DNSSD
INTERNET-DRAFT
Intended Status: Informational
Expires: November 30, 2015

H. Rafiee
Rozanak

May 30, 2015

Multicast DNS (mDNS) Threat Model and Security Consideration <draft-rafiee-dnssd-mdns-threatmodel-03.txt>

Abstract

This document describes threats only specific to 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 November 30, 2015.

Copyright Notice

Table of Contents

1. Introduction 3
2. Terminology 3
3. Threat Analysis 4
3.1. Human Mistakes 4
3.2. DoS attack 4
3.2.1. Large Traffic from mDNS gateway 4
3.2.2. Single point of failure 5
3.3. IPv6 specific mDNS scope problems 5
3.4. Malicious update on unicast DNS 5
3.4.1. mixing unicast names with mDNS names 5
3.5. Privacy Problems 6
3.5.1. Storing mDNS names in unicast DNS 6
3.6. Internationalized label and Rogue service 6
3.7. Dual stack attacks 6
3.8. Privacy Protection Mechanisms 6
3.8.1. The Use of Random Data 6
3.8.2. Data Encryption 7
3.9. Evaluation of Security Protection Mechanisms 7
3.9.1. Unicast DNS protection mechanisms 7
3.9.1.1. DNSSEC 7
3.9.1.2. CGA-TSIG 7
3.9.1.3. DNS over DTLS 7
3.9.2. Authorization of a Service Requester 7
3.9.2.1. The Use of an Access List 7
3.9.2.2. SAVI-DHCP 8
3.9.2.3. The Use of Shared Secret 8
3.9.3. Authorization of a Service 8
3.9.3.1. SAVI-DHCP 8
3.9.3.2. Router advertisement 8
3.9.4. ULA and GUA Considerations 9
3.9.4.1. mDNS proxy and Security consideration 9
3.9.5. Other Security Considerations 9
3.10. Not Usable Security Mechanisms 9
3.10.1. IPsec 9
4. Security Considerations 9
5. IANA Considerations 9
6. Acknowledgements 10
7. References 10
7.1. Normative 10
7.2. Informative 11
Authors' Addresses 12

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 (SD) use DNS- like query messages. The main assumption is that these services also use DNS security protocols such as DNSSEC. However, it cannot use DNSSEC for security because DNSSEC is not zero configuration service. Therefore, it cannot be used for Requirements A, B,C in [requirement]. Besides, DNSSEC cannot be implemented in all nodes, especially nodes with limited resources, e.g. 6LoWPAN [RFC4944]. This is why the existing implementations use no security in local links. This might be not a critical problem when the service was only advertised in local link but it is not the same when the service is going to be advertised over layer 3 and in larger scope. Furthermore, during this step, DNS-SD did not consider the impact of [RFC4193] that should be carefully considered when using mDNS to populate DNS. As such, a Universal Local Address (ULA) prefix is not to be advertised outside the network domain. This is also similar to the scenario where address preference rules employed by a proxy device as defined in section 2.4. [RFC7368].

The purpose of this document is to introduce threat models for 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 applicable to DNS-SD. We also introduce new possible threats that could result from extending DNS-SD 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.)

Service advertiser or service: a node that has a service to advertise, e.g. a printer

Service Requester: a node in the network that requests a service by the use of DNS-SD protocols. One example of service requester is a computer that discovers a printer in the network and tries to use it.

3. Threat Analysis

This section only focuses on threats that are specific to mDNS/DNS-SD. Here we explain them in different example scenarios. The definition of different use case scenarios are defined in [requirement].

3.1. Human Mistakes

For those deployments that needs configuration, mis-configuration of DNS-SD scope on edge devices such as a router or a gateway might allow an attacker to gain access to services or expose the network topology to outside of an administrative domains. This is applicable to all scenarios including PAN, WPAN, home, enterprise, campus, mesh networks.

3.2. DoS attack

3.2.1. Large Traffic from mDNS gateway

There are several scenarios 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 Live (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: a malicious node can spoof the source IP address of a legitimate victim node and question several services in the link. This will result in a large traffic return to the victim node from both gateway and also services.

3.2.2. Single point of failure

a service (like a printer) can overwhelmed with many service discovery requests from a malicious service requester. This might result in long waiting times (delay) for a legitimate node to receive a service.

3.3. IPv6 specific mDNS scope problems

When the ISP, home router/gateway, and a service (like a printer) support IPv6 addressing, these services may automatically announce over mDNS both Unique Local Addresses (ULA) [RFC4193] and Global Unicast Addresses (GUA). Since a GUA is accessible over the internet, the associated node may become available to the public. The advertisement needs to be under control to avoid a GUA for a service becomes known to an attacker. Furthermore, the ULA scope should be clearly defined so that it does not advertise it to unwanted scope. This is because it might grant unintended access to a service otherwise limited by boundaries imposed by mDNS discovery. This attack is applicable to home, public hotspot, enterprise, campus and mesh networks.

3.4. Malicious update on unicast DNS

A malicious node can spoof the content of DNS update message and add malicious records to unicast DNS. This attack is applicable on enterprise networks.

3.4.1. mixing unicast names with mDNS names

A fake service might poison the cache of a service requester with records that has global unicast name, if the service requester's deployment needs configuration and is poorly configured or the

implementation has problem, then the mDNS request might have priority over DNS request which will lead to phishing attacks.

3.5. Privacy Problems

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 DNS-SD discloses some critical information about resources in this network which might be harmful to privacy. This attack is applicable to temporary public hotspot and enterprise networks.

3.5.1. Storing mDNS names in unicast DNS

When a name of a service is stored in unicast DNS Resource Records, in case this unicast DNS is accessible over the internet or over several networks, it might expose the services to unwanted nodes and harms privacy. This is applicable to campus networks, mesh networks, temporary public hotspots and enterprise networks.

3.6. Internationalized label and Rogue service

Using Internationalized label might allow an attacker to advertise a fake service with similar looking character as legitimate service. This might lead to the case where user chooses fake advertised service as a legitimate one.

3.7. 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 translation or aggregation of this traffic. It might lead to wide range of spoofing attacks or leak service advertisements (the service advertisement is no longer under control). This attack is applicable to home, enterprise, campus, mesh and temporary public hotspots.

3.8. Privacy Protection Mechanisms

3.8.1. The Use of Random Data

Using a random name for services or devices or the use of random numbers wherever possible, might prevent exposing the exact model or exact information regarding the DNS-SD service providers (e.g. printers, etc.) in the network to the attackers. However, this approach cannot be used for some standard information that the protocol needs to carry in order to offer service to other nodes. Otherwise, this random information was exchanged and agreed on

between service providers and service requesters beforehand. This is exactly against the nature of zero conf protocols, i.e., DNS-SD

3.8.2. Data Encryption

Encrypting the whole DNS-SD message is another way to hide the critical information in the network. But this approach might not fit well to the nature of this protocol. The reason is because these devices usually respond to anonymous service discovery requests. So, the attacker can also submit and request the same information. In other words, encryption in this stage is only extra efforts without having any benefit from it.

3.9. Evaluation of Security Protection Mechanisms

3.9.1. Unicast DNS protection mechanisms

3.9.1.1. DNSSEC

DNSSEC can be used to allow any services to update its records on unicast DNS that supports DNSSEC. However, it is not a zero configuration mechanism and need the introduction of the DNSSEC key to a service or availability of a trust model. Furthermore, this mechanism does not provide data confidentiality.

3.9.1.2. CGA-TSIG

CGA-TSIG [cga-tsig] is another possible solution that can provide the node with secure authentication, data integrity and data confidentiality. It provides the node with zero or minimal configuration when it is integrated with SAVI-DHCP or secure RA message [RFC7113]. This is useful when the node needs to update any record on an unicast DNS or there is an access list on services. This approach can be used to authenticate and authorize a node to use a service or a device.

3.9.1.3. DNS over DTLS

3.9.2. Authorization of a Service Requester

3.9.2.1. The Use of an Access List

There can be an access list on each service with the list of IP addresses that can use these services. Then the service can use mechanisms to authorize the service requester or to securely authenticate them with minimum interaction (zero configuration). This

approach prevents the service from unauthorized use by an attacker. There are currently some mechanisms available -- SAVI-DHCP, CGA-TSIG,

etc.

3.9.2.2. 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 and can make sure that nobody can spoof the IP address of the service providers.

3.9.2.3. The Use of Shared Secret

A shared secret (e.g. a password) can be shared among the service requesters. Then this value can be used to access the services and authenticated to them. However, this approach has a disadvantage. This is because when one of the nodes in this network that carries this shared secret is compromised then the attacker can also have unauthorized access to these services. Sharing and re-sharing this shared secret does not fit to the zero conf nature of DNS-SD protocol.

3.9.3. Authorization of a Service

It is really important for the service requesters to ensure that the one claim to be a service (e.g. a printer) is really a service and its identity has not been forged by the attacker. The service requester needs to receive the IP address of services in a secure manner. There are some approaches that can be used for this purpose such as SAVI-DHCP, Router Advertisement. There are also some mechanisms that can be used in service requesters to complete this authentication and authorization processes such as CGA-TSIG, DNS over TLS

3.9.3.1. SAVI-DHCP

The DHCP server can carry this information and send it to the service requesters at the same time as the service requesters receive a new IP address from the DHCP servers.

3.9.3.2. Router advertisement

If Neighbor Discovery Protocol (NDP) [RFC4861] or Secure Neighbor Discovery (SeND) [RFC3971] are in use, then an option can be added to a router advertisement message which carries required information regarding the IP addresses of services. This is especially secure

when SeND is in use. There can be also other protection mechanisms that is explained in [RFC7113].

3.9.4. ULA and GUA Considerations

As explained earlier, a ULA prefix is not to be advertised outside the network domain. Administrators need to clearly set the scope of the ULAs and configure ACLs on relevant border routers to enforce this scope. If internal DNS is used, administrators should use internal-only DNS names for ULAs and perhaps use split horizon DNS to ensure internal names do not resolve on the Internet as described in RFC6950.

3.9.4.1. mDNS proxy and Security consideration

Unlike IPv4, there can be multiple IP address assignments per interface. For example, a printer might return both GUA and ULA. From a security standpoint, it becomes essential only ULAs be published in DNS-SD populated by mDNS.

3.9.5. Other Security Considerations

Since a WLAN might also cover a part of city, it is really important to make sure that there is required filtering in edge networks to avoid distribution of mDNS/DNS-SD messages beyond the enterprise networks.

3.10. Not Usable Security Mechanisms

There are some other security mechanisms that are not fit to DNS-SD protocol but might be useable in future.

3.10.1. IPsec

IPsec is a security protection mechanism. It requires manual step for the configuration of the nodes. However, recently there are some new drafts to automate this process. This is, of course, might not be an ideal solution for DNS-SD. It is because it might not fit to nodes with limited resources (e.g. battery). Data encryption, as explained in section 3.12.2. is not suitable for DNS-SD.

4. Security Considerations

This document documents the security of mDNS and DNS-SD. It does not introduce any additional security considerations

5. IANA Considerations

There is no IANA consideration

6. Acknowledgements

The author would like to thank all those people who directly helped in improving this draft, especially John C. Klensin, Douglas Otis, Dan York and Harald Albrecht

7. References

7.1. 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

[RFC3971] Arkko, J., Kempf, J., Zill, B., and Nikander, P., "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., Soliman, H., "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., Culler, D., "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC7113] Gont, F.,"Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, February 2014.

[RFC4193] Hinden, R., Haberman, B., "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005

[RFC7368] Chown, T., Arkko, J., Brandt, A., Troan, O., Weil, J., "Unique Local IPv6 Unicast Addresses", RFC 7368,

7.2. Informative References

[requirement] Lynn, K., Cheshire, S., Blanchet, M., Migault, D., " Requirements for Scalable DNS-SD/mDNS Extensions", http://tools.ietf.org/html/draft-ietf-dnssd-requirements-06, March 2015

[DHCP-SAVI] Bi, J., Wu, J., Yao, G, Baker, F.,"SAVI Solution for DHCP", http://tools.ietf.org/html/draft-ietf-savi-dhcp-34, February 2015

[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 , June 2014

Authors' Addresses

Hosnieh Rafiee
http://www.rozanak.com
Munich, Germany
Phone: +49 (0)176 57587575
Email: ietf@rozanak.com