IETF91
13 November 2014
Honolulu
DNSSD WG

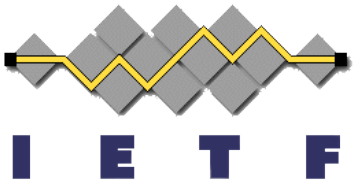
mDNS/DNSSD Threat Model

draft-rafiee-dnssd-mdns-threatmodel-01

Author:

Hosnieh Rafiee

HuaweiTechnologies Duesseldorf GmbH, Munich, Germany



Unicast DNS vs. mDNS/DNSSD - Differences (Scope of Threats)

- mDNS/DNSSD submits multicast messages
- mDNS/DNSSD is adhoc
  - Only the names are valid inside the local networks therefore, it does not expose names and IP addresses beyond local networks
  - Translates names to IP addresses when there is no DNS infrastructure available (efficient translation)
  - Discover services in the network by service instance enumeration (browsing)
- mDNS/DNSSD is a zero configuration protocol
  - mDNS/DNSSD is efficient to use for constrained devices (WSN)
- mDNS checks uniqueness of names only in limited scope while unicast DNS can check the uniqueness of names globally

Unicast DNS vs. mDNS/DNSSD - Similarities

- DNSSD can also use unicast messages similar to unicast DNS
- Both translates names to IP addresses and check the uniqueness of names
- Both caches some data.
  - For example DNSSD caches the service names with their TTL in the client and unicast DNS caches domain names and IP addresses
- Both do not encrypt the message contents
- Both are dependent to other mechanisms for security

Threats: unicast DNS vs. DNS-SD

- RFC 3833 covers a limited list of threats for unicast DNS. Here is the categorization of all those attacks

Similar Threat Groups	Specific to DNS-SD	Specific to unicast DNS
• Spoofing (source IP spoofing, identity spoofing, MITM, cache poisoning) • DoS attacks • Data tampering • Similar names with different character sets (internationalized labels) – fake domains	MAC spoofing	• Privacy issue (IP address, names leakage) • Unauthorized update to DNS zone file • Human errors (configuration mistakes, etc.)

Scalable DNS-SD (SSD) vs. mDNS/DNSSD -- Differences

- SSD covers larger scope and not only local link (explained in section 3 requirement document)
- In SSD, names and IPs are exposed to larger groups and increase the privacy risks
- SSD might not be zero config
  - Zero configuration only for home and PAN networks
  - Requires configuration on switches and routers to increase the scope of discovery
  - Might require SLA between domain administrators especially in campus networks

Threats: Scalable DNS-SD (SSD) vs. DNS-SD - I

Similar Threat Groups	Specific to DNS-SD	Specific to SSD
• Spoofing (source IP spoofing, identity spoofing, MITM, cache poisoning, MAC spoofing) • DoS attacks • Data tampering • Names with different character sets (internationalized labels)		•Privacy issue •(IP address, names leakage) •Network topology leakage • Unauthorized update to unicast DNS • Especial type of DoS attack -- Resource exhaustion (especially applicable to constrained devices)

Threats: Scalable DNS-SD (SSD) vs. DNS-SD - II

Similar Threat Groups	Specific to DNS-SD	Specific to SSD
		• Unauthorized access to service providers (like a printer) • Human errors (incorrect configuration of middle boxes) allows wide range of attacks • Node compromising: resulting in flooding the network with false information (larger traffic if it supposed to be broadcast)

Solution Scope

Threats	Solution Scope
Unauthenticated Device	The Use of access lists, policies, secure authentication, proof of IP ownership/MAC ownership
DoS	Authentication, network monitoring
Unauthorized Access	Access lists, policies
Data tampering	Data integrity check
Privacy issue	Randomization (efficient), data encryption (cost effective), Control on Discovery scope

Not in SSD Charter but in a scope of service discovery

In virtualized network many services are software based and can be accessed by their names/labels

- The use of DNSSD to discover security functions in Network Function Virtualization (NFV)
  - Advantage
    - Abstraction
  - Disadvantage
    - All the threats explained in t his presentation
- The use of DNSSD to discover different APIs or users who wants to request any functions in the network

Next steps?

- WG adoption?