رمزهای بی‌مرز
مرزهای بی‌رمز

نویسنده: دن گودین
ترجمه: فرزانه برهمت

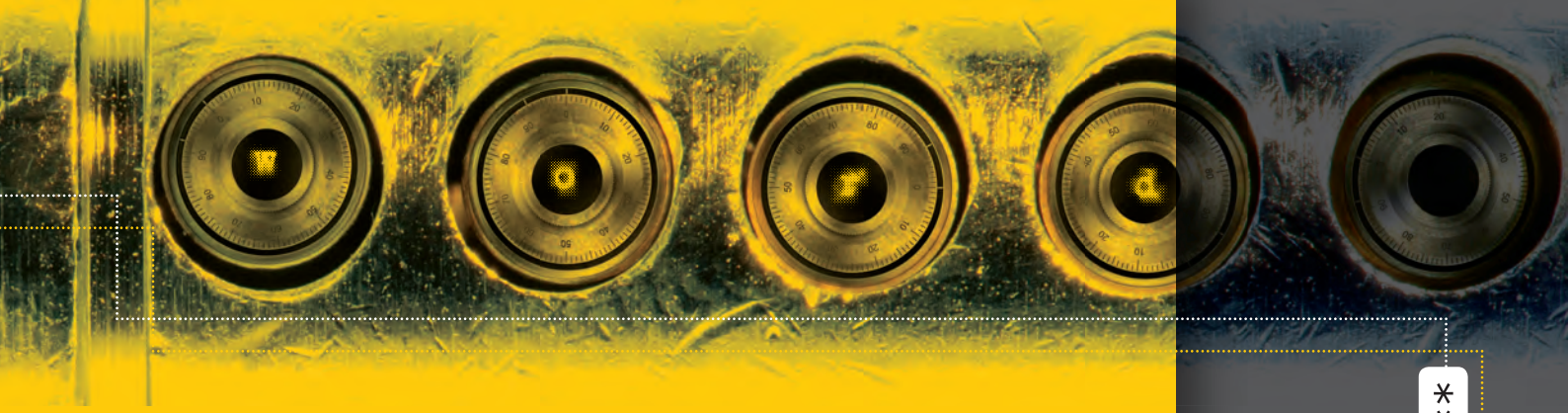
چرا گذرواژه‌ها هیچ‌گاه تا این حد ضعیف و نفوذگران تا این حد قدرتمند نبوده‌اند؟

در اواخر سال ۲۰۱۰، شون بروکس (Sean Brooks)، در یک بازه ۳۰ ساعته، سه ایمیل دریافت کرد که به او هشدار می‌داد حساب‌های کاربری‌اش در Battle.net، Linked In و یکی دیگر از سایت‌های مشهور در معرض خطر قرار دارد. او در ابتدا آن‌ها را شایعه و هرزنامه پنداشت و تصمیم داشت آن‌ها را پاک کند که متوجه شد این ایمیل‌ها حاوی اطلاعات ریز و دقیقی هستند که در ایمیل‌های معمول فیشینگ مشاهده نمی‌شوند. این ایمیل‌ها می‌گفتند که اطلاعات ورود او به حساب‌های کاربری مجموعه سایت‌های Gawker توسط هکرهایی که به سرورهای این سایت‌ها نفوذ کرده‌اند، به سرقت رفته و در فضای آنلاین منتشر شده است. اگر بروکس از همان ایمیل‌ها و گذرواژه‌ها برای ورود به سایت‌های دیگر نیز استفاده می‌کرد، آن‌ها نیز در معرض خطر بودند.

هشدارهایی که بروکس و میلیون‌ها نفر دیگر در آن ماه دسامبر دریافت کردند، جعلی نبودند. در طی چند ساعتی که هکرها توانسته بودند به سایت‌های Gawker نفوذ کرده و به اطلاعات رمزنگاری‌شده گذرواژه‌های ۱/۳ میلیون نفر از اعضای آن دست یابند، بات‌نت‌ها در حال شکستن این گذرواژه‌ها و استفاده از آن‌ها برای در اختیار گرفتن حساب‌های کاربری توییتر و انتشار هرزنامه بودند. در طی چند روز پس از آن، دامنه سایت‌هایی که از کاربران خود می‌خواستند گذرواژه‌هایشان را عوض کنند، به یاهو، آمازون و توییتر نیز کشیده شد.

به لطف داده‌های موجود از
دنیای واقعی، کلید دروازه‌های
قلمرو دیجیتال شما
در معرض خطر قرار دارد.

SHABAKEH
[NETWORK]
شبکه
۲۰۵
اسفند
۱۳۹۱



بروکس که در آن زمان به‌عنوان همکار پروژه مرکز دموکراسی و فناوری، به وبلاگ‌نویسی درباره این هشدارها می‌پرداخت، می‌گوید: «خطر استفاده از گذرواژه‌های ضعیف کم‌وبیش شناخته شده است.» او درباره این هشدارها می‌افزاید: «این هشدارها به این شرکت‌ها نشان می‌دهد که یک نفوذ امنیتی در جایی خارج از سیستم‌های آن‌ها می‌تواند باعث به وجود آمدن نفوذپذیری در شبکه‌های آن‌ها شود.»

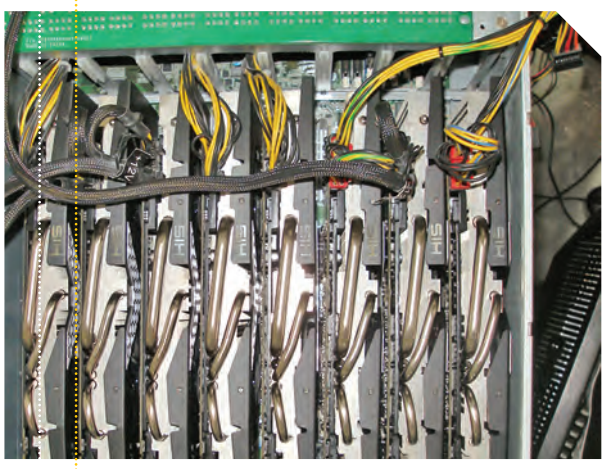
هنر باستانی شکستن و کشف رمزهای عبور، در پنج سال گذشته چندین برابر بیش از چندین دهه قبل پیشرفت کرده است. در عین حال، عادت خطرناک استفاده مجدد از گذرواژه‌ها در همه‌جا دیده می‌شود. با این اوصاف، باید گفت امنیتی که توسط گذرواژه‌های معمول در سال ۲۰۱۲ به دست می‌آید، هیچ گاه تا این حد اندک نبوده است.

دنیایی تازه

براساس تحقیقی که در سال ۲۰۰۷ انجام شده است، یک کاربر معمولی وب حدود ۲۵ حساب کاربری جداگانه دارد، اما به‌طور متوسط از ۶/۵ گذرواژه برای حفظ امنیت آن‌ها استفاده می‌کند. همان‌گونه که نفوذ به سایت‌های Gawker نشان داد؛ استفاده دوباره از گذرواژه‌ها در ترکیب با کاربرد معمول ایمیل‌ها به‌عنوان نام کاربری در سایت‌های مختلف، به این معنی خواهد بود که هنگامی که هکرها به مجوزهای ورود به یک سایت دسترسی پیدا کنند، ابزار لازم برای نفوذ به چندین حساب کاربری دیگر را نیز دراختیار خواهند داشت.

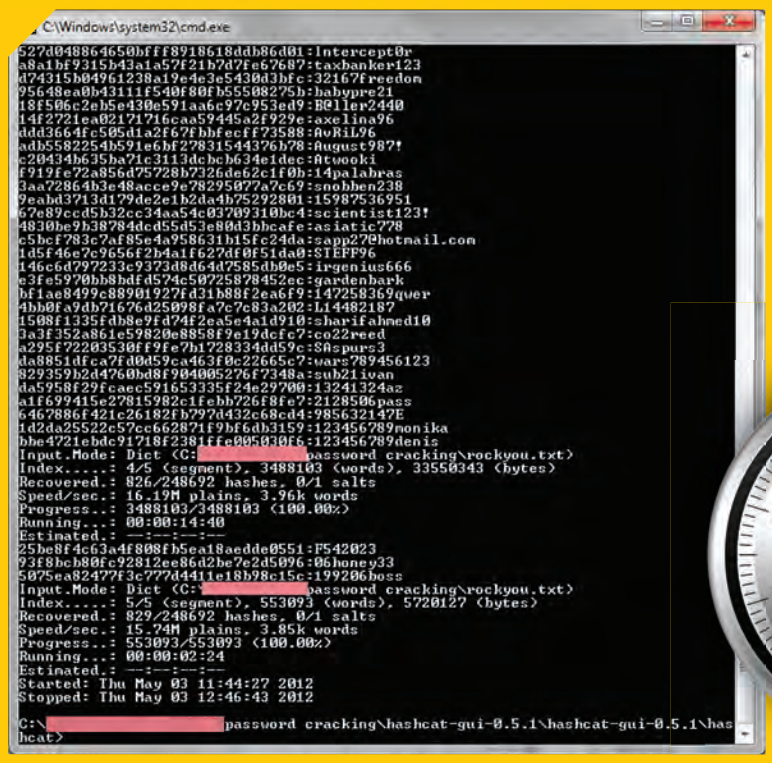
سخت‌افزارهای جدید و روش‌های نوین، به این رشد شدید کشف رمزهای عبور کمک کرده است. پردازنده‌های گرافیکی که این روزها به کرات برای انجام محاسبات کامپیوتری به کار برده می‌شوند، این امکان را برای برنامه‌های شکستن رمزهای عبور فراهم می‌کنند که به سرعتی هزاران برابر برنامه‌های ده سال پیش دست یابند؛ همان برنامه‌هایی که یک دهه قبل روی کامپیوتری با قیمت کامپیوترهای فعلی، اما تنها با استفاده از پردازنده مرکزی اجرا می‌شدند. به‌عنوان مثال یک کامپیوتر شخصی که تنها از یک پردازنده گرافیکی AMD Radeon HD7970 استفاده می‌کند، می‌تواند به‌طور متوسط تعداد ۸/۲ میلیارد گذرواژه را (بسته به الگوریتم به کار رفته برای رمزنگاری) در هر ثانیه بیازماید. یک دهه پیش، دست یافتن به چنین سرعتی تنها به کمک سوپرکامپیوترهای گران‌قیمت امکان‌پذیر بود.

پیشرفت‌ها به همین مورد محدود نمی‌شود. کامپیوترهای شخصی مجهز به دو یا چند پردازنده گرافیکی پانصد دلاری می‌توانند به سرعت‌هایی دو، سه یا چندین برابر نمونه ذکر شده دست یابند. در عین حال، برنامه‌های رایگان شکستن رمزهای عبور مانند oclHashcat-plus با نیاز به کمترین میزان تغییرات، روی تمام آن‌ها اجرا خواهند شد. علاوه‌بر این، هکرهایی که به چنین ابزارهایی مجهز شده‌اند، در نشست‌های آنلاین به همکاری با یکدیگر پرداخته و به این ترتیب به‌سادگی به منابع و چندوچون شکستن گذرواژه‌های یک فهرست صد هزارتایی در کمتر از یک ساعت دست می‌یابند. از همه مهم‌تر این که مجموعه‌ای از گذرواژه‌های لو رفته در چند سال اخیر که شامل بیش از یکصد میلیون گذرواژه واقعی بوده است، درک بهتری را برای نفوذگران فراهم آورده است تا راحت‌تر بفهمند که افراد در دوره‌های مختلف زندگی، در سایت‌های مختلف یا در شرایط متفاوت چگونه گذرواژه‌هایشان را انتخاب می‌کنند. فهرست در حال رشد گذرواژه‌های لو رفته، به برنامه‌نویسان این امکان را می‌دهد که به نوشتن قوانینی بپردازند که الگوریتم‌های شکستن رمزهای عبور را سریع‌تر و دقیق‌تر می‌کنند. حمله برای شکستن رمزهای عبور دیگر به‌سادگی یک کپی و پیست معمولی شده است که حتی بچه خلاف‌کارهای تازه‌وارد نیز می‌توانند به آسانی آن را انجام دهند.



شکل ۱: این کامپیوتر ۱۲ هزار دلاری توسط d3ad0ne از روی کامپیوتر پروژه Erebus کپی شده است و از هشت کارت گرافیکی AMD Radeon HD7970 استفاده می‌کند. این سیستم که نسخه ۰/۱۰ برنامه oclHashcat-lite را اجرا می‌کند، برای شکستن کل فضای کلید ممکن برای هر گذرواژه هشت حرفی شامل حروف بزرگ و کوچک، اعداد و نشانه‌های خاص از طریق تلاش کور (Brute Force) تنها به ۱۲ ساعت زمان نیاز دارد. این کامپیوتر به گروه Hashcat کمک کرد که در رقابت امسال «اگه میتونی رمز من رو بشکن» برنده شوند.

یک کاربر معمولی وب حدود ۲۵ حساب کاربری جداگانه دارد، اما به‌طور متوسط از ۶/۵ گذرواژه برای حفظ امنیت آن‌ها استفاده می‌کند.



شکل ۲:
تصویری از برنامه Hashcat در حال شکستن لیستی از هش‌های گذرواژه‌ها که به صورت آنلاین منتشر شده است.

> مجموعه‌ای از گذرواژه‌های لو رفته در چند سال اخیر (شامل بیش از یکصد میلیون گذرواژه واقعی)، درک بهتری را برای نفوذگران فراهم آورده است تا راحت‌تر بفهمند که افراد در سایت‌های مختلف چگونه گذرواژه‌هایشان را انتخاب می‌کنند.

ریک ردمن (Rick Redman) آزمون‌گر نفوذ در موسسه مشاوره امنیتی KoreLogic است. او که مسابقه شکستن رمز عبور «اگه می‌تونی رمز من رو بشکن» (Crack Me If You Can) را در سه کنفرانس هکری Defcon پیشین ترتیب داده است، می‌گوید: «این پیشرفت‌ها شب و روز ادامه دارند. امسال به‌واسطه حجم داده‌ها [ی لو رفته]، سال خوبی برای نفوذگران بوده است. شکستن یک گذرواژه ۱۶ حرفی، کاری بود که من ۴ یا ۵ سال پیش نمی‌توانستم انجام بدهم. اما دلیل این پیشرفت این نیست که اکنون کامپیوترهای بیشتری در اختیار دارم.»

ردمن معمولاً در هر لحظه‌ای که تصور کنید در حال بررسی هزاران گذرواژه رمزنگاری شده است. او این کار را از طریق یک کامپیوتر شخصی که چهارکارت گرافیک GeForce GTX 480 دارد، به انجام می‌رساند. هرچند او این سیستم را قدیمی می‌داند، اما همین سیستم قدیمی نیز امکان پردازش و آزمودن ۶/۲ میلیارد ترکیب را در هر ثانیه فراهم می‌کند. او به‌صورت معمول از یک فرهنگ واژگان شامل ۲۶ میلیون کلمه استفاده می‌کند. او در کنار این فرهنگ واژگان از الگوریتم‌های برنامه‌نویسی استفاده می‌کند که کارایی این مجموعه لغات را با افزودن اعداد، اعراب‌گذاری و سایر کاراکترها به هر یک از آن‌ها، چندین برابر افزایش می‌دهد. ردمن بسته به کاری که در دست دارد، گاه از یک فهرست ۶۰ میلیون‌تایی از کلمات قوی و چیزی که به‌اصطلاح جدول رنگین‌کمان (Rainbow Table) نامیده می‌شود، استفاده می‌کند. درباره جدول رنگین‌کمان کمی بعدتر توضیح خواهیم داد.

ردمن به عنوان یک آزمون‌گر نفوذ که برای آزمودن و نفوذ به خطوط دفاعی شرکت‌های بزرگ فهرست Fortune 500 پول دریافت می‌کند، تلاش دارد تا همیشه پیش از خرابکاران به ضعف‌های امنیتی دست یافته و آن‌ها را از نفوذ به شبکه‌های مشتریانش بازدارد. یکی از اصلی‌ترین راه‌هایی که به او کمک می‌کند از خلافکاران جلوتر باشد، دانلود کردن فهرست هش‌هایی است که به صورت روزانه در سایت pastebin.com و نمونه‌های مشابه قرار داده می‌شوند. به این ترتیب، او می‌تواند متوجه شود که این گذرواژه‌ها به سازمان‌های طرف قراردادش مربوط هستند یا خیر.

به‌تازگی او موفق به شکستن رمز عبوری ۱۳ حرفی شد که چندین ماه برای شکستن آن تلاش کرده بود. برای محافظت از صاحب حساب، او از افشای ترکیب دقیق این گذرواژه خودداری کرده و در عوض برای توصیف کلمه عبور به دست آمده از ترکیب ساختگی Sup3rThinkers استفاده کرد. کلمه Sup3rThinkers تعدادی از الگوهای معمول گذرواژه‌ها را در خود دارد. نخست این که با یک کلمه ۵ حرفی معمولی شروع می‌شود که حرف اول آن بزرگ است و در آن حرف E با 3 جایگزین شده است.

در ادامه یک کلمه ۸ حرفی دیده می‌شود که آن هم با حروف بزرگ شروع شده است. هر چند سرعت سیستم او در این امر بی‌تأثیر نبود، اما شکستن این گذرواژه بیشتر مدیون تجربه و تخصصی است که او در چند سال اخیر در حوزه شکستن رمز به صورت آنلاین کسب کرده است.

یکی از مهم‌ترین پیشرفت‌ها در دانش شکستن گذرواژه‌ها در سال ۲۰۰۹ حاصل شد. یعنی زمانی که یک حمله تزریق کدهای SQL روی سایت بازی‌های آنلاین RockYou.com باعث لو رفتن ۳۲ میلیون گذرواژه شد. این گذرواژه‌ها که توسط کاربران و برای ورود به حساب‌های کاربری استفاده می‌شد، به صورت متن ساده ذخیره شده بود. این گذرواژه‌ها که تعدادشان پس از حذف موارد تکراری به ۱۴/۳ میلیون می‌رسید، به صورت آنلاین منتشر شد. ظرف کمتر از یک شب، این حجم عظیم داده‌های اعتبارسنجی کاربران، شیوه شکستن گذرواژه‌ها را هم برای هکرهای کلاه‌سفید و هم برای هکرهای کلاه‌سیاه تغییر داد.

> یکی از مهم‌ترین پیشرفت‌ها در دانش شکستن گذرواژه‌ها در سال ۲۰۰۹ حاصل شد. یعنی زمانی که یک حمله تزریق کدهای SQL روی سایت بازی‌های آنلاین RockYou.com باعث لو رفتن ۳۲ میلیون گذرواژه شد.

آن را هش کنید

مانند بسیاری از نمونه‌های لو رفتن گذرواژه‌ها، هیچ یک از ۱/۳ میلیون گذرواژه‌ای که در دسامبر ۲۰۱۰ از سایت Gawker به بیرون درز کرد، متن عادی قابل خواندن توسط انسان نبودند. در عوض با خوراندن آن‌ها به یک تابع رمزنگاری یک‌طرفه، به چیزی تبدیل شده بودند که آن را مقادیر هش (Hash Value) می‌نامیم. یک مقدار هش، دنباله‌ای یکتا از کاراکترها را برای هر مقدار دلخواه ورودی تولید می‌کند. به عنوان مثال، با عبور دادن کلمه‌ای مانند password از تابع MD5 به رشته‌ای نظیر 5f4dcc3b5aa765d61d8327deb882cf99 دست خواهیم یافت.

با اعمال کوچک‌ترین تغییر در مقدار ورودی، مقدار خروجی به کلی متفاوت خواهد بود. مثلاً تبدیل کلمه password به Password یا password1 باعث به‌دست آمدن کدهای dc647eb65e6711e155375218212b3964 و 7c6a180b36896a0a8c02787eeafb0e4c خواهد شد. اگر برای این کار از الگوریتم SHA1 استفاده شود، مقادیر به‌دست آمده به ترتیب 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 (برای password)، 8be3c943b1609fffbfc51aad666d0a04adf83c9d (برای Password) و درنهایت مقدار e38ad214943daad1d64c102faec29de4afe9da3d (برای password1) خواهد بود.

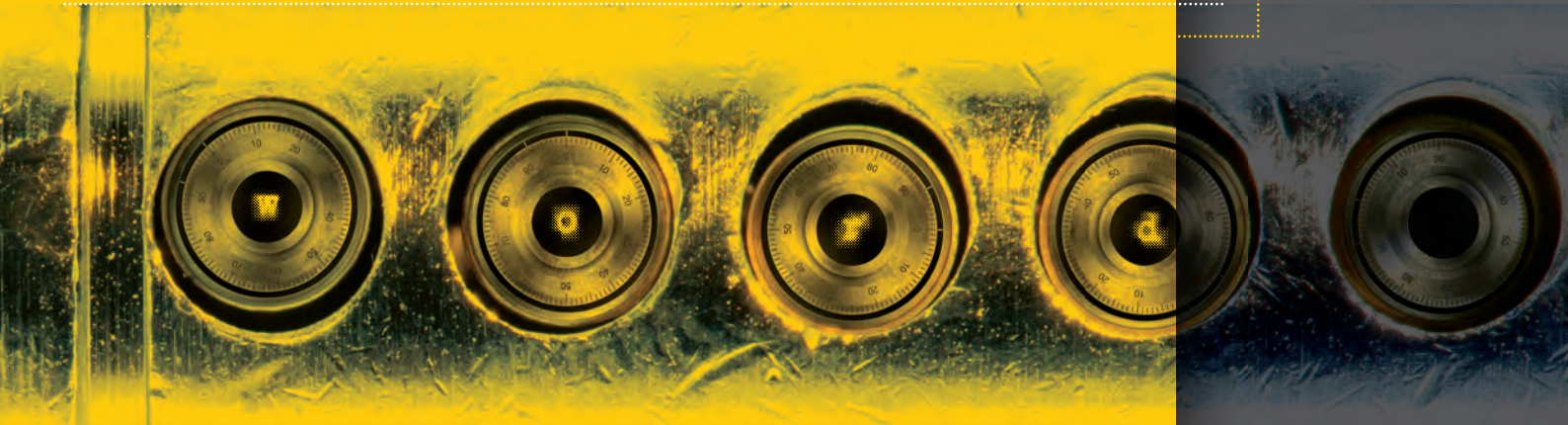
در تئوری هنگامی که عبارتی به هش تبدیل شد، دیگر با ابزارهای رمزنگاری نمی‌توان آن را به متن اصلی تبدیل کرد. در نتیجه فرآیند شکستن رمزهای عبور به صورت معمول به معنای اجرای تابع رمزنگاری به‌کار رفته روی گذرواژه‌های حدسی و تصادفی و مقایسه نتیجه با هش موجود است. اگر دو مقدار هش با یکدیگر برابر باشند، گذرواژه مورد نظر به دست آمده است.

اگرچه لو رفتن گذرواژه‌های RockYou متأثرکننده بود، اما بعدتر مشخص شد که این تازه آغاز پدیده‌ای عظیم‌تر در زمینه شکستن رمزهای عبور بوده است. با در دسترس قرار گرفتن ۱۴ میلیون گذرواژه پرکاربرد، این امکان برای کسانی که روی گذرواژه‌های رمزنگاری‌شده (هش شده) کار می‌کردند، فراهم شد تا به سرعت ضعیف‌ترین گذرواژه‌ها را بشکنند و نتیجه این بود که زمان بیشتری برای کار روی گذرواژه‌های قوی‌تر باقی می‌ماند.

به عنوان مثال، ظرف چندین روز اول هک شدن Gawker، درصد بسیاری از هش‌های گذرواژه‌ها به متن ساده تبدیل شدند. موفقیتی که برای هکرهای گذرواژه‌ها، این امکان را فراهم آورد تا با در اختیار داشتن حجم بیشتری از گذرواژه‌های واقعی، با دانشی بیشتر به سراغ نفوذهای بعدی خود بروند. این حجم عظیم گذرواژه‌ها از آن روز تا کنون به صورت مداوم بزرگ‌تر شده و در هر نفوذ جدید بزرگ‌تر نیز می‌شود. تنها شش روز پس از لو رفتن شش و نیم میلیون هش گذرواژه LinkedIn در ماه ژوئن، ۹۰ درصد آن‌ها شکسته شده بودند! به گفته ردمن تنها در سال گذشته، بیش از ۱۰۰ میلیون گذرواژه چه در قالب متن ساده یا متن‌های قابل تبدیل، به‌صورت آنلاین منتشر شده‌اند. ردمن می‌گوید: «در حال حاضر هر فصل سال، یک مورد دیگر شبیه RockYou خواهید داشت.»

شما را در هم می‌شکنیم!

پس از وقوع حادثه RockYou همه‌چیز تغییر کرد. دیگر به فهرست‌هایی که از ترکیب لغات دیکشنری‌های وبستر و نمونه‌های مشابه به‌وجود آمده و دست‌کاری می‌شدند تا لغات مورد استفاده کاربران برای دسترسی به سرویس‌های آنلاین را حدس بزنند، احتیاجی نبود. مجموعه‌ای منفرد از حروف، اعداد و علامت‌ها که شامل همه‌چیز (از نام حیوانات تا شخصیت‌های کارتونی) بود، در حملات بعدی جایگزین آن فهرست لغات شده بود.



ردمن در مورد فهرست RockYou می‌گوید: «دیگر لازم نیست به لیست‌های خیالی سیارات Klingon (مربوط به سریال Star Trek) مراجعه کنیم. دیگر کلماتی مانند dragon و princess و مواردی مشابه در فهرست وجود دارند که به احتمال زیاد می‌توانند ۶۰ درصد گذرواژه‌های هر سایت هک شده‌ای را رمزگشایی کنند. حالا شما بدون هیچ تفکر و تلاشی ۶۰ درصد کار را انجام داده‌اید! شما تنها از دانش قبلی‌تان استفاده کرده‌اید.»

چیز دیگری که در حادثه RockYou درست به اندازه خود کلمات به کار رفته توسط کاربران اهمیت داشت، این بود که حادثه RockYou شیوه تفکر استراتژیک افراد هنگام انتخاب گذرواژه را نیز آشکار کرد. برای بیشتر مردم، هدف انتخاب گذرواژه‌ای است که به یاد سپردن آن برای خودشان راحت و در عین حال حدس زدنش برای دیگران دشوار باشد. فهرست RockYou نشان داد که تقریباً تمام حروف بزرگ در ابتدای گذرواژه‌ها قرار دارند و تقریباً تمام اعداد و نشانه‌گذاری‌ها به انتهای گذرواژه‌ها منتقل می‌شوند؛ که البته جای هیچ تعجبی هم نبود. همچنین این فهرست نشان داد که علاقه زیادی به استفاده از ترکیب نام و سال تولد (مثلاً Julia1984 و Christopher1965) وجود دارد.

کلمه Sup3rThinkers در فهرست RockYou وجود نداشت و بنابراین در میان ۴۰ درصد باقیمانده قرار داشت که ردمن را مجبور می‌کرد برای شکستن آن به شیوه‌هایی فراتر از حمله‌های ساده مبتنی بر فهرست لغات متوسل شود. خوشبختانه (البته از دید ردمن) فهرست RockYou شامل sup3r و thinker به‌صورت لغات جداگانه بود. همین امر به ردمن امکان داد تا این گذرواژه را از طریق افزودن هر کلمه موجود در لیست به انتهای تمام کلمات دیگر، به دست آورد. هرچند این تکنیک بسیار ساده است، اما تعداد حدس‌های (در نتیجه محاسبات) مورد نیاز را به شدت بالا می‌برد. یعنی آن را از رقم ۲۶ میلیون با درنظر گرفتن فهرست لغات مورد استفاده ردمن به بیش از ۶۷۶ تریلیون می‌رساند.

سایر گذرواژه‌های پیچیده و ترکیبی نیز به چنین دستکاری‌هایی نیاز دارند. فهرست RockYou و بیش از صد میلیون گذرواژه‌ای که پس از آن لو رفته‌اند، گروه پرشماری از شیوه‌های متفاوت را آشکار می‌کنند که افراد هنگام انتخاب گذرواژه برای در امان ماندن از حمله‌های مبتنی بر فهرست لغات به‌کار می‌برند. یکی از این روش‌ها، استفاده از اعداد یا کاراکترهای غیرحروفی نظیر «!!!» است که معمولاً به انتها و گاهی به ابتدای گذرواژه‌ها افزوده می‌شوند. روش دیگری که له‌کردن (Mangling) نامیده می‌شود، تبدیل لغاتی مانند super و princess به کلماتی مانند sup34 یا

در تئوری هنگامی که عبارتی به هش تبدیل شد، دیگر با ابزارهای رمزنگاری نمی‌توان آن را به متن اصلی تبدیل کرد. در نتیجه فرآیند شکستن رمزهای عبور به صورت معمول به معنای اجرای تابع رمزنگاری به‌کار رفته روی گذرواژه‌های حدسی و تصادفی و مقایسه نتیجه با هش موجود است. اگر دو مقدار هش با یکدیگر برابر باشند، گذرواژه مورد نظر به دست آمده است.

$$prince است. روش دیگر هم افزودن وارون آینه‌ای لغت به انتهای آن است. مثلاً book به bookkoob و password به passworddrowssap تبدیل می‌شود.

گذرواژه‌هایی نظیر mustacheehcatsum (استفاده از تکنیک آینه‌ای روی کلمه mustache) هرچند ممکن است ظاهراً قوی به‌نظر برسد، اما با شناسایی الگوهایشان و نوشتن قانون‌هایی که لغات فهرستی نظیر RockYou یا موارد مشابه را کم‌وزیاد می‌کنند، به‌سادگی کشف خواهند شد. ردمن برای شکستن کلمه عبور Sup3rThinkers قوانینی را به‌کار گرفت که نرم‌افزارش را وادار می‌کرد که نه‌تنها کلمه super بلکه کلماتی نظیر Super، sup3r، Sup3r، super!!! و موارد مشابه را نیز آزمایش کند. این قوانین سپس نرم‌افزار را وادار می‌کرد که ترکیب این کلمات با thinkers، Thinkers، think3rs و Think3rs را نیز بیازماید!

این شیوه‌های شکستن رمزهای عبور، بیش از یک دهه است که در دسترس هستند اما اکنون کارایی بیشتری یافته‌اند؛ زیرا نفوذگران درک عمیق‌تری از شیوه‌هایی که مردم بر اساس آن گذرواژه انتخاب می‌کنند، پیدا کرده‌اند.

راب گراهام (Rob Graham) مدیرعامل شرکت آزمون نفوذ Errata Security می‌گوید: «به‌واسطه فهرست‌های عظیم گذرواژه‌های لو رفته، این کار نسبت به گذشته تغییر شدیدی داشته است. ما هیچ‌گاه فهرست بزرگی از گذرواژه‌ها در اختیار نداشتیم که کار را با آن شروع کنیم. اما اکنون که آن را در اختیار داریم، یاد می‌گیریم که چگونه انتروپی آن را کاهش دهیم. وضعیت هنر شکستن رمزهای عبور نسبت به گذشته بسیار ظریف‌تر شده است؛ زیرا در گذشته ما از حدس‌های کور استفاده می‌کردیم.»

راب گراهام مدیرعامل شرکت آزمون نفوذ Errata Security: «به‌واسطه فهرست‌های عظیم گذرواژه‌های لو رفته، این کار نسبت به گذشته تغییر شدیدی داشته است. ما هیچ‌گاه فهرست بزرگی از گذرواژه‌ها در اختیار نداشتیم که کار را با آن شروع کنیم. اما اکنون که آن را در اختیار داریم، یاد می‌گیریم که چگونه انتروپی آن را کاهش دهیم. وضعیت هنر شکستن رمزهای عبور نسبت به گذشته بسیار ظریف‌تر شده است؛ زیرا در گذشته ما از حدس‌های کور استفاده می‌کردیم.

اندکی ظرافت

ظرافتی که گراهام از آن سخن می‌گوید، شکل‌های متعددی به خود می‌گیرد. یکی از تکنیک‌های نویدبخش در این زمینه استفاده از برنامه‌هایی نظیر Passpal (اپن‌سورس) است که با یافتن الگوهای مشابه در درصد عظیمی از گذرواژه‌های موجود، زمان مورد نیاز برای شکستن آن‌ها را کاهش می‌دهد. به عنوان مثال، همان‌گونه که پیش‌تر گفتیم، بسیاری از کاربران سایت‌ها تمایل دارند که عدد یک سال را به انتهای یک نام، کلمه یا سایر رشته‌های حروفی بیافزایند که آن رشته با یک حرف بزرگ شروع می‌شود. استفاده از تلاش کور (Brute Force) برای شکستن گذرواژه‌ای نظیر Julia1984 به آزمودن ۶۲۹ جایگشت ممکن نیاز دارد. این عدد سایز فضای کلیدی (keyspace) است که از جمع کردن تعداد حروف و علامت‌های صفحه کلید (۵۲ مورد) با تعداد ارقام (۱۰ عدد) و سپس رساندن آن به توان تعداد حروف در نظر گرفته شده برای گذرواژه (که هکر آن را تعیین می‌کند) به‌دست می‌آید. با استفاده از یک کارت گرافیک AMD Radeon HD7970 برای آزمودن تمام حالت‌های ممکن هنوز به ۱۹ روز زمان نیاز خواهیم داشت!

با استفاده از قابلیت‌هایی که در برنامه‌های شکستن رمزهای عبور نظیر Hashcat یا Extreme GPU Bruteforcer وجود دارد، می‌توان همین گذرواژه را ظرف تنها ۹۰ ثانیه شکست. تکنیکی که در این حالت مورد استفاده قرار می‌گیرد، حمله نقابی یا Mask Attack نامیده می‌شود. این

حمله به گذرواژه‌ها:

۶/۵: متوسط تعداد گذرواژه‌هایی که هر کاربر وب استفاده می‌کند (به‌رغم وجود تعداد متوسط ۲۵ حساب کاربری برای هر نفر!)

بیش از ۱۰۰ میلیون: تعداد گذرواژه‌هایی که در سال گذشته به‌صورت آنلاین منتشر شده‌اند.

۴۷: تعداد سال‌هایی که از لو رفتن نخستین پایگاه داده‌های رمزهای عبور در سال ۱۹۶۵ می‌گذرد.

۸/۲ میلیارد: تعداد متوسط گذرواژه‌هایی که می‌توان با استفاده از یک کامپیوتر شخصی مجهز به یک کارت گرافیک AMD Radeon HD7970 در هر ثانیه آزمایش کرد.

۳۱۰۸ ترابایت: حجم فضای ذخیره‌سازی که برای ذخیره کردن تمام گذرواژه‌های ده حرفی ممکن (با حروف کوچک) به همراه هش‌های MD5 آن‌ها لازم است.

۱۶۷ گیگابایت: فضای مورد نیاز برای ذخیره کردن جدول رنگین‌کمان (Rainbow Table) ۹۹/۹ درصد گذرواژه‌های فوق!

تکنیک با کاهش هوشمندانه تعداد حالت‌های ممکن فضای کلید به مواردی که احتمالاً با یک الگوی مشخص سازگار هستند، سرعت را افزایش می‌دهد. به‌جای آزمودن تمام حالت‌های ممکن از aaaaa0000 تا zzzzz9999، این تکنیک حروف بزرگ و کوچک را تنها روی کاراکتر اول گذرواژه امتحان می‌کند و مثلاً چهار حرف باقیمانده را از حروف کوچک در نظر می‌گیرد. پس از آن، او تمام اعداد چهار رقمی را به انتهای این رشته می‌افزاید. در این صورت فضای کلید مسئله به عدد (به نسبت) ناچیز ۲۳۷/۶ میلیون حالت کاهش می‌یابد.

با شکسته شدن ۵۰ درصد گذرواژه‌های یک فهرست، متخصصان شکستن رمز نظیر اتم، می‌توانند از Passpal و سایر نرم‌افزارهای مشابه استفاده کرده و الگوهایی را که مختص آن سایت خاص هستند، استخراج کنند. پس از آن نفوذگران می‌توانند به نوشتن قانون‌هایی برای رمزگشایی سایر گذرواژه‌های باقی‌مانده بپردازند. در بیشتر مواقع، هیچ میزانی از پیچیدگی الگوریتم‌ها و قدرت سخت‌افزاری برای شکستن تمام گذرواژه‌ها کافی نیست. برای ادامه کار در چنین شرایطی، نفوذگران به انجام تلاش کور (Brute Force) روی درصدی از گذرواژه‌ها (حتی با طول‌های ۹

با شکسته شدن ۵۰ درصد گذرواژه‌های یک فهرست، متخصصان شکستن رمز، می‌توانند از Passpal و سایر نرم‌افزارهای مشابه استفاده کرده و الگوهایی را که مختص آن سایت خاص هستند، استخراج کنند.

یکی دیگر از تکنیک‌های قدرتمندتر، حمله ترکیبی یا Hybrid Attack است. این شیوه با استفاده از چندین قانون، تعداد گذرواژه‌هایی را که فهرستی از لغات (نظیر آن‌چه توسط ردمن استفاده می‌شد) می‌توانند رمزگشایی کنند، به شدت افزایش می‌دهد. به جای استفاده از تلاش کور برای حدس زدن پنج حرف اول Julia1984، هکرها به سادگی لیستی از اسامی تک‌تک کاربران فیس‌بوک تهیه می‌کنند و آن‌ها را به یک فرهنگ‌لغات با سایز متوسط (مثلاً ۱۰۰ میلیون کلمه‌ای) می‌افزایند. هرچند تعداد آزمون‌های مورد نیاز برای این شیوه حمله از حالت Mask Attack بیشتر است (حدود ۱ تریلیون)، اما هنوز با استفاده از همان کارت AMD7970 تنها به ۲ دقیقه زمان نیاز خواهد داشت! اما نتیجه حاصل ارزش این تلاش اضافه را خواهد داشت؛ زیرا در این روش گذرواژه‌هایی نظیر Christopher2000، thomas1964 و موارد مشابه دیگر را نیز به سرعت پیدا خواهد کرد.

«اتم» (Atom) نام مستعار توسعه‌دهنده Hashcat است. او که تیمش برنده رقابت «اگه می‌تونی رمز من رو بشکن» در Defcon سال ۲۰۱۲ شده است، می‌گوید: «روش ترکیبی یا Hybrid، روش مورد علاقه من است. این کاراترین روش ممکن است. اگر من فهرستی از هش‌های جدید، مثلا شامل ۵۰۰ هزار هش، به دست بیاورم، می‌توانم ۵۰ درصد آن‌ها را تنها به کمک روش ترکیبی به سادگی بشکنم.»

داستان طولانی گذرواژه‌ها

به گفته ژوزف بونو، نخستین نمونه ثبت شده استفاده از کلمات سری برای احراز هویت یک انسان حداقل به زمان رم باستان بازمی‌گردد. بونو یکی از دانشجویان دانشگاه کمبریج است که به تازگی تز دکترایش را به اتمام رسانده است. تز دکترای او درباره گذرواژه‌ها و شماره‌های تعیین هویت بود و «حدس زدن رازهای انتخاب شده توسط انسان» نام داشت. ارتش رم روشی محافظه‌کارانه و دقیق را برای تعویض روزانه گذرواژه‌هایی که signa نامیده می‌شدند، توسعه داده بود که مانع کشف آن توسط سربازان دشمن می‌شد.

رد پای کلمات سری احراز هویت، حتی در داستان‌های علی‌بابا و چهل دزد بغداد هم به چشم می‌خورد و در برخی نسخه‌های کتاب هزار و یک شب نیز آورده شده است؛ همان جایی که سردسته دزدان برای باز کردن یک غار مخفی از ورد «کنجد، کنجد بازشو!» استفاده می‌کند.

به‌نظر می‌رسد برناردو در نمایشنامه هملت شکسپیر نیز، هنگامی که در شروع نمایش خود را با جمله «زنده باد پادشاه» به نگهبانان قلعه معرفی می‌کند، به نوعی از گذرواژه‌ها استفاده کرده باشد. به گفته بونو، نخستین استفاده از گذرواژه روی سیستم‌های کامپیوتری، در دهه ۱۹۶۰ میلادی در MIT و روی سیستم‌های Compatible Time-Sharing System صورت گرفته است. برای هر حساب کاربری یک گذرواژه در یک فایل مادر رمزگذاری نشده، ذخیره شده و از آن برای تقسیم زمان ارزشمند کامپیوترها استفاده می‌شد. به گفته بونو (و تایید رابرت مک‌میلان در یکی از مقالات وایرد) یکی از دانشجویان دکترا به چیزی اعتراف کرده است که به نظر می‌رسد نخستین هک گذرواژه کامپیوتری باشد. او با این کار توانسته بود زمان بیشتری از کامپیوتر را برای پروژه‌اش در اختیار بگیرد.

این سیستم نخستین نشت اطلاعات بانک گذرواژه‌ها را در سال ۱۹۶۵ تجربه کرد؛ یعنی زمانی که یک باگ به اشتباه فایل حاوی گذرواژه‌ها را به یکی از پرینترهای عمومی ارسال کرد و مدیران سیستم مجبور شدند تمام گذرواژه‌ها را به‌صورت دستی تغییر دهند.

کاراکتر یا بیشتر) مجبور خواهند شد.

موکسی مارلین‌اسپایک، یکی دیگر از متخصصان رمزگشایی می‌گوید: «هزینه چنین کاری بسیار زیاد است، اما باید این کار را انجام دهیم تا مدل و درک خودمان را بهبود بخشیم و با گذرواژه‌های جدیدی که مردم انتخاب می‌کنند، همگام باشیم. با در اختیار داشتن چنین دانشی، می‌توانیم به عقب برگردیم و قوانین و فهرست لغاتی بسازیم که ما را به صورتی موثر در شکستن سایر گذرواژه‌ها بدون استفاده از تلاش کور یاری کنند. وقتی شما بازخورد موفقیت خود را دوباره در فرآیند دخیل کنید، می‌توانید چیزهای بیشتر و بیشتری یاد بگیرید و این موضوع همانند یک گلوله برفی بزرگ و بزرگ‌تر می‌شود.»

حمله فرهنگ لغت‌ها

این شیوه شکستن رمزهای عبور، به‌لطف کتاب یا به عبارتی تریلر هکری «تخم فاخته» (The Cuckoo's Egg) توجه عمومی را به خود جلب کرد. در این تریلر، کلیف استول (Cliff Stoll) داستان تلاش‌های خود را در جریان تعقیب و جست‌وجوی یک هکر که به سیستم‌های کامپیوتری ایالات متحده نفوذ کرده بود، نوشته است. هکر تحت تعقیب توانسته بود اسناد سری و مهم نظامی را از شبکه کامپیوتری امریکا دزدیده و در اختیار کاگ ب روسیه قرار دهد.

این کتاب پر از داستان افراد رده بالا بود که با راهبردهایی ضعیف در قبال گذرواژه‌ها، امنیت ملی را به خطر می‌انداختند. یک حساب کاربری در شبکه شرکت SRI (یکی از پیمانکاران وزارت دفاع) وجود داشت که نام کاربری و گذرواژه آن هر دو SAC بود! یا یکی از حساب‌های دارای دسترسی سطح بالا در آزمایشگاه‌های لاورنس برکلی، سال‌ها بود که گذرواژه‌اش عوض نشده بود. استول، یک ستاره‌شناس اخراج شده که به ناگاه تبدیل به سردمدار شکارچیان هکرها شده بود، در کتابش می‌نویسد: «هنگامی که پول در گاوصندوق‌ها نگه‌داری می‌شد، سارقان به قفل‌های ترکیبی حمله می‌کردند. اکنون که امنیت تبدیل به بیت‌های اطلاعات در حافظه کامپیوترها شده است، دزدها به سراغ گذرواژه‌ها می‌روند.»

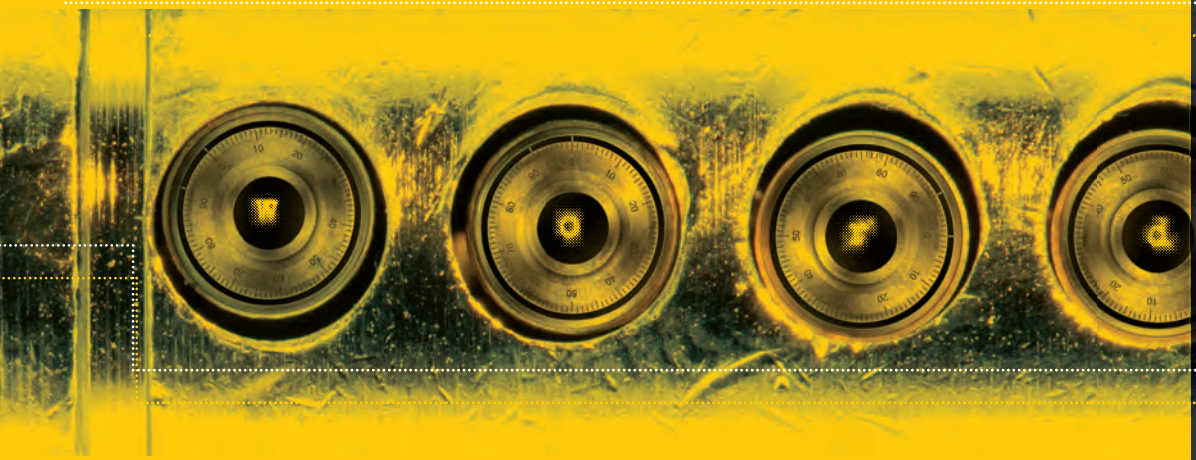
ماجرای استول یکی از نخستین نمونه‌هایی بود که نشان داد چگونه یک هکر با استفاده از یک فرهنگ لغت و یک کامپیوتر یونیکسی می‌تواند هر گذرواژه‌ای را که به زبان انگلیسی باشد، هک کند؛ حتی اگر این گذرواژه در کامپیوتر هک شده به‌صورت هش نگه‌داری شود.

استول در یکی از بخش‌های کتابش تابع رمزنگاری گذرواژه را با یک چرخ گوشت یک طرفه مقایسه کرده است که هر کلمه قابل خواندن توسط انسان را به یک متن رمزنگاری شده منحصر به فرد تبدیل می‌کند. البته تابعی که در آن زمان برای رمزنگاری استفاده می‌شد، مبتنی بر Data Encryption Standard یا به‌اصطلاح DES بود که اکنون دیگر روشی منسوخ شده است. استول می‌پرسد: «آیا این هکر یک فرمول رمزگشایی جادویی در اختیار داشت؟ اگر شما چرخ دنده‌های یک ماشین تولید سوسیس را وارونه به گردش درآورید، از سمت دیگر قطعات گوشت (یک خوک زنده) بیرون نخواهد آمد.» او بعدها متوجه شد که هکر در واقع تمام لغات یک فرهنگ لغت را به خورد الگوریتم رمزنگاری DES (همان الگوریتمی که در ماشین یونیکس هک شده استفاده شده بود) می‌داده است. این لغات با aardvark آغاز شده و با zymurgy خاتمه می‌یافت. پس از آن خروجی را با محتویات رمزنگاری شده فایل لو رفته، مقایسه می‌کرد.

استول می‌نویسد: «این مشکلی جدی بود. به این معنا که هر زمان او یک فایل حاوی گذرواژه‌ها را کپی می‌کرد، می‌توانست به گذرواژه‌های کاربران معتبر سیستم دست یابد و این خبر بدی بود.» اگرچه استول در آن زمان نمی‌دانست، اما در همان زمانی که این نفوذگر از فرهنگ لغات برای حدس زدن گذرواژه‌ها استفاده می‌کرد، رمزنگاران و نفوذگران در حال شکل دادن نوع جدیدی از حملات بودند که درنهایت می‌توانست هش‌های بیشتری را در کسری از زمان لازم برای حملات مبتنی بر فرهنگ لغت بشکند.

اتصالات رنگین‌کمانی

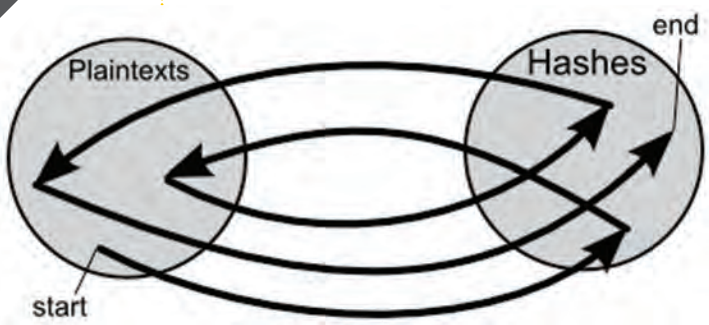
زیربنای این روش جدید توسط مارتین ای.هلمن (Martin E.Hellman) پایه‌ریزی شد. هلمن در سال



> خلاقیت موجود در جدول‌های رنگین کمانی ناشی از یک فرمول پیچیده ریاضی است که هر ترکیب ممکنی از گذرواژه‌ها را به‌صورت مجازی و بدون نیاز به ذخیره آن‌ها روی دیسک یا در حافظه تولید می‌کند.

۱۹۸۰ مقالـــه‌ای را با نام «مصالحه زمان- حافظه در امور رمزنگاری» منتشر کرد و در آن جدول‌هایی را معرفی کرد که به جدول‌های هلمن معروف شدند.

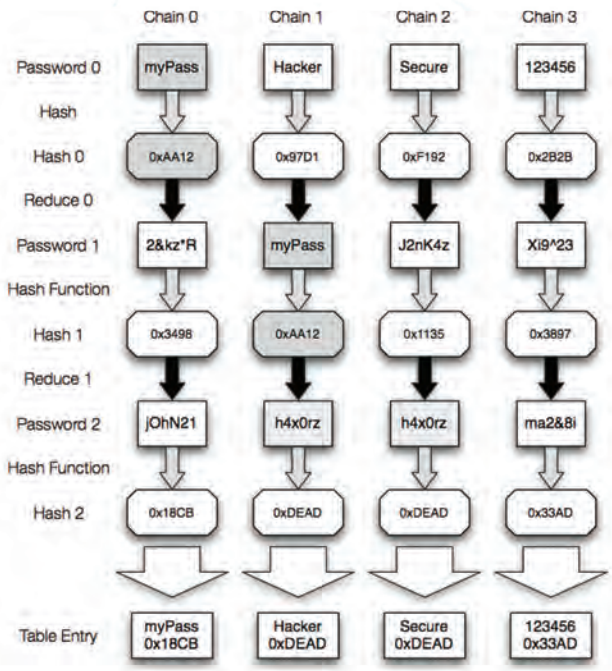
این جدول‌ها پیش از حمله و نفوذ برای به‌دست آوردن گذرواژه‌ها تهیه می‌شدند و کارشان را با داده‌های ازپیش محاسبه شـــده روی هارددیســـک به انجام می‌رساندند. جدول‌هـــای هلمـــن هزینه منابـــع کامپیوتـــری لازم برای شکســـتن گذرواژه‌های رمزگذاری شده با الگوریتم DES را از ۵ هـــزار دلار بـــه کمتـــر از ۱۰ دلار کاهش داد. فیلیپ اوکسلین (Phillippe Oechslin) در سال ۲۰۰۳ تغییرات و بهبودهایی را در تکنیک هلمن به وجود آورد که کارایی آن را تا حد زیـــادی افزایش می‌داد. نتیجه این تلاش‌ها چیزی اســـت که امروزه جدول‌های رنگین‌کمانی نامیده می‌شود. این جدول‌ها یک‌شبه شیوه شکستن گذرواژه‌های هش شده را تغییر دادند. نظیر نخستین شیوه‌های هلمن که مبتنی بر مصالحه میان زمان و حافظه بود، ایده این شیوه‌های جدید نیز ساده است. به‌جای این‌که از کامپیوتر خواسته شود که



شکل ۳: یک زنجیره از جدول رنگین‌کمانی با یک گذرواژه متنی ساده شروع می‌شود. این گذرواژه هش می‌شـــود. مقدار هش حاصل با استفاده از توابع کاهش به یک متن ساده دیگر تبدیل می‌شود. این متن ســـاده دوباره هش می‌شود. جدول موردنظر تنها مقدار متن ساده شروع و مقدار هـــش نهایی را ذخیره می‌کند و به این ترتیب یک زنجیره که حاوی میلیون‌ها مقدار هش اســـت، می‌تواند تنها توسط یک گذرواژه متنی ساده و یک مقدار هش نهایی تعریف شود.

هـــر گذرواژه ممکن را به‌صورت بی‌درنگ هش و با مقادیر موجود مقایســـه کند، هش‌هـــای گذرواژه‌های ممکن پیش از حمله محاســـبه شده و با فرمتی فشرده شده در حافظه یا روی دیســـک ذخیره می‌شـــوند. در این حالت کامپیوتر مســـتقیماً مقادیر هش گذرواژه‌های ممکن را با جدول هش موجود مقایســـه می‌کند و به این ترتیب، فرآیند ســـریع‌تر شـــده و تجهیزات کامپیوتری مـــورد نیاز برای تلاش کور روی تعداد زیاد هش‌ها بسیار کاهش می‌یابد.

اگرچه شـــیوه‌های قبلی نیز از همین سیستم استفاده می‌کردنـــد، خروجی آن‌هـــا جدول‌هایی بود کـــه بی‌دلیل بزرگ بودند و به همین دلیل به کار شکســـتن گذرواژه‌ها نمی‌آمدنـــد. خلاقیت موجـــود در جدول‌های رنگین‌کمانی ناشـــی از یک فرمول پیچیده ریاضی اســـت که هر ترکیب ممکنـــی از گذرواژه‌ها را به‌صـــورت مجازی و بدون نیاز به ذخیره آن‌ها روی دیســـک یا در حافظـــه تولید می‌کند. هـــر جدولی یـــک الگوریتم و یک فضای کلید مشـــخص را هدف می‌گیرد و شـــامل مجموعه‌ای از زنجیره‌ها است. هر زنجیره با یک گذرواژه دلخواه شـــروع شده و با یک مقدار هش شـــده پایان می‌یابد. گـــذرواژه اولیه به الگوریتم داده



شکل ۴: نمایی کلی از یک جدول رنگین‌کمانی که چهار رشته را در خود ذخیره کرده است.

پیشرفت‌های شگرف در زمینه استفاده از کارت‌های گرافیک برای شکستن گذرواژه‌ها، باعث کم‌رنگ شدن مزیت‌های جدول‌های رنگین کمانی شده‌است. گذرواژه‌هایی با ۶ حرف یا کمتر با دردسر بسیار اندکی به کمک کامپیوترهای مجهز به کارت‌های گرافیکی شکسته می‌شوند، گذرواژه‌های ۹ یا ۱۰ حرفی هنوز به جدول‌های رنگین کمانی با اندازه فایل‌های بسیار بزرگ نیاز دارند و در نتیجه این روزها جدول‌های رنگین کمانی تنها برای بازه کوچکی از گذرواژه‌های ۷ یا ۸ حرفی مفید واقع می‌شوند.

می‌شود تا مقدار هش شده آن تولید شود.

مقدار هش حاصل از یکی از انواع «توابع کاهش» عبور داده می‌شود تا یک حدس جدید برای گذرواژه تولید شود. این گذرواژه جدید از نو هش می‌شود. این فرآیند تا رسیدن به مقدار هش نهایی در انتهای زنجیره ادامه می‌یابد (شکل ۳ و ۴).

افزایش سرعت شکستن گذرواژه‌ها تنها مزیت این جدول‌ها نبود. مزیت مهم‌تر این بود که این جدول‌ها می‌توانستند تقریباً هر گذرواژه ممکن را که در فضای کلید هدف گرفته شده قرار داشت، بشکنند.

به این دلیل این جدول‌ها را رنگین‌کمانی نامیده‌اند که هر حلقه این زنجیره‌ها از تابع کاهش جداگانه‌ای استفاده می‌کند، اما تمام زنجیره‌ها از الگوی یکنواختی پیروی می‌کنند. درست مانند رنگ‌های یک رنگین‌کمان که گرچه با یکدیگر متفاوت هستند، همه از ترتیب قرمز، نارنجی، زرد، سبز، آبی، نیلی، بنفش پیروی می‌کنند.

میزان صرفه‌جویی حاصل در فضای ذخیره‌سازی خود بسیار زیاد بود. ذخیره‌سازی جدول تمام گذرواژه‌های ۱۰ حرفی که تنها از حروف کوچک استفاده کرده‌اند به همراه هش‌های MD5 مربوط به هرکدام به ۳۰۱۸ ترابایت فضا روی دیسک سخت نیاز خواهد داشت. اما یک جدول رنگین‌کمانی که ۹۹/۹ درصد این گذرواژه‌ها را در خود داشته باشد، تنها به ۱۶۷ گیگابایت فضا نیاز دارد.

در دوران ویندوز اکس‌پی، برنامه مدیریت شبکه (LANManager) مایکروسافت تنها می‌توانست گذرواژه‌هایی با طول حداکثر ۱۴ حرف را نگه‌داری کند که در طولانی‌ترین حالت به دو گذرواژه ۷ حرفی تقسیم شده و تماماً به حروف بزرگ تبدیل می‌شدند.

در آن دوران نتیجه استفاده از جدول‌های رنگین‌کمانی بسیار خیره‌کننده بود! هکرها در سال ۲۰۰۳ میلادی Ophcrack را عرضه کردند. Ophcrack برنامه‌ای اپن‌سورس بود که می‌توانست غالب گذرواژه‌های ویندوزی را ظرف چند دقیقه بشکند. پس از آن نیز برنامه‌های قدرتمندتر شکستن گذرواژه‌ها به سرعت عرضه شدند.

مارلین اسپایک سرویسی را با نام CloudCracker راه‌اندازی کرد که می‌توانست گذرواژه یک شبکه وای‌فای را ظرف حدود ۲۰ دقیقه با ۳۰۰ میلیون کلمه احتمالی مقایسه کند! او می‌گوید: «این واقعیت که شما ابزاری در اختیار دارید که هر کسی می‌تواند آن را دانلود کند و تقریباً هر گذرواژه‌ای را روی ویندوز اکس‌پی بشکند، بسیار جالب است. موضوع این نبود که من ۲۰ درصد، ۵۰ درصد یا حتی ۸۰ درصد گذرواژه‌ها را پیدا می‌کردم. تقریبا تمام آن‌ها قابل شکستن بودند! و این اتفاق بزرگی بود.»

به هر حال، پیشرفت‌های شگرف در زمینه استفاده از کارت‌های گرافیک برای شکستن گذرواژه‌ها، باعث کم‌رنگ شدن مزیت‌های جدول‌های رنگین‌کمانی شده‌است. گذرواژه‌هایی با ۶ حرف یا کمتر با دردسر بسیار اندکی به کمک کامپیوترهای مجهز به کارت‌های گرافیکی شکسته می‌شوند، گذرواژه‌های ۹ یا ۱۰ حرفی هنوز به جدول‌های رنگین‌کمانی با اندازه فایل‌های بسیار بزرگ نیاز دارند و در نتیجه این روزها جدول‌های رنگین‌کمانی تنها برای بازه کوچکی از گذرواژه‌های ۷ یا ۸ حرفی مفید واقع می‌شوند.

اما این جدول‌ها هنوز جایگاه خود را به عنوان ابزاری کارآمد (حتی اگر بگوییم کم‌کاربرد) برای برخی هکرها حفظ کرده‌اند. مثلاً پروژه جدول‌های رنگین‌کمانی رایگان (Free Rainbow Tables) را در نظر بگیرید. این پروژه به داوطلبان امکان می‌دهد که چرخه‌های بی‌استفاده کامپیوترشان را در اختیار پروژه قرار دهند تا به‌کمک این توان پردازشی، مجموعه‌ای از جدول‌های رنگین‌کمانی تهیه شود که این جدول‌ها در دسترس عموم قرار گرفته و می‌توانند هش‌های حاصل از الگوریتم‌های SHA1، MD5 و NTLM را بشکنند.

سازمان‌دهندگان این پروژه به حجم عظیمی از داده‌ها معادل ۶ ترابایت دست یافته‌اند. به گفته جیمز نوبیس که یکی از توسعه‌دهندگان پروژه است، با شرکت بیش از ۳۹۰۰ کامپیوتر داوطلب، هر ثانیه چیزی در حدود ۳۶ مگابایت به اندازه جدول‌های رنگین‌کمانی آزاد این پروژه افزوده می‌شود.

به نمک بیشتری نیاز است!

نسخه جدیدی از برنامه مدیریت شبکه به همراه نسخه ۳/۱ ویندوز NT عرضه شد که NTLM نام داشت. این مدیر شبکه جدید نفوذپذیری گذرواژه‌های ویندوزی را در برابر حمله‌های مبتنی بر جدول‌های رنگین‌کمانی کاهش داد اما خطر را به صورت کامل رفع نکرد. حتی امروزه نیز سیستم احراز هویت ویندوز هنوز از افزودن به‌اصطلاح «نمک»های رمزگذاری به گذرواژه‌ها برای عقیم گذاشتن چنین حملاتی استفاده نمی‌کند!

فرآیند «نمک زدن» در واقع چندین کاراکتر مشخص را پیش از هش کردن به انتهای هر یک از گذرواژه‌ها می‌افزاید و در نتیجه مقادیر موجود در جدول‌های رنگین‌کمانی و

سایر شیوه‌های از پیش محاسبه شده را بی‌اثر می‌کند.

به عنوان مثال، برای شکستن یک فرآیند نمک زدن ۱۶ بیتی به ۶۵۵۳۵ (برابر ۲۱۶) جدول مجزا نیاز خواهیم داشت. استفاده از نمک تصادفی ۳۲ بیتی، جدول‌های رنگین‌کمانی را بیش از پیش ناکارآمد می‌سازد؛ زیرا برای شکستن آن به بیش از ۴ میلیارد جدول نیاز خواهیم داشت. این نمک باید برای هر کاربر ذخیره شود و معمولا در کنار نام کاربری و هش گذرواژه نگه‌داری می‌شود و به این ترتیب در هر بار لاگین، اطلاعات لازم در دسترس سیستم خواهد بود.

نمک‌ها به ندرت جدا از هش‌ها نگه‌داری می‌شوند. حتی در صورت معلوم بودن نمک‌ها، نقطه قوت آن‌ها در منحصر به‌فرد بودن‌شان است که امکان پیش‌بینی و ایجاد جدول‌های رنگین‌کمانی را از میان می‌برد.

برای این‌که متوجه شوید این کار در عمل چگونه انجام می‌شود، ما یک حساب کاربری جدید با نام testuser ایجاد کردیم. سیستم‌عامل اطلاعات ورود به حساب کاربری را در یک خط طولانی از فایل /etc/shadow که محل نگه‌داری گذرواژه‌های لینوکس است، ذخیره می‌کند. این خط به شکل زیر است:

```
testuser:$6$2lvEhpi5$KnVn901C4Y23zsVZK1/
UILbTkKIU6hA6V/opXZ3yQU.EhVxQS6/KjaO2bH7VZOOr/
DTGko9LjqWOi7CrU.Ggy0:15569:0:99999:7:::
```

این خط به‌وسیله علامت «:» به چندین قسمت تقسیم شده است. در بخش نخست، نام کاربری را می‌بینید. قسمت طولانی پس از آن حاوی گذرواژه است. پس از آن، اطلاعات مربوط به زمان اعمال آخرین تغییرات در این گذرواژه، عمر گذرواژه فعلی، تاریخ انقضای این حساب کاربری و موارد مشابه را مشاهده خواهید کرد.

مهم‌ترین بخش این اطلاعات برای هدف ما، قسمت گذرواژه است که خود به کمک علامت «$» به چند بخش تقسیم شده است. در بخش نخست عددی را می‌بینید که الگوریتم استفاده شده برای هش را نگه‌داری می‌کند. در این مثال عدد ۶ نشان‌دهنده الگوریتم SHA512 است. بخش بعدی همان «نمک» است که در مثال ما برابر 2lvEhpi5 است و در نهایت هش دیده می‌شود که ردیفی طولانی از حروف و علامت‌ها است.

علاوه بر بی‌اثر کردن جدول‌های رنگین‌کمانی، فرآیند نمک زدن منابع مورد نیاز برای شکستن کلمه عبور به سایر روش‌های سنتی را نیز به شدت افزایش می‌دهد؛ زیرا با استفاده از این شیوه حتی اگر دو کاربر گذرواژه یکسانی را انتخاب کرده باشند، هش ذخیره شده برای هر کدام متفاوت خواهد بود. به همین دلیل، هر یک از هش‌های جدول گذرواژه لو رفته، باید جداگانه شکسته شوند؛ حتی اگر مربوط به گذرواژه‌های متنی یکسان باشند.

به‌رغم مزایای این شیوه و سادگی پیاده‌سازی آن، تعداد زیادی از سایت‌ها شامل LinkedIn، Yahoo و eHarmony که به تازگی هک شده‌اند، از این شیوه استفاده نمی‌کردند! با توجه به این‌که NTLM از فرآیند نمک‌زدن استفاده نمی‌کند، شکستن هش‌های به دست آمده از آن بسیار ساده است.

عدم استفاده از نمک تنها یکی از کوتاهی‌هایی است که سایت‌های معمول و مشهور اینترنتی در حق کاربران اینترنتی انجام می‌دهند و در نتیجه امنیت گذرواژه‌های کاربران را با خطر مواجه می‌کنند.

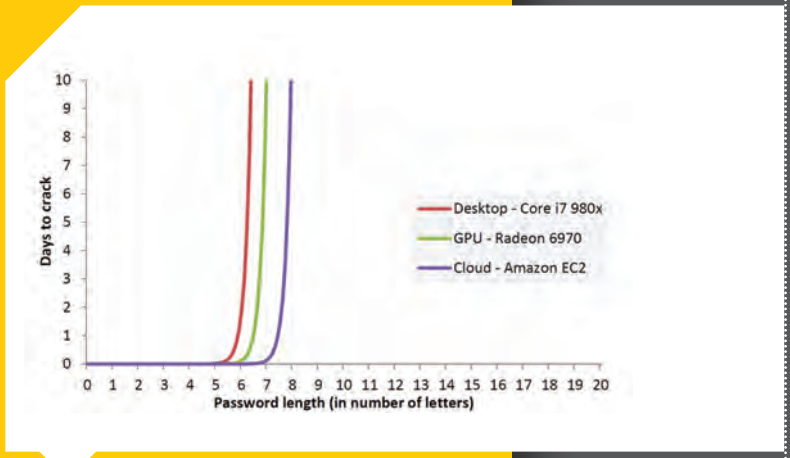
نه! SHA1 الگوریتم امنی برای هش کردن نیست

درصد بسیاری از سایت‌هایی که قربانی هک‌های گذرواژه می‌شوند، اشتباهی را مرتکب می‌شوند که امنیت گذرواژه‌ها را بیش از پیش به خطر می‌اندازد. آن‌ها از الگوریتم‌هایی استفاده می‌کنند که برای محافظت از کلمات عبور ساخته نشده‌اند! دلیل این امر آن است که الگوریتم‌های SHA1، DES و MD5 برای تبدیل سریع متن ساده به هش با کمترین میزان مصرف منابع کامپیوتری طراحی شده‌اند؛ و این درست همان چیزی است که هکرهای گذرواژه‌ها بیش از هر چیز دوست دارند! الگوریتم NTLM که هنوز از MD4 استفاده می‌کند، به شدت در برابر هک شدن ضعیف عمل می‌کند.

برای این‌که درک کنید این الگوریتم‌های بدون نمک چه انتخاب‌های ضعیفی برای هش کردن گذرواژه‌ها هستند، توجه شما را به این مورد جلب می‌کنیم: هک کردن ۹۰ درصد از ۶/۵ میلیون گذرواژه لو رفته LinkedIn که توسط الگوریتم SHA1 هش شده بودند، برای جرمی گاسنی، محقق امنیتی مستقل، تنها به ۶ روز زمان نیاز داشت. او یک پنجم گذرواژه‌های متنی را تنها ظرف ۳۰ ثانیه هک کرد! در دو ساعت بعدی، او موفق به هک کردن یک سوم دیگر از گذرواژه‌ها شد. ظرف یک روز، این میزان به ۶۴ درصد رسیده بود و در پنج روز بعدی ۲۶ درصد دیگر از گذرواژه‌ها هک شدند.

یکی از دلایل موفقیت او، در کنار فهرست عظیم ۵۰۰ میلیون کلمه‌ای و به کارگیری کامپیوتری مجهز به چهار کارت گرافیک AMD Radeon HD6990 تصمیم مهندسان LinkedIn مبنی بر استفاده از SHA1 بود. این الگوریتم تنها از یک پله رمزنگاری برای تبدیل متن به هش استفاده می‌کند.

> درصد بسیاری از سایت‌هایی که قربانی هک‌های گذرواژه می‌شوند، اشتباهی را مرتکب می‌شوند که امنیت گذرواژه‌ها را بیش از پیش به خطر می‌اندازد. آن‌ها از الگوریتم‌هایی استفاده می‌کنند که برای محافظت از کلمات عبور ساخته نشده‌اند! دلیل این امر آن است که الگوریتم‌های SHA1، DES و MD5 برای تبدیل سریع متن ساده به هش با کمترین میزان مصرف منابع کامپیوتری طراحی شده‌اند.



شکل ۵: تلاش کور (brute force) به‌خوبی در مورد گذرواژه‌های کوتاه کار می‌کند. این روش برای گذرواژه‌های طولانی‌تر ممکن است روزها یا ماه‌ها به‌طول بیانجامد، حتی اگر برای آن از سرویس‌های ابری EC2 آمازون استفاده شود.

همین امر این امکان را برای گاسنی فراهم کرد که در هر ثانیه بیش از ۱۵/۵ میلیون گذرواژه را آزمایش کند.

درمقابل، الگوریتم‌هایی که به‌صورت خاص برای محافظت از گذرواژه‌ها طراحی شده‌اند، به زمان و منابع پردازشی بیشتری برای تبدیل متن به هش احتیاج دارند. مثلاً SHA512crypt که در Mac OS X و غالب سیستم‌های یونیکسی مورد استفاده قرار می‌گیرد، متن‌ها را از ۵ هزار پله رمزنگاری عبور می‌دهد. چنین کاری باعث می‌شود که حتی گاسنی هم در هر ثانیه تنها امکان آزمودن ۲۶۰۰ واژه حدس زده شده را داشته باشد. الگوریتم Bcrypt به لحاظ منابع پردازشی مورد نیاز بسیار سنگین‌تر است. دلیل این امر آن است که متن را از چندین پله رمزنگاری Blowfish cipher عبور می‌دهد که به طور اختصاصی طراحی شده‌اند تا زمان لازم برای هش کردن را افزایش دهند. استفاده از تابعی به‌نام PBKDF2 که در فریم‌ورک دات‌نت مایکروسافت تعبیه شده است نیز همین مزایا را به دنبال خواهد داشت.

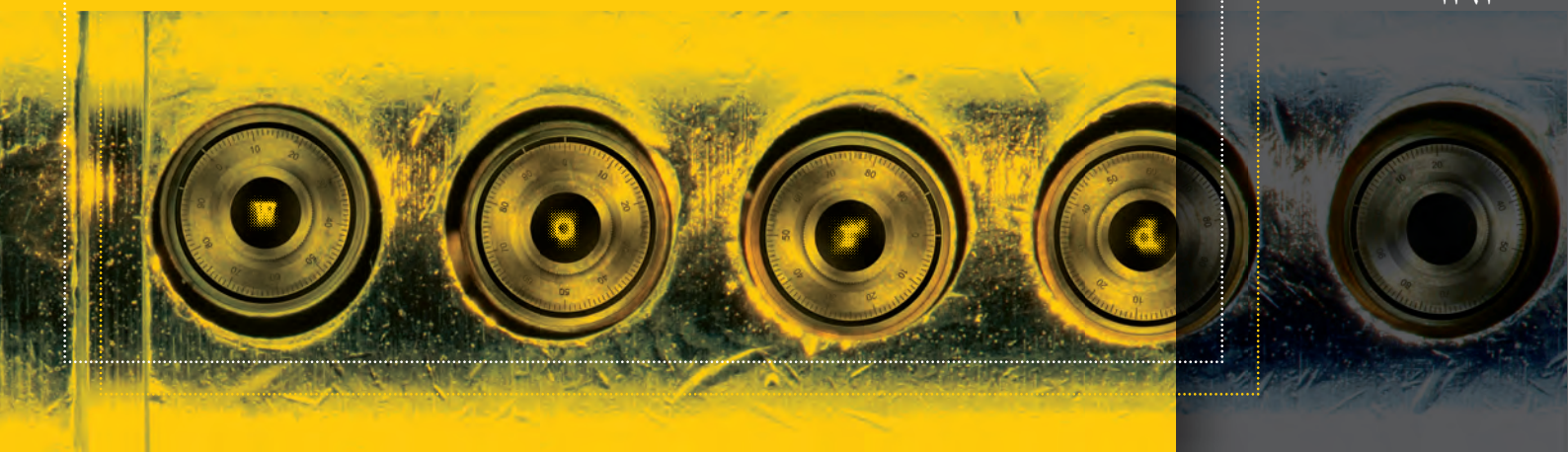
این توابع که به منابع پردازشی زیادی نیاز دارند، در سمت سرور نیز بار کاری بیشتری ایجاد می‌کنند. مت ویر (Matt Weir) یکی از دانشجویان فوق‌دکترای دانشگاه ایالتی فلوریدا که موضوع پایان‌نامه‌اش درباره رمزهای عبور بود، معتقد است که این امر می‌تواند به سرور فشار آورده و حتی آن را در معرض گونه جدیدی از حملات DoS قرار دهد. اما به عقیده بسیاری از متخصصان امنیتی، مزیت‌های حاصل از افزایش امنیت سایت، ارزش هزینه انجام شده را دارد. اگر مهندسان LinkedIn به عنوان مثال از الگوریتم Bcrypt استفاده کرده بودند، تعداد کلماتی که گاسنی می‌توانست در هر ثانیه بیازماید، به کمتر از ۱۷۵۰ کاهش می‌یافت.

گاسنی می‌گوید: «اگر گذرواژه‌های LinkedIn با استفاده از Bcrypt هش شده بودند، هیچ‌گاه نمی‌توانستم ۹۰ درصد آن‌ها را هک کنم. تعداد و پیچیدگی حمله‌هایی که باید انجام می‌دادم تا به تعداد زیادی از گذرواژه‌ها، به‌خصوص آن‌هایی که بیش از ۱۵ کاراکتر بودند، دست پیدا کنم در عمل باعث می‌شد که این فرآیند به چندین قرن زمان نیاز داشته باشد. من خودم بعد از یک هفته تسلیم می‌شدم.»

برخورد با دیوار

حتی قوی‌ترین تجهیزات کامپیوتری هم برای شکستن گذرواژه‌های طولانی با استفاده از تلاش کور، با مشکل روبه‌رو خواهند شد. در نظر بگیرید که چنین حمله‌ای بخواهد گذرواژه‌های ۵ حرفی را که شامل تمام ۹۵ حرف، عدد و علامت یک صفحه‌کلید انگلیسی استاندارد هستند، با تلاش کور بشکند. انجام این کار با یک سیستم دسکتاپ مجهز به پردازنده Core i7 980x تنها به چند ساعت زمان نیاز خواهد داشت. افزایش طول گذرواژه تنها به اندازه یک کاراکتر، زمان مورد نیاز را به یک روز افزایش خواهد داد. افزودن کاراکتر بعدی زمان مورد نیاز را به شکل خیره‌کننده‌ای تا ۱۰ روز افزایش خواهد داد. راب گراهام، مدیرعامل Errata Security که این زمان‌ها و نیازهای پردازشی را محاسبه کرده است، این محدودیت را «دیوار نمایی (توانی) هک با تلاش کور» می‌نامد.

افزودن یک پردازنده گرافیکی به سیستم، به یقین مفید خواهد بود اما نه به اندازه‌ای که بسیاری از افراد تصور می‌کنند. هک کردن گذرواژه‌های ۷ حرفی با استفاده از یک کارت گرافیکی AMD Radeon 6970 هنوز به ۱۰ روز زمان نیاز دارد. اما این دیوار حتی در برابر منابع پردازشی به شدت قوی‌تر نیز مقاومت می‌کند. با استفاده از



سیستم‌های ابری EC2 آمازون که توان پردازشی بیش از ۱۰۰۰ پردازنده گرافیکی را با هم ترکیب می‌کند، شکستن یک گذرواژه ۸ حرفی باز هم به حدود ۱۰ روز زمان نیاز خواهد داشت.

به جز در برخی موارد استثنایی، این دیوار به ندرت مانع هکرهای گذرواژه‌ها خواهد شد. همان‌گونه که قضیه RockYou نشان داد، افراد معمولی در هنگام انتخاب گذرواژه‌ها ضعیف و بی‌دقت عمل می‌کنند. ۷۰ درصد گذرواژه‌ها در فهرست RockYou هشت حرف یا کمتر داشتند! تنها ۱۴ میلیون از ۳۲ میلیون گذرواژه لو رفته منحصر به فرد بودند و این نشان می‌دهد که درصد عظیمی از گذرواژه‌ها تکراری هستند. اتم، متخصص امنیت و توسعه‌دهنده Hashcat، تخمین می‌زند که یک فرد عادی ظرف کمتر از ۲ روز می‌تواند حدود ۶۶ درصد از گذرواژه‌های هر فهرست هش بدون «نمکی» را استخراج کند.

با این تفاسیر، یک فرد عادی چگونه می‌تواند گذرواژه‌ای را انتخاب کند که ظرف چندین ساعت شکسته نشود؟ پر تورس‌هایم (Per Thorsheim) یک مشاور امنیتی شرکت‌های بزرگ در نروژ که در زمینه گذرواژه‌ها تخصص دارد، معتقد است که مهم‌ترین ویژگی که گذرواژه‌ها باید داشته باشند، این است که در سایت‌های مختلف باید یکتا باشند.

او توضیح می‌دهد: «در مورد بیشتر سایت‌ها، شما هیچ ایده‌ای ندارید که آن‌ها چگونه گذرواژه‌ها را ذخیره می‌کنند. اگر اطلاعات این سایت‌ها لو برود، اطلاعات شما هم لو خواهد رفت. اگر گذرواژه لو رفته شما منحصر به‌فرد باشد نگرانی چندانی، وجود نخواهد داشت.»

علاوه بر این، مهم است که گذرواژه‌ای که انتخاب می‌کنید در فهرست صدها میلیون گذرواژه لو رفته‌ای که در اختیار هکرها قرار دارد، نباشد. این گذرواژه باید به‌صورت تصادفی توسط یک کامپیوتر تولید شود و حداقل ۹ حرف داشته باشد تا حملات مبتنی بر تلاش کور را عقیم کند. با توجه به این‌که امروزه داشتن یک دوجین حساب کاربری چیزی طبیعی است، ساده‌ترین راه عمل کردن به این توصیه‌ها استفاده از برنامه‌هایی نظیر 1Password و PasswordSafe است. هر دوی این برنامه‌ها امکان تولید گذرواژه‌های تصادفی طولانی و ذخیره ایمن و رمزنگاری شده آن را برای کاربران فراهم می‌کنند. این گذرواژه‌ها به نوبه خود، به کمک یک گذرواژه اصلی محافظت می‌شوند. استفاده از برنامه‌های مدیریت گذرواژه برای تعویض منظم و دوره‌ای آن‌ها نیز الزامی است.

با توجه به پیچیدگی فرآیندهایی که هکرها به کار می‌برند، هرگونه کوتاهی از این دستورالعمل‌ها به سادگی گذرواژه شما را در معرض خطر قرار خواهد داد.

ویر می‌گوید: «کل صحنه هک گذرواژه‌ها در چند سال اخیر به‌شدت تغییر کرده است. شما می‌توانید فضای آنلاین را زیر نظر بگیرید و به‌صورت کلی گذرواژه‌های مربوط به هر کسی را بالاخره از جایی به دست آورید. من نام کاربری و گذرواژه‌های خودم را روی سایت‌های متعددی پیدا کردم. اگر فکر می‌کنید که تک‌تک سایت‌هایی که در آن‌ها حساب کاربری دارید، امن هستند و هیچ‌گاه تاکنون هک نشده‌اند، شما حتی از من هم خوش‌بین‌تر هستید!» شبکه

حفاظت صحیح از گذرواژه‌ها

از برنامه‌هایی نظیر Password Safe یا PassLast برای تولید و ذخیره‌سازی گذرواژه‌هایتان استفاده کرده و اطمینان حاصل کنید که خود این برنامه‌ها به‌وسیله یک گذرواژه اصلی واقعا قوی، منحصر به‌فرد و قابل به خاطر سپردن محافظت می‌شوند.

از این برنامه‌های مدیریت گذرواژه برای تولید گذرواژه‌های تصادفی با طول حداقل ۱۳ کاراکتر استفاده کنید. اگر نمی‌خواهید این گذرواژه را روی تلفن هوشمند یا ابزارهایی با صفحه‌کلیدهای محدود وارد کنید، مطمئن شوید که در آن حتما از علامت‌هایی غیر از حرف و عدد هم استفاده شده است. در غیر این صورت ترکیبی از حروف بزرگ و کوچک و اعداد کافی خواهد بود.

برای هر حساب کاربری که اطلاعاتی شخص از شما را در خود دارد، گذرواژه‌ای جداگانه و منحصر به‌فرد تولید کنید.

گذرواژه‌هایتان را حداقل هر ۶ ماه یک بار تغییر دهید و برای حساب‌های کاربری حساس‌تان، این کار را در فواصل زمانی کوتاه‌تری انجام دهید. این کار را هر بار که از یک شبکه ناامن استفاده کردید نیز تکرار کنید. اگر متوجه شدید که سایت مورد استفاده شما هک شده است، بلافاصله گذرواژه خود را تغییر دهید.

وقتی در سایت‌ها وارد می‌شوید، سعی کنید از آدرس‌هایی استفاده کنید که با https آغاز می‌شوند.