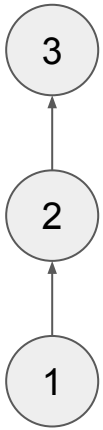
# Resync Risks

# What is a Resync Operation?

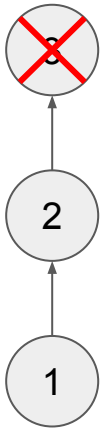
- Alice is in a group
- Somehow her local state gets corrupted
- Alice needs to rejoin the group
- Alice fetches a GroupInfo
- Alice does an external commit (with a Remove proposal)
- Alice is back in the group!

# Problem: GroupInfo is not checked properly



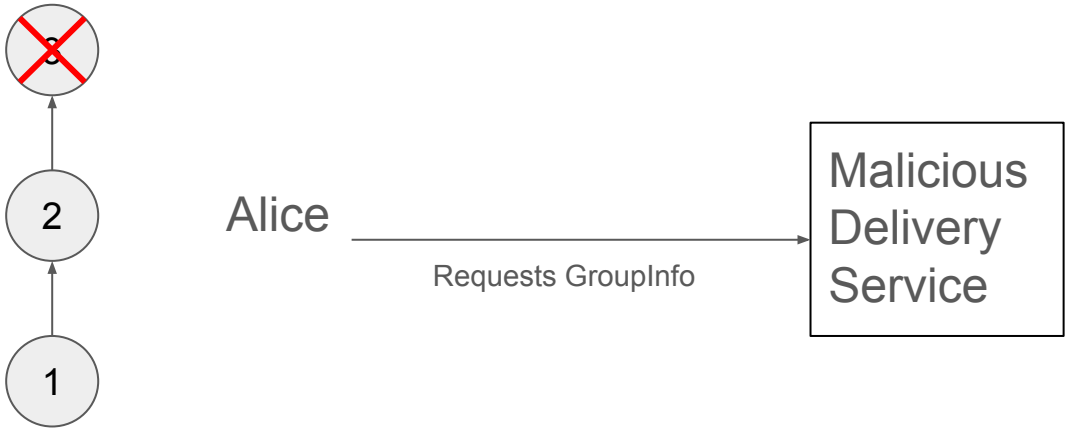

Alice

# Problem: GroupInfo is not checked properly

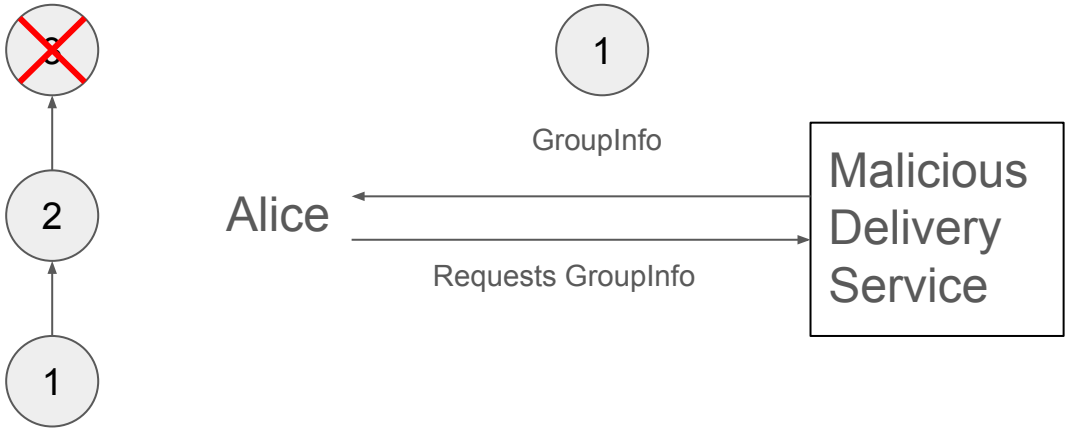



Alice

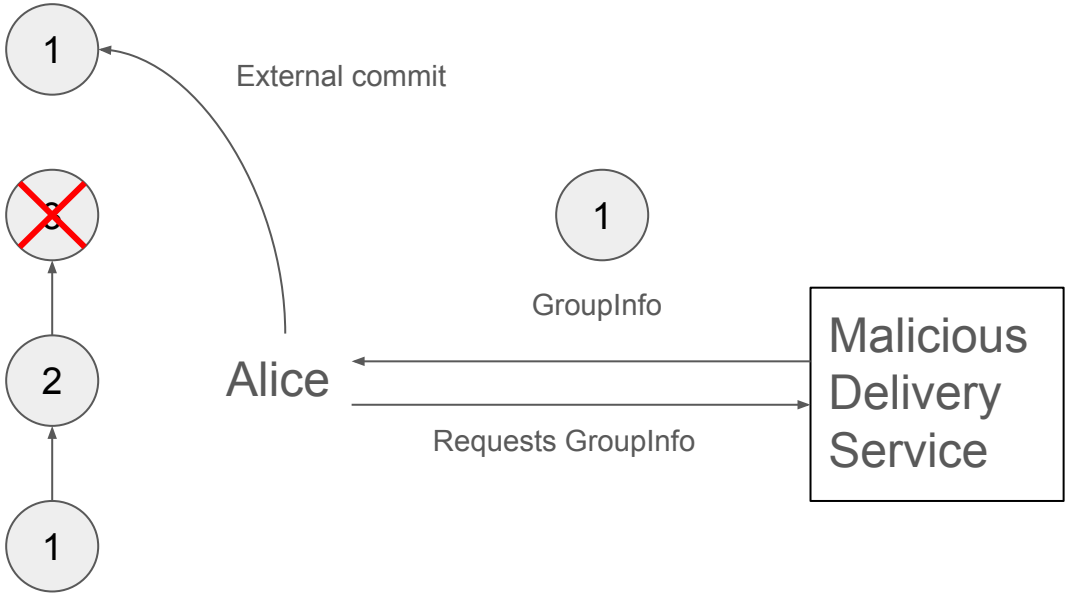
# Problem: GroupInfo is not checked properly



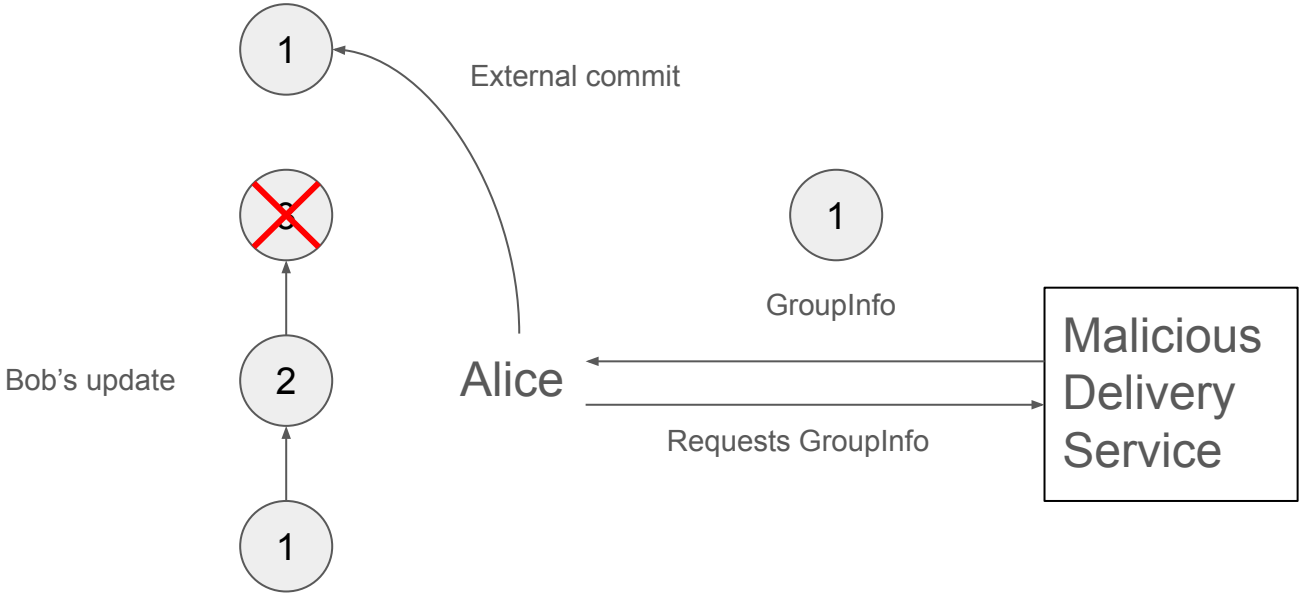
# Problem: GroupInfo is not checked properly



# Problem: GroupInfo is not checked properly



# Problem: GroupInfo is not checked properly



# How bad is this attack?

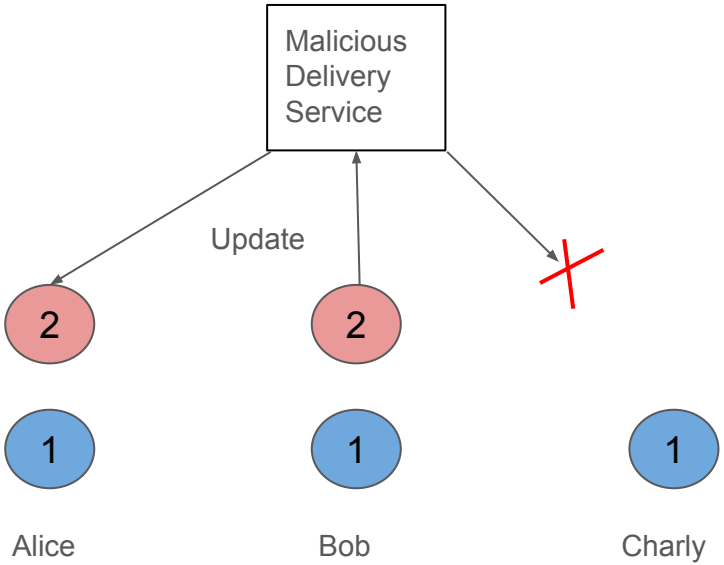
- Allows the DS to roll back a previously processed PCS update
- Not prevented by any validation rules in RFC 9420 (to my knowledge)
- Somewhat similar to blocking PCS updates in the first place, but can be launched at any time after compromise (assuming the GroupInfo is still valid)

# Mitigations discussed (in parts)

- Checking the epoch number and only accept increasing epoch numbers
- Transcript verification
- Client-side bookkeeping of public keys

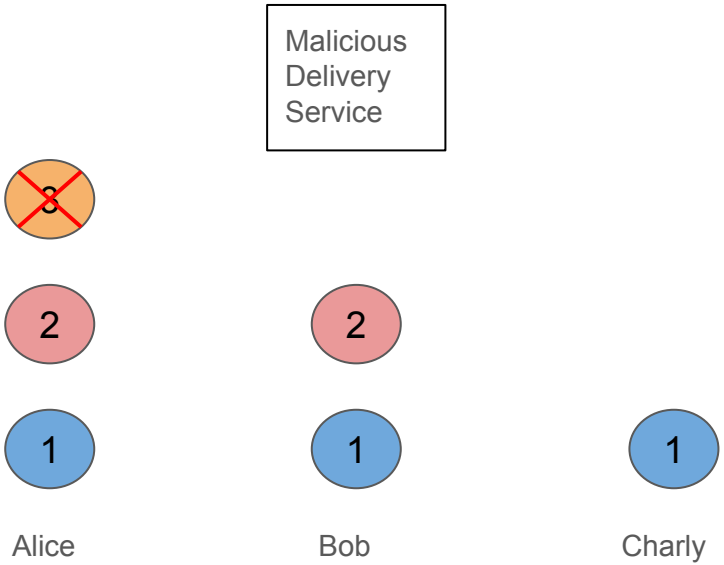
# Mitigations: Epoch checking?

- Checking the epoch to make sure Alice's state doesn't get downgraded?



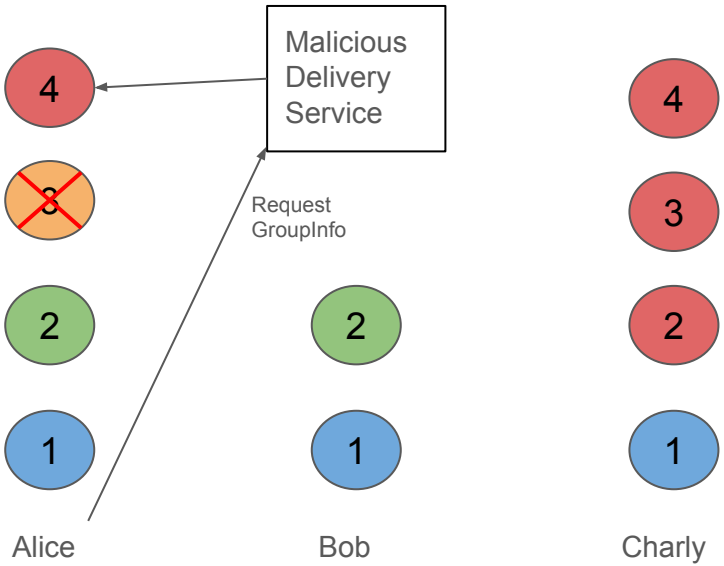
# Mitigations: Epoch checking?

- Checking the epoch to make sure Alice's state doesn't get downgraded?



# Mitigations: Epoch checking?

- Checking the epoch to make sure Alice's state doesn't get downgraded?

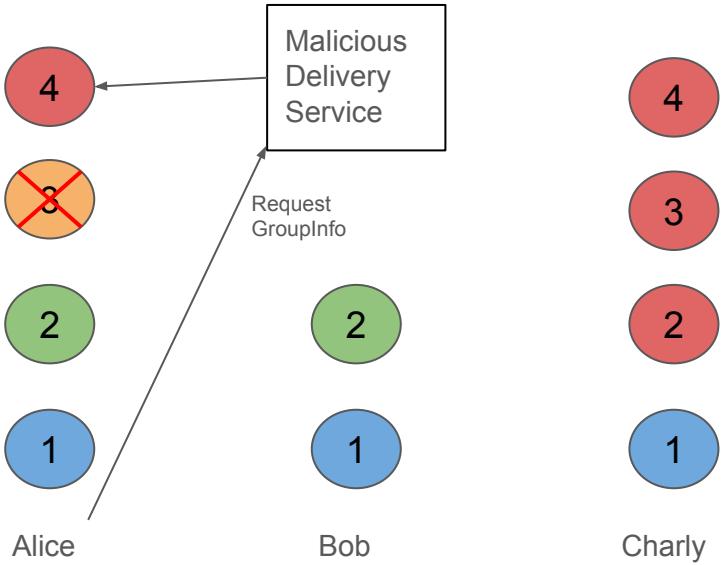


# Mitigations: Epoch checking?

- Checking the epoch to make sure Alice’s state doesn’t get downgraded?
- Pro: Good low-cost countermeasure that makes the attack harder
- Con: Not a complete defense, as the epoch is just an integer and says nothing about the cryptographic state

# Mitigations: Transcript verification?

- Before accepting a GroupInfo, Alice also requests transcript hashes
- Alice then checks that the transcript hashes extend her last known-good state
- If it doesn't check out, Alice rejects the GroupInfo



# Mitigations: Transcript verification?

- Before accepting a GroupInfo, Alice also requests transcript hashes
- Alice then checks that the transcript hashes extend her last known-good state
- If it doesn’t check out, Alice rejects the GroupInfo
- Con: Requires DS to keep around transcript hashes

# Mitigations: PublicKey bookkeeping?

- Alice keeps track of outdated leaf public keys for each group (HPKE and signature)
- When she does a Resync, she checks that none of the keys are outdated
- Con: Requires bookkeeping on the clients

# Next steps

- Do we like the mitigations?
- Do we want to recommend any in the arch document?
- Do we want to put any in the Errata for 9420?
- Do we want to have an extension?