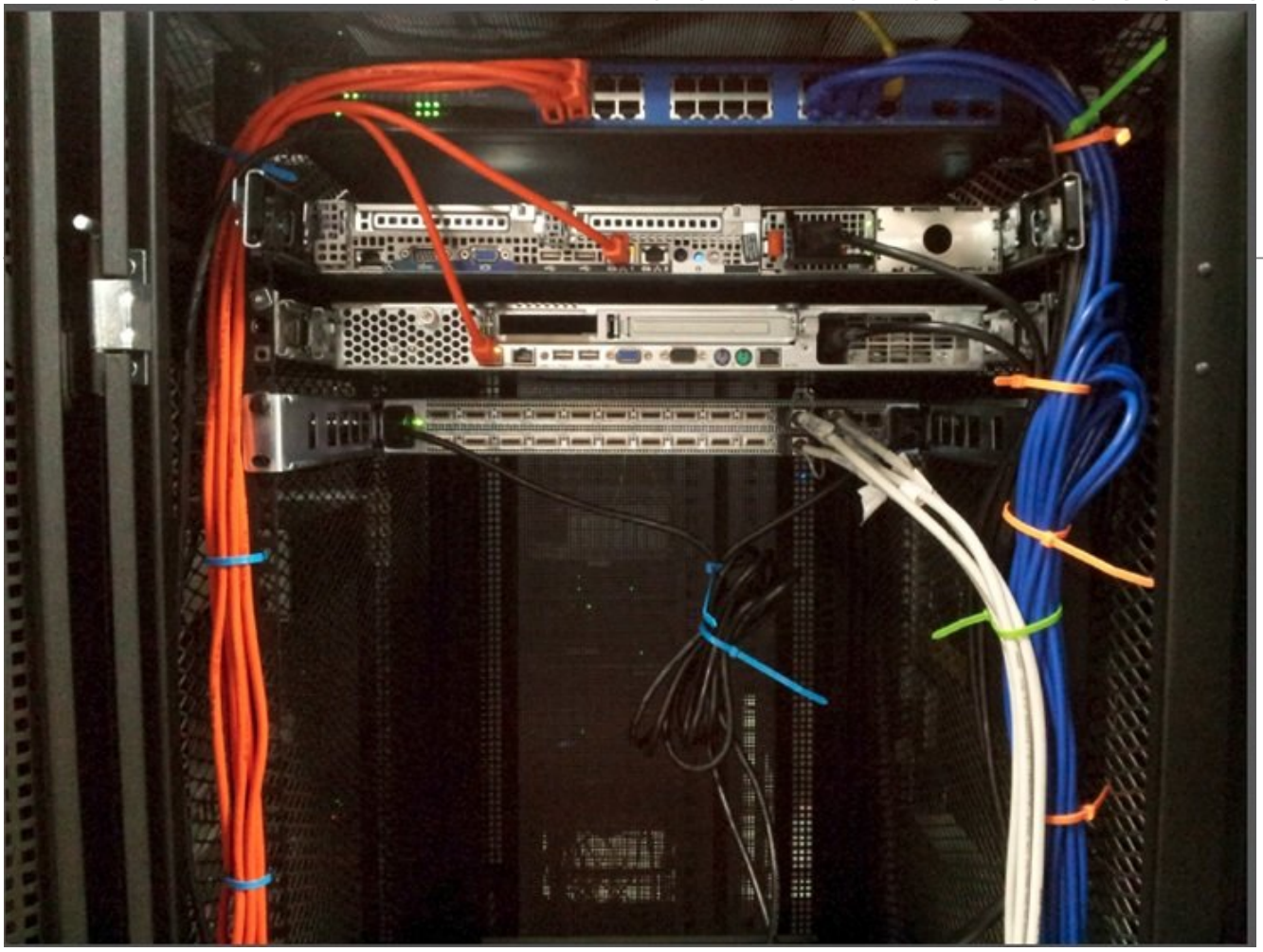
رایانش خوشه‌ای با توان‌مندی پردازش گرافیکی

این کامپیوتر هر ویندوزی را در کمتر از 6 ساعت هک می‌کند!



یک کارشناس امنیتی و متخصص در شکستن گذرواژه‌ها به تازگی کامپیوتر ویژه‌ای را طراحی کرده است که از تکنیک رایانش خوشه‌ای (Computer cluster) استفاده می‌کند. کامپیوتر جدید این توانایی را دارد تا 350 میلیارد پیش‌بینی را در هر ثانیه انجام داده و هر گذرواژه ویندوز را در 5 ساعت و نیم یا کمتر بشکند. ایده رایانش خوشه‌ای اولین بار در دهه 60 میلادی توسط IBM مطرح شد اما به دلیل محدودیت‌های مختلفی که به لحاظ سخت‌افزاری، شبکه و ابزارهای مناسب این مدل پردازش‌ها، وجود داشت تا اوایل دهه 80 میلادی کاربرد جدی و گسترده پیدا نکرد.

آیا گذرواژه شما ایمن است؟ آیا به طول گذرواژه خود اطمینان دارید؟ کافی است یک دقیقه زمان گذاشته و این مقاله را مطالعه کنید، بعد به این دو سؤال پاسخ دهید. به تازگی یک کارشناس خبره امنیتی موفق شده است با استفاده از راهکار رایانش خوشه‌ای گذرواژه‌های متعلق به سیستم‌عامل ویندوز را در کمتر از 6 ساعت هک کند.

رایانش خوشه‌ای شامل مجموعه‌ای از سیستم‌های متصل به یکدیگر بوده که با یکدیگر کار می‌کنند. چینش این کامپیوترها به گونه‌ای است که در عمل همه آن‌ها به صورت یک کامپیوتر واحد شناخته می‌شوند. بر عکس رایانش مشبک (grid computers) در کلاسترهای کامپیوتری هر گره به گونه‌ای تنظیم می‌شود که توانایی انجام وظایف یکسانی را دارد که توسط نرم‌افزار ویژه‌ای کنترل و زمان‌بندی می‌شوند.

هفته گذشته در کنفرانس Passwords^12 از کلاستر جدیدی در اسلو نروژ رونمایی شد. جرمی گاسنی که پیش‌تر سابقه طراحی چنین سیستم‌هایی را دارد و در گذشته با استفاده از چهار کارت گرافیک رادئون مدل HD6990 موفق شده بود کلاستری را طراحی کند که توانایی پیش‌بینی 88 میلیارد پیش‌بینی در هر ثانیه را بر پایه هش NTLM داشت، از کلاستر جدید خود رونمایی کرد.

جرمی گاسنی در زمان طراحی کلاستر جدید سه سؤال اصلی را برای خود و اعضاء تیمی که روی این پروژه کار می‌کردند مطرح کرد:

مشکل: توانایی کرک کردن گذرواژه‌ها با توان زیاد

راهکار: به کارگیری تعداد زیادی GPU

سؤال فنی: چه تعداد هسته پردازشی گرافیکی برای این منظور لازم است؟

خروجی این سؤالات در نهایت باعث ساخت یک کلاستر کامپیوتر قدرتمند شده است. این کلاستر کامپیوتر قدرتمند این توانایی را دارد تا در هر ثانیه 350 میلیارد پیش‌بینی را ارائه کرده و به بهترین شکل ممکن از نرم‌افزار مجازی سازی که از 25 هسته گرافیکی (GPU) مبتنی بر کارت‌های رادئون ای‌ام‌دی استفاده می‌کند، بهره ببرد. این 64 بیتی مبتنی بر کلاستر GPU روی پلتفرم OpenCL که از پلتفرم‌های منبع باز در زمینه برنامه‌نویسی گرافیکی به شمار می‌رود و به کارت‌های گرافیکی اجازه می‌دهد روی یک کامپیوتر با یکدیگر کار کنند استفاده می‌کند.

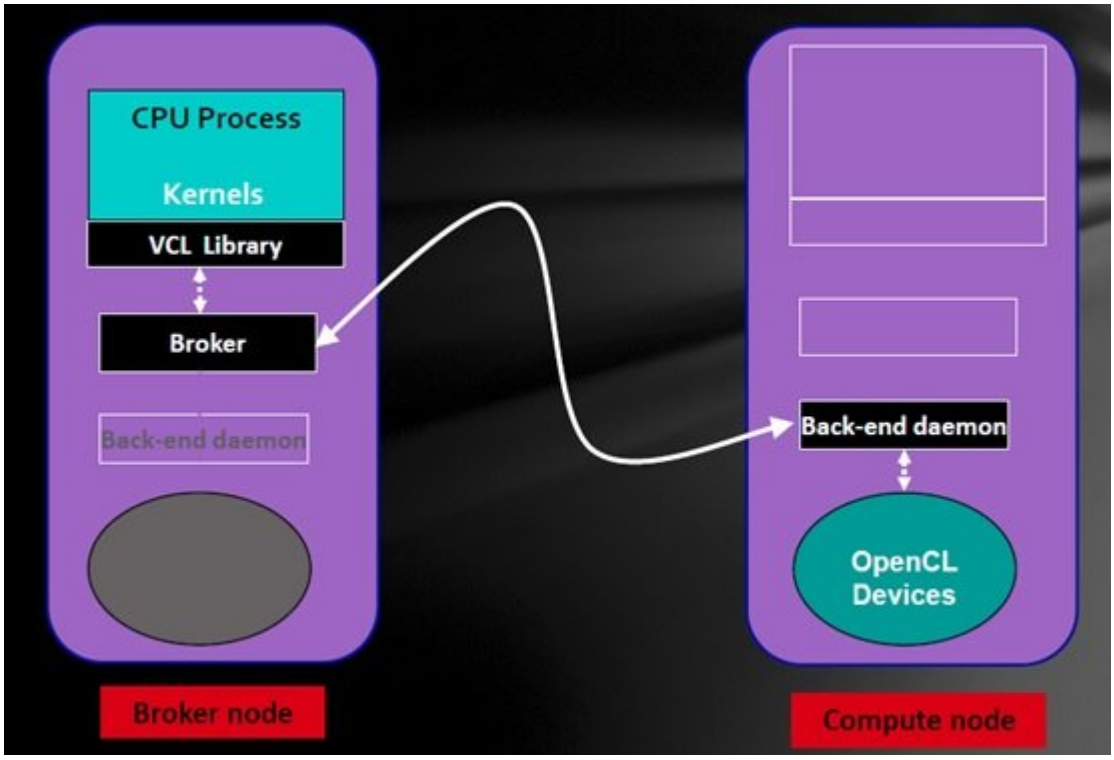
برای اطلاعات بیشتر در مورد نحوه برنامه‌نویسی گرافیکی و پردازش‌های موازی با کارت‌های گرافیکی به ویژه‌نامه آینده برنامه‌نویسی مراجعه کنید.

سایت آرس تکنیکا در این‌باره نوشته است که این کلاستر به راحتی توانایی پیش‌بینی 350 میلیارد پیش‌بینی را در هر ثانیه دارد. سرعت بالای این کلاستر به آن اجازه داده است تا در هر سیکل کاری بتواند از سد دفاعی الگوریتم رمزنگاری NTLM که مایکروسافت در سیستم‌عامل‌های ویندوز از آن استفاده می‌کند گذر کند. البته این کلاستر از بسته رایگان کرک گذرواژه‌ها موسوم به ocl-Hashcat Plus استفاده می‌کند. بسته فوق به گونه‌ای طراحی شده است که از کارت‌های گرافیک به بهترین شیوه ممکن استفاده می‌کند. گاسنی با استفاده از این ماشین موفق شده است نزدیک به 90 درصد گذرواژه‌های 6.5 میلیون کاربر سایت لینکدین را بشکند. در کنار سخت‌افزار قدرتمندی که برای این منظور استفاده شده است، کلاستر جدید از 500 میلیون گذرواژه قدرتمند و طیف گسترده‌ای از دستورالعمل‌های پیشرفته برنامه‌نویسی برای این منظور استفاده می‌کند. البته کلاستر جدید چهار برابر سریع‌تر از

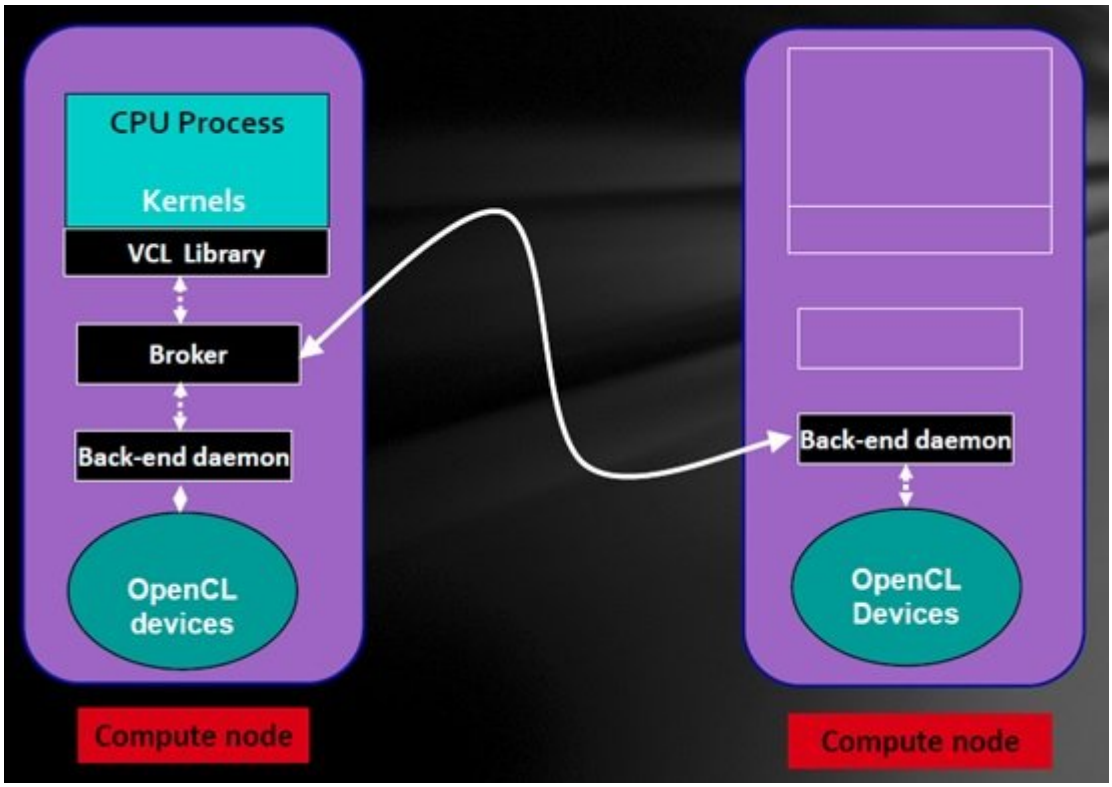
نمونه قبلی خود عمل می‌کند. به دلیل این‌که این ماشین توانایی پیش‌بینی 64 میلیارد گذرواژه مبتنی بر الگوریتم SHA1 که توسط لینکدین مورد استفاده قرار می‌گیرد را دارد. این کلاستر همچنین این توانایی را دارد تا 180 میلیارد ترکیب گذرواژه را زمانی که از الگوریتم رمزنگاری MD5 استفاده شده باشد پیش‌بینی کند که در مقایسه با نمونه قبلی خود چهار برابر سریع‌تر است. در یک دهه اخیر به کارگیری محاسبات مبتنی بر پردازنده‌های گرافیکی به ویژه برای شکستن آفلاین گذرواژه‌ها رواج زیادی پیدا کرده است. اما تا به امروز محدودیت‌هایی در ارتباط با مادربردها، بایوس سیستم‌ها و درایورهای سخت‌افزاری و کارت‌های گرافیکی وجود داشت.

آمار و ارقام‌های ارائه شده درباره این کلاستر نشان می‌دهند که کلاستر فوق توانایی ترکیب کردن 95 به توان 8 گذرواژه را در 5 ساعت و نیم دارد. این مجموعه شگفت‌انگیز این توانایی را دارد تا به هر گذرواژه 8 کاراکتری که ترکیبی از ارقام، کاراکترهای بزرگ و کوچک و سمبل‌ها است به راحتی نفوذ کند. پلتفرم خوشه‌ای Virtual OpenCL همراه با ocl-Hashcat Plus که یک ابزار کرک گذارواژه است کار می‌کند. البته لازم به توضیح است که این کلاستر محدود به حملات brute force نیست و این توانایی را دارد تا از تکنیک‌های دیگری شبیه به لغت‌نامه هکری برای شکستن هر ترکیبی از گذرواژه‌ها استفاده کند. جرمی ام گاسنی مدیرعامل و مؤسس Stricture Consulting Group در این‌باره به سایت آرس تکنیکا گفته است: « در گذشته مردم از VCL و راهکارهای مختلفی برای دستیابی به سطحی از موفقیت استفاده می‌کردند.» او در ادامه صحبت‌های خود افزود: «VCL به عنوان آخرین راهکار می‌تواند مورد استفاده قرار گیرد، ما اکنون راه‌حلی در اختیار داریم که خارج از چهارچوب موجود عمل کرده و توانایی اداره کردن خودکار پیچیدگی‌ها را دارد. همچنین به آسانی مدیریت می‌شود، به دلیل این‌که همه گره‌های محاسباتی شما فقط و فقط روی VCL نصب می‌شود. شما نرم‌افزار خود را روی یک کنترلر کلاستر نصب می‌کنید.»

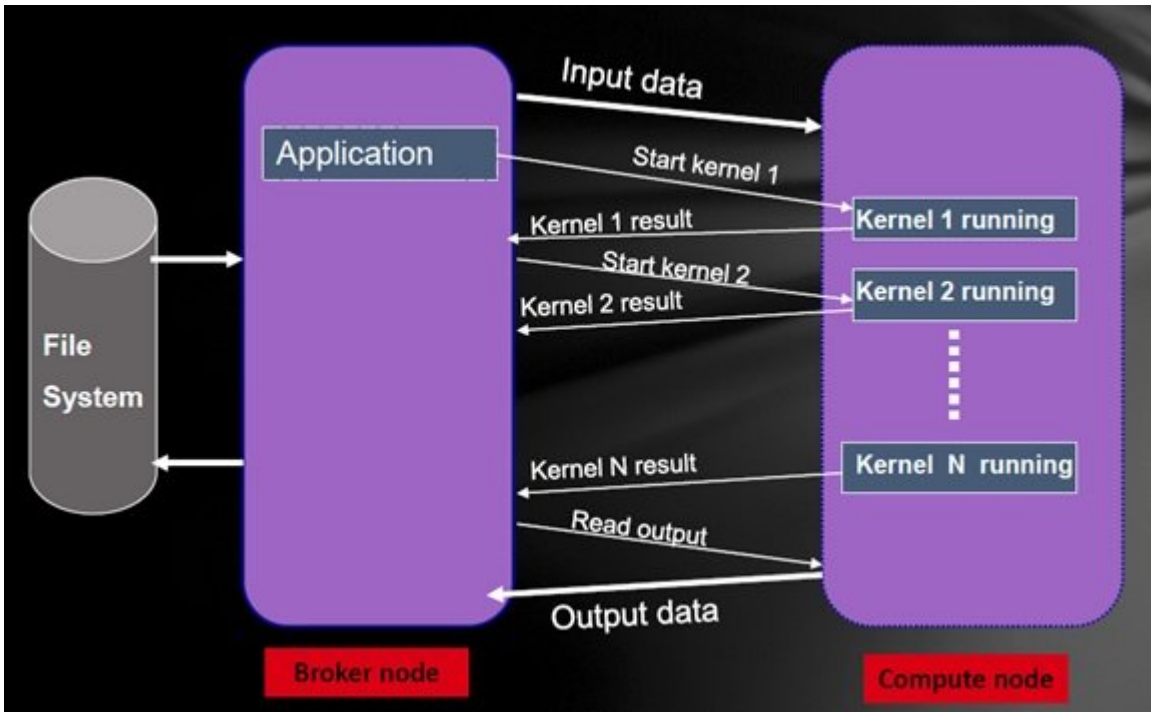
معماری پایه و اصلی VCL همانند تصویر زیر است:



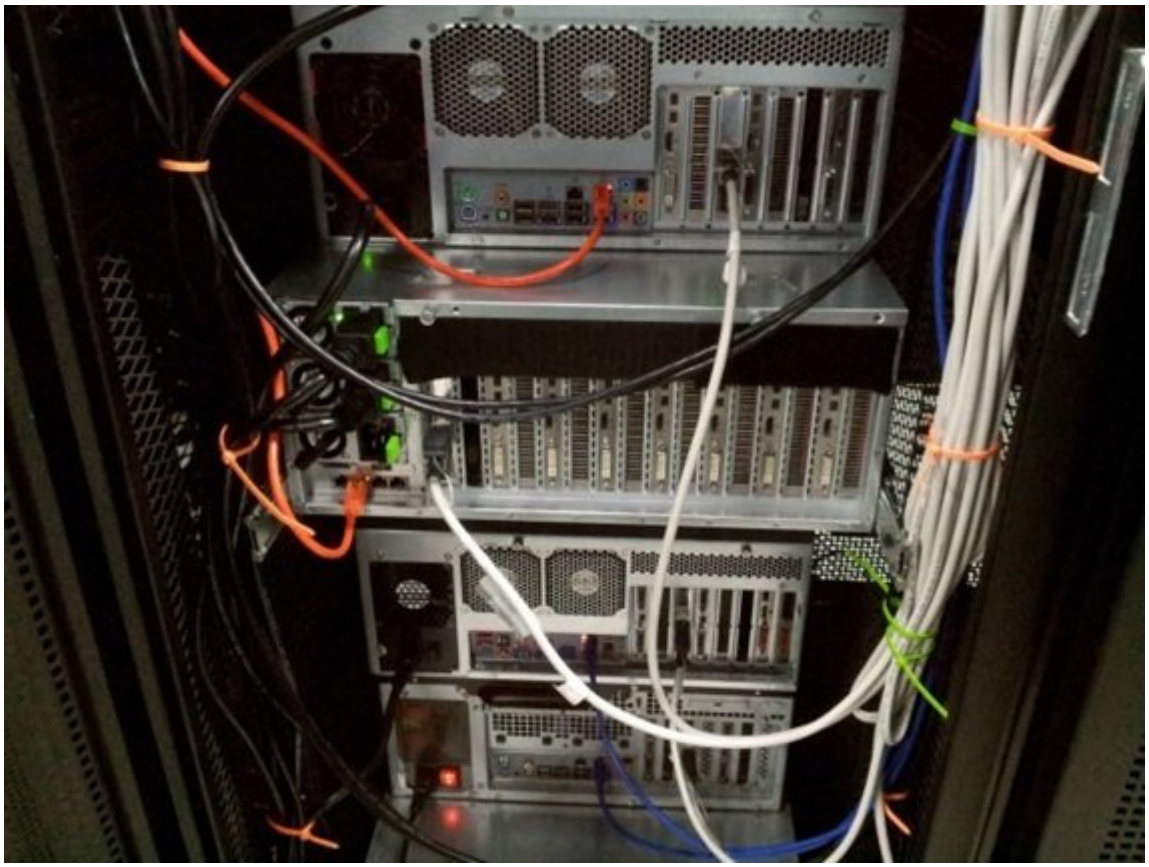
اما جرمی معماری خود را به جای الگوی استاندارد VCL پیشنهاد کرده است. این معماری را در تصویر زیر مشاهده می‌کنید:



در نهایت چرخه کاری VCL همانند تصویر زیر خواهد بود.



تصویر زیر نمای فیزیکی این کلاستر را نشان می دهد



اجزاء تشکیل دهنده این کلاستر عبارتند از:

Five 4U servers

25 AMD Radeon GPUs

10x HD 7970

4x HD 5970 (dual GPU)

3x HD 6990 (dual GPU)

1x HD 5870

4x SDR Infiniband interconnect

7kW of electricity

همان‌گونه که مشاهده کردید، شکستن گذرواژه‌ها بر خلاف آن‌چه بسیاری از کاربران تصور می‌کنند کار پیچیده‌ای نبوده و دیگر همانند گذشته نیست که یک هکر ماه‌ها برای انجام چنین کاری وقت سپری کند.

تاریخ انتشار:
23 مهر 1394

نشانی منبع: https://www.shabakeh-mag.com/information-feature/1902