La crittografia nella messaggistica istantanea

Edoardo Ferri

Studio Tecnico
Ferri & Costantino

2019

Protocollo crittografico Off-the-Record Messaging (OTR)

Off-the-Record Communication, or, Why Not To Use PGP

Nikita Borisov
UC Berkeley
nikitab@cs.berkeley.edu

Ian Goldberg
Zero-Knowledge Systems
ian@cypherpunks.ca

Eric Brewer
UC Berkeley
brewer@cs.berkeley.edu

ABSTRACT

Quite often on the Internet, cryptography is used to protect private, personal communications. However, most commonly, systems such as PGP are used, which use long-lived encryption keys (subject to compromise) for confidentiality, and digital signatures (which provide strong, and in some jurisdictions, legal, proof of authorship) for authenticity.

In this paper, we argue that most social communications online should have just the opposite of the above two properties; namely, they should have *perfect forward secrecy* and *repudiability*. We present a protocol for secure online communication, called "off-the-record messaging", which has properties better-suited for casual conversation than do systems like PGP or S/MIME. We also present an implementation of off-the-record messaging as a plugin to the Linux GAIM instant messaging client. Finally, we discuss how to achieve similar privacy for high-latency communications such as email.

Categories and Subject Descriptors

K.4.1 [**Management of Computing and Information**

over the last decade to become the basis for a wide variety of forms of communication, ranging from electronic commerce, to the sharing of music and video, to social conversation.

Along with the growing population of the Internet came growing concern over the security of the data flowing across it. Your online communications could be observed by any number of third parties on their way to their destinations. Even data residing on your own PC could be vulnerable if you were unlucky enough to open the wrong email attachment.

The protections developed were twofold: use firewalls and host security to lock down the endpoints, and use *cryptography* to protect the information in transit. Popular cryptographic systems, such as SSL [9], PGP [6, 33], and S/MIME [4], were developed and used to protect diverse forms of data.

The majority of electronic commerce is protected by SSL. What about social communication? Some of it takes place over email, for which PGP and S/MIME are common tools of protection. And an increasing portion of it uses instant messaging protocols, such as AIM [3], MSN [20], ICQ [16], and many others. To protect instant messages there are sev-

Cronologia

- 2004 - Presentazione OTR Nikita Borisov, Ian Avrum Goldberg e Eric A. Brewer come miglioramento rispetto all'OpenPGP e al sistema S / MIME
- 2005 - Mario Di Raimondo, Rosario Gennaro e Hugo Krawczyz scoprono diverse vulnerabilitá, viene pubblicata la versione 2 del protocollo
- 2012 - Version 3 Corretto problema intercettazione messaggi multiclient e introduzione chiave aggiuntiva in operazioni AKE permette di utilizzare comunicazioni sicure su altri canali (es. trasferimento file, chat vocale)

Cronologia

- 2013 - TextSecure / Signal Protocol basato su OTR e Silent Circle Instant Messaging Protocol (SCIMP)
- 2014 - Partnership per crittografia end-to-end tra Open Whisper System / WhatsApp
- 2016 - Google Allo per chat incognito e Facebook per chat sergrete

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.
https://en.wikipedia.org/wiki/Off-the-Record-Messaging

Diffie - Hellman key exchange protocol

- Pubblicato per la prima volta da Whitfield Diffie e Martin Hellman nel 1976
- Nel 1997 fu rivelato che James H. Ellis , Clifford Cocks e Malcolm J. Williamson del GCHQ nel 1969 implementarono un metodo di scambio chiavi

WhatsApp

Sistema sviluppato in collaborazione con Open Whisper Systems utilizzando le librerie open source del protocollo Signal

Telegram

Protocollo di crittografia MTProto 2.0 due diversi tipi di cifratura: *Cloud Chats* sistema client-server/server-client e *Secret Chats* con cifratura end-to-end

Signal

Software sviluppato da Open Whisper Systems e rialsciato sotto licenza GPL v3

Possibili alternative

Client con protocollo di cifratura end-to-end OTR nativo:

- Pidgin (per Windows o Linux)
- Adium (per macOS)
- ChatSecure (per iOS)