DNSSD
INTERNET-DRAFT
Intended Status: Informational
Expires: April 27, 2015

H. Rafiee

October 27, 2014

Multicast DNS (mDNS) Threat Model and Security Consideration <draft-rafiee-dnssd-mdns-threatmodel-01.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 April 27, 2015.

Copyright Notice

Table of Contents

1. Introduction 3
2. Terminology 3
3. Threat Analysis 4
3.1. DoS attack on any node in the DNS-SD enabled network . . 4
3.1.1. Personal Area Network (PAN) 4
3.1.2. Temporary Public Hotspot 5
3.2. Node compromising 5
3.2.1. Home, Enterprise, Mesh networks 5
3.3. Spoofing Attacks & forge the Identity 5
3.3.1. Public Hotspot, Home, Enterprise, Mesh networks . . . 5
3.3.2. Enterprise network 5
3.4. Malicious update on unicast DNS 5
3.5. Cache Poisoning 6
3.6. Harming Privacy 6
3.7. Resource spoofing 6
3.8. Dual stack attacks 6
3.9. MAC address spoofing 6
3.10. Privacy Protection Mechanisms 6
3.10.1. The Use of Random Data 6
3.10.2. Data Encryption 7
3.11. Authorization of a Service Requester 7
3.11.1. The Use of an Access List 7
3.11.1.1. SAVI-DHCP 7
3.11.1.2. CGA-TSIG 7
3.11.1.3. DNS over DTLS 8
3.11.2. The Use of Shared Secret 8
3.12. Authorization of a Service Provider 8
3.12.1. SAVI-DHCP 8
3.12.2. Router advertisement 8
3.13. Other Security Considerations 8
3.14. Not Usable Security Mechanisms 9
3.14.1. DNSSEC 9
3.14.2. IPsec 9
4. Security Considerations 9
5. IANA Considerations 9
6. Acknowledgements 9
7. References 9
7.1. Normative 9
7.2. Informative 10
Authors' Addresses 11

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. 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 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 Providers: a node that offer a service to other nodes. One example of a service provider in DNS-SD is 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

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 DNS-SD. This is why DNS-SD 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. The definition of different use case scenarios are defined in [requirement].

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 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.

3.1. DoS attack on any node in the DNS-SD enabled network

3.1.1. Personal Area Network (PAN)

When service provider and service requester are connected via a network cable or USB, then the only threat is virus or other malware that might infect any of these nodes. This might cause DoS.

Wireless PAN (WPAN) is where service provider and service requester are connected via Bluetooth or wireless. Since WPANs are short range

and their coverage are usually limited, the attacker should be so close to any of those nodes to be able to perform any attacks. If this happens, the attacker might be able to forge the identity of the

service provider or perform DoS attack.

3.1.2. Temporary Public Hotspot

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 service owner.

3.2. Node compromising

3.2.1. Home, Enterprise, Mesh networks

When ISP, home router/gateway and service provider (like a printer) support IPv6 address, then service providers usually automatically sets an IPv6 address. Since this address is global, this node is accessible over the internet. If the address of this service provider is known to the attacker, then it might be able to compromise this service provider and access to this network (because service providers usually supports weak security features).

3.3. Spoofing Attacks & forge the Identity

3.3.1. Public Hotspot, Home, Enterprise, Mesh networks

Scenario 1: A malicious node can spoof the source IP address of a legitimate victim node advertises fake services in the network. This might result in compromising the victim nodes or having malicious access to the victim nodes' resources.

Scenario2: 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.

3.3.2. Enterprise network

A virus or any malware can compromise a legitimate node in this network. Then this node can forge the identity of service providers or perform DoS attack on this network.

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.

3.5. Cache Poisoning

Usually a list of service providers is cached in the service requester. When a malicious node has a chance to compromise this cache by advertising fake services, then the service requester might always connect to this fake service provider. This attack is applicable to temporary public hotspot, home, enterprise, Mesh and 6LowPAN networks.

3.6. 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 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.

3.7. 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. This is applicable to temporary public hotspot and enterprise networks.

3.8. 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. This attack is applicable to home, enterprise and temporary public hotspots.

3.9. MAC address spoofing

In a wireless environment where MAC address filtering is in use 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. This attack is applicable to temporary public networks and enterprise networks.

3.10. Privacy Protection Mechanisms

3.10.1. 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

3.10.2. 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.

3.11. Authorization of a Service Requester

3.11.1. The Use of an Access List

There can be an access list on each service providers with the list of IP addresses that can use these services. Then the service providers can use mechanisms to authorize the service requesters or to securely authenticate them with minimum interaction (zero configuration). This approach prevents the service providers from unauthorized use by an attacker. There are currently some mechanisms available -- SAVI-DHCP, CGA-TSIG, etc.

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

3.11.1.2. 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 and prevents IP spoofing. This is useful when the node

needs to update any record on an unicast DNS or there is an access list on service providers. This approach can be used to authenticate and authorize a node to use a service or a device.

3.11.1.3. DNS over DTLS

3.11.2. 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 service providers and authenticated on them. However, this approach has a disadvantage 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.

3.12. Authorization of a Service Provider

It is really important for the service requesters to ensure that the one claim to be a service provider (e.g. a printer) is really a service provider and its identity has not been forged by the attacker. The service requester needs to receive the IP address of service providers 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

3.12.1. 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.

3.12.2. 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 service providers. This is especially secure when SeND is in use.

3.13. 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.

3.14. Not Usable Security Mechanisms

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

3.14.1. DNSSEC

Due to the pre-configuration required for DNSSEC on each nodes and DNS servers, it is not an ideal solution mechanism for zero config services. It might also necessary to access to internet to verify the DNSSEC keys and prevent IP spoofing (ask the trusted anchors the validity of the DNSSEC keys)

3.14.2. 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. This is, of course, might not be an ideal solution for DNS-SD. This is because as explained in section 4.1.2 encryption of the whole message might not be really helpful since the attacker can also request the same service.

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 and Dan York

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.

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-04, October 2014

[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 , June 2014

Authors' Addresses

Hosnieh Rafiee
HUAWEI TECHNOLOGIES Duesseldorf GmbH
Riesstrasse 25, 80992
Munich, Germany
Phone: +49 (0)162 204 74 58
Email: ietf@rozanak.com