عنوان مقاله:
تحلیل امنیت یک پروتکل احراز اصالت و تبادل کلید در کاربرد VoIP

محل انتشار:
چهاردهمین کنفرانس مهندسی برق ایران (سال: 1385)

تعداد صفحات اصل مقاله: 7

نویسندگان:
بهروز ترک لادانی - *گروه کامپیوتر ، دانشکد ه مهندسی، دانشگاه اصفهان*

سعید جلیلی - *گروه کامپیوتر، دانشکد ه مهندسی، دانشگاه تربیت مدرس*

خلاصه مقاله:
در این مقاله چگونگی کشف یک سناریوی حمل ه جدید علیه پروتکل احراز اصالت و تبادل کلید VSP- که جهت برقراری سرویس های امنیتی در VoIP طراحی شده است- را تشریح نموده ایم. برای یافتن این حمله از روشی که اخیرا جهت مدل سازی راهبرد انجام حمله به عنوان بخشی از قابلیت های یک نفوذی هوشمند ارائه شده، استفاده نموده ایم. در سناریوی حمل ه کشف شده، نفوذی قادر است با ایجاد دو نشست موازی، آغازگر پروتکل را فریب داده، نقش مخاطب را برای وی بازی کند. علاوه بر این، نفوذی می تواند یک کلید نشست قابل قبول بین خود (به عنوان مخاطب) و آغازگر برقرار نماید. روشی برای اصلاح پروتکل VSP و جلوگیری از انجام پذیری حمل ه کشف شده نیز ارائه شده است.

کلمات کلیدی:
تحلیل پروتکل های رمزنگاری، تحلیل آسیب پذیری, وارسی صوری, سناریوی حمله