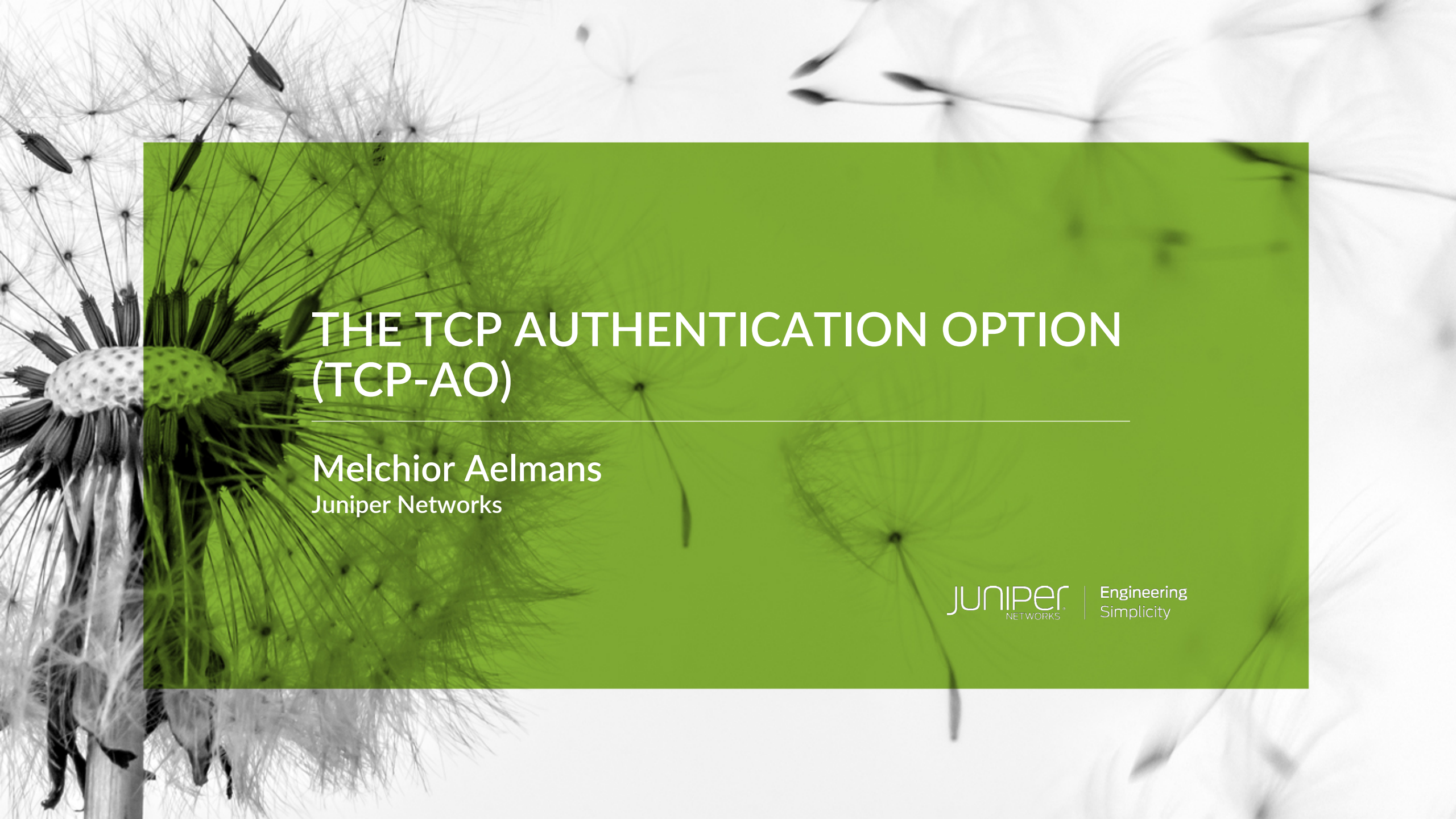

# THE TCP AUTHENTICATION OPTION (TCP-AO)

Melchior Aelmans
Juniper Networks

Juniper Networks | Engineering Simplicity

# MOTIVATION

- What are we protecting?
  - Long-lived TCP sessions
  - Examples
    - Routing protocols (BGP, LDP)
    - Long-lived TCP sessions between other applications
- What are we protecting against?
  - Blind insertion attacks
  - Replay attacks

# BLIND INSERTION ATTACK ON A BGP SESSION

- Router A maintains a BGP session with Router B
  - They exchange many routes over many hours
- Node C sends a few packets per second to Router B for many hours
  - IP source address: Router A (spoofed)
  - Payload: TCP
    - RST bit set
    - Source and destination ports: BGP (179)
    - Random sequence numbers
- B discards most packets, because their sequence numbers are invalid
- Sooner or later, C sends a packet with a valid sequence number
- BGP session resets

# LEGACY SOLUTION: TCP-MD5 [RFC 2385]

- Sending and receiving nodes are configured with a pre-shared key
- Sending node procedures
  - Calculate a Message Authentication Code (MAC) for each TCP segment
    - Use MD5 to calculate MAC
    - Calculate MAC over the TCP segment and the pre-shared key
  - Include an MD5 Signature Option in each segment
    - MD5 Signature Option includes MAC
- Receiving node procedures
  - Calculate a MAC for each received TCP segment
  - Discard the packet if the calculated MAC does not match the received MAC

# TCP-MD5 IS DEPRECATED

- New requirements
  - Change pre-shared keys without resetting TCP session
  - Support multiple authentication algorithms
- Pre-shared key change
  - It is difficult to change TCP-MD5 pre-shared keys without resetting the TCP session
  - It is difficult to reset TCP sessions that support BGP
  - Therefore, TCP-MD5 pre-shared keys were rarely changed
- Authentication algorithm agility
  - MD5 has been replaced by stronger authentication algorithms
  - Even stronger authentication algorithms are expected in the future

# TCP-AO [RFC 5925] REPLACES TCP-MD5

- Supports
  - Pre-shared key change without resetting TCP session
  - Multiple authentication algorithms

# TCP-AO CONCEPTS

- Master Key Tuple (MKT)
  - One or more MKTs are configured on each node
  - Used to derive traffic keys
- Traffic key
  - Used to generate a MAC for each TCP segment
- TCP-Authentication Option
  - Used to authenticate TCP segments
  - Contains a MAC, KeyID and RNextKeyID
    - KeyID identifies MKT and traffic key that were used to generate MAC
    - RNextKey identifies MKT and traffic key that the receiving node should use when generating a MAC for the next segment it sends

# MKT CONTENTS

- A TCP connection identifier
  - Source address, destination address, source port, destination port
  - Wildcards allowed
- A TCP Options flag (determine which TCP options are covered by MAC)
- Identifiers
  - Sending: Used to generate KeyID on outbound segments
  - Receiving: Used to resolve KeyID on inbound segments
- An authentication algorithm
- Master key (i.e., keying material)
- A key derivation algorithm

# PULLING IT ALL TOGETHER: KEYING

- Each node is each configured with one or more MKTs
- Each node derives four traffic keys from each MKT
- Each node independently determines which MKT is active
  - Method is beyond the scope of RFC 5925
  - Many implementations specify a start-time and an end-time for each MKT

# PULLING IT ALL TOGETHER: AUTHENTICATION

- Sending node procedures
  - Calculate a Message Authentication Code (MAC) for each TCP segment
    - Use the appropriate authentication algorithm
    - Calculate MAC over the TCP segment and an active traffic key
  - Include a TCP-AO in each segment
    - MD5 Signature Option includes MAC, KeyID and RNextKeyID
- Receiving node procedures
  - Calculate a MAC for each received TCP segment
    - Use algorithm and traffic key associated with the received KeyID
  - Discard the packet if the calculated MAC does not match the received MAC

# RELATIONSHIP WITH GTSM [RFC 5082]

- GTSM protects eBGP sessions
  - Sender sets TTL to 255
  - Receiver rejects packets containing eBGP if TTL is less than 254
- TCP-AO still needed to protect eBGP sessions from attackers that are one hop away
- TCP-AO still needed to protect iBGP sessions from internal attack

# IMPLEMENTATION STATUS AND FURTHER READING

## Implementation status:

- Juniper Networks: Committed for 20.3R1 (20.3R1 release candidate tested with Nokia)
- Nokia: SR OS 16.0.R15, 19.10.R7 and 20.5.R1 (interop tested with Juniper)
- Cisco: Stable since IOS XR 6.6.3 and 7.0.1

## Further reading:

- Nokia & Juniper interoperability test: https://github.com/TCP-AO/Interoperability-testing
- Configuration examples: https://github.com/TCP-AO/Configuration-examples


THANK YOU
JUNIPER NETWORKS
Engineering
Simplicity