Oral: An efficient protocol for multi-party deniable communication

Hong Liu Eugene Y. Vasserman

Kansas State University

Off-The-Record Messaging (OTR) is an online analog of face-to-face private conversation first proposed by Borisov, Goldberg and Brewer. Like an in-person conversation, the two parties authenticate to each other, but *unlike traditional public-key cryptography*, the protocol is unconditionally repudiable: neither party of a two-person conversation can prove what was said (or who said it) to an external observer no matter how many messages the observer records or how much computational power he possess. The initial OTR concept was limited to two parties, and the inherent complexity of group communication makes it nontrivial to extend OTR to a group setting. First, authentication in group chat requires identifying the origin of messages among group members, which may conflict with repudiability, which is to deny one is the origin of a message. Second, in a two-person conversation, or with a reliable broadcast channel, we guarantee that every participant "hears" the same talk, but reliable broadcast is difficult and expensive to achieve in the presence of adversaries. Consistency in participants' views of the group conversation is a problem unique to group communication. Furthermore, malicious insiders may easily disrupt communication, and utilize the repudiable natural of the protocol to avoid punishment — another problem unique to group off-the-record communication. Finally, there is the persistent problem of whether the group protocol retains the same security properties when multiple participants collude against one or more other participants. Existing multi-party OTR schemes such as the recent multi-party off-the-record messaging (mpOTR) protocol do not provide security that matches an intuitive notion of private group conversations, and have several other drawbacks like vulnerability to denial of service if a single participant misbehaves or leaves the conversation.

We propose a group off-the-record (GOTR) scheme which provides unconditional repudiability and authentication within the group off-the-record environment. We do not rely on reliable broadcast, using asynchronous point-to-point communication links instead, so our design is robust to network failure and gracefully and efficiently handles membership events (like join and leave) without disrupting the group conversation or voiding its security properties. Counter-intuitively, authentication in our design is *made possible as a by-product of repudiability.* GOTR operates in a uniform mode without the need to establish a group order or a group leader.

We devise a formal method to analyze the properties of a category of GOTR protocols that use mutual authentication, and show that existing GOTR schemes such as mpOTR do not provide security that well matches one's intuitive notion of private conversation and show that our scheme provides unconditional repudiability. We use the Burmester-Desmedt group key agreement algorithm, although several others can be employed as long as they are "contributory", that is the group key is derived from cryptographic contribution from every group member. This special instance of our scheme has high efficiency both in computation and in the number of communication rounds. We have implemented the protocol as a plugin for the popular Pidgin instant messaging platform.