

Using OTR (Off-The-Record) for Encrypted IRC Chat

OTR (Off-the-Record) messaging is a cryptographic protocol that provides end-to-end encryption, authentication, deniability, and perfect forward secrecy for instant messaging conversations. Implementing OTR on IRC ensures that private communications remain confidential and secure.

What is OTR?

OTR enhances IRC private messages by:

- **Encryption:** Ensures that messages cannot be read by unauthorized parties.
- **Authentication:** Confirms the identity of the communicating parties.
- **Deniability:** Prevents third parties from proving the content of the conversation.
- **Perfect Forward Secrecy:** Protects past communications even if long-term keys are compromised in the future.

For a comprehensive understanding of OTR, refer to the [OTR official website](#).

Supported IRC Clients

Several IRC clients support OTR, either natively or through plugins:

- **HexChat:** Supports OTR via plugins.
- **Irssi:** Supports OTR through the irssi-plugin-otr.
- **WeeChat:** Supports OTR via the python-potr plugin.
- **Pidgin:** Supports OTR through the pidgin-otr plugin.

For a detailed comparison of IRC clients and their features, visit the [Comparison of IRC clients](#) page.

Authenticating Contacts

OTR provides several methods to authenticate contacts:

- **Question and Answer:** Ask a question that only your contact can answer.
- **Shared Secret:** Share a secret passphrase with your contact.
- **Manual Fingerprint Verification:** Compare the OTR fingerprints of both parties.

For detailed instructions on authentication methods, refer to the [Off-the-Record Messaging guide](#).

Best Practices

- **Verify Fingerprints:** Always verify the OTR fingerprints of your contacts to prevent man-in-the-middle attacks.
- **Use Strong Passphrases:** Ensure that your passphrases are strong and unique.
- **Regularly Update Software:** Keep your IRC client and OTR plugins up to date to benefit from security patches.
- **Be Cautious of Logs:** Some clients may log OTR conversations; ensure logging is disabled if privacy is a concern.

Additional Resources

- [OTR Official Website](#)
- [OTR Wikipedia Page](#)
- [Off-the-Record Messaging Guide](#)

From:

<https://wiki.transirc.chat/> - TransIRC.Chat Wiki

Permanent link:

https://wiki.transirc.chat/doku.php?id=guides:irc:otr_encryption

Last update: **2025/05/19 11:22**

