Mobile Ad hoc Networking (MANET)
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

J. Yi
T. Clausen
LIX, Ecole Polytechnique
U. Herberg
Fujitsu Laboratories of America

July 4, 2014

Security Threats for Simplified Multicast Forwarding (SMF)
draft-yi-manet-smf-sec-threats-00

Abstract

This document analyzes security threats of the Simplified Multicast Forwarding (SMF), including the vulnerabilities of duplicate packet detection and relay set selection mechanisms. This document is not intended to propose solutions to the threats described.

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 January 5, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

This document analyzes security threats of the Simplified Multicast Forwarding (SMF) mechanism [RFC6621]. SMF aims at providing basic Internet Protocol (IP) multicast forwarding, in a way which is suitable for limited wireless mesh and Mobile Ad hoc NETworks (MANET). SMF is constituted of two major functional components: Duplicate Packet Detection and Relay Set Selection.

SMF is typically used in decentralized wireless environments, and is potentially exposed to different kinds of attacks and misconfigurations. Some of the threats are of particular significance as compared to wired networks. In [RFC6621], SMF does not define any explicit security measures for protecting the integrity of the protocol.

This document is based on the assumption that no additional security mechanism such as IPsec is used in the IP layer, as not all MANET deployments may be suitable to deploy common IP protection mechanisms (e.g., because of limited resources of MANET routers to support the IPsec stack). The document analyzes possible attacks on and mis-configurations of SMF and outlines the consequences of such attacks/ mis-configurations to the state maintained by SMF in each router (and, thus, made available to protocols using this state).

This document aims at analyzing and describing the potential vulnerabilities of and attack vecors for SMF. While completeness in such an analysis always is a goal, no claims of being complete are made. The goal of this document is to be helpful for when deploying SMF in a network and needing to understand the risks thereby incurred - as wll as for providing a reference and documented experience with SMF as input for possibly future developments of SMF.

This document is not intended to propose solutions to the threats described. [RFC7182] provides a framework, which can be used with SMF, and which - depending on how it is used - may offer some degree of protection against the threats described in this document related to identity spoofing.

2. Terminology

This document uses the terminology and notation defined in [RFC2119], [RFC5444], [RFC6621] and [RFC4949].

Additionally, this document introduces the following terminology:

SMF router: A MANET router, running SMF as specified in [RFC6621].

Attacker: A device that is present in the network and intentionally seeks to compromise the information bases in SMF routers.

Compromised SMF router: An attacker, present in the network and which generates syntactically correct SMF control messages. Control messages emitted by a compromised SMF router may contain additional information, or omit information, as compared to a control message generated by a non-compromized SMF router located in the same topological position in the network.

Legitimate SMF router: An SMF router, which is not a compromised SMF Router.

3. SMF Threats Overview

SMF requires an external dynamic neighborhood discovery mechanism in orde to maintain suitable topological information describing its immediate neighborhood, and thereby allowing it to select reduced relay sets for forwarding multicast data traffic. Such an external dynamic neighborhood discovery mechanism MAY be provided by lower-layer interface information, by a concurrently operating MANET routing protocol which already maintains such information such as [RFC7181], or by explicitly using MANET Neighborhood Discovery Protocol (NHDP) [RFC6130]. If NHDP is used for neighborhood discovery by SMF, SMF implicitly inherits the vulnerabilities of NHDP, as discussed in [RFC7186]. This document assumes that NHDP is used.

Based on neighborhood discovery mechanisms, SMF specified two major functional components: Duplicate Packet Detection (DPD) and Relay Set Selection (RSS).

DPD is required by SMF in order to be able to detect duplicate packets and eliminate their redundant forwarding. An Attacker has several ways in which to harm the DPD mechanisms:

- It can "deactivate" DPD, so as to make it such that duplicate packets are not correctly detected, and that as a consequence they are (redundantly) transmitted, increasing the load on the network, draing the batteries of the routers involved, etc.

- It can "pre-activate" DPD, so as to make DPD detect a later arriving (valid) packet as being a duplicate, which therefore won’t be forwarded"

The attacks on DPD are detailed in Section 4.

RSS produces a reduced relay set forforwarding multicast data packets across the MANET. SMF supports the use of several relay set algorithms, including E-CDS (Essential Connected Dominating Set), S-MPR (Source-based Multi-point Relay, as known from [RFC3626] and [RFC7181]), or MPR-CDS. An Attacker can disrupt the RSS algorithm, by degrading it to classical flooding, or by "masking" certain part of the routers from the multicasting domain. The attacks to RSS algorithms are illustrated in Section 5.

4. Threats to Duplicate Packet Detection

Duplicate Packet Detection (DPD) is required for packet dissemination in MANET because the packets may be transmitted via the same physical interface as the one over which they were received. A router may also receive multiple copies of the same packets from different neighbors. DPD is thus used to check if an incoming packet has been received or not.

DPD is achieved by a router maintaining a record of recently processed multicast packets, and comparing later received multicast herewith. A duplicate packet detected is silently dropped, and is not inserted into the forwarding path of that router, nor is it delivered to an application. DPD, as proposed by SMF, supports both IPv4 and IPv6 and for each suggests two duplicate packet detection mechanisms: 1) header content identification-based DPD (I-DPD), using packet headers, in combination with flow state, to estimate temporal uniqueness of a packet, and 2) hash-based DPD (H-DPD), employing hashing of selected header fields and payload for the same effect.

As they are distinct mechanisms, the threats to I-DPD and H-DPD are discussed separately.

4.1. Threats to Identification-based Duplicate Packet Detection

I-DPD uses a specific DPD identifier in the packet header to identify a packet. By default, such packet identification is not provided by the IP packet header (for both IPv4 and IPv6). Therefore, additional identification header, such as the fragment header, a hop-by-hop header option, or IPSec sequencing, must be employed in order to support I-DPD. The uniqueness of a packet can then be identified by the [source IP address] of the packet originator, and the [sequence number] (from the fragment header, hop-by-hop header option, or IPsec). By doing so, each intermediate router can keep a record of recently received packet, and determine the coming packet has been received or not.

4.1.1. Pre-activation Attacks (Pre-Play)

In a wireless environment, or across any other shared channel, a compromised SMF router can perceive the identification tuple [source IP, sequence number] of a packet. If sequence number progression is predictable, then it is trivial to generate aand inject invalid packets with "future" identification information into the network. If these invalid packets arrive before the legitimate packets that they’re spoofing, the latter will be treated as a duplicates and discarded. This can prevent multicast packets from reaching parts of the network.

Figure 1 gives an example of pre-activation attack. A, B, and C are legitimate SMF routers, and X is the compromised SMF router. The line between the routers presents the packet forwarding. Router A is the source and originates a multicast packet with sequence number n. When router X receives the packet, it generates an invalid packet with the the source address of A, and sequence number n. If the invalid packet arrives at router C before the forwarding of router B, the valid packet will be dropped by C as duplicate packet. In a wireless environment, jitter is commonly used to avoid systematic collisions at MAC layer [RFC5148], thus an attacker can increase the probability that its invalid packets arrive first by retransmitting them without jittering.

```
                                .---.
                                | X |
                              --'---' __
       packet with seq=n     /          \  invalid packet with seq=n
                            /            \
                        .---.              .---.
                        | A |              | C |
                        '---'              '---'
       packet with seq=n    \    .---.   /
                             \-- | B |__/  valid packet with seq=n
                                 '---'
```

Figure 1

4.1.2. De-activation Attacks (Sequence Number wrangling)

A compromised SMF router can also seek to de-activate DPD, by modifying the sequence number in packets that it forwards. Thus, routers will not be able to detect an actual duplicate packet as a duplicate - rather, they will treat them as new packets, i.e., process and forward them. This is similar to DoS attack. The consequence of this attack is an increased channel load, the origin of which appears to be a router other than the compromised SMF router.

Given the topology shown in Figure 1, on receiving packet with seq=n, the attacker X can forward the packet with modified sequence number n+i. This has two consequences: firstly, router C will not be able to detect the packet forwarded by X is a duplicate packet; secondly, the consequent packet with seq=n+i generated by router A probably will be treated as duplicate packet, and dropped by router C.

4.2. Threats to Hash-based Duplicate Packet Detection

When it is not feasible to have explicit sequence numbers in packet headers, hash-based DPD can be used. A hash of the non-mutable fields in the header of and the data payload can be generated, and recorded at the intermediate routers. A packet can thus be uniquely identified by the source IP address of the packet, and its hash-value.

The hash algorithm used by SMF is being applied only to provide a reduced probability of collision and is not being used for cryptographic or authentication purposes. Consequently, a digest collision is still possible. In case the source router or gateway identifies that it recently has generated or injected a packet with the same hash-value, it inserts a "Hash-Assist Value (HAV)" IPv6 header option into the packet, such that calculating the hash also over this HAV will render the resulting value unique.

4.2.1. Replay Attack

A replay attack implies that control traffic from one region of the network is recorded and replayed in a different region at (almost) the same time, or in the same region at a different time.

One possible replay attack is based on the Time-to-Live (TTL, for IPv4) or hop limit (for IPv6) field. As routers only forward packets with TTL > 1, a compromised SMF router can forward an otherwise valid packet, while drastically reducing the TTL hereof. This will inhibit recipient routers from later forwarding the same multicast packet, even if received with a different TTL - essentially a compromised SMF router thus can instruct its neighbors to block forwarding of valid multicast packets. As the TTL of a packet is intended to be manipulated by intermediaries forwarding it, classic methods such as integrity check values (e.g., digital signatures) are typically calculated with setting TTL fields to some pre-determined value (e.g., 0) - such is for example the case for IPsec Authentication Headers - rendering such an attack more difficult to both detect and counter. If the compromised SMF router has access to a "wormhole" through the network (a directional antenna, a tunnel to a collaborator or a wired connection, allowing it to bridge parts of a network otherwise distant) it can make sure that the packets with such an artificially reduced TTL arrive before their unmodified counterparts.

4.2.2. Attack on Hash-Assistant Value

The HAV header is helpful when a digest collision happens. However, it also introduces a potential vulnerability. As the HAV option is only added when the source or the ingressing SMF router detects that the coming packet has digest collision with previously generated packets, it actually can be regarded as a "flag" of potential digest collision. A compromised SMF router can discover the HAV header, and be able to conclude a hash collision is possible if the HAV header is removed. By doing so, other SMF routers receiving the modified packet will be treated as duplicate packet, and be dropped because it has the same hash value with precedent packet.

In the example of Figure Figure 2, Router A and B are legitimate SMF routers, X is a compromised SMF router. A generate two packets P1 and P2, with the same hash value h(P1)=h(P2)=x. Based on SMF specification, a hash-assistant value (HAV) is added to the latter packet P2, so that h(P2+HAV)=x’, to avoid digest collision. When the attacker X detects the HAV of P2, it is able to conclude that a collision is possible by removing the HAV header. By doing so, packet P2 will be treated as duplicate packet by router B, and be dropped.

```
           P2            P1                 P2         P1
.---.  h(P2+HAV)=x’    h(P1)=x    .---.  h(P2)=x     h(P1)=x    .---.
| A |--------------------------> | X | ----------------------> | B |
’---’                             ’---’                          ’---’
```

Figure 2

5. Threats to Relay Set Selection

A framework for RSS mechanism, rather than a specific RSS algorithm is provided by SMF. It is normally achieved by distributed algorithms that can dynamically generate a topological Connected Dominating Set based on 1-hop and 2-hop neighborhood information. In this section, the common threats to the RSS framework are first discussed. Then the three commonly used algorithms: Essential

Connection Dominating Set (E-CDS) algorithm, Source-based Multipoint Relay (S-MPR) and Multipoint Relay Connected Dominating Set (MPR-CDS) are analyzed.

5.1. Relay Set Selection Common Threats

The common threats to RSS algorithms, including Denial of Service attack, eavesdropping, message timing attack and broadcast storm have been discussed in [RFC7186].

5.2. Threats to E-CDS Algorithm

The "Essential Connected Dominating Set" (E-CDS) algorithm [RFC5614] forms a single CDS mesh for the SMF operating region. It requires 2-hop neighborhood information (the identify of the neighbors, the link to the neighbors and neighbors’ priority information) collected through NHDP or another process.

An SMF Router select itself as a relay, if:

- The SMF Router has a higher priority than all of its symmetric neighbors, or

- There does not exist a path from the neighbor with largest priority to any other neighbor, via neighbors with greater priority.

A Compromised SMF Router can disrupt the E-CDS algorithm by link spoofing or identity spoofing.

5.2.1. Link Spoofing

Link spoofing implies that a Compromised SMF Router advertises non-existing links to another router (present in the network or not).

A Compromised SMF Router can declare itself with high route priority, and spoofs the links to as many Legitimate SMF Routers as possible to declare high connectivity. By doing so, it can prevent Legitimate SMF Routers from self-selecting as relays. As the "super" relay in the network, the Compromised SMF Router can manipulate the traffic relayed by it.

5.2.2. Identity Spoofing

Identity spoofing implies that a compromised SMF router determines and makes use of the identity of other legitimate routers, without being authorised to do so. The identity of other routers can be obtained by overhearing the control messages or source/destination address from datagram. The compromised SMF router can then generate control or datagram traffic, pretending to be a legitimate router.

Because E-CDS self-selection is based on the router priority value, a compromised SMF router can spoof the identity of other legitimate routers, and declares a different router priority value. If it declares a higher priority of a spoofed router, it can prevent other routers from selecting themselves as relays. On the other hand, if the compromised router declares lower priority of a spoofed router, it can enforces other routers to selecting themselves as relays, to degrade the multicast forwarding to classical flooding.

5.3. Threats to S-MPR Algorithm

The source-based multipoint relay (S-MPR) set selection algorithm enables individual routers, using 2-hop topology information, to select relays from their set of neighboring routers. MPRs are selected so that forwarding to the router’s complete 2-hop neighbor set is covered.

An SMF router forwards a multicast packet if and only if:

- the packet is not received before, and

- the neighbor from which the packet was received has selected the router as MPR.

Because MPR calculation is based on the willingness declared by the SMF routers, and the connectivity of the routers, it can be disrupted by both link spoofing and identity spoofing. The threats and its impacts have been illustrated in section 5.1 of [RFC7186].

5.4. Threats to MPR-CDS Algorithm

MPR-CDS is a derivative from S-MPR. The main difference between S-MPR and MPR-CDS is that while S-MPR forms a different broadcast tree for each source in the network, MPR-CDS forms a unique broadcast tree for all sources in the network.

As MPR-CDS combines E-CDS and S-MPR, the vulnerabilities of E-CDS and S-MPR that discussed in Section 5.2 and Section 5.3 apply to MPR-CDS also.

6. Security Considerations

This document does not specify a protocol or a procedure. The document, however, reflects on security considerations for SMF for packet dissemination in MANETs.

7. IANA Considerations

This document contains no actions for IANA.

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.

[RFC5614] Ogier, R. and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding", RFC 5614, August 2009.

[RFC6621] Macker, J., "Simplified Multicast Forwarding", RFC 6621, May 2012.

[RFC7186] Yi, J., Herberg, U., and T. Clausen, "Security Threats for the Neighborhood Discovery Protocol (NHDP)", RFC 7186, April 2014.

8.2. Informative References

[RFC3626] Clausen, T. and P. Jacquet, "The Optimized Link State Routing Protocol", RFC 3626, October 2003.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5148] Clausen, T., Dearlove, C., and B. Adamson, "Jitter Considerations in Mobile Ad Hoc Networks (MANETs)", RFC 5148, February 2008.

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized MANET Packet/Message Format", RFC 5444, February 2009.

[RFC6130] Clausen, T., Dean, J., and C. Dearlove, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol version 2", RFC 7181, April 2014.

[RFC7182] Herberg, U., Clausen, T., and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", RFC 7182, April 2014.

Authors' Addresses

Jiazi Yi
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Phone: +33 1 77 57 80 85
Email: jiazi@jiaziyi.com
URI: http://www.jiaziyi.com/

Thomas Heide Clausen
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Phone: +33 6 6058 9349
Email: T.Clausen@computer.org
URI: http://www.thomasclausen.org/

Ulrich Herberg
Fujitsu Laboratories of America
1240 E Arques Ave
Sunnyvale, CA 94085
USA

Email: ulrich@herberg.name
URI: http://www.herberg.name/