Workgroup: anima Working Group
Internet-Draft:
draft-richardson-saag-onpath-attacker-00
Published: 27 December 2020
Intended Status: Standards Track
Expires: 30 June 2021
Authors: M. Richardson
Sandelman Software Works

A toxonomy of eavesdropping attacks

Abstract

The terms on-path attacker and Man-in-the-Middle Attack have been used in a variety of ways, sometimes interchangeably, and sometimes meaning different things.

This document offers an update on terminology for network attacks. A consistent set of terminology is important in describing what kinds of attacks a particular protocol defends against, and which kinds the protocol does not.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

A number of terms have been used to describe attacks against networks.

In the [dolevyao] paper, the attacker is assumed to be able to:

*view messages as they are transmitted

*selectively delete messages

*selectively insert or modify messages

Some authors refer to such an attacker as an "on-path" attack [reference], or a "Man-in-the-Middle" attack [reference]. In general, most authors form a clear consensus about this mode. Some authors are not happy with the gender of the attack ("Man") being assumed, and have sought other terminology.

Where opinions diverge is what to call other forms of attack or eavesdropping.

The term "passive attack" has been used in many cases to describe situations where the attacker can only observe messages, but can not intersept, modify or delete any messages.

There are situations where an eavesdropper has a better network connection than the actual corresponds, and so while no messages can be removed, such an attacker may be able to beat the original packet in a race.

The summary is that there are probably three variations of attack:

1. An on-path attacker that can view, delete and modify messages. This is the Dolev-Yao attack.

2. An off-path attacker that can view messages and insert new messages.

3. An off-path attacker that can only view messages.

2. Three proposals on terminology

This document aspires to pick a single set of terms and explain them.

2.1. QUIC terms

[quic] ended up with a different taxonomy:

*On-path [Dolev-Yao]

*Off-path

*Limited on-path (cannot delete)

2.2. Malory/Man in various places

[malory] proposes:

*man-in-the-middle [Dolev-Yao]

*man-on-the-side

*man-in-the-rough

Alternatively:

*Malory-in-the-middle [Dolev-Yao]

*Malory-on-the-side

*Malory-in-the-rough

2.3. Council of Attackers

[alliteration] proposes the "the council of attackers"

*malicious messenger [Dolev-Yao: who rewrites messages sent]

*oppressive observer [who uses your information against you]

3. Security Considerations

This document introduces a set of terminology that will be used in many Security Considerations sections.

4. IANA Considerations

This document makes no IANA requests.

5. Acknowledgements

The SAAG mailing list.

6. Changelog

7. References

7.1. Normative References

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

7.2. Informative References

[alliteration] "Council of Attackers", 2020, <https://mailarchive.ietf.org/arch/msg/saag/R0uevzT0Vz9uqqaxiu98GtK1rks/>.

[dolevyao] "On the Security of Public Key Protocols", 1983, <https://www.cs.huji.ac.il/~dolev/pubs/dolev-yao-ieee-01056650.pdf>.

[malory] "Man-in-the-Middle", 2020, <https://mailarchive.ietf.org/arch/msg/saag/b26jvEz4NRHSm-Xva6Lv5-L8QIA/>.

[quic] "QUIC terms for attacks", 2020, <https://mailarchive.ietf.org/arch/msg/saag/wTtDYlRAADMmgqd6Vhm8rFybr_g/>.

Contributors

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca