Off-the-Record Messaging

Off-the-Record Messaging (**OTR**) is a cryptographic protocol that provides encryption for instant messaging conversations. OTR uses a combination of AES symmetric-key algorithm with 128 bits key length, the Diffie–Hellman key exchange with 1536 bits group size, and the SHA-1 hash function. In addition to authentication and encryption, OTR provides forward secrecy and malleable encryption.

The primary motivation behind the protocol was providing deniable authentication for the conversation participants while keeping conversations confidential, like a private conversation in real life, or off the record in journalism sourcing. This is in contrast with cryptography tools that produce output which can be later used as a verifiable record of the communication event and the identities of the participants. The initial introductory paper was named "Off-the-Record Communication, or, Why Not To Use PGP".[1]

The OTR protocol was designed by cryptographers Ian Goldberg and Nikita Borisov and released on 26 October 2004.[2] They provide a client library to facilitate support for instant messaging client developers who want to implement the protocol. A Pidgin and Kopete plugin exists that allows OTR to be used over any IM protocol supported by Pidgin or Kopete, offering an auto-detection feature that starts the OTR session with the buddies that have it enabled, without interfering with regular, unencrypted conversations. Version 4 of the protocol[3] is currently being designed by a team led by Sofía Celi, and reviewed by Nik Unger and Ian Goldberg. This version aims to provide online and offline deniability, to update the cryptographic primitives, and to support out-of-order delivery and asynchronous communication.

Contents

History

OTR was presented in 2004 by Nikita Borisov, Ian Avrum Goldberg, and Eric A. Brewer as an improvement over the OpenPGP and the S/MIME system at the "Workshop on Privacy in the Electronic Society" (WPES).[1] The first version 0.8.0 of the reference implementation was published on 21 November 2004. In 2005 an analysis was presented by Mario Di Raimondo, Rosario Gennaro, and Hugo Krawczyk that called attention to several vulnerabilities and proposed appropriate fixes, most notably including a flaw in the key exchange.[4] As a result, version 2 of the OTR protocol was published in 2005 which implements a variation of the proposed modification that additionally hides the public keys. Moreover, the possibility to fragment OTR messages was introduced in order to deal with chat systems that have a limited message size, and a simpler method of verification against man-in-the-middle attacks was implemented.[5]

In 2007 Olivier Goffart published `mod_otr`[6] for ejabberd, making it possible to perform man-in-the-middle attacks on OTR users who don't check key fingerprints. OTR developers countered this attack by introducing socialist millionaire protocol implementation in libotr. Instead of comparing key checksums, knowledge of an arbitrary shared secret can be utilised for which relatively low entropy can be tolerated by using the socialist millionaire protocol.[7]

Version 3 of the protocol was published in 2012. As a measure against the repeated reestablishment of a session in case of several competing chat clients being signed on to the same user address at the same time, more precise identification labels for sending and receiving client instances were introduced in version 3. Moreover, an additional key is negotiated which can be used for another data channel.[8]

Several solutions have been proposed for supporting conversations with multiple participants. A method proposed in 2007 by Jiang Bian, Remzi Seker, and Umit Topaloglu uses the system of one participant as a "virtual server".[9] The method called "Multi-party Off-the-Record Messaging" (mpOTR) which was published in 2009 works without a central management host and was introduced in Cryptocat by Ian Goldberg et al.[10]

In 2013, the Signal Protocol was introduced, which is based on OTR Messaging and the Silent Circle Instant Messaging Protocol (SCIMP). It brought about support for asynchronous communication ("offline messages") as its major new feature, as well as better resilience with distorted order of messages and simpler support for conversations with multiple participants.[11] OMEMO, introduced in an Android XMPP client called Conversations in 2015, integrates the Double Ratchet Algorithm used in Signal into the instant messaging protocol XMPP ("Jabber") and also enables encryption of file transfers. In the autumn of 2015 it was submitted to the XMPP Standards Foundation for standardisation.[12][13]

Currently, version 4 of the protocol has been designed. It was presented by Sofía Celi and Ola Bini on PETS2018.[14]

Implementation

In addition to providing encryption and authentication — features also provided by typical public-key cryptography suites, such as PGP, GnuPG, and X.509 (S/MIME) — OTR also offers some less common features:

- Forward secrecy: Messages are only encrypted with temporary per-message AES keys, negotiated using the Diffie–Hellman key exchange protocol. The compromise of any long-lived cryptographic keys does not compromise any previous conversations, even if an attacker is in possession of ciphertexts.
- Deniable authentication: Messages in a conversation do not have digital signatures, and after a conversation is complete, anyone is able to forge a message to appear to have come from one of the participants in the conversation, assuring that it is impossible to prove that a specific message came from a specific person. Within the conversation the recipient can be sure that a message is coming from the person they have identified.

Authentication

As of OTR 3.1, the protocol supports mutual authentication of users using a shared secret through the socialist millionaire protocol. This feature makes it possible for users to verify the identity of the remote party and avoid a man-in-the-middle attack without the inconvenience of manually comparing public key fingerprints through an outside channel.

Limitations

Due to limitations of the protocol, OTR does not support multi-user group chat as of 2009[15] but it may be implemented in the future. As of version 3[8] of the protocol specification, an extra symmetric key is derived during authenticated key exchanges that can be used for secure communication (e.g., encrypted file transfers) over a different channel. Support for encrypted audio or video is not planned. (SRTP with ZRTP exists for that purpose.) A project to produce a protocol for multi-party off-the-record messaging (mpOTR) has been organized by Cryptocat, eQualitie, and other contributors including Ian Goldberg.[10][16]

Since OTR protocol v3 (libotr 4.0.0) the plugin supports multiple OTR conversations with the same buddy who is logged in at multiple locations.[17]

Client support

libotr

Developer(s)	OTR Development Team (https://otr.cypherpunks.ca/people.php)
Stable release	4.1.1 / 9 March 2016
Written in	C
Operating system	Cross-platform
Type	Software Library
License	LGPL v2.1+[18]
Website	https://otr.cypherpunks.ca/index.php#downloads

Native (supported by project developers)

These clients support Off-the-Record Messaging out of the box. (incomplete list)

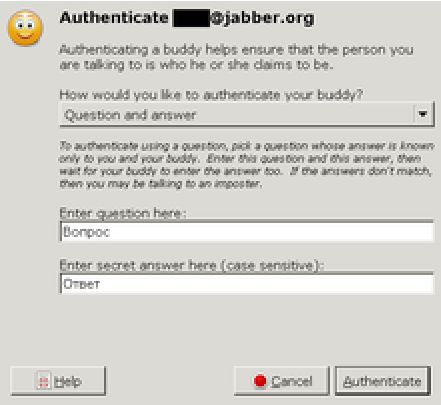
- Adium (OS X)
- Blink SIP client (OS X)
- BitlBee (cross-platform), since 3.0 (optional at compile-time)[19]
- CenterIM (Unix-like), since 4.22.2
- ChatSecure (iOS)
- Zom Mobile Messenger (Android)
- climm (Unix-like), since (mICQ) 0.5.4
- IronChat, based on Xabber (Android)
- Jitsi (cross-platform)
- Kadu (cross-platform), since 1.0[20]
- Kopete (Unix-like)[21][22]
- LeechCraft (cross-platform)[23][24]
- MCabber (Unix-like), since 0.9.4[25]

- Profanity, since 0.4.1
- Psi (cross-platform)[26]
- Psi+ (cross-platform)[26][27]
- Textual 5 (OS X), since 5.1.2
- Mozilla Thunderbird, since 68
- Xabber (Android)
- Tkabber (cross-platform), since version 1.1[28]
- irssi , in (future) releases released after August 2018, currently in 'master' repo

Via third-party plug-in

The following clients require a plug-in to use Off-the-Record Messaging.

- xchat, with a third-party plugin[29]
- Miranda IM (Microsoft Windows), with a third-party plugin[30]
- Pidgin (cross-platform), with a plugin available from the OTR homepage[31]
- WeeChat, with a third-party plugin[32]
- HexChat, for *nix versions, with a third-party plugin[33]



Authenticate [redacted]@jabber.org

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?

Question and answer

To authenticate using a question, pick a question whose answer is known only to you and your buddy. Enter this question and this answer, then wait for your buddy to enter the answer too. If the answers don't match, then you may be talking to an imposter.

Enter question here:

Вопрос

Enter secret answer here (case sensitive):

Ответ

Off-The-Record authentication in Pidgin using Socialist millionaires protocol

Confusion with Google Talk "off the record"

Although Gmail's Google Talk uses the term "off the record", the feature has no connection to the Off-the-Record Messaging protocol described in this article, its chats are not encrypted in the way described above—and could be logged internally by Google even if not accessible by end-users.[34][35]

See also

- foss Free software portal

References

1. Nikita Borisov, Ian Goldberg, Eric Brewer (28 October 2004). "Off-the-Record Communication, or, Why Not To Use PGP" (https://otr.cypherpunks.ca/otr-wpes.pdf) (PDF). *Workshop on Privacy in the Electronic Society*. Retrieved 6 March 2014.
2. Ian Goldberg (26 October 2014). *[OTR-users] Happy 10th anniversary!* (https://lists.cypherpunks.ca/pipermail/otr-users/2014-October/002515.html). Retrieved 27 April 2015.
3. Sofía Celi, Ola Bini (15 February 2019). "Off-the-Record Messaging Protocol version 4" (https://github.com/otrv4/otrv4).

4. Mario Di Raimondo; Rosario Gennaro; Hugo Krawczyk (2005). "Secure off-the-record messaging" (https://www.dmi.unict.it/diraimondo/web/wp-content/uploads/papers/otr.pdf) (PDF). *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. Association for Computing Machinery: 81–89.
5. "Off-the-Record Messaging Protocol version 2" (https://otr.cypherpunks.ca/Protocol-v2-3.1.0.html).
6. "mod_otr" (http://www.ejabberd.im/mod_otr).
7. Chris Alexander; Ian Avrum Goldberg (February 2007). *Improved User Authentication in Off-The-Record Messaging* (https://cypherpunks.ca/~iang/pubs/impauth.pdf) (PDF). *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*. New York: Association for Computing Machinery. pp. 41–47. doi:10.1145/1314333.1314340 (https://doi.org/10.1145%2F1314333.1314340). ISBN 9781595938831. S2CID 17052562 (https://api.semanticscholar.org/CorpusID:17052562).
8. "Off-the-Record Messaging Protocol version 3" (https://otr.cypherpunks.ca/Protocol-v3-4.0.0.html).
9. Jiang Bian; Remzi Seker; Umit Topaloglu (2007). *Off-the-Record Instant Messaging for Group Conversation* (https://www.researchgate.net/publication/4272374). IEEE International Conference on Information Reuse and Integration. IEEE. doi:10.1109/IRI.2007.4296601 (https://doi.org/10.1109%2FIRI.2007.4296601).
10. Ian Avrum Goldberg; Berkant Ustaoğlu; Matthew D. Van Gundy; Hao Chen (2009). *Multi-party off-the-record messaging* (https://cypherpunks.ca/~iang/pubs/mpotr.pdf) (PDF). *Proceedings of the 16th ACM Computer and Communications Security Conference*. Association for Computing Machinery. pp. 358–368. doi:10.1145/1653662.1653705 (https://doi.org/10.1145%2F1653662.1653705). hdl:11147/4772 (https://hdl.handle.net/11147%2F4772). ISBN 9781605588940. S2CID 6143588 (https://api.semanticscholar.org/CorpusID:6143588).
11. Nik Unger; Sergej Dechand; Joseph Bonneau; Sascha Fahl; Henning Perl; Ian Avrum Goldberg; Matthew Smith (2015). "SoK: Secure Messaging" (http://ieee-security.org/TC/SP2015/papers-archived/6949a232.pdf) (PDF). *Proceedings of the 2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society's Technical Committee on Security and Privacy: 232–249.
12. Straub, Andreas (25 October 2015). "OMEMO Encryption" (https://web.archive.org/web/20160129003540/https://xmpp.org/extensions/inbox/omemo.html). *XMPP Standards Foundation website*. Archived from the original (https://xmpp.org/extensions/inbox/omemo.html) on 29 January 2016. Retrieved 16 January 2016.
13. Gultsch, Daniel (2 September 2015). "OMEMO Encrypted Jingle File Transfer" (https://xmpp.org/extensions/inbox/omemo-filetransfer.html). *XMPP Standards Foundation website*. Retrieved 16 January 2016.
14. Sofía Celi, Ola Bini (21 July 2018). *No evidence of communication: Off-the-Record Protocol version 4* (https://petsymposium.org/2018/files/hotpets/7-bini.pdf) (PDF). Retrieved 29 November 2018.
15. Ian Goldberg (27 May 2009). "multi-party OTR communications? (and other OTR details)" (http://lists.cypherpunks.ca/pipermail/otr-users/2009-May/001647.html). *OTR-users mailing list*.
16. Nadim Kobeissi (1 February 2014). "mpOTR Project Plan" (https://github.com/cryptocat/cryptocat/wiki/mpOTR-Project-Plan). *Cryptocat wiki on GitHub*.
17. Ian Goldberg (4 September 2012). "pidgin-otr and libotr 4.0.0 released!" (https://lists.cypherpunks.ca/pipermail/otr-announce/2012-September/000058.html). *OTR-announce mailing list*.
18. "Off-the-Record Messaging" (https://otr.cypherpunks.ca/index.php#faqs).
19. "BitlBee Wiki" (http://wiki.bitlbee.org/bitlbee-otr). Wiki.bitlbee.org. 25 January 2014. Retrieved 15 May 2014.

20. "Kadu 1.0 Release Notes" (https://web.archive.org/web/20161207084931/http://www.kadu.im/w/English:ReleaseNotes1). Archived from the original (http://www.kadu.im/w/English:ReleaseNotes1) on 7 December 2016. Retrieved 15 February 2015.
21. "kopete-otr in KDE for 4.1" (https://web.archive.org/web/20080328080733/http://kopete-otr.follefuder.org/news.html). Archived from the original (http://kopete-otr.follefuder.org/news.html) on 28 March 2008.
22. "kopete-otr review request" (http://lists.kde.org/?t=120397998900007&r=1&w=2).
23. 0xd34df00d. "OTR Plugin" (https://github.com/0xd34df00d/leechcraft/tree/master/src/plugins/azoth/plugins/otroid). Github.com. Retrieved 6 September 2017.
24. "Short description" (http://leechcraft.org/plugins-azoth). Leechcraft.org. Retrieved 15 May 2014.
25. "source code" (https://web.archive.org/web/20140517132343/http://mcabber.com/hg/index.cgi/file/a18e1b488f1c/mcabber/otr.c). MCabber.com. 25 October 2013. Archived from the original (http://mcabber.com/hg/index.cgi/file/a18e1b488f1c/mcabber/mcabber/otr.c) on 17 May 2014. Retrieved 15 May 2014.
26. "OTR Plugin" (https://github.com/psi-im/plugins/tree/master/generic/otrplugin). Github.com. Retrieved 6 September 2017.
27. "Psi+ snapshots" (https://github.com/psi-plus/psi-plus-snapshots/tree/master/plugins/generic/otrplugin). Github.com. Retrieved 6 September 2017.
28. "Tkabber OTR Plugin" (https://web.archive.org/web/20140311093019/https://svn.xmpp.ru/repos/tkabber/trunk/tkabber-plugins/otr/). Archived from the original (https://svn.xmpp.ru/repos/tkabber/trunk/tkabber-plugins/otr/) on 11 March 2014.
29. "irssi-otr / xchat-otr plugin" (http://irssi-otr.tuxfamily.org). 4 February 2019.
30. "Miranda OTR Plugin" (https://code.google.com/p/mirotr/).
31. "OTR plugin for Pidgin" (https://otr.cypherpunks.ca/#downloads).
32. "OTR plugin for WeeChat" (https://github.com/mmb/weechat-otr). January 2019.
33. "TingPing/hexchat-otr" (https://github.com/TingPing/hexchat-otr). *GitHub*. Retrieved 14 March 2017.
34. "Chatting off the record - Talk Help" (https://support.google.com/talk/answer/29291?hl=en).
35. "Google Talk - Privacy Policy" (https://www.google.com/intl/en/policies/privacy/).

Further reading

- Joseph Bonneau; Andrew Morrison (21 March 2006). "Finite-State Security Analysis of OTR Version 2" (http://www.jbonneau.com/doc/BM06-OTR_v2_analysis.pdf) (PDF). Retrieved 5 September 2013.
- Mario Di Raimondo; Rosario Gennaro & Hugo Krawczyk (2005). "Secure Off-the-Record Messaging" (http://www.dmi.unict.it/diraimondo/web/wp-content/uploads/papers/otr.pdf) (PDF). Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. Association for Computing Machinery. Retrieved 27 August 2013.

External links

- Official website (https://otr.cypherpunks.ca/)
- Protocol specification (https://otr.cypherpunks.ca/Protocol-v3-4.1.1.html)
- Off-the-Record Messaging: Useful Security and Privacy for IM (https://csclub.uwaterloo.ca/media/Off-the-Record%20Messaging:%20Useful%20Security%20and%20Privacy%20for%20IM.html), talk by Ian Goldberg at the University of Waterloo (video)
- 'Off-the-Record' Instant Messaging Tutorial (encryption, authentication, deniability, ..) (https://www.youtube.com/watch?v=aV6-s9o9bVw) on YouTube

Retrieved from "https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&oldid=1000281387"