TCP Authentication Option

SwiNOG #38, 21. June 2023

Remi Locherer, remi@arista.com

A normal BGP configuration …

```
router bgp 65005
   router-id 10.255.255.42
   bgp missing-policy direction in action deny
   bgp missing-policy direction out action deny
   neighbor ISP peer group
   neighbor ISP ttl maximum-hops 1
   neighbor ISP route-map EVERYTHING in
   neighbor ISP route-map OWN-AS out
   neighbor 10.11.12.5 peer group ISP
   neighbor 10.11.12.5 remote-as 65001
   neighbor 10.11.12.5 password 7 42yEZ7Db8KU/4m8Is9OcJw==
```

… with a problem!

```
router bgp 65005
   router-id 10.255.255.42
   bgp missing-policy direction in action deny
   bgp missing-policy direction out action deny
   neighbor ISP peer group
   neighbor ISP ttl maximum-hops 1
   neighbor ISP route-map EVERYTHING in
   neighbor ISP route-map OWN-AS out
   neighbor 10.11.12.5 peer group ISP
   neighbor 10.11.12.5 remote-as 65001
   neighbor 10.11.12.5 password 7 42yEZ7Db8KU/4m8Is9OcJw==
```

TCP MD5 Option obsoleted in 2010

Challenge: Securing TCP Sessions

SYN Flooding
TCP FIN Attacks
TCP RST Attacks
TCP Session Hijacking
Replay Attacks

Securing TCP Sessions

SYN Cookies

→ Mitigating DoS caused by SYN floods

IPsec

→ Protects IP payload (transport mode) or IP packet (tunnel mode)

→ Overhead

TLS

→ Secures TCP data stream but not the TCP header

Generalized TTL Security Mechanism (GTSM)

→ Protects eBGP sessions
(Sender sets TTL to 255, Receiver rejects packets if TTL is less than 254)

→ No protection for eBGP sessions from attackers that are one hop away

→ No protection for iBGP sessions from internal attack

TCP MD5

→ Aims to protect the TCP session through authentication

→ Based on a weak hashing algorithm

→ Changing the key is disruptive

RFC 4953: Defending TCP Against Spoofing Attacks

TCP Authentication Option

TCP Authentication Option (TCP-AO)

- Protects long-lived TCP connections (BGP, LDP, RPKI-RTR) by preventing attacks from disabling the TCP connection

- Obsoletes TCP MD5

Properties:

- Supports **strong** cryptographic algorithms
- Supports **multiple** cryptographic algorithms
- Key rollover and negotiation built in
- Replay protection for long-lived connections

RFC 5925: The TCP Authentication Option
RFC 5926: Cryptographic Algorithms for the TCP Authentication Option

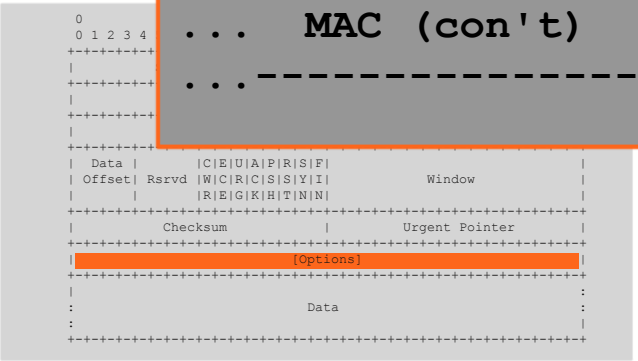
TCP Header - RFC 9293

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |       |C|E|U|A|P|R|S|F|                               |
| Offset| Rsrvd |W|C|R|C|S|S|Y|I|            Window             |
|       |       |R|E|G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            [Options]                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               :
:                             Data                              :
:                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TCP-AO Header

```
+-------------+-------------+-------------+-------------+
|  Kind=29    |   Length    |   KeyID     | RNextKeyID  |
+-------------+-------------+-------------+-------------+
|                         MAC                ...
+-----------------------------------------...

...-----------------+
...   MAC (con't)   |
...-----------------+
```



TCP-AO Concepts: Master Key Tuple (MKT)

MKT is composed of:

- TCP connection identifier
- TCP option flag
- IDs (KeyID or RNextKeyID)
- Master Key
- Key Derivation Function (KDF)
- Message Authentication Code (MAC) algorithm

Properties of MKTs

- MKT parameters are not changed.
- New MKTs can be installed
- Connection can change which MKT it uses.

TCP-AO Concepts: Traffic Keys

Key derived from:

- MKT (master key)
- Local and remote IP address pairs
- TCP port numbers
- TCP Initial Sequence Numbers (ISNs) in each direction.

→ Keys are unidirectional!

Mandatory algorithms (RFC 5926):

- KDF_HMAC_SHA1
- KDF_AES_128_CMAC

traffic_key = KDF_alg(master_key, context, output_length)

TCP-AO Concepts: Message Authentication Code

Mandatory algorithms (RFC 5926):

- HMAC-SHA-1-96
- AES-128-CMAC-96

Message used for calculating MAC consists of:

- Sequence Number Extension (SNE)
  → Replay protection!
- IP pseudoheader (as used for the TCP checksum)
- TCP header
- TCP data

MAC = MAC_alg(traffic_key, message)

TCP-AO Configuration

EOS Configuration Example

```
+------------+------------+------------+------------+
|  Kind=29   |   Length   |   KeyID    | RNextKeyID |
+------------+------------+------------+------------+
|                     MAC           ...
+-----------------------------------...
```

```
service routing protocols model multi-agent

management security
   session shared-secret profile BGP
      secret 10 7 $1c$zXHy2/5IOz6JEc5qRNYMBA== receive-lifetime 2023-01-01 00:00:00 infinite \
         transmit-lifetime 2023-01-01 00:00:00 infinite
      secret 0 7 $1c$zXHy2/5IOz6JEc5qRNYMBA== receive-lifetime 2023-01-01 00:00:00 infinite \
         transmit-lifetime 2023-01-01 00:00:00 infinite

router bgp 65006
   neighbor 10.255.255.5 remote-as 65001
   neighbor 10.255.255.5 password shared-secret profile BGP algorithm hmac-sha1-96
   neighbor 10.255.255.10 remote-as 65002
   neighbor 10.255.255.10 password shared-secret profile BGP algorithm aes-128-cmac-96
```

https://www.arista.com/en/support/toi/eos-4-28-2f/16087-bgp-tcp-authentication-option-tcp-ao

TCP-AO Configuration Examples

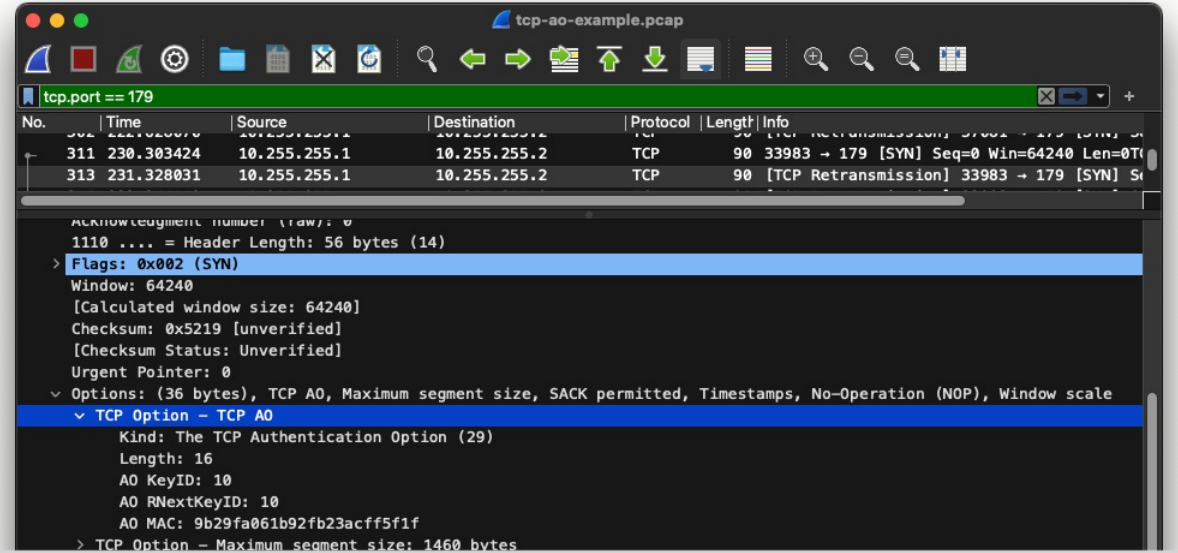
https://github.com/TCP-AO/Configuration-examples

TCP-AO Availability

TCP-AO Support in Network OSs

- Arista (EOS 4.28.2F)
- Cisco (IOS-XR 6.5.3, IOS-XE 16.12)
- Juniper (Junos OS 20.3R1, Junos OS Evolved 22.2R1)
- Nokia (SR OS 16.0.R15, 19.10.R7, 20.5.R1)
- Huawei
- Others?

TCP-AO Support in Wireshark and Tcpdump




```
$ tcpdump --version
tcpdump version 4.99.1
libpcap version 1.10.1 (with TPACKET_V3)
OpenSSL 3.0.2 15 Mar 2022
$ tcpdump -r tcp-ao-example.pcap -t
IP 10.255.255.1.33983 > 10.255.255.2.bgp: Flags [S], seq 1371347505, win 64240, options [tcp-ao
keyid 10 rnextkeyid 10 mac 0x9b29fa061b92fb23acff5f1f,mss 1460,sackOK,TS val 1337951907 ecr
0,nop,wscale 7], length 0
```

TCP-AO Open Source Kernel Implementations

- Linux patches by Leonard Crestez
  - https://lwn.net/Articles/907153/
- Linux patches by Dmitry Safonov
  - Initiative to upstream Arista's TCP-AO implementation
  - Per-socket keys, without a centralized key database in the kernel.
  - https://lwn.net/Articles/934738/
- FreeBSD patches by Philip Paeps
  - Development started in 2021 but now stalled. Will be continued in the future.
  - Code: https://github.com/TCP-AO/freebsd-src/tree/pp-tcp-ao

ARISTA

TCP-AO and Open Source Routing Stacks

Sign up

FRRouting / frr Public

Notifications | Fork 1.1k | Star 2.6k

Code | Issues 407 | Pull requests 188 | Discussions | Actions | Projects 7

Feature Request: TCP-AO (RFC 5925) #7240

New issue

Open netravnen opened this issue on Oct 3, 2020 · 3 comments

netravnen commented on Oct 3, 2020 • edited Contributor

Feature Request: Support for TCP Authentication Option

> This document specifies the TCP Authentication Op
> which obsoletes the TCP MD5 Signature option of R
> MD5). TCP-AO specifies the use of stronger Messag

Assignees

No one assigned

donaldsharp commented on Oct 3, 2020 Member

Someone needs to implement this in the linux kernel first. We have no way to do it from FRR until then

https://github.com/FRRouting/frr/issues/7240

ARISTA

Main Takeaways

TCP-AO …

… obsoletes the TCP MD5 option.

… supports strong cryptographic algorithms.

… allows rekeying during a TCP connection.

… supported by major networking vendors.

… not yet supported in Linux and BSD kernels.

ARISTA

ARISTA

Thank You

www.arista.com