دوشنبه 30 خرداد 1390 - 08:07

افزايش ضريب ايمني رمز عبور

هيچ رمز عبور (پسوردي) 100 درصد تضمين شده و ايمن نيست. در واقع همواره براي خرابكاران و كساني كه سوءنيت دارند راه‌ها و ابزارهايي براي هك‌كردن، شكستن رمز و دستيابي به رمز عبور افراد وجود دارد.

جام جم آنلاين: هيچ رمز عبور (پسوردي) 100 درصد تضمين شده و ايمن نيست. در واقع همواره براي خرابكاران و كساني كه سوءنيت دارند راه‌ها و ابزارهايي براي هك‌كردن، شكستن رمز و دستيابي به رمز عبور افراد وجود دارد.
هر روز وب‌سايت‌ها و بانك‌هاي اطلاعاتي بيشتري در فعاليت‌هاي روزانه خود در معرض خطر اين‌گونه سوءاستفاده‌هاي افراد مخرب و هكرها قرار مي‌گيرند.

اكنون روش جديدي براي بررسي صحت و سقم پسورد ابداع شده كه مي‌تواند از سرقت آن جلوگيري كرده و همچنين پسورد به سرقت رفته را بي‌اعتبار كند.

در اين روش از سرعت تايپ كلمه عبور توسط كاربر و همچنين فاصله تايپ بين كاراكترها به عنوان افزايش ضريب امنيت استفاده مي‌شود.

مقاله‌اي مربوط به اين كار در مجله بين‌المللي فناوري اينترنت و تراكنش‌هاي امن توسط متخصصان كامپيوتر دانشگاه آمريكايي بيروت در لبنان منتشر شده است. در اين مقاله مشكلات و نقص‌هاي تلاش‌هاي قبلي در آناليز الگوي كليد (KPA) را توضيح داده‌اند.

KPA فرآيندي است كه در آن سرعت ضربه زدن كاربر به صفحه كليد و همچنين فاصله بين هر ضربه و ضرب‌آهنگ (ريتم) تايپ‌كردن اندازه‌گيري مي‌شود.

اين روش با صفحه كليدهاي اصلاح‌شده هم مورد آزمايش قرار گرفته و نيروي واردشده به هر كليد اندازه‌گيري مي‌شود.

نتيجه تمام اين تجزيه و تحليل‌ها از روش‌هاي تايپ پسورد توسط هر كاربر يك پروفايل بيومتريك مخصوص به هر كاربر است.

اگر اين پروفايل بيومتريك با پروفايل مخصوص هر كاربر تطابق نداشته باشد، حتي در صورت درست بودن پسورد مورد قبول واقع نمي‌شود.

متخصصان نشان دادند كه چگونه يك صفحه كليد اصلاح‌شده مي‌تواند براي يك شخص يا سازمان دردسرآفرين باشد. همچنين نشان دادند كه در روش‌هاي قبلي KPA اگر فشردن 2 كليد همپوشاني داشت، باعث شكست‌خوردن آناليزها مي‌شد.

تلاش‌هاي اوليه روي روش زمانبندي متقابل تمركز داشت، يعني فاصله زماني بين فشردن يك كليد و كليد بعدي مدنظر بود كه براي تضمين اين كه پسورد فقط توسط كاربر مشروع قابل استفاده است، كافي نبود. در عوض روشي كه متخصصان پيشنهاد كرده‌اند روي زمانبندي داخلي متمركز بود، يعني مدت زماني كه يك كليد تحت فشار قرار دارد، اين پارامتر قابل اطمينان‌تري نسبت به روش زمانبندي متقابل است.

در روش جديد، برنامه، اطلاعات راجع به چگونگي تايپ پسورد توسط كاربر را با ثبت سيگنال‌هاي رسيده از صفحه كليد استاندارد هنگام فشرده‌شدن يك كليد تا رهاكردن آن جمع‌آوري مي‌كند سپس با استفاده از اين اطلاعات، يك الگو توليد كرده و آن را با الگوي تايپ اوليه هنگام ثبت حساب مقايسه مي‌كند.

الگوريتم اعتبارسنجي با نگاه‌كردن به پارامترهاي مختلفي همچون زمانبندي متمركز، زمانبندي داخلي، ديگراف، تري‌گراف و طول پسورد به كاربر اجازه ورود يا عدم ورود مي‌دهد.

واضح است كه هرچه طول پسورد بيشتر باشد، پروفايل پيچيده‌تري از نحوه تايپ كلمه عبور توليد شده و خطر توليد اين الگو توسط فرد غيرمجاز يا هكر كاهش مي‌يابد.البته مزيت ديگر چنين پسورد بزرگ و طولاني اين است كه كاربر نتواند هر بار دقيقا همان الگوي اوليه ثبت شده را ايجاد كند و شايد مجبور شود چند بار تايپ پسورد را تكرار كند.

منبع: internet technology