عنوان مقاله:
آنالیز و تحلیل های حمله های موجود در فناوری ارتباط حوزه نزدیک NFC و ارایه راهکار نوین برای ارتقا رمزنگاری برای جلوگیری از شنود

محل انتشار:
سومین کنفرانس سراسری نوآوری های اخیر در مهندسی برق و کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 12

نویسندگان:
محمود فتحی - *استاد دانشکده کامپیوتر دانشگاه علم و صنعت*

سیدعلی صموتی - *مدیر پژوهش مرکز علمی کاربردی فرهنگ و هنر واحد 49*

خلاصه مقاله:
فناوری ارتباط حوزه نزدیک (NFC)، یک فناوری نوین و کارا برای ارتباطفی ما بین دستگاه های سیار می باشد. داده ها بین دستگاه ها در محدوده کوتاه انتقال می یابند، که این ارتباط شامل ارتباط بین دو گوشی موبایل ، ارتباط بین گوشی موبایل و تگ و ارتباط بین گوشی موبایل و قرایت گر می باشد. یکی از کاربردهای کارا در این فناوری سامانه های پرداخت الکترونیک است که، با توسعه NFC گوشی موبایل می تواند مانند کارت های پرداخت در کاربردهای مختلف عمل می نماید؛ با گسترش هر فناوری در حوزهIT ، المان مهمی که باید مد نظر قرار گیرد امنیت آن فناوری است. بنابراین امنیت این فناوری و جلوگیری از حملات مختلف و شنود ناپذیری گوشی تلفن همراه ، امری مهم و حیاتی در این عرصه خواهد بود. در این مقاله ابتدا به معرفی اجمالی این حوزه و تکنولوژی مربوطه می پردازیم. سپس تهدیدهای وارده بر سیستم شناسایی می گردد تا ابعاد مختلف حملات معلوم شوند. سپس سناریوهایی برای مقابله با این حملات تعریف خواهد شد. در فناوری ارتباط حوزه نزدیک، رمزنگاری در دو مرحله صورت می گیرد ، ابتدا یک کلید جلسه به صورت رمزنگاری نامتقارن بین دو هویت جابجا شده و سپس دو هویت برای تبادل سایر داده ها از آن کلید جلسه استفاده نموده و با بهره گیری از رمزنگاری متقارن استاندارد AES ، داده ها را جابه جامی نمایند. در این مقاله با توجه به استاندارد امنیتی تعریف شده برای ارتباط حوزه نزدیک، در بخش رمزنگاری کلید عمومی روش های مختلفی مانند بلوفیش، AES ، Twofish و DES را با یکدیگر مقایسه و تحلیل می نماییم و با توجه به حالت کاری ارتباط حوزه نزدیک (فعال، غیر فعال)، روش مناسب تری را با توجه به نوع کاربرد را از نظر نتایج تیوری به دست آمده پیشنهاد خواهیم داد. نشان خواهیم داد که الگوریتم توفیش می تواند یک جایگزین مناسب تر برای الگوریتم AES در استاندارد تعریف شده ارتباط حوزه نزدیک باشد و توان مصرفی و پردازش مصرفی را نیز به اندازه معقولی کاهش یابد.

کلمات کلیدی:
ارتباط حوزه نزدیک ، NFC ، Twofish، power conception ، CPU conception