Secure Messaging
For Normal People
DEFCON 23
Messages
Threats

- Opportunistic, Low-resource adversaries
- Targeted, Low-resource adversaries
- Opportunistic, High-resource adversaries
- Targeted, High-resource adversaries
Transport Layer Security
End-to-End Encryption
End to End Server Matchmaking

Alice

Key request

Server response

Bob

- Unencrypted
- Encrypted
- End-to-end Encrypted
Evil Server
Transitive Trust
Metadata Collection

Bob

Carol

Alice

Frank

Encrypted