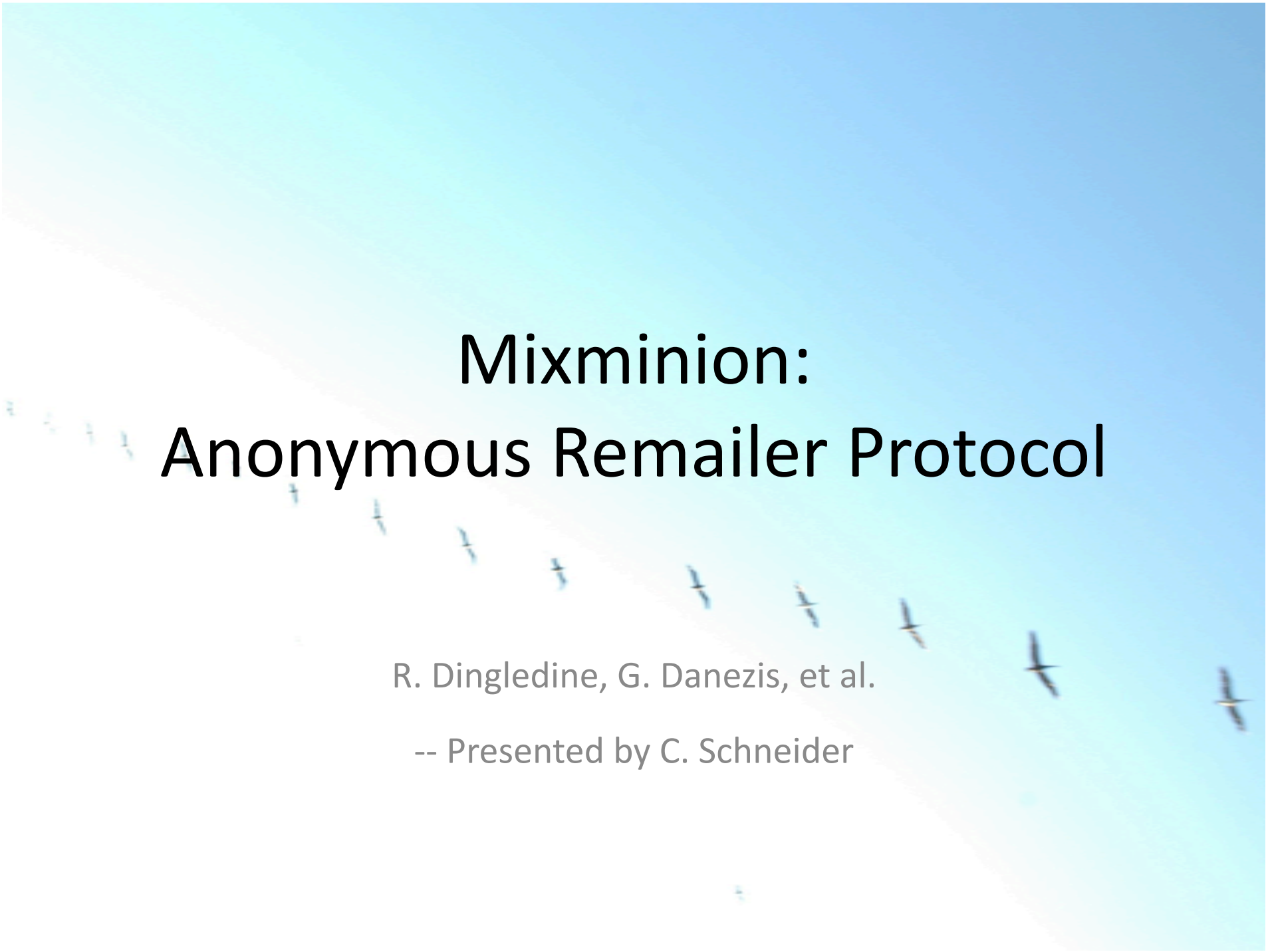

Mixminion: Anonymous Remailer Protocol

R. Dingledine, G. Danezis, et al.

-- Presented by C. Schneider

What is Mixminion?

- FTA: "… a message-based anonymous re-mailer protocol with secure single-use reply blocks."
- Based off of David Chaum's MIX's/Tor

Tenets of Mixminion

- Send & Receive E-mail Anonymously
  - *"... users should be able to receive messages from anonymous senders and send messages to anonymous recipients with a standard email client."*
- Preserve Message Integrity

Tenets (cont.)

- Be Simple to Deploy
  - Work with Existing Architecture and “commodity” hardware.
- Forward Anonymity
  - If a message is compromised, other messages are not compromised.

Features:
Things That Accomplish Goals

- Free-route Mix-Net; Ad Hoc
- Forward, Direct Reply, Anon-Reply
- Link Encryption
  - Prevent Eavesdropping, Reply Attacks, Preserve Forward Anonymity.
  - FA Assumes DH(k(1)(2)) are deleted by each node

Architecture

- Node
  - The initial requesting node. Part of a group of nodes, otherwise no-anon.
- Directory Servers
  - Maintain A list of nodes' current keys, capabilities and state.
  - Includes Statistics/Reputation

Architecture (cont)

- NYM Servers
  - Used to send / receive mail without revealing identities.
    - 1.) Create a PGP key-pair
    - 2.) Submit it to the NYM server, along with instructions (called a reply block) to anonymous remailers on how to send a message to your real address.
    - 3.) The NYM server returns a confirmation through this reply block.
    - 4.) You then send a message to the address in the confirmation.

Architecture (cont)

- SURBs (Single-Use Reply Blocks)
  - Mixminion uses tokens which work to forward to a hidden address.
  - Real World Example: Craigslist.

Known Attacks

- Tagging
  - "an attacker can use tagging to trace a message from the point t which it is tagged to the point at which the corrupted output appears.“
- Exit Nodes
  - An exit node will have access to a decrypted email, and can collude.
  - Without a proper exit node, it is impossible to avoid corruption in such a network.

Known Attacks

- Denial of Service
  - It is possible to corrupt other nodes and cause general network disruption.
  - There are some mechanisms in place for modeling behaviour but these behaviours can be fooled.
- User Behaviour
  - Users are responsible to maintain their ID or lack of ID as appropriate.

Future Work

- Preventing Message Tagging Attacks
- Introducing Dummy Data; Smoothing Statistical Inferences
- Zero Knowledge Proofs/Implementation

Conclusion

- Mixminion Protocol as a Positive.
- Mixminion Protocol as a Negative.

- Prognosis of Future Work?

Questions?