

What can an onpath attacker do?

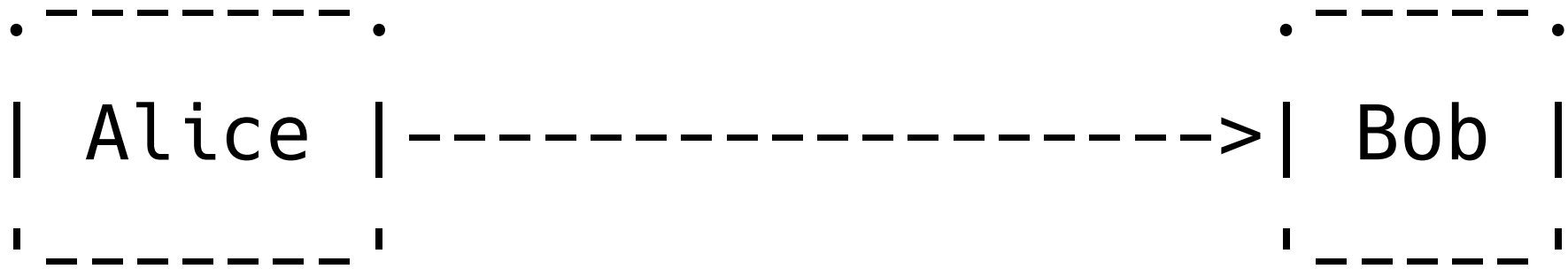
[draft-richardson-saag-onpath-attacker](#)

Michael Richardson <mcr+ietf @ sandelman.ca>

Jonathon Hoyland <jhoyland @ cloudflare.com>

For discussion.

Alice and Bob



Alice and Bob and Mallory (1)

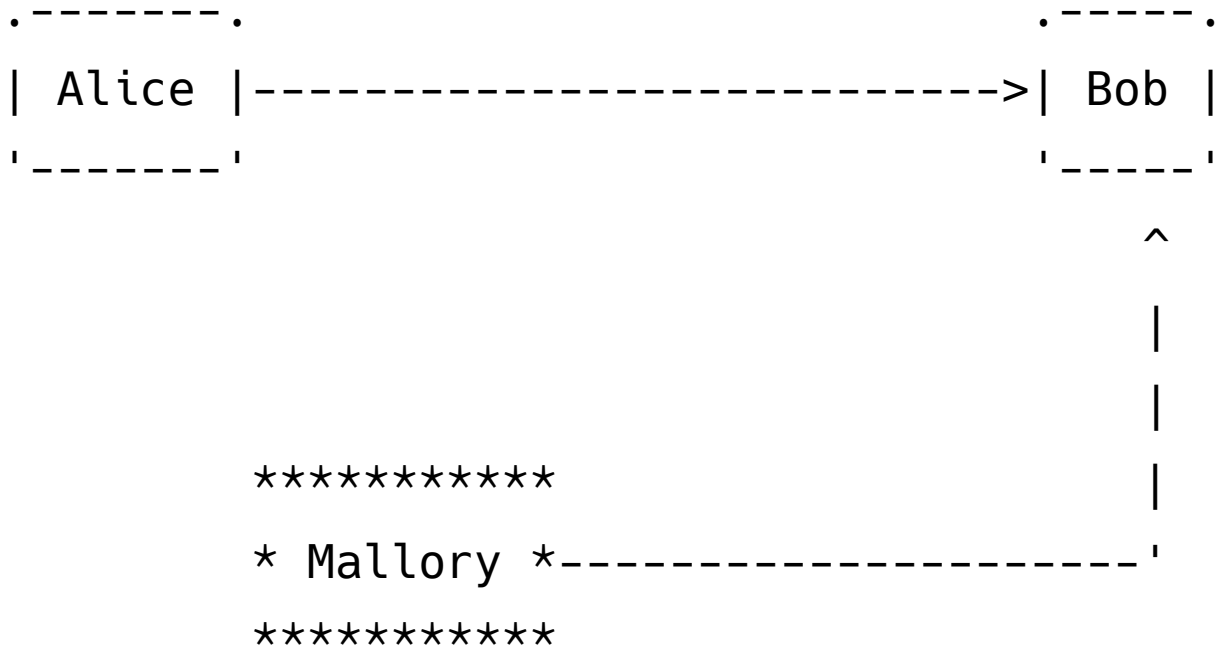
```
.-----.*-----.*-----.  
| Alice |-----* Mallory *----->| Bob |  
'-----' *-----'-----'
```

Alice and Bob and Mallory (2)

Diagram illustrating a quantum channel between Alice and Bob. Alice is on the left, Bob is on the right. A dashed line connects them, with a vertical line labeled 'v' in the middle.

* Mallory *

Alice and Bob and Mallory (3)



Alice and Bob and Mallory (4)

```

.----- .->-- .-----
| Alice |-----| | | .>| Bob |
'-----'      | | | | '-----'
                | | v | ^
                | | | |
                v '---> '--->|
                *****|
                * Mallory *-----'
                *****

```

Literature!

- (1) is a Dolev-Yao attack
 - view, delete and modify messages
- What do we call (2), (3), and (4)?
 - (2) can view, but not delete or modify
 - (3) can not view, but can send new ones
 - TCP SYN cookies, for instance, defends against (3)
 - (4) is a variation of (2), has been seen in the wild through BGP attacks

Proposals

- Replace “MAN” with “Mallory” (not sure who to blame here)
- Retains MITM TLA.
 - MITM is Dolev-Yao attack.
- “on-the-side” (2)
- “in-the-rough” (3)
 - “rough” is a golf term

Proposals

- From QUIC:
 - “on-path”
 - Limited-on-path
 - off-path
- Council of Attackers
 - Malicious messenger
 - Who rewrites messages sent
 - Oppressive observer
 - “uses your information against you”
 - Off-path attacker

Discussion

- Do **we** need to do anything?
- This is a higher level question than SECDISPATCH, at this point.