Avis de soutenance de thèse

M. Mourad ABDELJEBBAR

Soutiendra sa thèse pour obtenir le grade de Docteur

de l'Institut National des Postes et Télécommunications

Le Mardi 24 Juillet 2018 à 10h00 à l'amphithéâtre de l'INPT.

Sujet de thèse :

« Nouvelles approches de sécurisation des processus d'authentification dans le système 4G-EPS»

Devant le jury :

M. Mostafa BELLAFKIH, PES, INPT, Rabat (Président) ;

M. Mohammed BOULMALF, PES, UIR, Rabat (Rapporteur) ;

M. Abdellah NAJID, PES, INPT, Rabat (Rapporteur) ;

M. Nabil MRANI, PH, EST, Meknès (Rapporteur) ;

M. Rachid EL KOUCH, PES, INPT, Rabat (Directeur de thèse);

Abstract:

During the past three decades, many new mobile network systems have been developed after the first generation, like the EPS system. Indeed, the EPS system is a fourth-generation network (4G), which is the result of a combination between an evolved access network, called LTE, and an IP-based core network, called SAE. It has been modeled by the 3GPP group to increase not only the mobile users' data rate and communications security, but also the network reliability. In addition, the information security of mobile operator and its mobile users is becoming one of the main issues to be dealt carefully when designing the EPS system. In this context, the 3GPP group has standardized a set of algorithms and protocols to improve the security of EPS system compared to second (2G) and third (3G) generation systems. In particular, he defined the EPS-AKA protocol to ensure the authentication of mobile user who wants to use network resources.

However, the current authentication procedure has many weaknesses that can be exploited by intruders to execute malicious attacks and thereby affect the confidentiality and privacy of the system and its mobile users. For this reason, many researchers have been carried out to address these weaknesses by improving or modifying totally or partially the initial procedure in order to design a very strong authentication protocol. However, most of the proposed solutions in the literature do not offer a good level of security. In addition, the complexity of some solutions does not allow their implementation on mobile devices of a low energy and storage space. Therefore, the design of simple and secure solutions is mostly needed.

In this context, we propose in this thesis two solutions. The first is designed to improve the procedure standardized by the 3GPP group. The overall idea is to combine simplicity of deployment, full mutual authentication and secure communications between all entities involved in the authentication process. The second is designed to improve the authentication process proposed by Cristina-Elena Vintilă. The solution was designed to change completely the standard procedure by using the J-PAKE protocol mechanism in order to perform mutual authentication between the mobile user and the serving MME. While our improvements rely on the mechanisms allowing the design of a complete mutual protocol and the security of the exchanged authentication data. Finally, in order to validate our solutions, we used the AVISPA tool to verify the achievement of the desired objectives.