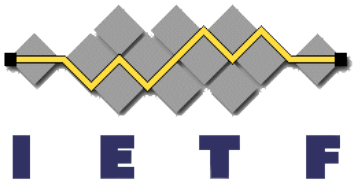
IETF91
23 March 2015
Dallas
DNSSD WG

mDNS/DNSSD Threat Model

draft-rafiee-dnssd-mdns-threatmodel-02

Author:
Hosnieh Rafiee



Threat Analysis Current Status

- Draft draft-rafiee-dnssd-mdns-threatmodel-02 posted on 22 March to apply last discussions on the mailinglist and last IETF
- The updates includes:
  - Categorized threats and describe them in different use case scenarios e.g. PAN, home network, enterprise, 6LowPAN, etc.
  - Added more attacks (human errors, internationalized label, ULA and GUA (scope attacks)
  - Improved solution scope:
    - Authentication/authorization mechanisms for both a service and a service requester
    - Privacy consideration
    - Evaluation of some of existing protection mechanisms

Human Errors

Threat	How
DoS	Mis-configuration of a service, Virus and malware
Harm Privacy	Expose service to wide scopes

Unicast DNS update and DNS names

Threat	How
Rogue Service	Similar character internationalized labels
Harm Privacy	Storing names in unicast DNS which is accessible over the Internet
Unauthorized access	Unauthorized update on unicast DNS
Mixing unicast and mDNS names	Poison service requester's cache with global unicast DNS names so that doing phishing attacks

Node Compromising

Threat	How
Rogue Service	(attacker is inside a network) Advertise fake non-existance services
DoS attack	Overwhelm victim node with several requests
Unauthorized access	Unauthorized access to a service as a legitimate node
Forge a service	Claim to be one of the services used for load balancing and responds to service requests

Spoofing

Threat	How
Forge a Service	Advertise fake services by spoofing IP or mac address of a service
Forge a service requester and unauthorized access to it	When there is an ACL on a service, spoof IP or mac address of a legitimate service requester
Cache poisoning	List of services are stored on service requester's caches -> fake service advertisement remains in cache
IP spoofing and DoS on a service requester	Overwhelmed service requester by sending several requests with legitimate service requester's source IP

ULAs and GUAs

Threat	How
Harm privacy	Expose a service to unwanted scope in IPv6 networks
Unauthorized access	A service is available to broader scope when ULAs are not correctly configured on routers or a service set a GUA automatically from a DHCP server
Dual stack attacks	Expose a service to unwanted scope

DoS

Threat	How
Virus or malware	Driver corruption (service unavailable)
DoS on a service	Large traffic and Single point of failure
DoS on a mDNS proxy	Large traffic and Single point of failure

Evaluation of Existing Protection mechanisms

- DNSSEC
  - **Disadvantage:** not zero configuration protocol, no privacy protection, Performance might not be good for 6LowPAN nodes, establish a trust model
  - **Advantages:** authentication, authorization (with using a trust model), interoperability with unicast DNS
- SAVI-DHCP
  - **Advantages:** Prevent IP spoofing
  - **Disadvantages:** need special device to support it, no privacy protection
- IPsec
  - **Advantages:** Privacy (by tunnel mode), Authentication
  - **Disadvantages:** establish a trust model, not zero configuration protocol, Performance for 6LowPAN nodes

Any Other Open Issues?

Thank you!