Background

This study focuses on protecting cellphone user data in mobile communication networks that are critical infrastructures with approximately four billion users in the world. Mobile communication plays an important role in the military, economic, and political spheres. In recent years, the data security of a large number of mobile communication users has become a major concern.

The cellphone user's data (Hereinafter referred to as user data), which are directly related to communication events, contain cellphone users' identification, location identification, routing identification, security parameters set, service profile list, and the like. Facts and studies have shown that these user data are facing serious security problems like being illegally acquired and tampered due to the vulnerabilities in the No. 7 signaling system that is used as one of the fundamental protocols in mobile communication networks.

For cellphone users, their MSISDN numbers (i. e., cell phone number), which are used as communication identifiers, are normally open to the public, while MSISDN numbers are usually stored and transmitted in mapping state with other data (e. g., IMSI, location identification, subscribed service list, security parameters set), and based on the mapping relationship, almost all the other data items can be retrieved according to MSISDN numbers. Thus, once a cellphone users' MSISDN numbers have been known, it is easy for attackers to access to the user's other data. We infer that user data's mapping-relationship may be a main way that leads to user data leakage. This problem motivates us to incorporate the data dynamics and virtualization technology to develop a mobile communication user data mimic defense mechanism. The core idea of this mechanism is to diversify the mapping relationships between MSISDN numbers and other data by introducing virtual MSISDN number in the uncontrollable communication process and network equipment, which can effectively resist the attacker through signaling filtering and database access to access user data. The method is characterized by no change in the existing mobile communication network protocol system, and to ensure that the user's open MSISDN number is the only real. The author gives the core idea of MSISDN number dynamics and virtualization, demonstrates its feasibility, and gives the implementation scheme. Finally, a theoretical analysis model is established to verify and analyze the security efficiency of the security mechanism.

This work was supported by the Funds for Creative Research Groups of China under Grant NSFC-No. 61521003, the National Key Research Program of China under Grant Nos. 2016YFB0800100 and 2016YFB0800101, and the Visiting Scholar Program of China under Grant of China Scholarship Council-201407820028.