Privacy and deniability by design: Off-the-Record messaging version 4

Sofa Celi[1]

Centro de Autonoma Digital, Quito, Ecuador
sofia@autonomia.digital

Cryptography is commonly used to secure private communications over the Internet, or to solve the secure messaging problem. It is commonly used to solve this problem because that is the most fundamental privacy problem that one can work on. Working on this question addresses the idea that the Internet, while at the beginning used mostly as a medium for the transfer of technical information, is now manly used as a communication tool.

One of these types of communication is what is often called "casual personal conversations", that mimic the idea of casual non-digital world conversations. The difference between non-digital and digital conversations resides in the fact that, on the latter, privacy is diminished, as third parties can always be listening without the knowledge of the participants in it.

There are some protocols that have tried to improve this situation by providing encryption and digital signatures. Often times, though, the encryption keys used are long-lived and subject to compromise; and the digital signatures are not deniable. In order to tackle this problem, the Off-The-Record messaging protocol (OTR) was created. It achieved two core properties: perfect forward secrecy and deniability.

Nevertheless, OTR is a protocol that was created in 2004, and, since then, protocol properties have changed to adapt to new forms of communication, to new cryptographic primitives and properties. For this reason, a new version of the OTR protocol, OTRv4, has been created. This new version of the protocol provides end-to-end encryption, different types of deniability, and stronger notions of forward and post-compromise secrecy. It has higher security properties than other protocols, like the Signal protocol. In this short talk, we will discuss the properties of OTRv4, its privacy by design thinking and how it is necessary to have this kind of thinking.