Related Work

David Mis

March 22, 2014

Anonymous connections in GSM was first proposed in a scheme by Lin and Jan [Lin, Jan]. Unfortunately, they included a faulty proof-of-security, and [Barbancho, Peinado] subsequently demonstrated that the LJ scheme was insecure. Specifically, the LJ scheme used ticket-based anonymous credentials that could be forged, transered, and reused [YTWY, LJ, BP, B]. In this paper, we avoid these pit-falls by using provably unforgable, one-time-use authentication tickets. Tickets can still be transfered between users, but re-use compromises the offender's anonymity, making it easy for network administrators to detect and identify abusive users (discussed more in section ??).

Several schemes have expanded and improved the LJ scheme [P, HLH, YTWY]. These schemes focus on providing anonymous connections (are these just for calls or location update too?) for mobile stations while roaming in a visitng network. In contrast, our scheme provides anonymity for users even when connecting to their home network Our scheme also accomodates preserving a user's anonymity while traveling in a visiting network, as discused in section ??. It should be noted that we allowed ourselves more freedom in changing a customer's experience when using their phones; where previously proposed schemes only require changes that are transparent to the user, we have added an additional handshake between mobile stations before the first time they wish to call each other (similar to the user handshake found in many VOIP systems like Skype).

There has also been extensive research into the privacy properties of VOIP systems. [WCJ, BS] shows how a network attacker could introduce "timing watermarks" into call data in order to identify two communicating parties. [M et al] proposed a system to solve this issue by introducing dummy messages to make calls unobservable in a system with a limited number of users. paper complements this existing body of work by introducing an address register system that prevents even system administrators from identifying the addresses of particular users. This is especially important in peer-to-peer systems like Skype where the location register is distributed among thousands of untrusted nodes [Garfinkel, Perenyi]. The ideal VOIP system will protect users from identification from inside the system as in our scheme as well as protect from identification from external attackers at call-time like in Melchor et al.