عنوان مقاله:

Analysis of an RFID Authentication Protocol in Accordance with EPC Standards

محل انتشار:

مجله بین المللی ارتباطات و فناوری اطلاعات, دوره 6, شماره 4 (سال: 1393)

تعداد صفحات اصل مقاله: 6

نویسندگان:

Behzad Abdolmaleki
Hamidreza Bakhshi
Karim Baghery
Mohammad Reza Aref

خلاصه مقاله:

In the past few years, the design of RFID authentication protocols in accordance with the EPC Class-١ Generation-٢ (EPC C١ G٢) standards, has been one of the most important challenges in the information security domain. Although RFID systems provide user-friendly services for end-users, they can make security and privacy concerns for them. In this paper we analyze the security of an RFID mutual authentication protocol which is based on EPC Class-١ Generation-٢ standard and proposed in ٢٠١٣. The designers of protocol claimed that their protocol is secure against different security attacks and provides user privacy. In this paper, we show that unlike their claims, their protocol is not secure against most of the security attacks such as replay attack, the tag’s ID exposure, and the spoofing attacks. As a result, their protocol cannot provide security of RFID users in different authentication applications. Finally, in order to prevent the aforementioned attacks and overcome all the existing weaknesses, we apply a modification in the .updating procedure of the protocol and propose a strengthened version of it

کلمات کلیدی:

Security and Privacy, RFID Authentication protocols, EPC Class-١ Generation-٢ standards

لینک ثابت مقاله در پایگاه سیویلیکا: