dual stack, mis-configuration of a service or network edge devices e.g. a router, ULA and GUA Considerations
- mDNS poor implementation & Cache poisoning
  - Rogue mDNS service response to unicast DNS query request by a client faster than the unicast DNS.

Possible Protection mechanisms

- DANE
- DNSSEC
- SAVI-DHCP
- IPsec
- etc.
- **Other Security consideration**
  - Controlling scope of advertisements
    - mDNS proxy and IPv6 (multiple IP on interfaces)

Question?

Thank you!