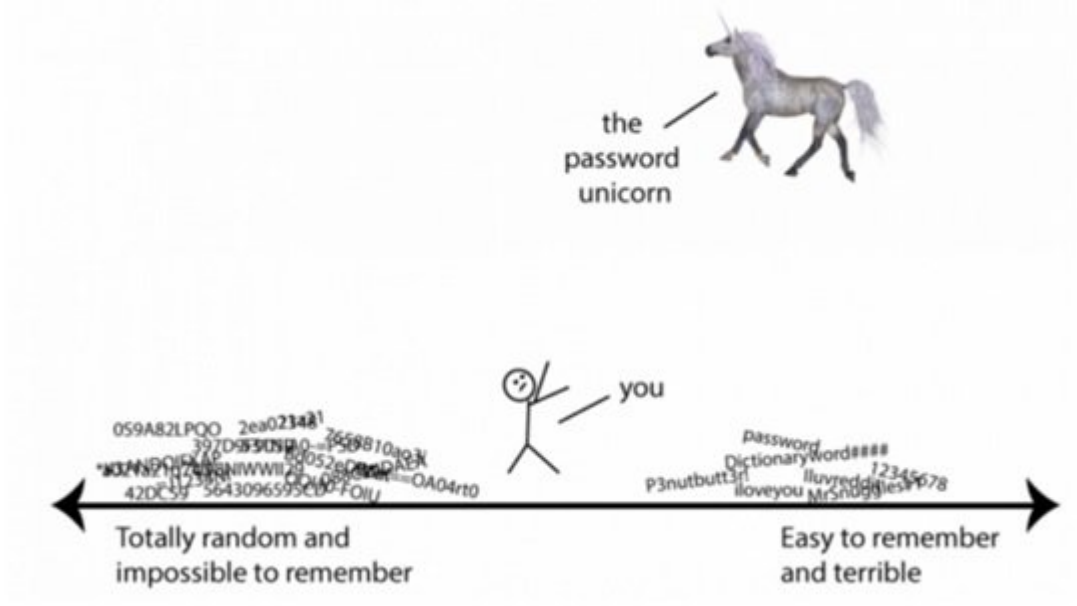
موفقیتی جدید در زمینه گذرواژه‌ها

چگونه پیچیده‌ترین رمزها را به سادگی بسازید و به خاطر بسپارید

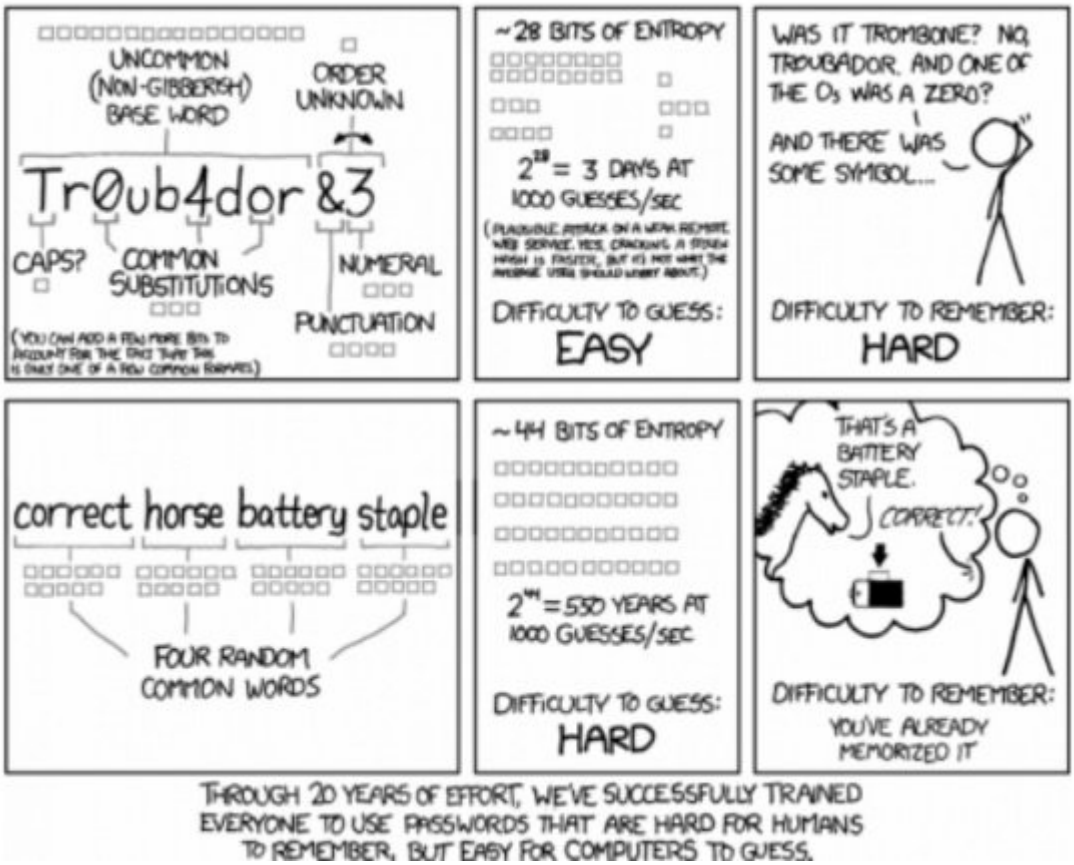
گذرواژه‌هایی که این روزها از طرف بسیاری از شرکت‌های فناوری مورد نکوهش قرار گرفته‌اند و بعضی از شرکت‌ها در صدد حذف آن‌ها هستند در نظر دارند یک‌بار دیگر قیام کرده و جایگاه خود را از فناوری‌های نوین امنیتی باز پس گیرند. در جدیدترین مطالعه‌ای که در این زمینه انجام شده است دو محقق دانشگاه کالیفرنیای جنوبی به روشی نوین و منحصر به فرد در زمینه ساخت گذرواژه‌های ایمن دست یافته‌اند. شیوه جدید به کاربران این توانایی را می‌دهد تا پیچیده‌ترین گذرواژه‌ها را به راحتی ایجاد کرده و به راحتی به یاد آورند.

اولین نکته‌ای که در زمان ساخت یک گذرواژه خوب با آن برخورد می‌کنید، به حافظه شما باز می‌گردد. آیا می‌تواند یک گذرواژه پیچیده را به یاد آورید یا خیر؟ حتی اگر جزء آن دسته از میلیون‌ها انسانی که از گذرواژه‌های 12345678 یا password استفاده می‌کنند، نباشید، ممکن است باز هم اشتباهات تازه‌کاران را انجام دهید.

به‌طور مثال از یک عبارت به عنوان گذرواژه خود استفاده کنید، اما جای کاراکترهای i را با 1 یا a را با @ جایگزین کرده و از چنین ترکیبی استفاده کنید، یا ممکن است از عبارت یا لغاتی استفاده کرده و اعداد را به انتهای این عبارات اضافه کنید، به جای آن‌که این اعداد را به‌طور اتفاقی در مکان‌های مختلف این جملات قرار دهید، حتی این احتمال وجود دارد، به جای آن‌که تغییری در ساختار یک گذرواژه به وجود آورید از یک گذرواژه یکسان در سایت‌های مختلف استفاده کنید. اما واقعیت این است که پیدا کردن گذرواژه قدرتمندی که یادآوری آن ساده باشد کار ساده‌ای نیست. در حقیقت دستیابی به چنین گذرواژه قدرتمندی همانند تصویری که آنا سوانسون آن‌را رسم کرده است همانند پیدا کردن یک اسب شاخ‌دار است.



خوب، اکنون ممکن است با خود بگویید چه گزینه‌هایی پیش روی من قرار دارند؟ حقیقت این است که هر گذرواژه‌ای که از امنیت کافی برخوردار باشد، به همان نسبت یادآوری آن غیرممکن می‌شود و برعکس، هر گذرواژه‌ای که یادآوری آن ساده باشد، به احتمال زیاد گذرواژه به شدت غیر ایمنی خواهد بود. به نظر می‌رسد این جملات شبیه یک قانون در دنیای گذرواژه‌ها هستند. اما اکنون خبرهای خوشی از دنیای گذرواژه‌ها به گوش می رسد. به تازگی دو محقق دانشگاه کالیفرنیای جنوبی توانسته‌اند راه حل جامعی را در این زمینه ابداع کنند. مرجان قزوینی‌نژاد و کوین نایت دو محقق این دانشگاه در مقاله‌ای به راه حل جدیدی در زمینه ساخت گذرواژه‌هایی که در مقابل کرک مقاوم بوده و یادآوری آن‌ها ساده می‌باشد اشاره کرده‌اند. این گذرواژه بر مبنای اشعاری که تصادفی تولید می‌شوند عمل می‌کند. در واقع الهام‌بخش مطالعه این دو محقق در زمینه گذرواژه‌ها کارتون Kxcd بوده است. کارتونی که توسط رندال مونرو ساخته شده و در آن نشان می‌دهد چگونه یک گذرواژه با استفاده از چهار کلمه تصادفی شبیه به " correct horse battery staple " می‌تواند ایجاد شود.



گذرواژه‌ای که بر پایه این مکانیزم تولید می‌شود ضمن آن‌که از امنیت بالاتری برخوردار است، به سادگی در ذهن مردم نقش می‌بندد. به کارگیری این تکنیک بسیار ساده‌تر از مجموعه‌ای آشفته و تصادفی از حروف، اعداد و سمبل‌هایی است که هر روزه توسط کارشناسان امنیتی توصیه می‌شود. کارتون مونرو به این حقیقت اشاره دارد که حتی اگر یک لغت غیر مرسوم شبیه به troubadour انتخاب کنید و تعدادی از کاراکترهای آن‌را با سمبل‌های مختلفی جایگزین کنید، این ترکیب ممکن است تنها برای چند ثانیه، چند دقیقه یا نهایتا چند ساعت در کار کامپیوتر وقفه ایجاد کند. اما ترکیبی از چهار کلمه تصادفی کار یک هکر برای شکستن یک گذرواژه را سخت کرده و در طرف مقابل یادآوری آن برای هر فردی به آسانی امکان‌پذیر است. واقعیت این است که این چهار کلمه تصادفی در حقیقت بر مبنای طیف گسترده‌ای از اعداد تصادفی تولید شده‌اند. اعداد تصادفی در ادامه به بخش‌هایی شکسته شده که هر کدام از آن‌ها متناظر به یک لغت قرار گرفته در یک لغت‌نامه هستند.

□□□□ □□□□□□□□□: [illegible]

این روش در اصل یکی از اصول رمزنگاری است. نایت در خصوص این الگوی ابداع شده می‌گوید: « یک کامپیوتر برای حدس زدن یک عدد تصادفی که به این روش تولید می‌شود باید میلیاردها، میلیارد حالت ممکن را بررسی کرده تا به جواب درست برسد.» در حالی‌که مونرو پیش‌نهاد داده است از اعداد طولانی برای چهار لغت تصادفی استفاده شود، قزوینی‌نژاد و نایت از ایده به کارگیری اشعار کوچک استفاده کرده‌اند. در مقاله قزوینی‌نژاد و نایت این دو محقق به روش‌های متفاوتی که برای تولید گذرواژه‌های تصادفی مورد استفاده قرار می‌گیرند؛ نگاهی داشته‌اند. روش Xkcd از الگوی تولید کلمات تصادفی و همچنین الگوی تولید جملات تصادفی استفاده می‌کند. اما آن‌ها کشف کرده‌اند که ایمن‌ترین روش و در عین حال ساده‌ترین روش برای ایجاد و یادآوری گذرواژه‌ها، ساخت یک شعر کوتاه با قافیه از این کلمات تصادفی است. در روشی که این محققان به آن اشاره کرده‌اند، انسان‌ها در طول هزاران سال از اشعار به عنوان روشی برای یادآوری اطلاعات استفاده کرده‌اند. این یک اتفاق تصادفی نیست که حماسه‌های طولانی همچون اودیسه از 12 هزار خط یا Canterbury Tales از 17 هزار خط تشکیل شده‌اند. امروزه بسیاری از مردم نمی‌توانند تمامی این داستان را از حفظ بخوانند اما برخی از آوازهایی که با یکدیگر هم قافیه هستند را به یاد

می‌آورند، شبیه به "Thirty days hath September" یا "the weather beacon rhymes" که با یک‌بار خواندن در حافظه نقش می‌بنند. به گفته این محققان چهار لغت در کنار یکدیگر معنی خاصی نمی‌دهد، اما یادآوری آن خیلی ساده‌تر از یک رشته 44 بیتی است. مثال زیر نمونه‌ای از گذرواژه‌های 44 بیتی و لغت انگلیسی معادل آن‌هاست.

44-bit password English phrase

10101101010 -> correct

10010110101 -> horse

01010101010 -> battery

10110101101 -> staple

آن‌ها از یک برنامه کامپیوتری برای تولید یک عدد تصادفی بسیار طولانی استفاده کردند، و سپس آن عدد را در قطعاتی شکسته و سپس این اشعار را به جمله کوچک‌تری ترجمه کردند. برنامه کامپیوتری که آن‌ها از آن استفاده کردند، تضمین می‌کند که دو خط پایانی هر لغت با یکدیگر هم قافیه هستند و کل عبارت از یک وزن شعری مشخص برخوردار خواهد بود، موارد زیر نمونه‌ای از خروجی‌های این برنامه هستند.

The reigning Hagen journeyman

believers mini minivan

- - - - - - - - - - - - -

And teaches scripture bungalow

or celebrate or Idaho

این دو محقق در مقاله خود به این موضوع اشاره کرده‌اند که کامپیوترها برای شکستن یک گذرواژه 44 بیتی تقریبا یک ساعت وقت صرف می‌کنند، در حالی که اگر از یک گذرواژه 60 بیتی استفاده شود این زمان به بیش از 11 سال افزایش پیدا می‌کند. قزوینی‌نژاد و نایت یک مترجم آنلاین برای این اشعار کوچک طراحی کرده‌اند. برای دسترسی به این مترجم آنلاین از این آدرس استفاده کنید.

البته لازم به توضیح است که آن‌ها در خصوص این ابزار آنلاین هشدار داده‌اند، این سایت تنها با این هدف طراحی شده است که نشان دهد، هکرها به‌طور بالقوه ظرفیت دانلود همه این موارد را داشته و چنین آزمایش‌هایی را روی گذرواژه‌ها انجام خواهند داد، در نتیجه از کلمات نشان داده شده در این صفحه برای گذرواژه‌های خود نباید استفاده کنید. اگر در نظر دارید از گذرواژه شعری مورد نظر خود استفاده کنید، باید آن‌را به این آدرس ایمیل کرده تا این برنامه گذرواژه ایمن را برای شما ارسال کند.

بعد از ارسال، گذرواژه از سرور این سایت حذف خواهد شد. متأسفانه بیشتر سایت‌های امروزی با محدودیت تعداد کاراکترهای مورد استفاده در گذرواژه روبرو هستند و از طرفی به دلیل این‌که بیشتر اشعار معمولا طولانی هستند ممکن است در بعضی از سایت‌ها نتوانید از این روش استفاده کنید. اما شاید روزی فرا خواهد رسید که شما توانایی به کارگیری چنین روشی را روی بیشتر سایت‌ها داشته باشید و از گذرواژه‌های کوتاه‌تر اما ایمن‌تری روی سایت‌ها استفاده کنید.

تاریخ انتشار:
25 آبان 1394

نشانی منبع: https://www.shabakeh-mag.com/security/2131