Enhancing privacy of paging procedure in LTE

ABSTRACT

The mechanisms adopted by cellular technologies for user identification allow an adversary to collect information about individuals and track their movements within the network; and thus exposing privacy of the users to unknown risks. Despite efforts have been made by Long Term Evolution LTE toward enhancing privacy preserving capabilities, LTE does not eliminate the possibility of user privacy attacks. LTE is still vulnerable to user privacy attacks. This paper includes an evaluation of LTE security architecture and proposes a security solution for the enhancement of paging procedure privacy in LTE. The solution is based on introducing of frequently changing unrelated temporary mobile subscriber identifiers (TMSI) used for identification. The scheme provides secure and effective identity management in respect to the protection of user privacy in LTE during paging process. The scheme is formally verified using proVerif and proved to provide an adequate assurance of user privacy protection.

Keyword: LTE (Long Term Evolution); TMSI (Temporary Mobile Subscriber Identifier); Linkability; Traceability; Paging