پسورد، پسفریز، رمز عبور

نویسنده: سویل .ک

ما در طبیعت برای شناخت هر پدیده‌ای ابتدا یک الگوی ذهنی می‌سازیم تا در برخوردهای بعدی این پدیده برای ما یک الگوی شناخته شده باشد، سپس در گذر زمان و تکرر تقابل با این پدیده منجر به تکمیل اطلاعات ذهنی ما می‌شود و عقبه رشته اطلاعات ما به تدریج کامل‌تر می‌شود.

به عبارتی منحنی تجربه منجر به تکمیل و اصلاح اطلاعات ما می‌شود و اینچنین ما الگویی شناخته شده را به تاریخچه خود می‌افزاییم، وجه اشتراک بین همنوعان (پروتکلی ارتباطی مانند زبان) بین ما منجر به اشتراک این اطلاعات می‌شود و این الگوی شناخته شده تبدیل به یک الگوی جمعی می‌شود.

این الگوهای مرجع و مشترک منجر می‌شود ما قدرت تشخیص و تمیز دادن را پیدا کنیم. در ابتدا این مساله بسیار ساده‌تر بوده است زیرا پیچیدگی و تنوع در نمودار زمان همیشه صعودی بوده است، تشخیص هم نوع، تشخیص دشمن یکی از کلاسیک‌ترین‌های تاریخ بشری است.

در طول زمان طبیعتا معایبی در تشخیص الگوها پیدا شده است و این منجر به اصلاح و پیشرفت روش‌های تشخیص شده است، در طرف مقابل پدیده‌ها نیز پیچیده و هوشمندتر شده‌اند.

در زمان‌های نه چندان دور برای شناخت افراد یک اسم از او کافی بود، بعدها نام خانوادگی دیگری کنار این اسم آمد تا به شناخت کمک کند و امروز گرچه در دایره کوچک نام و نام خانوادگی شما کارساز است ولی شما بدون کد ملی قابل شناسایی نیستید.

همیشه تصدیق این الگوها برای بشر پر از چالش بوده است، برای تصدیق اصالت این الگوها همیشه راه حل‌هایی داشته است تا از اصالت الگو اطمینان حاصل پیدا کند.

اینجا بود که چیزی که در حال حاضر ما آن را با عنوان گذرواژه یا پسورد یا پسفریز می‌نامیم پدید آمده است و روز به روز روش ها و مدل های جدیدی از آن اصلاح و تکامل یافته است.

با نگاهی به طبیعت و پیشینه‌مان چنان به نظر می‌آید که این مدل ریشه در تاریخ طبیعی داشته است و پا به پای ما تا به امروز تکامل یافته است.

امروز ما در جهان حال حاضر هر کدام شناسه‌ای داریم (برای نمونه: ID توییتر) که کاملا یکتا و منحصر بفرد است و حتما برای تصدیق اصالت آن به Password داریم.

با کوچک‌ترین نگاهی اهمیت پسورد یا گذرواژه را در جهان حاضر به سادگی می‌توان درک کرد، در حال حاضر پسورد عموما رشته‌ای از کاراکترها، اعداد و علائم است که هر چقدر پیچیده‌تر (تنوع عدد، کاراکتر و علائم +

طول بیشتر) باشد منجر به امنیت بیشتری می‌شود، معمولا امروزه همه ما انسان‌ها دستکم چندین پسورد داریم و در مدیریت آنها دچار مشکلیم.

راه و روش‌های ما برای مدیریت پسوردها از نوشتن و مخفی کردن در یک گوشه‌ای از کاغذ گرفته تا حفظ کردن آن همه دارای ایرادهای اساسی است، لذا برای بهینه‌سازی این مساله ابزارهای مدیریت پسورد توسعه داده شده‌اند تا ما را در مدیریت پسوردهایمان یاری کنند.

در بخش دوم این مطلب به صورت فنی یکی از کارآمدترین ابزارهای مدیریت پسورد را که در بستر خانواده nix* قابل استفاده است را بررسی خواهم کرد.

پیش‌نیازها:

- سیستم‌عامل‌های nix*
- ابزار مدیریت نسخه Git
- آشنایی با الگوریتم رمزنگاری کلید عمومی

در ادامه در مورد هرکدام مختصری توضیح خواهم داد.

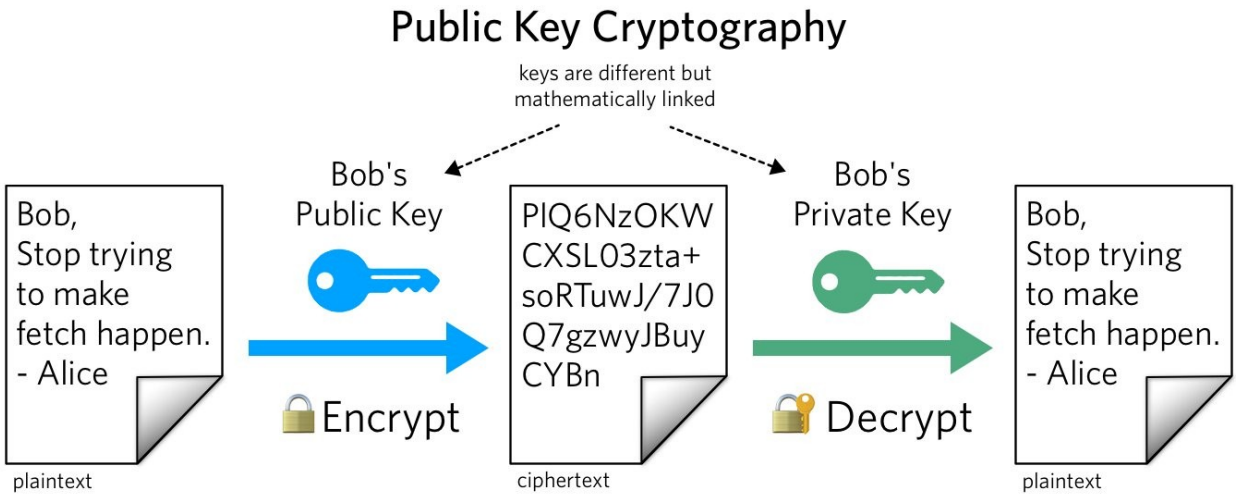
به نظر لزومی به توضیح در مورد سیستم‌عامل‌های پایه لینوکس و یونیکس نیست و همه کم و بیش در مورد آن‌ها می‌دانیم، لذا از این مورد می‌گذرم.

اما Git ابزاری بسیار مهم و کاربردی برای کنترل ورژن است، هسته بسیاری از نرم افزارهای کنترل ورژن از جمله گیتهاب و گیتلب از گیت بهره می‌برند.

با استفاده از گیت ما یک نقطه شروعی را ایجاد می‌کنیم و این ابزار تمام رویدادها، تغییرات و اتفاقاتی را که در طول زمان بر روی محیط رخ می‌دهد را ضبط و ثبت می‌کند، این ویژگی به ما این اختیار را می‌دهد تا مانند یک فیلم به هر برشی از تغییراتمان منتقل شویم و در طول زمان حرکت کنیم.

بدین شکل ما از وقتی Git را در داخل یک دایرکتوری تعریف می‌نمایم، یک تاریخچه دقیقا از تغییرات و اتفاقات را با امکان دسترسی آنی به هر تغییر (Commit) می‌دهد و می‌توانیم تمام تاریخچه را مورد مطالعه قرار دهیم.

اما الگوریتم کلید عمومی چیست؟



به شکل ساده در الگوریتم‌های Symmetric رمزنگاری بدین صورت است که برای مثال شما یک متن را رمزنگاری می‌کنید و به دوستتان ارسال می‌کنید، دوست شما برای باز کردن فایل نیاز به پسورد آن دارد، در اینجا باید کلید (رمز فایل) را به او بصورت (Plain text) ارسال نمایید تا او بتواند فایل را باز کند.

در این نوع رمزنگاری با یک مشکل جدی مواجه هستیم، اگر رمز بدست یک بیگانه بیفتد امنیت بصورت جدی به خطر میافتد، ما هیچ چاره‌ای نداریم و تنها پیشگیری می‌تواند ارسال در یک کانال امن باشد. همانگونه که می‌بینید یک اشکال اساسی امنیتی وجود دارد، با افتادن رمز در دست هر کسی بازی را باخته‌اید.

برای حل این مشکل الگوریتم‌های رمزنگاری Asymmetric به وجود آمدند که بصورت عمومی الگوریتم‌های رمزنگاری کلید عمومی نامیده می‌شوند. با توجه به تصویری که در بالا ارائه دادیم هر فرد ۲ کلید دارد:

1. کلید عمومی که در دسترس همگان است.
2. کلید خصوصی که باید به صورت امن فقط نزد شما باشد.

به طور مثال دوستتان با کلید عمومی شما متنی را رمزنگاری می‌کند و به برایتان ارسال می‌کند، در طرف دیگر شما با کلید خصوصی خودتان آن متن را رمزگشایی می‌کنید. بدین صورت هیچ فردی نمی‌تواند متن را بخواند و چون کلیدی (رمز فایل) رد و بدل نشده است خطر لو رفتن آن منتفی می‌شود.

در حال حاضر بسیاری از تکنولوژی های روز دنیا از این الگوریتم رمزنگاری در سیستم خود استفاده می‌کنند از آنها میتوان Bitcoin را نام برد که به صورت صریح از این رمزنگاری در هسته خود استفاده می‌کند.

خب تا به اینجا ما با موارد پیش‌نیاز آشنا شدیم و می‌توانیم ابزار مدیریت پسورد را معرفی کنیم.

از ویژگی‌های بارز ابزار پسورد منیجر ما می‌توان به نکات زیر اشاره کرد:

1. ساده (Bare bone) و مبتی بر فلسفه یونیکس "Do One Thing And Do It Well".
2. ساختار کاملا نرم و منعطف بطوری که همه چیز برای سازماندهی schema در دستان شماست .
3. هسته رمزنگاری مبتی بر کلید عمومی
4. پشتیبانی از Git
5. پیشنهاد خودکار پسورد
6. جایگذاری و فلش رمز در حافظه
7. پشتیبانی از چند کلید عمومی
8. و...

به صورت خلاصه (با فرض اینکه در حال حاضر روی یک سیستم خانواده *nix هستیم):

1. یک کلید عمومی برای خودمان تعریف میکنیم (اگر داریم نیازی نیست).
2. کلید عمومی را به پسورد منیجر معرفی میکنیم.
3. با استفاده از گیت ساختار اسکلت پسورد ها را معرفی میکنیم(initialise).

دو نکته بسیار مهم:

فایل .gnupg موجود در دایرکتوری Home حاوی اطلاعات حساس کلید عمومی شما است، پس باید در نگهداری آن به شدت کوشا باشید، در ادامه این مساله پاراگراف بعدی را دریابید.

Because an attacker with enough rights on the folder could manipulate folder contents.

Make sure, the folder+contents belong to you:
chown -R $(whoami) ~/.gnupg/

Correct access rights for .gnupg and subfolders:
find ~/.gnupg -type f -exec chmod 600 {} \;

```
find ~/.gnupg -type d -exec chmod 700 {} \;
```

نکته دوم برای اینکه همه سوابق شما از ابتدای استفاده شما ثبت و ضبط شود و امکان دسترسی و تغییر در کل تاریخچه را داشته باشید حتما بعد از تعریف کلید به پسورد منیجر با استفاده از دستور زیر ساختار پسوردهایتان را به گیت معرفی نمایید.

```
pass git init
```

وب سایت:

passwordstore.org

صفحه man:

https://git.zx2c4.com/password-store/about

مشاهده Pass - The Standard Unix Password Manager در یوتیوب:

https://www.youtube.com/watch?v=hlRQTj1D9LA&ab_channel=DistroTube