

عنوان مقاله:

نیازهای امنیتی طرح رای گیری سی آز

محل انتشار:

اولین کنفرانس مهندسی برق و کامپیوتر (سال: 1397)

تعداد صفحات اصل مقاله: 8

نویسندگان:

سمیه رمضانیا - دانشجوی کارشناسی ارشد مهندسی کامپیوتر نرم افزار، دانشگاه آزاد اسلامی، واحد شهید آملی

علی خسرو زاده - استادیار دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد شهید آملی

میثم محمدی - استادیار دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد شهید آملی

خلاصه مقاله:

الزامات امنیتی بعنوان معیارهای امنیت پروتکل های رای گیری معرفی می شوند. غالباً هر پروتکل یکسری از الزامات را برآورده می کند. استفاده از امضای کور منجر به برآورده سازی حداکثری این الزامات می شود. طرح امضای کور توسط چایوم مطرح شد و به عنوان روشی برای اعتبارسنجی دیجیتالی یک پیغام بدون این که محتوای آن پیغام مشخص شود، به کار می رود. یکی از روش های تشخیص امضاهای مخفی، غیر اتصالی بودن آنها است. یعنی امضا کننده نمی تواند تطابق میان فرآیند امضا و خود امضا را نتیجه بگیرد. این روش در نرم افزارهایی برای وصول پول نقد و ... هم به کار می رود. طرح سی آز در این مقاله معرفی و تحلیل می شود و سپس راهکاری برای برآورده سازی الزام عدم اجبار در آن پیشنهاد می شود.

کلمات کلیدی:

الزامات امنیتی، امضای کور، طرح سی آز

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/838379>

