No evidence of communication: OTRv4

Sofía Celi, Jurre van Bergen
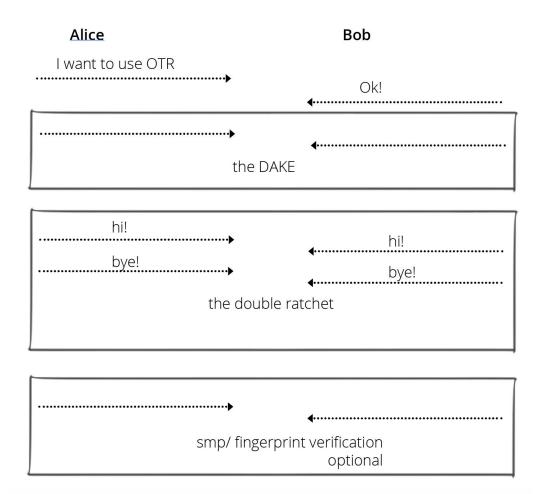
what is OTR?

- OTR, Off-the-Record messaging, began with an academic paper by Ian Goldberg, Nikita Borisov and Eric Brewer.
- Provides encryption with forward secrecy; authentication; and, most importantly, deniability.
- Different versions.
- Other protocols take inspiration from it.

OTRv4

- New definitions of deniability: online, offline, participation, message.
- New security properties: security level, forward and backwards secrecy, post-compromise security.
- New cryptographic primitives.
- New network model.
- Has a specification.

Alice   **Bob**

I want to use OTR
···············▶

                              Ok!
                    ◀···············

···············▶   ◀···············
              the DAKE

hi!   hi!
···············▶   ◀···············
bye!   bye!
···············▶   ◀···············
         the double ratchet

···············▶   ◀···············

       smp/ fingerprint verification
                    optional

the flow

the state

- Specification on github
- Implementation, called libotr-ng, which is written in the C language.
- Plugin for pidgin.
- Plans to package for different OS.
- Java and Golang implementations underway

- Theory + practice

check out our repos!

The protocols:

https://github.com/otrv4/otrv4

https://github.com/otrv4/otrv4-prekey-server

The library:

https://github.com/otrv4/libotr-ng

The plugin:

https://github.com/otrv4/pidgin-otrng

The prekey server:

https://github.com/otrv4/otrng-prekey-server

https://github.com/otrv4/prekey-server-xmpp

The toolkit:

https://github.com/otrv4/libotr-ng-toolkit

Thanks!

Jurre van Bergen   Sofía Celi
@DrWhax   @cherenkov_d