پروتکلهای تبادل کلید، احراز اصالت، تبادل کلید توام با احراز اصالت (AKE) و تبادل کلید و احراز اصالت مبتنی بر گذر واژه (PAKE)

محسن تورانی

toorani@ieee.org

دانشکده مهندسی برق

دانشگاه علم و صنعت ایران

دی ماه ۱۳۸۵

چکیده

در این گزارش در ابتدا اصول کلی پروتکلهای مبادله کلید[1] تحت بررسی قرار می گیرند. همچنین برخی از پروتکلهای کاربردی جهت احراز اصالت[2] و تعدادی از پروتکلهایی که مبادله کلید را همراه با احراز اصالت انجام می دهند، معرفی می‌شوند. سپس به معرفی پروتکلهای مبادله کلید و احراز اصالت مبتنی بر گذر واژه خواهیم پرداخت و در پایان نیز به طور مختصر روشهای مختلف تحلیل و معیارهای ارزیابی میزان امنیت یک پروتکل معرفی می‌شود.

کلمات کلیدی: پروتکلهای مبادله کلید(KE)، پروتکلهای احراز اصالت، پروتکلهای مبادله کلید توام با احراز اصالت (AKE)، پروتکلهای مبادله کلید و احراز اصالت مبتنی بر گذر واژه (PAKE)، حملات لغتنامه‌ای، روشهای تحلیل پروتکل

[1] Key Exchange
[2] Authentication

فهرست مطالب