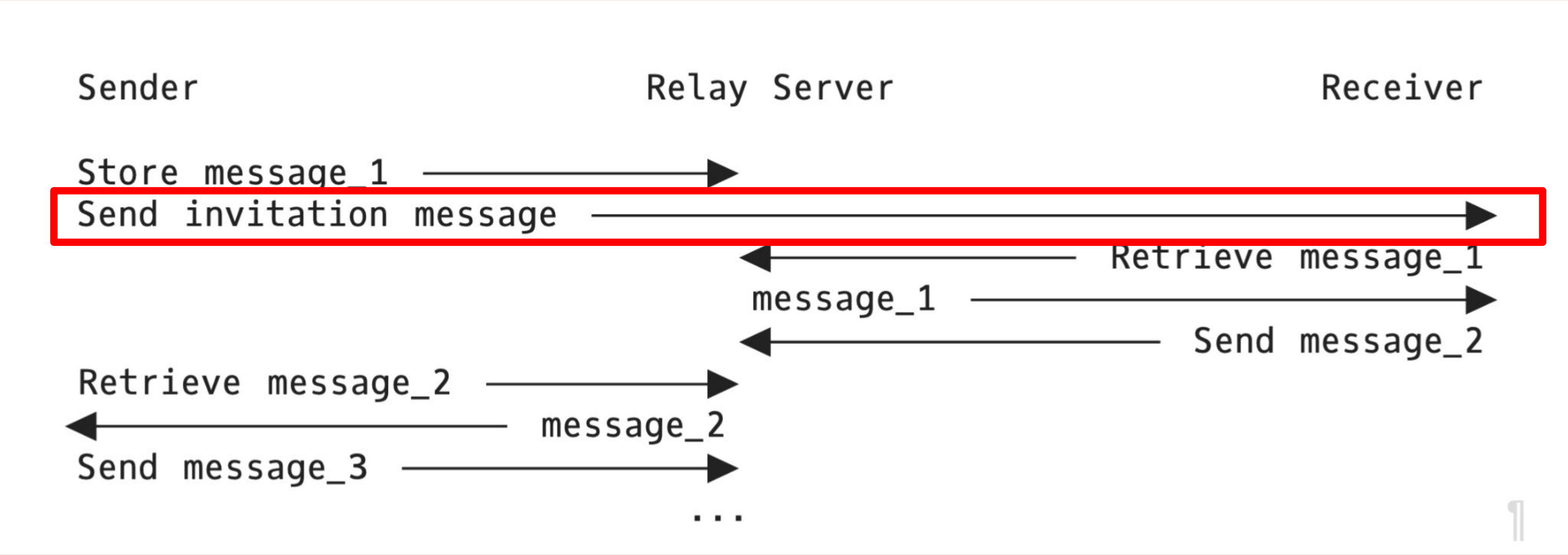
TIGRESS Introduction Channel Security

Eric Rescorla
ekr@rtfm.com

IETF 118

Introduction Channel



Sender

Relay Server

Receiver

Store message_1

Send invitation message

Retrieve message_1

message_1

Send message_2

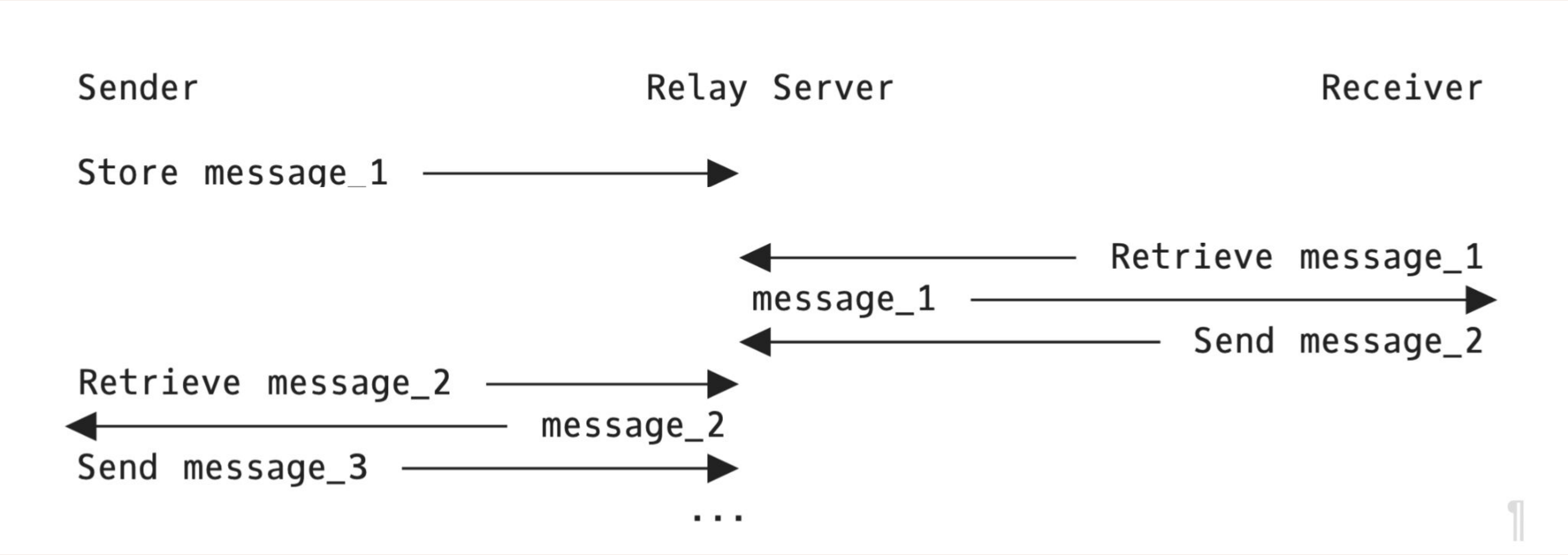
Retrieve message_2

message_2

Send message_3

...

Relay Channel



Sender

Relay Server

Receiver

Store message_1

Retrieve message_1

message_1

Send message_2

Retrieve message_2

message_2

Send message_3

...

Secret Invitations

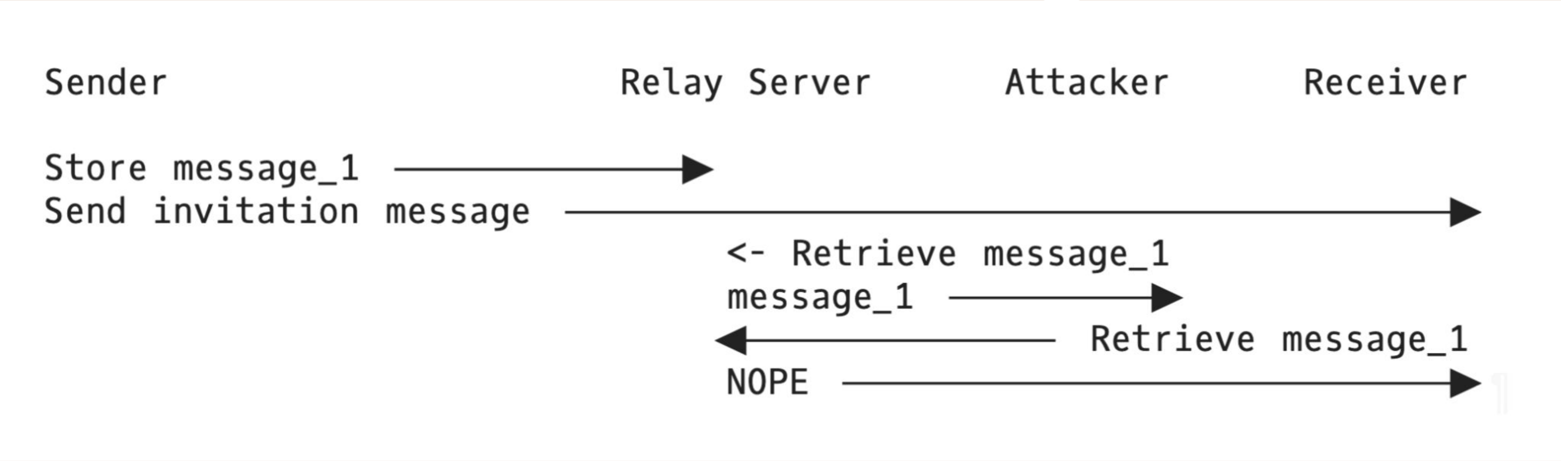
- Invitations identify Relay Channel
  - And are high entropy
- Correct invitation is needed to access the appropriate Relay Channel
- As long as Invitation remains secret, only the Receiver can access the Relay Channel

At-most-once semantics

- Both protocols are designed to provide at-most-once semantics
- The first agents to initiate a connection to the Relay Channel can access it
- Subsequent agents get denied access to the channel

Public Invitations

- If the attacker learns the invitation, then there is a race with the receiver
- The winner of the race gets the credential
- The attacker is often going to win this race



Sender Relay Server Attacker Receiver

Store message_1

Send invitation message

<- Retrieve message_1

message_1

Retrieve message_1

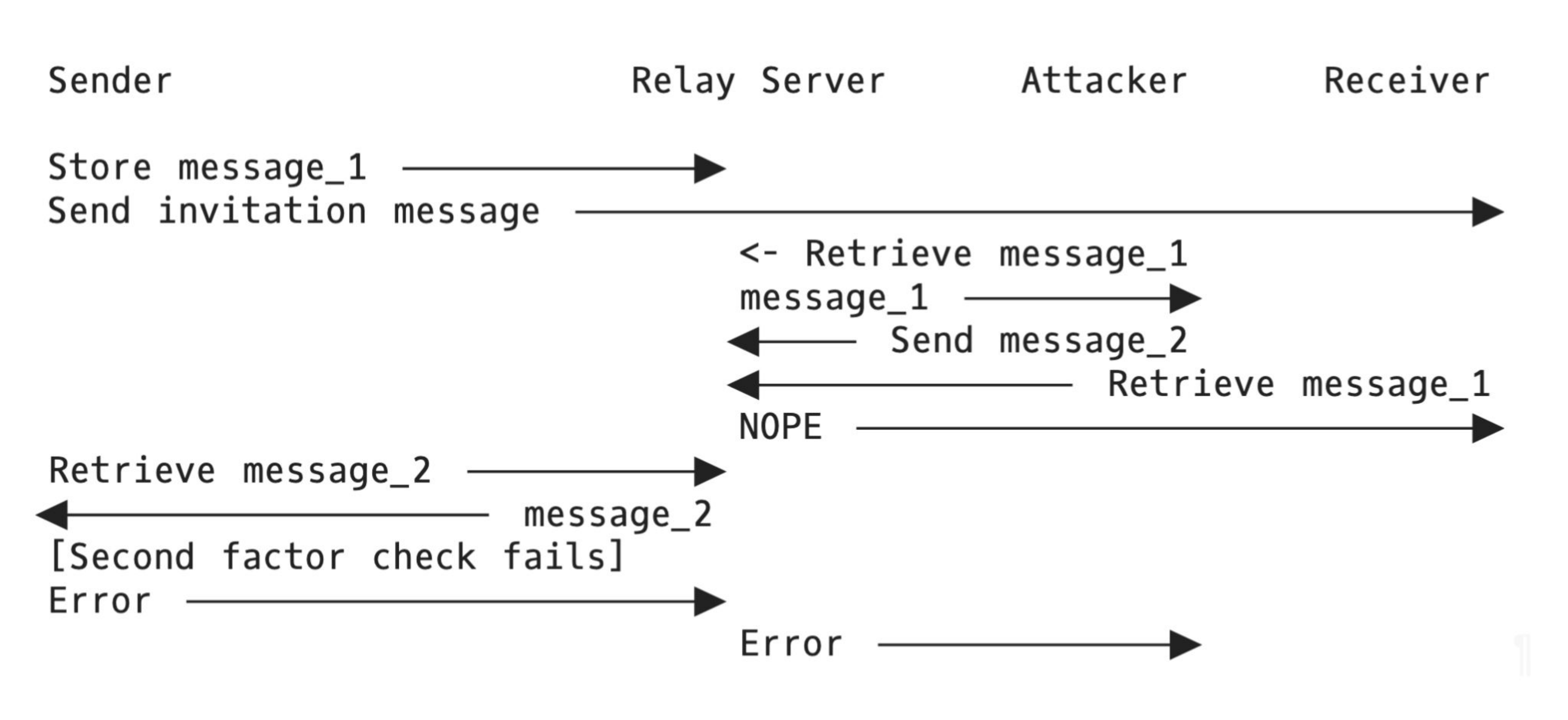
NOPE

Second Factor

- What if you have a second factor?
  - Delivered over a secure channel
- Examples
  - A cryptographic key
  - A PIN
  - An identity check*
- This controls credential issuance **but not the channel**
- Result: the attacker can access the channel but not get the credential

* Strictly speaking that's not delivered

Denial of Service



```
Sender                          Relay Server      Attacker        Receiver

Store message_1
Send invitation message
                                  <- Retrieve message_1
                                  message_1
                                          Send message_2
                                                    Retrieve message_1
                                  NOPE
Retrieve message_2
                       message_2
[Second factor check fails]
Error
                                  Error
```

Properties of Introduction Channel

- Lots of different channels
  - e-mail, SMS, iMessage, WhatsApp, NFC
- Widely varying security properties
- In practice we tend to treat these all as “secure” for other applications…
  - Password reset
  - 2FA
  - WebPKI certificate issuance

Options

1. Assume that the Introduction Channel is secure and move forward to protocol selection.
2. Assume that the Introduction Channel is insecure and ask what the properties of the “second factor” are and what needs to be done to bind it to the Relay Channel. This should happen prior to protocol selection.

Questions?