OMEMO support in Tails

The OMEMO encryption /ˈmiːmoʊ/ (OMEMO Multi-End Message and Object Encryption) gives you all the advantages you would expect from a modern-day encryption protocol like Future and Forward Secrecy and deniability while allowing you to keep the benefits of message synchronization and offline delivery.

OMEMO not only gives you a better encryption features than OpenPGP and OTR but is also much easier to setup. OMEMO is the encryption you can actually use in your daily life. Turn it on once and forget you ever did.

OMEMO uses the Signal Protocal ratchet to establish secure sessions between every combination of devices for you and your contact. Those sessions are then being used to communicate secure keys to all devices. OMEMO will generate a new key for every message. That key is used to encrypt your message with AES-GCM. The long-lived Signal Protocal sessions in the background deal with the challenges of message reordering, message loss and accidental duplication.

Being built upon PEP (Personal Eventing Protocol) to announce the pre-keys used by Signal Protocal to establish new sessions, OMEMO requires little to no change to the existing XMPP server infrastructure.

https://conversations.im/omemo/

Tails could work upstream to help Pidgin impliment OMEMO by assisting with this ticket: https://developer.pidgin.im/ticket/16801

Alternatively, Tails could include Gajim https://packages.debian.org/jessie/net/gajim and Kalkin's Gajim OMEMO plugin.

OTR is the current default chat encryption option on Tails. OTR is 10 years old and was never designed for modern day instant messaging.
#3 - 08/24/2016 03:58 AM - sajolida
- Related to Feature #7868: Use gajim instead of pidgin (more secure OTR chat) added

#4 - 08/24/2016 03:58 AM - sajolida
- Related to Bug #8573: Hopefully replace Pidgin some day added

#5 - 09/17/2016 12:14 PM - Kurtis
Gajim's omemo plugin was put into the Debian sid repository a few weeks ago: https://packages.debian.org/sid/gajim-omemo  I'm assuming it could be backported.

Pidgin might as well change their name to Ostrich, because their head is in the sand when it comes to adding support for OMEMO. 
https://developer.pidgin.im/ticket/16801

#6 - 01/07/2017 08:30 AM - intrigeri
https://current.workingdirectory.net/posts/2017/encrypted-mucs/ suggests that this needs polishing as the current UX is quite poor.

#7 - 01/08/2017 02:33 AM - Kurtis
Thanks for the link. I hadn't read that before.

Just got news that people are working to add OMEMO support to Pidgin: https://developer.pidgin.im/ticket/16801#comment:27 I'll try to dig some more to find more details.

I know that there is a chance that Tails could one day use Tor Messenger based on this: https://labs.riseup.net/code/issues/8577

Here's a ticket for TorMessenger OMEMO support: https://trac.torproject.org/projects/tor/ticket/17457

Here's a ticket for TorMessenger's upstream InstantBird OMEMO support: https://bugzilla.mozilla.org/show_bug.cgi?id=1237416

#8 - 01/23/2017 12:18 AM - Kurtis
Quick update: Two people that are working to add OMEMO support to Pidgin just posted at https://developer.pidgin.im/ticket/16801

If anyone wants to check out the OMEMO+XMPP+Pidgin alpha git repo that one of the devs posted, you can check it out here: https://git.imp.fu-berlin.de/mancho/libpurple-omemo-plugin

#9 - 02/10/2017 11:08 PM - Kurtis
Lurch is an alpha release plugin for libpurple that enables OMEMO encryption: https://github.com/gkdr/lurch

#10 - 12/11/2017 03:38 AM - Kurtis
Can you please un-Reject this issue? OMEMO is the future. The future shouldn't be rejected, it should be embraced.

#11 - 12/11/2017 04:29 AM - Kurtis
I know you guys are looking to move away from Pidgin, but I just created this an issue with Lurch asking them to make a debian repo. 
https://github.com/gkdr/lurch/issues/73
I should have said "make a debian package" not "make a debian repo". my bad.

This is a valid feature request. I think it'll be addressed either as part of #8573 or thanks to the upcoming changes to the Additional Software Package feature (which will soon become much more usable, better integrated, and thus an option for everyone who wants their preferred IM protocol/client, because we can't possibly ship them all).

This is a valid feature request. I think it'll be addressed either as part of #8573 or thanks to the upcoming changes to the Additional Software Package feature (which will soon become much more usable, better integrated, and thus an option for everyone who wants their preferred IM protocol/client, because we can't possibly ship them all).

libsignal-protocol-c is now in debian testing:

https://github.com/gkdr/lurch/issues/73#issuecomment-371144505
https://tracker.debian.org/pkg/libsignal-protocol-c

And our additional software feature will be in Tails 3.9, allowing anybody to install such things themselves now as long as they are available in Debian :)

But I'm unsure if this addresses the problem you are raising entirely?

Friends of mine have extensively tested OMEMO and they report that:

- If different clients are used, with different implementation status of some tech details, one can easily lose messages without knowing they lost it.
- Encrypted groups don't work well, especially (or only) when different clients are used.

Sorry I have nothing more specific such as links to bug reports, but I do trust these friends to have tested this extensively, in practical use cases, for a non-trivial duration.

I briefly tested lurch which has a Debian RFP (stating that "lurch is the more active of the two OMEMO libpurple plugins"). Some random observations:

- I had no issues with OMEMO for private messages!
- [continuing the previous point] ... well, except the experience was too automatic and transparent, so it wasn't clear at all that OMEMO was enabled. The only interface you have is via /lurch commands (and messages written to the chat log), and there's nothing reporting the status of OMEMO. The closest thing I found was that I could see that I have a key fingerprint, which I guess implies encryption at least is possible. IMHO this UX problem is a hard blocker for inclusion in Tails.
- Obviously lurch to lurch works fine, but I also successfully tested lurch to Conversations (which has a better UI and made it clear lurch managed to speak OMEMO) so at least some different implementations seem able to talk to each other. :)

- OMEMO for MUCs require that the room is non-anonymous (everyone's jid is exposed) and that everyone manually enables OMEMO (e.g. `/lurch enable`) which was pretty limiting and awkward.

- They seem to care about being included in Tails: https://github.com/gkdr/lurch/issues/73 :)

---

#20 - 12/05/2018 11:12 AM - anonym

One more thing: my Pidgin supported OTR and OMEMO at the same time, and this caused severe issues (impossible to send readable messages) with recipients that also support both.

#21 - 12/05/2018 12:29 PM - Anonymous

I only tried OMEMO with Gajim. It works very well and depending on the server config, messages are kept on the server until I reconnect, so this is great. In Gajim, OMEMO is supported by default now. (while using it with OTR is not, and their security model stinks: it requires downloading untrusted ZIP files from somewhere in the universe).

I've not tried group chats, but Gajim is clever and can send messages to several devices at once (again, this is a server config issue).

I'd say: we could test if it works with Additional Software in Tails (and can persist the settings and keys). And one should probably test what happens if people try to install plugins using the above described disgusting method.