Network Working Group
Internet-Draft
Intended status: Experimental
Expires: January 9, 2020

M. Bagnulo
UC3M
A. Andersdotter
Article 19
C. Paasch
Apple

July 8, 2019

Privacy threats and possible countermeasures for Multipath-TCP (MPTCP)

draft-bagnulo-mptcp-privacy-00.txt

Abstract

This note performs a differential analysis of the threats regarding privacy of the Multipath TCP protocol compared to regular TCP and proposes a set of countermeasures for the threats identified.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Multipath-TCP (MPTCP) [RFC6824] [I-D.ietf-mptcp-rfc6824bis] is a set of extensions to TCP that enable the use of multiple IP addresses throughout the lifetime of a (MP)TCP connection. The use of multiple addresses in a connection allows two main uses cases, namely mobility and multihoming. In the case of multihoming, if an endpoint is connected to the Internet through multiple interfaces simultaneously (each ones having a different IP address), the use of MPTCP allow additional fault tolerance as the connection can be preserved by using an alternative IP address even if the IP address originally used to establish the connection is rendered unavailable. In the case of mobility, as an endpoint changes is attachment to the Internet, it acquires a new IP address associated to its new attachment point. By using MPTCP, connections can be preserved throughout the changes of attachment points and their respective IP addresses by adding the new IP addresses to the ongoing MPTCP connections.

Because of its very nature, the operation of MPTCP presents privacy implications, as other protocols that bind multiple IP addresses to a given endpoint [I-D.nordmark-id-loc-privacy]. Because MPTCP explicitly associated multiple IP addresses to a given connection and hence to a given endpoint, it discloses information about the node whereabouts to third parties. In this note, we perform an analysis of the privacy implications of the operation of the MPTCP compared to regular TCP and we provide a set of countermeasures to address the identified threats. It is out of the scope of this document to identify privacy threats that equally affect both MPTCP and TCP, such as the ones resulting from exchanging unencrypted data that can be observed by eavesdroppers along the path. As mentioned earlier, we only identify threats against privacy introduced by MPTCP which are not present in TCP.

2. Threat Analysis

The threats concerning privacy of the use of MPTCP are essentially two:

Movement tracking: In the case that MPTCP is used for mobility, the use of multiple addresses in the same MPTCP connection can be used by an attacker to track the movement of the victim. Since IP addresses can be related to location (in a more or less accurate manner), by observing the different addresses used in a MPTCP connection, the attacker can track the itinerary of the victim.

More accurate positioning. If multiple address are used simultaneously in a MPTCP connection, this implies that the endpoint is connected at the multiple attachment points at the same time, potentially providing the means for a more accurate positioning of the endpoint (e.g. if an endpoint is exposing the IP address of the cellular access it is providing less information than when it also exposes the IP address of an Internet coffee wifi access).

2.1. Types of attackers

We classify the types of attackers based on their topological location, which determines the amount of information they have access to. the different types of attackers are:

Partially on-path attacker. This attacker is located along one or more, but not all the paths used to exchange MPTCP signaling information. As such, it is able to see some but not all the MPTCP packets.

Full On-path attacker. This attacker is able to eavesdrop all the MPTCP signaling message exchange, but it is not the other endpoint of the information.

Endpoint: in this case, the other endpoint of the MPTCP connection is the attacker (in the sense that it will use the information revealed through MPTCP for other purposes beyond the MPTCP operation e.g. the endpoint may decide to sell the location and tracking information of the MPTCP endpoints to third parties).

2.2. Detailed attack mechanics.

2.2.1. Attacks using MP_CAPABLE and MP_JOIN.

A MPTCP endpoint initiates a MPTCP connection by including the MP_CAPABLE option in the SYN message. After that, it uses the MP_JOIN option to add subsequent subflows using other IP address to the existent connection. The MP_JOIN message include a token that is used by the MPTCP receiver to identify which of the ongoing MPTCP connections this particular subflow is being added to. In order for an attacker to bind the different address together, it must be able to observe at least two messages carrying two different addresses. In particular, by observing the initial MP_CAPABLE SYN and a following MP_JOIN message, the attacker can relate these two IP addresses. Also, by observing two MP_JOIN messages carrying different IP addresses but the same toke, the attacker can also relate the two IP addresses together.

This attack can be executed by any attacker that is capable of observing the different MP_CAPABLE and MP_JOIN messages. So, for a partially on-path attacker, the attack will be as effective as the number of used path the attacker has access to. If it only has access to one path, the attacker would not gather any information. Both full on-path attackers and the endpoint would have access to all the information, so the attack effectiveness is complete.

Both versions of MPTCP, i.e. [RFC6824] [I-D.ietf-mptcp-rfc6824bis] are equally affected by this attack.

2.2.2. Attacks using ADD_ADDR.

The ADD_ADDR option allows the sender of the message to add an IP address to the existing connection. From a privacy perspective, the packet containing the ADD_ADDR information already discloses a binding between two addresses, the address used a source address of the packet and the address included in the ADD_ADDR option. This attack can be performed by any attacker who is able to observe the message, including partial and full on-path attackers and the endpoint itself. This attack can be combined with the attack done using MP_CAPABLE AND MP_JOIN messages described in the previous section, to retrieve a larger set of addresses. This attack affects both version [RFC6824] [I-D.ietf-mptcp-rfc6824bis] of MPTCP.

3. Countermeasures.

It is possible to design countermeasures to prevent the described attacks.

ADD_ADDR attack.

In order to prevent the ADD_ADDR based attack, it would be possible to encrypt the address carried in the ADD_ADDR message, for example with the key exchanged in the MP_CAPABLE exchange. By doing this, only the attackers who have observed the initial MP_CAPABLE message would be able to decrypt the content of the ADD_ADDR message, significantly limiting the attack surface.

MP_CAPABLE and MP_JOIN.

In order to prevent the MP_CAPABLE/MP_JOIN attack, it would necessary to change the token in every MP_JOIN message. the difficulty with this of course is that the token is used a key to identify which MPTCP connection this new subflow belongs to. Using different tokens would be possible as long as the receiver would be able to decrypt it and find the ongoing connection that this new subflow belongs to.

For instance, the token could be the hash of the concatenation of a trail of n zeros, the key and the new IP address of the flow. This token would change with every new subflow, since the IP address would change (we could also add the source port, to support the case of multiple subflows with the same source IP address). Upon the reception of an MP_JOIN message, the receiver would need to try with all the keys of ongoing connections. It will know it has succeeded, because the correct one will result in a trail of n zeros. The problem with this mechanism is that it imposes an additional cost in terms of computation upon the establishment of a new subflow.

Additional countermeasures could be int he form of a recommendation about when to establish a new subflow or when to announce new addresses using ADD_ADDR. Generating awareness that doing so discloses private information of the endpoint would make implementations more conservative when advertising IP addresses.

4. MPTCP privacy features.

MPTCP also provides some positive side effects with regard to privacy. In particular, because the information is spread across multiple paths, in order to be able to eavesdrop all the content of a MPTCP connection, the attacker needs to be present in all used paths, making more challenging for the attacker to fulfill its goal.

5. Security Considerations

6. IANA Considerations

7. Acknowledgements

This work was supported by the Spanish Ministry of Economy and Competitiveness through the 5G-City project (TEC2016-76795-C6-3-R).

8. Informative References

[I-D.ietf-mptcp-rfc6824bis]
Ford, A., Raiciu, C., Handley, M., Bonaventure, O., and C. Paasch, "TCP Extensions for Multipath Operation with Multiple Addresses", draft-ietf-mptcp-rfc6824bis-18 (work in progress), June 2019.

[I-D.nordmark-id-loc-privacy]
Nordmark, E., "Privacy issues in ID/locator separation systems", draft-nordmark-id-loc-privacy-00 (work in progress), July 2018.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, DOI 10.17487/RFC6824, January 2013, <https://www.rfc-editor.org/info/rfc6824>.

Authors' Addresses

Marcelo Bagnulo
UC3M

Email: marcelo@it.uc3m.es

Amelia Andersdotter
Article 19

Email: amelia@article19.org

Christoph Paasch
Apple

Email: cpaasch@apple.com