عنوان مقاله:
آسیب پذیری های امنیتی در DNS (سیستم نام دامنه) و DNSSEC (توسعه امنیت سیستم نام دامنه)

محل انتشار:
اولین همایش منطقه ای بهینه سازی و روش های محاسبه نرم در مهندسی برق و کامپیوتر (سال: 1392)

تعداد صفحات اصل مقاله: 9

نویسندگان:
کاظم فریدی - *، کارشناسی ارشد، دانشکده فنی مهندسی دانشگاه آزاد اسلامی واحد بافت*

زینب مرادیان - *کارشناسی ارشد، دانشکده فنی مهندسی دانشگاه آزاد اسلامی واحد بافت*

مهدی گلشن - *عضو باشگاه پژوهشگران و نخبگان دانشگاه آزاد اسلامی واحد سپیدان*

خلاصه مقاله:
داده های سیستم نام دامنه)DNS) که توسط سرورهای نامگذاری ایجاد می گردند فاقد پشتیبانی تایید منشاء داده و یکپارچگی داده ها می باشند. این فرایند، سیستم نام دامنه (DNS) را در معرض حمله کاربران (MITM) و همچنین مجموعه ای از حملات دیگر قرار می دهد. برای اینکه سیستم نام دامنه (DNS) قدرتمند تر شود DNSSEC توسط کمیته کارگروه مهندسی اینترنتی (IETF) مطرح شده است. DNSSEC مجوز منشاء داده و یکپارچگی داده ها را با استفاده از علائم دیجیتالی ایجاد می کند. اگرچه DNSSEC امنیتی را برای داده های سیستم نام دامنه (DNS) ایجاد می کند، از نقص های جدی عملیاتی و امنیتی زیان می بیند. ما به بررسی طرح های DNSSEC و DNS پرداخته، و آسیب پذیری امنیتی مربوط به آن ها را مد نظر قرار می دهیم.

کلمات کلیدی:
سیستم نام دامنه ، توسعه امنیت سیستم نام دامنه،پروتکل اینترنتی،ایستگاه پردازش،سرور و کلاینت