~~Viola~~Flute lessons

$93 \to \infty$

Secure messaging

- What's wrong with Skype/FB Messenger?
- Security properties:
  - End-to-end Confidentiality
  - Authentication
  - Perfect Forward Secrecy
  - Deniability
- Secure messaging tool: OTR
- Secure messaging tool: Signal

Secure multiparty messaging

- What is multiparty messaging?
- What's wrong with IRC/Viber groups?
- More security properties!
  - Transcript consistency
  - Room consistency
- Very few deployed secure multiparty messaging systems (only Signal groups?)

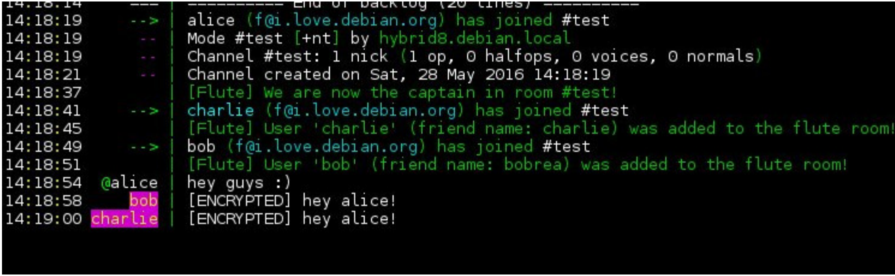
The Flute Protocol

- Flute is a secure multiparty messaging protocol
- Flute used to be a Celo and a Viola.
- Flute can work over IRC/XMPP/etc.
- Flute is currently implemented in Python over weechat
- Flute is an experiment

Flute workflow

- Every *flute room* has a *captain* that *manages* the room.
- 1) Alice establishes flute room and becomes room captain
- 2) Bob asks for room invite
- 3) Alice invites Bob to room (by passing him the crypto keys)
- 4) Charlie asks for room invite
- 5) Alice invites Charlie to room
- ...

Flute screenshot



```
14:18:14      --- | ---------- End of backlog (20 lines) ----------
14:18:19      --> | alice (f@i.love.debian.org) has joined #test
14:18:19       -- | Mode #test [+nt] by hybrid8.debian.local
14:18:19       -- | Channel #test: 1 nick (1 op, 0 halfops, 0 voices, 0 normals)
14:18:21       -- | Channel created on Sat, 28 May 2016 14:18:19
14:18:37          | [Flute] We are now the captain in room #test!
14:18:41      --> | charlie (f@i.love.debian.org) has joined #test
14:18:45          | [Flute] User 'charlie' (friend name: charlie) was added to the flute room!
14:18:49      --> | bob (f@i.love.debian.org) has joined #test
14:18:51          | [Flute] User 'bob' (friend name: bobrea) was added to the flute room!
14:18:54   @alice | hey guys :)
14:18:58      bob | [ENCRYPTED] hey alice!
14:19:00  charlie | [ENCRYPTED] hey alice!
```

Flute problems

- No room consistency
- No true message ordering
- Only one leader
- UX sucks (e.g. authentication, key management, etc.)
- Not deniable

How to help!

- `https://github.com/asn-the-goblin-slayer/flute`
- Lots of features needs to be implemented
- Lots of bugs needs to be fixed
- The weechat UI must improve
- More unittests are needed
- Get in touch!

Thanks! Questions?

https://github.com/asn-the-goblin-slayer/flute
Thanks! Questions?