DNSSD
INTERNET-DRAFT
Intended Status: Informational
Expires: December 10, 2014

H. Rafiee
Huawei Technologies

June 10, 2014

Multicast DNS (mDNS) Threat Model and Security Consideration <draft-rafiee-dnssd-mdns-threatmodel-00.txt>

Abstract

This document describes threats associated with extending multicast DNS (mDNS) across layer 3.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 10, 2014.

Table of Contents

1. Introduction

Multicast DNS (mDNS) was proposed in [RFC6762] to allow nodes in local links to use DNS-like names for their communication without the need for global DNS servers, infrastructure and administration processes for configuration. mDNS along with service discovery (DNS-SD) [RFC6763] provides nodes with the possibility to discover other services and the names of other nodes with zero configuration, i.e., connect a node into a local link and use resources such as a printer that are available in that network.

mDNS and service discovery use DNS- like query messages. The main assumption is that these services also use DNS security protocols such as DNSSEC. However, due to the limitation of DNSSEC in local link, i.e., the key authorization and configuration needed for DNSSEC, it is not easy to use this protocol for zero configuration services. This is why the current implementations use no security in local links and are vulnerable to several attacks.

The purpose of this document is to introduce threat models for mDNS and service discovery and allow implementers to be aware of the possible attacks in order to mitigate them with possible solutions. Since there are already old lists of known DNS threats available in [RFC3833], here we only analyze the ones that are which is applicable to mDNS. We also introduce new possible threats that could result from extending mDNS scope.

2. Terminology

Node: any host and routers in the network

Attack: an action to exploit a node and allow the attacker to gain access to that node. It can be also an action to prevent a node from providing a service or using a service on the network

Attacker: a person who uses any node in the network to attack other nodes using known or unknown threats

Threat: Anything that has a potential to harm a node in the network

Local link vulnerability: Any flaws that are the result of the assumption that a malicious node could gain access to legitimate nodes inside a local link network

Wide Area Network (WAN) vulnerability: Any flaws that are the result of the assumption that a malicious node could gain access to legitimate nodes inside any local links in an enterprise network with multiple Local Area Networks (LANs) or Virtual LANs (VLANs).

Host name: Fully qualified DNS Name (FQDN) of a node in the network

Constrained device: a small device with limited resources (battery, memory, etc.)

3. Threat Analysis

mDNS/DNS-SD cannot use DNSSEC approaches for security purposes. This is because, as mentioned earlier, DNSSEC is not a zero config protocol and it is not compatible with the plug and play nature of mDNS/DNS-SD. This is why mDNS is vulnerable to several attacks. Most threats in this section are a result of spoofing, Denial of Service (DoS), or a combination of them. Here we explain them in different example scenarios.

3.1. mDNS Gateway is a single point of failure

An mDNS gateway needs to process all queries sent to/from different networks that this gateway is connected to and filters the traffic based on the policy explained in section 3.4 [mdns-extend]. A malicious node in any of these subnets can send several queries and carry out the DoS attack on these gateways.

3.2. Large Traffic Production from mDNS Gateway

There are several scnearios associated with the Large Traffic Production case.

First scenario: a malicious node in any of the subnets that the gateway connects can advertise different fake services or spoof the information of the real services and replay the messages. This causes large traffic either in the local link or in other links since the gateway was also supposed to replicate the traffic to other links.

Second scenario : a malicious node spoofs the legitimate service advertisements of different nodes in the network and changes the Time To Leave (TTL) value to zero. This will result in producing large traffic since the mDNS gateway needs to ask all of the service advertisers to re-advertise their service. This is an especially effective attack in a network of constrained devices because it causes more energy consumption.

Third scenario: Since a hybrid proxy [hybrid-proxy] node aggregates all data and sends it back to the requester, a malicious node can generate several queries that produce large responses, spoof the source or MAC address of a victim node in this network, and forward all traffic to this victim node.

Forth scenario: A malicious node can replay hybrid proxy aggregation

messages [hybrid-proxy] and cause a DoS on a victim node.

3.3. DoS attack on any node in the mDNS enabled network

A malicious node spoofs the MAC address and source IP address of a legitimate victim node in this network and questions several services in the link. This will result in a large traffic return to the victim node from both mDNS gateway and also the service owner.

A malicious node can send a spoofed service probe message and direct all traffic to any victim node to this network (section 3.5 [mdns-extend]).

Second scenario: a malicious node claims the ownership of any name that the resource requester or a node uses and does not let the nodes choose a unique desired name for their service or for the devices.

3.4. Good mDNS gateway goes bad

mDNS gateway is compromised and submits wrong information to the links to which it is connected.

3.5. Fake mDNS gateway

A malicious node can play a role of gateway in any of those subnets and play a Man in the Middle (MITM) attack. Since the messages sent from gateway are usually unicast, no other nodes will detect these malicious activities of this fake gateway. (section 3.8.1 [mdns-extend]). This malicious node can then respond to any DNS-SD messages and play a role of passive gateway.

3.6. MAC address spoofing

In a wireless environment where [mdns-extend] is suggested to use MAC address filtering to avoid any malicious node joining to the network, a malicious node can easily spoof the MAC address of a legitimate node and join the network and perform malicious activities.

3.6.1. possible solution

Filtering can be based on the signature of the public key and MAC address of the devices . This process might be through manual adding of this signature to the whitelist filter. The verification is the process of verifying the signature signed by the private key and the public key signature. This solution might require some manual step and changes on the current implementation to filter based on this signature.

3.7. Cache Poisoning

mDNS gateway stores all of the information related to the available wireless nodes in its cache. In section 3.8.1 [mdns-extend], it is not clear how mDNS gateway knows when a node leaves a wireless link. If the node sends a "leave message" to mDNS gateway, a malicious node can send this message on behalf of a legitimate node and presume that that the legitimate node does not exist in that link, thereby causing delay or possible problems in offering service to that node.

Second scenario: a malicious node can send a location update message to mDNS home gateway and cause delay in offering services to a legitimate node.

Third scenario: similar to Mobile IPv6 [RFC6275] possible attacks, a malicious node can start large traffic from a streaming server and then send a fake ?location update message? to the home mDNS gateway and send a update message with a different, spoofed source IP address. This will forward all of the large streaming traffic to a victim node.

Forth scenario: To decrease traffic in the network [hybrid-proxy], a hybrid proxy aggregates all answers received from different resources and sends a unicast DNS message on behalf of all of the resources to the resource requester. A malicious node can play the role of hybrid proxy and poison the cache of resource requester.

3.7.1. Possible solution

IPsec can prevent this attack but it is not a zero configuration protocol and it needs a way to provide the initial trust between both end points of communication.

3.8. Malicious update on unicast DNS

A malicious node can spoof the content of DNS update message and add malicious records to unicast DNS.

3.9. Harming Privacy

If a malicious node is in any subnet (WLAN and WAN) of a network, it can learn about all services available in this network. The combination of mDNS and DNS-SD discloses some critical information about resources in this network which might be harmful to privacy.

3.10. IP spoofing

A malicious node spoofs the content of Dynamic Host Configuration

Protocol (DHCP) server messages and offers its own malicious information to the nodes in the network.

3.11. Resource spoofing

Resource owners in the network have permission to have the same name for load balancing. A malicious node can claim to be one of the load balanced resource devices and maliciously respond to requests.

3.12. Internet Group Management Protocol (IGMP) Attacks

IGMP that is suggested to be used in network bridging scenario [mdns-x] can be maliciously used by an attacker. Spoofing and DoS attacks are two sources of attack in IGMP protocol. A complete list of these attacks can be found in [IGMP-Attack].

3.13. Multicast Listener Discovery (MLD) attacks

The same as IGMP attacks, since these are signaling protocols, a simple DoS attack can use a lot of resources and produce large traffic. This is because a malicious node can send MLD to subscribe to a large number of high-bandwidth multicast groups. It can then cause bandwidth exhaustion, leading to a DoS. It might also lead to using more CPU resources on the nodes. This will be quite critical for constrained devices.

3.14. Fake Resource Advertisement

A malicious node in any subnet can advertise fake resources. The other nodes have no possibility to authenticate this node and authorize its resources. This can happen in both mDNS gateway scenario and hybrid proxy [hybrid-proxy].

3.15. Dual stack attacks

Having both IPv4 and IPv6 in the same network and trying to aggregate service discovery traffic on both IP stacks might cause new security flaws during the conversion or aggregation of this traffic. It can be similar to what explained here as an aggregated traffic or lead to a wide range of spoofing attacks.

4. Possible solutions

Since spoofing is the main source of attacks for many malicious activities, using approaches that can prevent IP spoofing or provide a means of secure authentication with minimum configuration is helpful.

4.1. SAVI-DHCP

SAVI-DHCP [DHCP-SAVI] approach uses a simple mechanism in switches or devices that knows information about the ports of switches to filter any malicious traffic. This mitigates attacks on DHCP server spoofing

4.2. DNS over TLS

The approaches in this category are discussed in DANE WG. It might be a good solution to automate the authentication processes or avoid spoofed DNS update messages

4.3. CGA-TSIG

CGA-TSIG [cga-tsig] is another possible solution that can provide the node with secure authentication, data integrity and data confidentiality. The new version supports both IPv4 and IPv6. It provides the node with zero or minimal configuration.

4.4. DNS Security Extension

Due to the manual step requirement for DNSSEC configuration on each nodes and DNS servers, it is not an ideal solution mechanism for zero config services.

4.5. SSAS

SSAS [ssas] can prevent the nodes from IP spoofing. This is dissimilar to other approach, CGA [RFC3972] that can only support IPv6 networks. The new version of this document supports both IPv4 and IPv6. It also offers a solution for MAC spoofing, however, due to operational barriers, MAC spoofing solution might not work well.

4.6. IPsec

IPsec is another security protection mechanism. Similar to DNSSEC, it requires manual step for the configuration of the nodes. However, recently there are some new drafts to automate this process.

5. Security Considerations

There is no security consideration

6. IANA Considerations

There is no IANA consideration

7. Acknowledgements

The author would like to thank all those people who directly helped in improving this draft, especially John C. Klensin

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6762] Cheshire, S., Krochmal, M.,"Multicast DNS", RFC 6762, February 2013

[RFC6763] Cheshire, S., Krochmal, M., "DNS-Based Service Discovery", RFC 6763, February 2013

[RFC6275] Perkins, C., Johnson, D., Arkko, J., "Mobility Support in IPv6", RFC 6275, July 2011

[RFC3833] Atkins, D., Austein, R., "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004

8.2. Informative References

[mdns-extend] Bhandari, S., Fajalia, B., Schmieder, R., Orr, S., Dutta, A., "Extending multicast DNS across local links in Campus and Enterprise networks", http://tools.ietf.org/html/draft-bhandari-dnssd-mdns-gateway-00, October 2013

[mdns-x] Otis, D., "mDNS X-link review", http://tools.ietf.org/html/draft-otis-dnssd-mdns-xlink-03, April 2014

[IGMP-Attack] http://www.securemulticast.org/GSEC/gsec3_ietf53_SecureIGMP1.pdf

[hybrid-proxy] Cheshire, S., "Hybrid Unicast/Multicast DNS-Based Service Discovery", http://tools.ietf.org/html/draft-cheshire-dnssd-hybrid-01,

[DHCP-SAVI] Bi, J., Wu, J., Yao, G, Baker, F.,"SAVI Solution for DHCP", http://tools.ietf.org/html/draft-ietf-savi-dhcp-23, April

2014

[cga-tsig] Rafiee, H., Loewis, M., Meinel, C.,"Transaction SIGnature (TSIG) using CGA Algorithm in IPv6", http://tools.ietf.org/html/draft-rafiee-intarea-cga-tsig , February 2014

[ssas] Rafiee, H., Meinel, C., "SSAS: a Simple Secure Addressing Scheme for IPv6 AutoConfiguration". http://tools.ietf.org/search/draft-rafiee-6man-ssas, 2013

Authors' Addresses

Hosnieh Rafiee
http://www.rozanak.com
Phone: +49 176 57 58 75 75
Email: ietf@rozanak.com