Workgroup: Security Area Working Group
Internet-Draft:
draft-richardson-saag-onpath-attacker-03
Updates: 4949 (if approved)
Published: 23 October 2022
Intended Status: Informational
Expires: 26 April 2023
Authors: M. Richardson   J. Hoyland
         Sandelman Software Works   Cloudflare Ltd.

A taxonomy 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" attacker [reference], or a "Man-in-the-Middle" [reference]. This type of attack is also refered to as a "monster-in-the-middle" attack.

Despite a broad consensus on what is meant by a MITM attack, there is less agreement on the how to describe its variants. The term "passive attacker" has been used in many cases to describe situations where the attacker can only observe messages, but can not intercept, modify or delete any messages.

Another variant is the case where an eavesdropper is not on the network path between the actual correspondants, and thus cannot drop messages, they may be able to inject packets faster than the correspondants, and thus beat legitimate packets in a race.

As summarised, there are three broad variations of the MITM attacker:

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 kinds of attack

The attacks are numbered in this section as no consensus on naming the attacks yet. In the diagrams below, the sender is named "Alice", and the recipient is named "Bob", as is typical in many cryptographic protocols [alicebob], as first introduced by [digisign].

The attacker is named "Mallory"

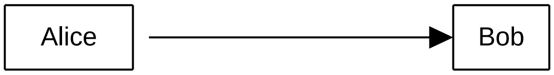

Figure 1: Alice communicating with Bob

2.1. First Kind of attack

In this attack, the attacker is involved with the forwarding of the packets. A firewall or network router is ideally placed for this attack.

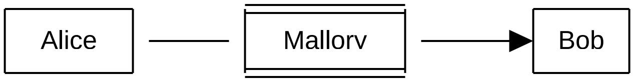

Figure 2: The first kind of attack

In this case Mallory can:

- *view all packets

- *selectively forward or drop any packet

- *modify any packets that is forwarded

- *insert additional packets

2.2. Second Kind of attack

In this attack, the attacker is not involved with the forwarding of the packets. The attacker receives a copy of packets that are sent. This could be from, for instance, a mirror port or SPAN [span]. Alternatively, a copy of traffic may be obtained via passive (optical) tap [fibertap]. This kind of attack is often associated with Pervasive Monitoring [RFC7258].

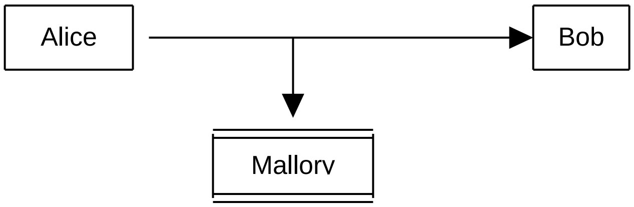

Figure 3: The second kind of attack

In this case Mallory can:

- *view all packets

2.3. Second Kind of attack with bypass

In some cases, Mallory may be able to send messages to Bob via another route which due to some factor will arrive at Bob prior to the original message from Alice.

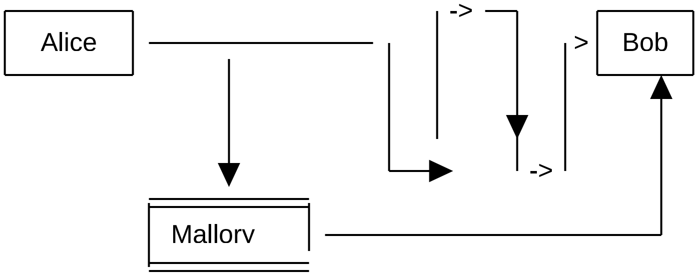

Figure 4: The second kind of attack with bypass

In that case Mallory can:

*view all packets

*insert additional/copied packets into the stream

But Mallory will be unable to drop or modify the original packets. Bob however, may be unable to distinguish packets from Alice vs packets sent from Mallory that purport to be from Alice.

2.4. Third Kind of attack

The third kind of attack is one in which Mallory can not see any packets from Alice. This is usually what is meant by an "off-path" attack. Mallory can usually forge packets purporting to be from Alice, but can never see Alice's actual packets.

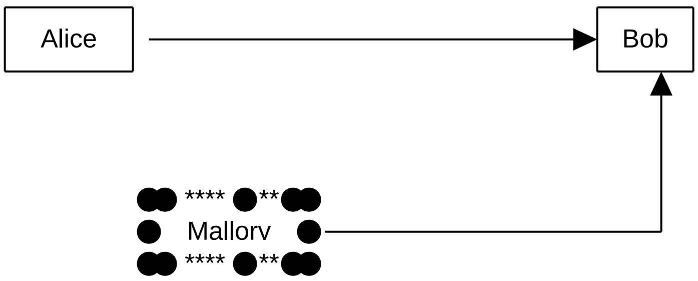

Figure 5: The third kind of attack

In this case Mallory can:

*insert additional packets

3. Three proposals on terminology

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

3.1. QUIC terms

[quic] ended up with a different taxonomy:

*on-path [Dolev-Yao]

*Limited on-path (cannot delete)

*Off-path

3.2. 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

3.3. 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]

*off-path attacker

4. Security Considerations

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

5. IANA Considerations

This document makes no IANA requests.

6. Acknowledgements

The SAAG mailing list.

7. Changelog

8. References

8.1. 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>.

8.2. Informative References

[alicebob] "Alice and Bob", 2020, <https://en.wikipedia.org/wiki/Alice_and_Bob>.

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

[digisign] Rivest, R. L., Shamir, A., and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", February 1978, <https://doi.org/10.1145/359340.359342>.

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

[fibertap] "Fiber Tap", 2020, <https://en.wikipedia.org/wiki/Room_641A>.

[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/>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[span] "Port Mirroring", 2020, <https://en.wikipedia.org/wiki/Port_mirroring>.

Contributors

Eric Rescola

Email: ekr@rtfm.com

Lou Berger

Email: lberger@labn.net

Alan DeKok

Email: aland@deployingradius.com

Christian Huitema

Email: huitema@huitema.net

Authors' Addresses

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Jonathan Hoyland
Cloudflare Ltd.

Email: jhoyland@cloudflare.com