ماهنامه علمی خبری

عصر رایانه

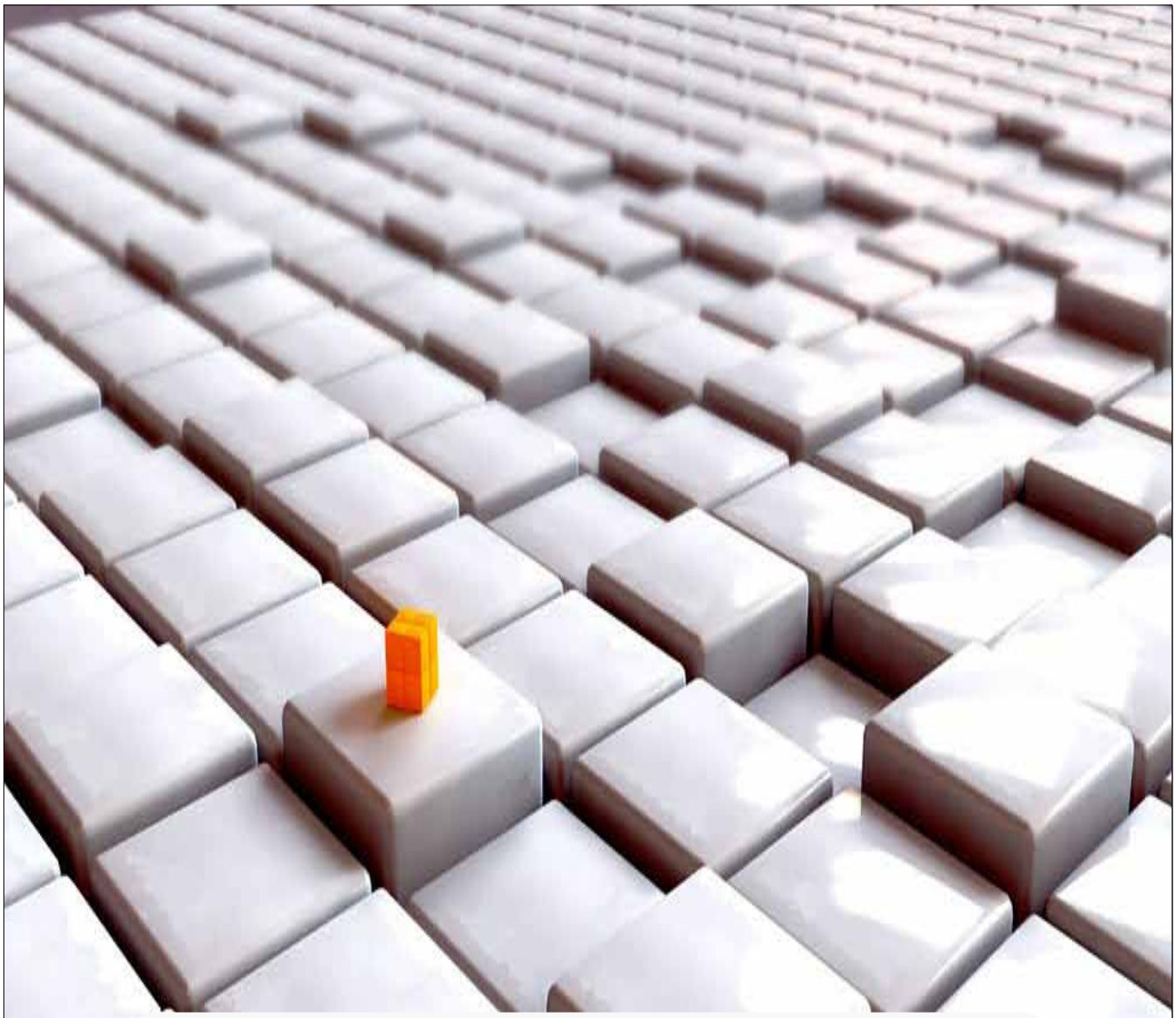
شماره ۸ - خرداد ۱۳۹۰ - ۱۶ صفحه - ۲۰۰ تومان

ماجرای عجیب و غریب هک شدن SSL !


فیس بوک
آینه ی جادویی


iPad2


کامپیوتر ها
مغز ندارند !



فرهنگ کامپیوتری

کامپیوترِ فرهنگی! چه ترکیب غریب و بی معنایی است! یعنی یک کامپیوتر آغشته به فرهنگ باشد؛ یعنی فرهنگ داشته باشدَ. کامپیوترها حتی عقل و شعور هم ندارند چه برسد به فرهنگ! کامپیوترها بزرگترین نقشی که ایفا می کنند نقش یک ابزار مدرن، کارآمد و سریع است. کامپیوتر به زندگی بشری خدمت می کند. کامپیوتر هیچگاه بر زندگی انسانها غالب نمی شود!

فرهنگ کامپیوتری! یعنی یک فرهنگ آغشته به کامپیوتری؛ یعنی یک فرد کامپیوتری فرهنگ داشته باشد. یعنی یک فرهنگِ[1] خاص برای کامپیوتری ها وجود داشته باشد. کامپیوتری ها اصلی ترین نقش را در حیات بشری دارند، چرا که ساده تَرین کار آنها طراحی، ساخت و کنترل اصلی ترین ابزار زندگی مدرن بشری است! کامپیوتری ها به بشریت خدمت می کنند. کامپیوتری ها بر زندگی انسانها مسلط هستند!

آری کامپیوتری ها برترینند! این را نه از روی تکبر، غرور و... بلکه از روی واقعیت می گویم. کامپیوتری ها ذهنی متفاوت و طرز فکری آزاد دارند. مولد و خلاق اند و همواره زنده! اگر قبول ندارید به اطراف خود نگاه کنید، چگونه است که به سادگی تشخیص می دهید یک نفر کامپیوتری است یا نه؟! چرا که کامپیوتری ها خاص اند!

---

۱ - ویکی پدیا: فرهنگ، واژه ای است درباره شیوه زندگی مردم؛ به معنی روشی که مردم، کارها را انجام می دهند. گروههای متفاوت مردم، ممکن است که فرهنگ های متفاوتی را دارا باشند. فرهنگ، بوسیله آموزش، به نسل بعدی منتقل می شود؛ در حالی که ژنتیک بوسیله وراثت منتقل می شود. ادوارد تایلور (۱۹۱۷–۱۸۳۲)، فرهنگ را مجموعه ی پیچیده ای از دانشها، باورها، هنرها، قوانین، اخلاقیات، عادات و هرچه که فرد بعنوان عضوی از جامعه، از جامعه خویش فرا می گیرد، تعریف می کند.

فهرست مطالب

سخن سردبیر

روز ثبت‌نام ورودی‌های ۸۹ بود. ثبت نام با ایده‌ی نابِ نمی‌دانم کی، داشت در کتابخانه‌ی دانشکده برگزار می‌شد (از اون حیث می‌گم ناب چون تونست همون روز اول به همه‌ی دانشجویان بفهمونه که وارد چه جور دانشگاهی شدند). در همان حینی که ثبت‌نام انجام می‌شد آمفی تئاتر دانشکده پر بود از مسئول‌های ریز و درشت. قرار بود طبق معمولِ برنامه‌های مفرح دانشگاه !!! مسئولین به نوبت برن پای تریبون و صحبت کنند. هرکسی که می‌رفت پای تریبون کم نمی‌ذاشت، خوبی بود که از دانشگاه می‌گفت. انگشت حیرت به معده‌هایمان رسیده بود که یا ما کور بودیم این خوبی‌ها را ندیدیم یا مسئولین از افعال معکوس استفاده می‌کردند (البته ورودی‌های جدید هم انگشت به دهن مونده بودن که وارد چه دانشگاه خفنی شدند!). یادم هست سال ۸۸ در برنامه‌ی گردهمایی کامپیوتری‌ها به درخواست دوستم رفتم پای تریبون تا چند بیتی شعر بخونم، بس که صدایم لرزید یحتمل کسی چیزی از آن شعر نفهمید. ولی این مسئولین پشت میکروفن انصافن خوب حرف می‌زنن. به معنای دقیق‌تر خوب دروغ می‌گن. دروغ؛ چون هیچ‌کدوم از اون مسئولین نگفتن اگر فلان افتخاری که از آن دم می‌زنم و یکسره به مصادره‌ی خودم در میارم، حاصل تلاش دانشجویان بوده (بدون سر سوزن حمایت از طرف من مسئول). دروغ؛ چون کسی نگفت دانشجویان برای شرکت در مسابقات مختلف از جیب خود هزینه می‌کنن.

اتفاقاً چند روز پیش، برای گرفتن مجوز برگزاری کلاسی، سر و کارم به ساختمان مرکزی افتاد. پس از تمام شدن استراحت آقایان! ، طبق معمول کارم به نتیجه نرسید.

در راه برگشت دیدم مسؤلین در و دیوارهای ساختمان مرکزی رو پر کردن از تبریکات مختلف به همدیگه، البته نه اینکه فکر کنین رنگ و بویی از چاپلوسی در آن بودها، اصلاً و ابداً! ولی بسیار کنجکاو شدم ببینم آیا بنری، پوستری، چیزی روی دیوار هست که در آن از دانشجویی تجلیل شده باشد، دریغ از یه کاغذپاره. حتی به آبدارخونه هم سرک کشیدم،گفتم شاید شیر پاک خورده ای با ماژیک روی دیوارش از دانشجویی قدردانی کرده باشد، یافت می‌نشد (آنچه یافت می‌نشود آنم آرزوست).

خلاصه فقط دونستن دو نکته برای شما دانشجویان این دانشگاه گل و بلبل بسه تا بفهمید تو چطور دانشگاهی دارین درس می‌خونین. اول اینکه بچه‌های رباتیکَ دانشگاه از جیب خودشون پول گذاشتن و رفتن مسابقات شرکت کردن و دانشگاه خودش رو زد به کوچه‌ی علی چپ که اصلاً موضوع چیه، کی؟! من؟! کی؟! این؟! ...

بعدشم تو همون مسابقاتی که گفتم، یک استاد شاخص از طرف تمام دانشگاه‌های تهران، برای حمایت از تیم دانشگاه‌هشان آمده بود، حتی دانشگاه آزاد، ولی این تنها دانشگاه پر افتخار خواجه نصیر بود که هیچ نماینده‌ای از طرف دانشگاه نداشت و این هم برای ما دانشجویان خیلی غرور انگیزه!!!

انشاء ا...

دانشگاه صنعتی خواجه نصیرالدین طوسی
انجمن علمی کامپیوتر و روبوتیک

گاهنامه علمی خبری

عصر رایانه

شماره ۸، خرداد ۱۳۹۰، ۱۶ صفحه
شمارگان: ۵۰۰ نسخه

صاحب امتیاز:
انجمن علمی کامپیوتر و روبوتیک
info@nasircom. com

مدیر مسئول:
محمد امینی
M. Amini@ee. kntu. ac. ir

سردبیر:
محمد حسام کلانتری
Kalantari. hesam@ee. kntu. ac. ir

دوستان یاری دهنده این شماره:
افشین جمشیدی
jamshidi. afshin@gmail. com
مجتبی قربانعلی بیک

حسین یاوری
zx4jj@yahoo. com
ویراستار: فریده داش خانه
farideh. d92@gmail. com
صفحه آرا: محمد حسن نیرومند
mh. niroomand91@yahoo. com

می توانید مطالب خود را براي ما بفرستید. عصر رایانه در چاپ یا عدم چاپ و ویرایش مطالب ارسالي آزاد است.
asrerayane@nasircom. com

عکس روی جلد:
به بهانه ی انتشار ubuntu 11.04 و جشن انتشار اوبونتو 11.04 در دانشکده ی کامپیوتر و برق دانشگاه صنعتی خواجه نصیرالدین طوسی.

iPad 2

فاطمه قائم پناه

صف تشکیل شده برای خرید آی‌پَد۲ در اولین روز فروش

تبلت (tablet)، محصولی که در نگاه اول گمان نمی‌رفت با استقبال عظیم مردم روبرو شود، بعد از معرفی توسط شرکت اپل (Apple)، بدل به یک فرهنگ شد. دیگر کمتر کسی را می‌توان پیدا کرد که تبلت نداشته باشد یا سودای تصاحب و آزمایش آن را در سر نپرورانده باشد. تا به حال اپل سه محصول راهبردی تولید کرده است که پی‌سی (PC) را محو کرده‌اند. اپل از آی‌پاد (iPod) شروع کرد و بعد آی‌فون (iPhone) را تحویل داد و سرانجام نوبت به محصول انقلابی آی‌پد (iPad) رسید. امروزه اپل به تنهایی ۹۰ درصد بازار تبلت دنیا را در دست دارد و همه رقبا را محو کرده است. تا به حال ۶۵۰۰۰ نرم افزار (App: Application software) به صورت اختصاصی برای آی‌پد نوشته شده است. امروزه مدارس هم از آی‌پد استفاده می‌کنند. پزشکان نیز استفاده گسترده از آی‌پد را شروع کرده‌اند و حتی در جراحی‌هایی مثل جراحی مغز هم، آی‌پد کاربرد پیدا کرده است. آی‌پد به کودکان مبتلا به اوتیسم (نوعی اختلال رشدی است که با رفتارهای ارتباطی و کلامی غیر طبیعی مشخص می شود) نیز کمک می‌کند، این وسیله گرچه بیماری این کودکان را درمان نمی‌کند، اما به آنها یاری می‌رساند.

تازه به اصل داستان رسیدیم، یعنی معرفی iPad2:

۱) طراحی تازه، پردازنده قوی‌تر: نخست گفته شده که این تبلت، طراحی کاملا تازه‌ای دارد و مجهز به تراشه جدیدی به نام تراشه A۵ است. این تراشه حاوی پردازنده ای دو هسته‌ای است که توان پردازشی آی‌پد را دو برابر و توان پردازش گرافیکی آن را ۹ برابر می کند !! اما با وجود این عملکرد بالا، مصرف برق این تراشه به اندازه تراشه A۴ است.

۲) دوربین: همان طور که گمان می رفت، آی‌پد ۲، دوربین جلو و عقب خواهد داشت. همچنین مجهز به ژیروسکوپ (وسیله‌ای برای اندازه گیری و یا حفظ جهت می‌باشد که از اصل بقای تکانه ی زاویه ای استفاده می‌کند.) هم خواهد بود. از آنجا که آی‌پد ۲، دوربین دارد، تعدادی نرم‌افزار برای کار با عکس به صورت پیش‌فرض در سیستم عامل جدید گنجانده شده است. یکی از آنها Photo Booth است. آی‌پد ۲ از لحاظ توان پردازشی آنقدر قوی است که می‌تواند ۹ ویدئوی جاری را به صورت همزمان به نمایش بگذارد. FaceTime هم یک App کنفرانس ویدئویی است و حالا در آی‌پد۲ هم کاربرد پیدا می‌کند. نوبت به معرفی نرم‌افزار iMovie می رسد. با این نرم‌افزار می‌توان به راحتی ویدئو را ویرایش کرد و یا در یوتیوب، فیس‌بوک و... به اشتراک گذاشت. نرم‌افزار بعدی GarageBand است. با این نرم‌افزار می‌توان آلات موسیقی مختلفی از پیانو گرفته تا گیتار و از درام تا ارگ را شبیه‌سازی کرد و به صورت لمسی آنها را نواخت.

۳) تبلتی نازک‌تر و سبک‌تر: آی‌پد ۲، ۳۳٪ از آی‌پد فعلی نازک‌تر خواهد بود، یعنی ضخامت آن از ۱۳/۴ میلیمتر به ۸/۸ میلیمتر، کاهش می‌یابد. این محصول، حتی از آی‌فون ۴ هم باریک‌تر است! وزن آی‌پد ۲، ۵۹۰ گرم است، در حالی که آی‌پد ۱، ۶۸۰ گرم وزن داشت. این یعنی یک وزن کاملا معقول. خوشبختانه آی‌پد ۲، همان طول عمر مفید شارژ ۱۰ساعته ی آی‌پد ۱ را دارد. اگر این تبلت در حالت stand by قرار بگیرد، شارژ آن یک ماه دوام می‌آورد!!

۴) خروجی HDMI: آی‌پد ۲، خروجی HDMI خواهد داشت! یعنی می‌تواند با کیفیت ۱۰۸۰p، ویدئو پخش کند. تازه، با همه نرم افزارها هم کار می‌کند!

۵) کاور هوشمند: اپل یک کاور بی‌نظیر برای آی‌پد۲ طراحی کرده است. این کاور، فقط کاور نیست! وقتی این کاور را از روی صفحه نمایش آی‌پد ۲ برمی‌دارید، تبلت خود به خود بیدار می‌شود و وقتی آن را روی تبلت می‌گذارید، تبلت به خواب می‌رود! این کاور وزن و ضخامت قابل توجهی ندارد، ازالیاف میکرو ساخته شده است و صفحه نمایش را تمیز می‌کند! و در پنج رنگ مختلف در دسترس خواهد بود.

از دید اپل، فناوری، همه چیز نیست و چیزی که اهمیت دارد، آمیختگی فناوری با انسانیت و علوم انسانی است. بر این اساس سخت‌افزار و نرم‌افزار باید بیشتر از دوره پی‌سی درهم تنیده و یکی شوند.

OS	iOS 4. 3. 2
Power	Built-in rechargeable Li-ion battery 25 W-h (90 KJ)
CPU	1st Generation: 1 GHz Apple A4 2nd Generation: 1 GHz Apple A5
Storage	16,32,or 64 GB flash memory
Memory	1st Generation: 256 MB DDR RAM 2nd Generation: 512 MB DDR2 RAM

OS	OS 4. 3. 2 Released April 14 , 2011
Power	Internal rechargeable non-removable 25 W-h (90 KJ) lithium-polymer battery
CPU	1 GHz dual-core (up to 2GHz) Apple A5
Storage Capacity	Flash memory 16 , 32 ,or 64 GB
Memory	512 MB DDR2 (1066 Mbit/s) RAM

Google Web Toolkit

امیرحسین بیات

چکیده

ماموریت GWT بهبود ریشه ای کیفیت app های تحت وب، با قادر ساختن توسعه گرها به استفاده از ابزارهای فعلی جاوا در تولید appهای Ajax با کیفیت بالا برای تمام مرورگرهای مدرن است. GWT گام بزرگی جهت کم کردن فاصله app های وب با appهای ویندوز است. GWT انتخاب مناسبی برای تولید Enterprise application ی تحت اینترانت و اینترنت است.

مقدمه

از اوایل سال ۲۰۰۵، که Ajax توسط یک معمار اطلاعات معرفی شد، تا بحال تکنولوژی ها و ابزارهای زیادی مبتنی بر آن ارائه شده است. جالب است که پس از گذشت ۲۰سال، برنامه نویس های Ajax با مشکلاتی دست و پنجه نرم می کنند که برنامه نویس های آن زمان در برنامه های TSR تحت DOS با آن روبرو بودند. البته خیلی از این مشکلات توسط framework های مختلفی که برای Ajax ارائه شده، برطرف شده است. مثلا در ATLAS که مایکروسافت ارئه کرده است، برنامه نویسی Ajax بسیار ساده شده است، ولی جالب است که خود مایکروسافت تمایل زیادی به استفاده از آن ندارد! مایکروسافت در واقع به همان اندازه که کار را ساده کرده، از کیفیت و کارایی آن نیز کاسته است؛ به نحوی که برنامه نویس ها در حین کار با Atlas بزودی متوجه می شوند که اساساً خیلی از کارها را با Atlas نمی توانند انجام بدهند و در مواردی که انجام می شود سرعت و قابلیت اطمینان آن رضایت بخش نیست. از بین تمام پیاده سازیهایی که از Ajax شده شاید بتوان Gmail و Google Map را جز بهترین به حساب آورد؛ به نحوی که شرکت های معظمی مانند یاهو و مایکروسافت هنوز نتوانسته اند محصولات قابل رقابتی با آنها ارائه کنند.

در اقدامی غیر منتظره در ماه می ۲۰۰۶، گوگل اقدام به ارائه frameworkای برای تولید appهای Ajax، مبتنی بر تجربه موفقgamil و google map نمود. همان گونه که از گوگل انتظار می رود، GWT کاری بزرگ ، باکیفیت و سرشار از ایده های نو است، که انتظار می رود تحول بزرگی را در تولید نرم افزار ایجاد کند و در بسیاری از موارد، انتخاب بهتری از appهای معمولی ویندوز (rich client) و یا وب باشد.

GWT

Google web toolkit یک framework سورس باز جاوا است که به شما امکان می دهد که از تکنولوژهایی که تولید appهای Ajax را دشوار و مستعد باگ می کنند، رهایی یابید. با GWT می توانید appهای java را با ابزارهای دلخواه java توسعه دهید و دیباگ کنید. زمانی که کار شما آماده ارائه به تولید شد، کامپایلر GWT آن را به javascript و html ی که با انواع مرورگرها سازگاری دارد، ترجمه می کند.

تفاوت GWT با frameworkهای دیگر، این است که شما کد سمت مرورگر را بجای javascript با java می نویسید. و این به این معنی است که شما از منابع و ابزارهای بسیار زیادی که هم اکنون در java موجود است، در طرف مرورگر (client side) استفاده کنید. همچنین شما می توانید از مزایای OOP، مانند encapsulation و ارث بری در طرف مرورگر بهره مند شوید و همچنین می توانید کد طرف مرورگر را به صورت واقعی دیباگ کنید. هسته GWT یک کامپایلر java به javascript است که کد جاوا اسکریپت سازگار با مرورگرهای ،Firefox ،Internet Explorer ،Safari ،Mozilla و Opera را تولید می کند. به همراه GWT یک کتابخانه از کنترلهای متداول مانند منو، پنل، کلید، درخت و .... عرضه شده است.

ساختار GWT

GWT ابزارهای جامعی را درخور چالشهایی که برای تولید rich internet application وجود دارد، گرد هم آورده است.

Java to js compiler، در طرف مرورگر، کدهای جاوا را به جاوا اسکریپت تبدیل می کند.

JSNI، کار فراخوانی مستقیم کد جاوا اسکریپت از جاوا را انجام می دهد.

JRE Emulation، یک زیر مجموعه از Java runtime library که برای برنامه نویسی سمت Client استفاده می شود.

Widgets and Panels، مجموعه ای از کنترلها که در GWT برای ساختن UI از آن استفاده می شود.

I18N، چند تکنیک برای بین المللی کردن app و تنظیمات مرتبط با آن ارائه می کند.

RPC، پیاده سازی گوگل از remote procedure call برای ارتباط برقرار کردن کدهای client با کدهای سمت سرور.

XML Parser، با توجه با اهمیت و گسترش روز افزون XML, GWT کلاسهایی را برای کار با آن فراهم آورده است.

Managing the browser history ، یکی از اشکالات موجهی که به rich internet application ها گرفته می شود، این است که آنها کلید برگشت مرورگر (back button) را نقض می کنند. این از آنجا ناشی می شود که وقتی شما با جاوااسکریپت محتوای صفحه را به صورت داینامیک عوض می کنید، کاربر انتظار دارد که با زدن کلید برگشت به حالت قبل بازگردد، ولی این اتفاق می افتد زیرا مرورگر متوجه تغییرات داینامیک شما نمی شود. GWT این مشکل را برطرف نموده است.

JUnit Integration همیشه نوشتن کدهایی برای تست برنامه به صورت اتوماتیک، تکنیک خوبی محسوب می شود. در حال حاضر frameworkهای متعددی سالهاست که این پروسه را ساده تر کرده اند، JUnit یکی از بهترین آنها برای توسعه گرهای جاوا است. GWT بجای نوشتن این framework از ابتدا، ازJUint پشتیبانی می کند.

مزایا:

زمان توسعه

GWT با فراهم آوردن امکان استفاده از جاوا در سمت کلاینت و سرور، امکان دیباگ واقعی هر دو طرف، استفاده از OOP در سمت UI ، بعهده گرفته سازگار بودن کد تولید شده با انواع مرورگرها، فراهم آوردن امکان استفاده از ابزارها و frameworkهای موجود جاوا، صرفه جویی بسیار زیادی را در زمان توسعه و پشتیبانی appهای Ajax به همراه دارد.

سرعت و کیفیت اجرا

appهای GWT همیشه به اندازه appهایی javascript که با دست نوشته می شوند، سریع اجرا می شوند. تیم GWT وسواس بسیار زیادی در این زمینه به خرج داده است؛ مثلا تمام تصاویر صفحه را، در سمت سرور به یک تصویر تبدیل می کند و در سمت کلاینت فقط بایک request آن را دریافت می کند، و به تصاویر اصلی می شکند. GWT همچنین در انتخاب اسم متغیرها و حتی فضای خالی بین کدها بهینه عمل کرده است. در نسخه اخیرGWT (۱.۴) ، برای دریافت جاوا اسکریپت و CSS ها از طرف سرور، از متد PKZip استفاده شده است.

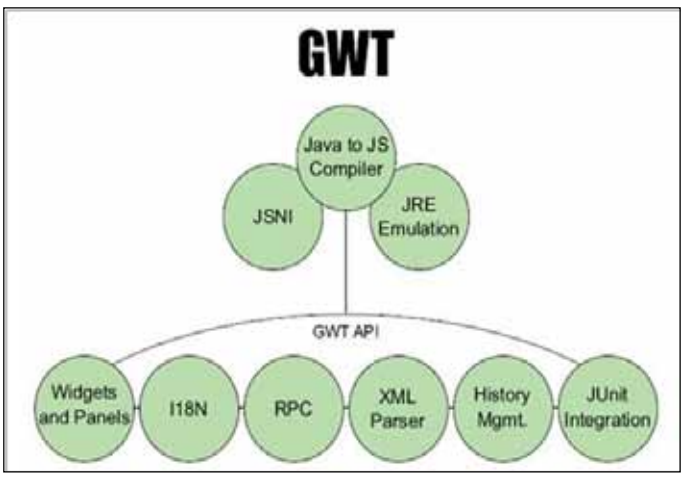
اندازه جاوا اسکریپت تولید شده

اندازه جاوا اسکریپت تولید شده برای یک برنامه کاربردی معمولیGWT با تمام امکانات حدود ۱۰۰ کیلوبایت خواهد بود، که قابل cache شدن بوسیله مرورگر نیز می باشد، بعد از آن فقط تکه های کوچک اطلاعات هستند که رد و بدل می شوند.

پهنای باند مورد استفاده

GWT مانند appهای معمولی وب postback ندارد و فقط اطلاعات مورد نیاز هستند که رد و بدل می شوند، در مقایسه با appهای معمولی وب که حتی با تیک زدن یک checkbox کل صفحه postback می شود و دوباره load می گردد، پهنای باند و ترافیک ss به طور قابل توجه ای صرفه جویی می شود.

ادامه در صفحه ی بعد...



ادامه از صفحه قبل

GWT

امنیت

GWT اطلاعات کمتری را در سمت کلاینت باقی می گذارد، که به صورت javascript فشرده شده است و قابلیت خوانایی ندارد، در نتیجه امنیت بهتری حاصل می شود

حل مشکلات پرداخت online

GWT برای مشکلاتی که به هنگام پرداخت آنلاین پیش می آید، راه حل های قطعی ارائه می دهد (حداقل در تئوری).

عدم وابستگی به platform

GWT مبتنی بر جاوا است و کد تولید شده توسط آن جاوااسکریپت و HTML معمولی است که باعث می شود به plateform وابسته نباشد.

سورس باز

GWT سورس باز (Open source) است که کمک زیادی به توسعه اجزاء و درک مکانیزم های آن می کند. همچنین تجربه نشان داده است که پروژهای سورس باز به دلیل داشتن توسعه گرها یی که در تمام جهان پراکنده هستند، بهتر پیشرفت می کنند و پشتیبانی بهتری دارند.

معایب

شرکتهایی که از GWT برای پیاده سازی وب سایت ها استفاده می کنند، ممکن است با این مشکل روبرو شوند که موتورهای جستجو محتوای صفحات آنها را ایندکس نمی کند. این مشکل در واقع مربوط به تمام وب سایتهای داینامیک می گردد و از آنجا ناشی می شود که وقتی محتوای صفحات بوسیلهjavascript تغییر می کند، آدرس آن ثابت می ماند؛ بنابراین موتورهای جستجو شاخصی برای دسترسی به صفحه جدید را ندارند. برای این مشکل راه حل های متعددی ارائه شده است مثلا یک وب سایت موازی استاتیک با وب سایت داینامیک وجود داشته باشد، که تاحدی مشکل را برطرف نموده اند.

نتیجه گیری

GWT قدرت appهای ویندوز را به app های وب می دهد و به شما امکان می دهد که نرم افزارهای تحت اینترانت و اینترنت غنی تر را در زمان کمتری تولید کنید. هزینه نگهداری آنها نیز به مراتب پایین تر خواهد بود. GWT نیز مانند جاوا دارای منابع فراوان به صورت وب سایت، کتاب، مقاله، ویدئو، کد آماده و ابزارهای 3rd party مانند GWT Designer است. GWT محصول زیربنایی شرکت گوگل در مدت کوتاهی که عرضه شده، رشد قابل توجهی داشته است و انتظار می رود که platform عمده برای تولید appهای دینامیک باشد. (برای مشاهده آهنگ رشد GWTو همچنین مقایسه بین فراگیر بودن java نسبت به C#، به www.google.com/trends مراجعه کنید و عبارت gwt یا java,C# را تایپ کنید)

برگرفته از: knol. google. com

فناوری محاسبات ابری و نگرش‌های گوناگون

حسین یاوری

براساس گزارش های منتشر شده، هر چند فناوری ابر یا کلاود مزیت‌های متعددی مانند هزینه کمتر و سهولت مدیریت دارد، اما موارد امنیتی همچنان یکی از عواملی است که گسترش این فناوری را کند کرده‌است. بررسی‌های اخیر مؤسسه تحقیقاتی فورستر نشان می‌دهد، بسیاری از شرکت‌ها و مراکز مختلف از سرویس‌های عمومی محاسبات ابری پرهیز می کنند؛ زیرا درباره امنیت داده‌های شرکتی خود مطمئن نیستند.

طبق بررسی‌های مؤسسه تحقیقاتی فورستر، تنها ۲۱ درصد مدیران آی‌تی اظهار داشته‌اند، مراکز آن‌ها در سال ۲۰۱۰ از سرویس‌های عمومی ابر تحت عنوان Iaas (سرنام Infrastructure-As-a-Service) استفاده کرده یا در آینده بیشتر استفاده خواهند کرد. خدمات عمومی محاسبات ابری باعث می‌شود تا شرکت‌های گوناگون بتوانند در شبکه اینترنت و باتوجه به میزان نیاز خود از نرم‌افزارها، قدرت محاسباتی و نیز منابع ذخیره‌سازی شرکت ارائه‌دهنده این خدمات بهره ببرند و این مزیت آن‌ها را از خرید تجهیزات اختصاصی بی‌نیاز می‌کند.

با وجود این، آن دسته از مدیران آی‌تی که در نظرسنجی فورستر شرکت کردند، نسبت به استفاده از خدمات ابری خوش‌بین نبودند و ۶۴ درصد آن‌ها اعلام کردند که مطمئن نیستند داده‌های کاریشان واقع در مراکز داده شرکت سرویس‌دهنده از امنیت کافی برخوردار باشند. نظرسنجی مؤسسه SunGard Availability Services از صد نفر از مدیران مالی شرکت‌ها نیز نشان می‌دهد، ۵۶ درصد این افراد به دلیل ترس درخصوص امنیت داده‌های حساس، در بخش خدمات عمومی ابر سرمایه‌گذاری نکرده‌اند.

مدیران مالی درباره مزیت‌های محاسبات ابری شک دارند و همین امر یکی از علل بی‌میلی آن‌ها در استفاده از این خدمات محسوب می‌شود؛ ضمن این‌که تنها ۳۴ درصد از این افراد اظهار داشتند، مزایای انتقال سیستم‌های آی‌تی به پلتفرم ابر را کاملاً درک کرده‌اند. از این‌رو چنین به نظر می‌رسد که برخی از مسئولان سازمان‌ها هنوز از ماهیت و کم و کیف این فناوری آگاهی چندانی ندارند.

نگرانی‌ها درباره امنیت خدمات عمومی cloud باعث شده تا برخی از شرکت‌ها، دیتاسنترهای اختصاصی یا درون سازمانی خود را به کلاودهای خصوصی تبدیل کنند که در این صورت این تجهیزات

بیشتر سازمان‌های بزرگ می‌خواهند همان سرویس‌های عمومی ابر را در درون مراکز داده خود ایجاد کنند، زیرا در این‌صورت می‌توانند بر نحوه استفاده از سرویس‌ها نظارت داشته و از امنیت دارایی‌های حساس سازمان اطمینان حاصل کنند

آی‌تی همان خدماتی را ارائه می‌کنند که در کلاودهای عمومی عرضه می‌شوند، با این تفاوت که چون تجهیزات تحت نظارت مستقیم خود شرکت‌ها است، درخصوص امنیت آن اطمینان بیشتری وجود دارد.

در نظرسنجی فورستر تقریباً یک چهارم (۲۵ درصد) رؤسای آی‌تی که مورد نظرسنجی واقع شدند، گفتند، ایجاد کلاود خصوصی یکی از اولویت‌های آن‌ها در سال ۲۰۱۰ بوده که این آمار در سال ۲۰۰۹ برابر نوزده درصد بود. چنین به نظر می‌رسد که شرکت‌های بزرگ‌تر به ایجاد زیرساخت‌های خصوصی ابر تمایل بیشتری دارند؛ زیرا بیش از شصت درصد شرکت‌هایی که ایجاد کلاود خصوصی را جزء اولویت‌های خود قلمداد کردند، بیش از هزار کارمند داشتند.

جیمز استاتن از تحلیلگران فورستر در گزارشی اظهار می‌دارد، بیشتر سازمان‌ها هنوز مایلند سیستم‌های آی‌تی خود را در خود سازمان نگه‌داری کنند. به گفته او بیشتر سازمان‌های بزرگ می‌خواهند همان سرویس‌های عمومی ابر را در درون مراکز داده خود ایجاد کنند؛ زیرا در این‌صورت می‌توانند بر نحوه استفاده از سرویس‌ها نظارت داشته و از امنیت دارایی‌های حساس سازمان اطمینان حاصل کنند.

اما چنان که پیدا است حتی این تردیدها نیز در گسترش فزاینده خدمات ابری مانعی ایجاد نخواهند کرد. به عنوان مثال، گزارشی که توسط مرکز تحلیلی TechMarketView منتشر شده، پیش‌بینی می‌کند، ارزش بازار محاسبات ابر در انگلستان که در سال ۲۰۱۰ برابر ۵٫۸ میلیارد پاوند بود، در سال ۲۰۱۴ به ۱۰٫۴ میلیارد پاوند افزایش پیدا کند.

می‌توان گفت، برخی از سازمان‌ها در شرایط کنونی ترجیح می‌دهند، هزینه‌های بالا را برای تهیه تجهیزات و ملزومات یک مرکزداده خصوصی مبتنی بر ابر بپذیرند و به‌جای استفاده از مزیت صرفه‌جویی در هزینه‌ها که یکی از نتایج بهره‌گیری از زیرساخت‌های ابری است، از مزیت دیگر آن، یعنی خود این فناوری بهره ببرند.

منبع:
Network Computing Magazine

IPv6 جایگزینی برای IPv4

■ فربد صراف ■

مقدمه

اینترنت از بدو پیدایش تاکنون، منشاء تحولات عظیمی در حیات بشریت بوده است و ضریب استفاده از آن در اکثر کشورهای جهان، همچنان سیر صعودی را طی می نماید. به جرأت می توان گفت که طراحان اولیه اینترنت هرگز تصور اینچنین رشدی را نمی کردند. بدیهی است که طراحی انجام شده در برخی موارد، پس از گذشت ده ها سال با چالش های جدی مواجه شود و انتظاری جز این هم وجود ندارد. به عنوان نمونه، پروتکل IP که یکی از پروتکل های اساسی در اینترنت است، به گونه ای طراحی نشده است که بتواند از تعداد بی شماری دستگاه و کاربر متصل به اینترنت حمایت نماید. علاوه بر این، هم اینک درخواست های متعددی مبنی بر استفاده از مواردی نظیر ویدئو، صوت و دستگاه های بی سیم (نظیر موبایل) توسط برنامه ها وجود دارد که قطعاً در آینده شتاب بیشتری خواهد گرفت.

در اوایل سال ۱۹۹۰، IETF (برگرفته از Internet Engineering Task Force) که مسئولیت استانداردسازی اینترنت را برعهده دارد، اعلام نمود که پروتکل IP (با نام Ipv۴) دارای محدودیت هائی در زمینه آدرس دهی است و از همان زمان بر طراحی نسخه ای جدید از پروتکل فوق تاکید و در نهایت در سال ۱۹۹۵ نسخه اولیه IPv۶,۰ آماده گردید.

پروتکل IP و جایگاه آن در شبکه های کامپیوتری

پروتکل IP (برگرفته از Internet Protocol) یکی از اعضاء خانواده پروتکل TCP/IP است که در لایه شبکه فعالیت می نماید. از پروتکل فوق به منظور انتقال دیتاگرام (datagram) بین کامپیوترها استفاده می گردد. دیتاگرام از یک هدر و فیلد داده تشکیل می گردد. هر هدر دیتاگرام شامل آدرس مقصد (اطلاعات مورد نیاز برای توزیع دیتاگرام به مقصد مورد نظر) است. بدین ترتیب، امکان ارسال هر دیتاگرام به صورت جداگانه وجود خواهد داشت. دیتاگرام هائی که دارای یک session می باشند، می توانند از مسیرهای مختلفی ارسال گردند. بدیهی است در چنین مواردی همواره این احتمال وجود خواهد داشت که دیتاگرام ها با همان اولویتی که ارسال شده اند، به مقصد مورد نظر نرسند و با توجه به شرایط موجود، اولویت دریافت آنها در مقصد، متفاوت از اولویت ارسال در مبداء باشد.

هر اینترفیس شبکه در شبکه های داخلی بزرگ، دارای یک و یا چندین آدرس IP منحصربفرد است. یک اینترفیس شبکه می تواند دارای یک و یا چندین آدرس IP باشد ولی یک آدرس IP نمی تواند به چندین اینترفیس شبکه نسبت داده شود.

استفاده از IPv۶ در سالیان گذشته روند کندی را داشته است ولی اخیراً این وضعیت، با توجه به ضرورت های موجود، تغییر و شتاب بیشتری پیدا نموده است (خصوصاً در اروپا و آسیا). بر اساس گزارش منتشر شده توسط NRO (برگرفته از Number Resource Organization)، فضای آدرس دهی IPv۴ قابل دسترس از طریق RIRs (برگرفته از Regional

Internet Registries)، تا دو سال دیگر به اتمام می رسد. علاوه بر این، تعداد زیادی از کشورهای در حال توسعه نمی توانند آدرس های IP مورد نیاز خود را، به منظور حمایت از کاربران خود، درخواست نمایند. در برخی از کشورها، نظیر امریکا، اعلام شده است که تا سال ۲۰۰۸ تمامی شبکه های عملیاتی می بایست از IPv۶ استفاده نمایند.

با توجه به این که اکثر نرم افزارها و تجهیزات مورد نیاز در شبکه می بایست از IPv۶ حمایت نمایند و شرکت های تولید کننده سیستم عامل نیز، در سیستم عامل خود بتوانند از آن بطور کامل حمایت نمایند، این انتظار وجود دارد که تا دو سال دیگر زمینه استفاده کامل از IPv۶ فراهم گردد.

IPv٤ و محدودیت های آن

قبل از بررسی پروتکل IPv۶، اجازه دهید در ابتدا

پروتکل IPv٤ در سال ۱۹۷۰ ابداع شده است و در آن زمان هیچکس فکر نمی کرد که زمانی فرا خواهد رسید که برای انجام بسیاری از کارها، استفاده از پروتکل فوق به یک ضرورت تبدیل گردد.

به برخی از ویژگی های پروتکل IPv۴ که هم اینک استفاده می گردد، اشاره ای داشته باشیم. پروتکل IP از جمله پروتکل های حیاتی در اینترنت است که هم اینک از نسخه شماره چهار که به آن IPv۴ گفته می شود، استفاده می گردد. با این که پروتکل IPv۴ دارای عملکردی فوق العاده است ولی دارای محدودیت های مختص به خود می باشد.

• پروتکل IPv۴ در سال ۱۹۷۰ ابداع شده است و در آن زمان هیچکس فکر نمی کرد که زمانی فرا خواهد رسید که برای انجام بسیاری از کارها، استفاده از پروتکل فوق به یک ضرورت تبدیل گردد. حمایت از یک شبکه سراسری با میلیون ها کامپیوتر، انتقال داده، صوت و تصویر نمونه هائی از کاربرد IP در شبکه های مدرن امروزی است.

• در IPv۴ امنیت تعبیه نشده است و به همین دلیل است که پروتکل هائی دیگر، نظیر IPSec، با رویکرد امنیتی پیاده سازی شده است.

• مهمترین چالش IPv۴، محدودیت فضای آدرس دهی آن است. پس از گذشت چندین سال از عمومیت اینترنت، عدم وجود تعداد آدرس های IP، به یکی از نگرانی های اصلی در اینترنت تبدیل گردید.

• NAT (برگرفته از Network Address Translation) به منظور غلبه بر محدودیت تعداد آدرس های IP ابداع گردید. فناوری فوق این امکان را فراهم می نماید که کامپیوترهای موجود در یک شبکه اختصاصی (داخلی)، از آدرس های خصوصی به منظور ارتباط با یکدیگر استفاده نمایند ولی از یک آدرس IP عمومی به اشتراک گذاشته شده برای تمامی ارتباطات اینترنت استفاده نمایند.

• پروتکل IPv۴ از ۳/ ۴ میلیارد آدرس IP حمایت می نماید. ظاهراً عدد قابل توجهی است ولی فراموش نکنید که هم اینک ۵ /۶ میلیارد انسان در کره زمین زندگی می کنند و برخی از آنان دارای بیش از یک دستگاه متصل به اینترنت می باشند (نظیر یک کامپیوتر در محل کار، یک کامپیوتر در منزل، تلفن های موبایل با قابلیت دستیابی به اینترنت و...). پروتکل IPv۶ قادر به حمایت از ۵۰ اکتیلیون (هر اکتیلیون معادل عدد یک بهمراه ۴۸ صفر است) آدرس IP است!

امکانات و ویژگی های جدید IPv٦

شاید نیاز به توسعه تعداد آدرس های IP، با توجه به وضعیت بحرانی موجود، به عنوان یکی از اهداف مهم طراحی و پیاده سازی IPv۶ ذکر شود، ولی تمام داستان به اینجا ختم نمی شود و دلایل متعدد دیگری نیز در این زمینه مطرح می باشد. IPv۶ بگونه ای طراحی شده است تا ضمن ایجاد یک محیط همگرا، زمینه ی استفاده از صوت، تصویر و سرویس های داده را بر روی شبکه ای با زیرساخت IP فراهم نماید. بدین منظور، امکانات و پتانسیل های پیشرفته ای در IPv۶ پیش بینی شده است:

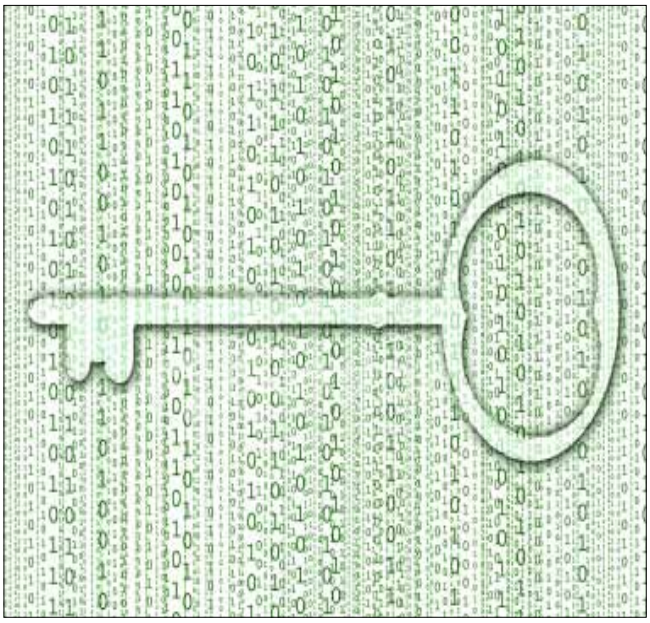
• افزایش فضای آدرس دهی: یکی از مهمترین مزایای IPv۶، افزایش تعداد فضای آدرس دهی است. فضای آدرس دهی IPv۶ به اندازه ای زیاد است که شاید نتوان آن را با فضای آدرس دهی IPv۴ مقایسه نمود. در IPv۴، تعداد ۴,۲۹۴,۹۶۷,۲۹۶ فضای آدرس دهی وجود دارد در حالی که این عدد در IPv۶ به عدد ۳۴۰,۲۸۲,۳۶۶,۹۲۰,۹۳۸,۴۶۳,۴۶۳,۳۷۴,۶۰۷,۴۳۱,۷ ۶۸,۲۱۱,۴۵۶ می رسد. افزایش آدرس های سراسری قابل روت، به سازمان ها این اجازه را خواهد داد که مسیر خود را از آدرس های IP غیرقابل روت ارائه شده توسط NAT جدا نموده و برنامه های مورد نیاز خود را در یک محیط واقعی end-to-end استفاده نمایند.

• پیکربندی اتوماتیک stateless: پیکربندی اتوماتیک IP در IPv۴ از طریق سرویس دهنده DHCP انجام می شود. در IPv۶ این کار توسط DHCPv۶ انجام خواهد شد. در IPv۶ این وضعیت توسعه و به پیکربندی اتوماتیک stateless تعمیم یافته است. با استفاده از پیکربندی اتوماتیک stateless به دستگاه ها اجازه داده می شود که پیکربندی آدرس های IPv۶ خود را از طریق ارتباط با یک روتر مجاور انجام دهند.

ادامه در صفحه ی ۹ ...

جهشی کوانتومی در رمزگذاری اطلاعات

حسین یاوری



یک گام به‌جلو

امروزه شرکت‌ها و دولت‌ها اطلاعات محرمانه و فوق‌العاده حساس خود را با استفاده از فرمول‌های ریاضی رمز گذاری می‌کنند. اطلاعات رمز گذاری شده با این روش، در صورت ردگیری و دسترسی غیرمجاز، تنها به شکل اطلاعاتی گنگ و نامفهوم ظاهر خواهد شد.

در حال حاضر، اکثر داده‌ها و اطلاعات با استفاده از متد موسوم به AES یا Advanced Encryption Standard رمزگذاری و محافظت می‌شوند. این متد اولین‌بار در سال ۲۰۰۲ توسط مؤسسه ملی استاندارد و فناوری (National Institute of Standards &Technology)، برای استفاده دولت‌ها، تصویب و تأیید گردید و سپس به شکل گسترده‌ای در بخش‌های خصوصی مورد استفاده قرار گرفت.

اکنون AES نیازها و مقاصد را برآورده کرده است و نفوذ به آن، دست کم در حال حاضر بعید به نظر می‌رسد. البته این قدرت و نفوذناپذیری ماندگار و همیشگی نخواهد بود.

اما گام بعدی در مقوله امنیت، رمزنگاری کوانتومی است و شرکت‌های معدودی محصولات رمزنگار امنیتی خود را با استفاده از این مفهوم توسعه داده‌اند و آن‌ها را تولید می‌کنند. MagiQ Technologies واقع در نیویورک یکی از این شرکت‌ها است.

محصولات این شرکت، با استفاده از خصوصیات فیزیک کوانتوم کلیدهای رمزگذاری تولید می‌کند که بنابر ادعای شرکت تولید کننده، قابل شکسته شدن و دسترسی غیرمجاز نیستند.

چرا MagiQ تا این حد به امنیت این روش مطمئن است؟ این سؤال تنها یک جواب دارد و آن، استفاده MagiQ از اصل عدم قطعیت است.

ادوات و تجهیزات MagiQ، ذرات نور بسیار کوچکی به نام فوتون تولید می‌کنند که قوانین متعارف فیزیک قادر به اجرا و به کارگیری آن نیستند. در سال ۱۹۲۷ یک فیزیکدان آلمانی به نام Werner Heisenberg دریافت که ذرات کوچک فوتون همیشه و هر لحظه در حال تغییر و دگرگونی هستند؛ به طوری که بعد از هر بار مشاهده دیگر هیچ‌گاه در آن حالت مشاهده نخواهند شد.

مراحل کار

اصل عدم قطعیت هایزنبرگ برای کسانی که از وضعیت و حالت فوتون‌ها برای ایجاد کلیدهای رمزدار استفاده می‌کنند، نتایج بسیار قابل اطمینانی را در تولید مجموعه‌ای واقعاً رمزی از اعداد تصادفی ارائه می‌کند و اگر شخص دیگری سعی در دسترسی غیرمجاز داشته باشد، به سهولت آن را تشخیص می‌دهد.

Mike LaGasse، نایب رئیس بخش فنی MagiQ، می‌گوید: اصل عدم قطعیت قانونی است که ما از آن بهره می‌گیریم. با این قانون اساساً دسترسی به کلید و کنترل آن غیرممکن است؛ زیرا فوتون تنها یک بار می‌تواند سنجیده و ارزیابی شود. کاربر غیرمجاز قادر به انجام این سنجش نیست و بنابراین نمی‌تواند کلید را به دست آورد.

MagiQ از یک کامپیوتر، یک اشعه لیزر نازک، یک آشکارکننده ذرات فوتون و یک رشته فیبرنوری استفاده می‌کند. اشعه لیزر از داخل جعبه MagiQ QPN، که برای تولید تک فوتون‌ها تنظیم شده است، عبور می‌کند و از طریق یک کابل فیبرنوری به جعبه QPN دیگری فرستاده می‌شود. در جعبه QPN دوم فوتون‌ها نمایان می‌شوند و زمان ورود آن‌ها با دقت ثبت می‌شود.

سپس چگونگی وضعیت فوتون‌ها در دو جعبه، در زمان ترک جعبه اول و در هنگام ورود به جعبه دوم با یکدیگر مقایسه می‌شود. اگر دو حالت همسان باشند، از فوتون برای تولید یک کلید به منظور رمزگذاری اطلاعات استفاده می‌شود. اما اگر دو حالت همسان نباشند، از آن صرف‌نظر می‌شود. مشاهدات و بررسی‌های مربوط به فوتون‌های مناسب ذخیره می‌شود و بر حسب نیاز برای تولید کلید به کار می‌رود و این فرایند صدها بار در ثانیه تکرار می‌شود.

وقتی که کلیدی تولید شد، به رمز درآوردن اطلاعاتی که قصد ارسال آن را دارید، موضوع نسبتاً ساده و آسانی است؛ خواه این اطلاعات یک مکالمه صوتی باشد یا یک طرح حساس شغلی. اما از زمانی که کلیدها تسخیرناپذیر و ایمن شدند، داده‌هایی که رمزگذاری می‌شوند، بسیار افزایش یافته است.

در حقیقت مشکل نفوذگران برای دسترسی غیرمجاز، روزبه‌روز پیچیدگی‌های بیشتری پیدا می‌کند؛ زیرا کلیدها با سرعت صدها بار در ثانیه ایجاد می‌شوند. بنابراین شانس و احتمال کسب اطلاعات کافی درباره آن‌ها، برای ایجاد یک کپی از کلید و به عبارت دیگر شکستن روال رمزگذاری در واقع به صفر می‌رسد.

وقتی که کلیدی تولید شد، به رمز درآوردن اطلاعاتی که قصد ارسال آن را دارید، موضوع نسبتاً ساده و آسانی است؛ خواه این اطلاعات یک مکالمه صوتی باشد یا یک طرح حساس شغلی

کاربرد در فواصل دور

کاربرد و استفاده از این روش حفاظت از اطلاعات، موسوم به Quantum Crypto به آرامی در دولت‌ها و صنایع مختلف در حال گسترش است. Bob Gelfond، مدیرعامل MagiQ و بنیانگذار شرکت در سال ۱۹۹۹، می‌گوید: اقدامات اولیه برای ساخت دستگاه تولید و توزیع کلیدهای کوانتومی با نام MagiQ QPN با همکاری شرکت Verizon Communications آغاز شد.

نتایج بررسی‌ها و آزمایش‌هایی که در ماه مارس منتشر شد، نشان داد که MagiQ موفق شده است با فناوری quantum crypto بر یکی از مشکلات بزرگ فائق آید؛ یعنی بُعد مسافت.

کلیدها بین دو نقطه مبادله می‌شوند و لازمه این مبادله، اتصال دو نقطه از طریق یک خط فیبرنوری است. شبکه‌های نوری به تکرارکننده‌هایی (repeater) در مسیر کابل‌ها و در فواصل معین، (به عنوان نمونه، فواصل هشتاد کیلومتری) برای حفظ سیگنال‌های ارتباطی نیاز دارند. این تکرارکننده‌ها یک مشکل اساسی ایجاد می‌کنند؛ زیرا شبیه یک شنودکننده باید کلیدها را برای عبور از خطوط انتقال مشاهده و کنترل کنند.

MagiQ اثبات کرد که استفاده از شبکه نوری Verizon قادر است با موفقیت کلیدها را در سرتاسر یک مسیر ۱۴۰ کیلومتری (در حدود ۸۷ مایل) دست‌نخورده و سالم حفظ کند. Gelfond می‌گوید: ما می‌توانیم با استفاده از اتصال دستگاه‌ها به صورت متوالی و با شیوه daisy-chaining، امکان پشتیبانی از مسافت‌های بیشتر را مهیا کنیم؛ البته در آمریکای شمالی فواصل شبکه‌های مخابراتی بسیار کمتر از این مسافت است. به طوری که می‌توانید تمام سواحل شرقی ایالات متحده را تحت پوشش درآورید؛ زیرا مسیر ارتباطی‌ای که شما در این منطقه نیاز دارید، کاملاً در محدوده ۱۴۰ کیلومتری می‌گنجد.

ادامه در صفحه ی بعد ...

ادامه از صفحه قبل

جهشی کوانتومی در رمزگذاری اطلاعات

Gelfond امیدوار است که MagiQ بتواند تجهیزات و ادوات تولیدی خود را به ارائه‌کنندگان سرویس‌های مخابراتی بفروشد و می‌گوید محصولات شرکت، هم خریدار دولتی و هم خریدار خصوصی دارد، اما نه در مورد هویت خریداران چیزی می‌گوید و نه در مورد این‌که چه مقدار از محصول فروخته شده است. فقط می‌گوید:

ما محصولات خود را در سرتاسر جهان توزیع کرده‌ایم و تا زمانی که میزان فروش محصول به رقم بسیار بالایی نرسیده است، تصور می‌کنیم مشتریان علاقمندند ما آن را در آینده گسترش دهیم و با قابلیت‌های بهتر عرضه کنیم. او اضافه می‌کند که شرکت هنوز به مرحله سودآوری نرسیده است.

Gelfond، یکی از سهامداران اولیه amazon.com بوده است. به علاوه، Jeff Bezos هم برای مساعدت و همراهی Gelfond به MagiQ بازگشته است.

او یکی از سهامداران MagiQ است و به عنوان یکی از مشاوران رؤسای RSA Security، قسمتی از EMC و شرکت امنیتی McAfee نیز فعالیت دارد.

Gelfond می‌گوید: برنامه بلند مدت MagiQ، گسترش و توسعه رمزگذاری کوانتومی (Quantum Crypto) به عنوان پدیدآورنده و صاحب امتیاز این فناوری و همچنین ایجاد فناوری تولید کارت‌های کوچک تیغه‌ای شکل (مانند کارت‌هایی که سازندگان کامپیوتر در سرورهای تیغه‌ای به کار می‌برند) است که می‌تواند در داخل روترها و سوییچ‌های مخابراتی تعبیه و نصب شود.

Greg Young، یکی از تحلیلگران شرکت Gartner، می‌گوید: در حال حاضر جذب سرمایه محدود شده است. تقاضای زیادی برای این نوع محصولات در یک دوره زمانی کوتاه وجود ندارد. گاهی قراردادهای سیستم‌های رمزگذاری دچار سقوط و افت ناگهانی می‌شوند و در زمان دیگری که انتظار نمی‌رود، تقاضا و مطالبه آن افزایش می‌یابد.

جمع‌بندی

Young می‌گوید: شکستن قواعد رمزنگاری، در واقع یک مسئله ریاضی است که برای حل، به انجام عملیات گوناگون روی مجموعه گسترده‌ای از اعداد و ارقام نیاز دارد. او می‌گوید: آن‌ها معماهای پیچیده‌ای هستند که برای حلشان هیچ مسیر کوتاه و میانبری وجود ندارد. اما رمزنگاری کوانتومی یک گام منطقی رو به جلو است؛ اگرچه همیشه متخصصی برای نفوذ و شکستن قواعد سیستم‌های رمزنگاری اطلاعات وجود دارد.

MagiQ رقبایی مانند شرکت‌های ID Quantique از سوییس، Smart Quantum از فرانسه و شرکت‌های ژاپنی از جمله Fujitsu، Toshiba، NEC و Nippon Telegraph & Telephone دارد که همگی مدعی برتری محصولات توسعه‌یافته بر پایه فناوری جدید شرکت خود هستند.

منبع:
Network World Magazine

IPv6 جایگزینی برای IPv4

ادامه از صفحه ی هفت...

با این که پیکربندی اتوماتیک stateless برای اکثر محیط ها دارای مزایائی است، ولی در شبکه هائی که دارای تعداد زیادی از دستگاه ها با قابلیت محدود مدیریتی می باشند، مسائلی را به دنبال خواهد داشت.

یک شبکه مبتنی بر تعداد زیادی سنسور، که ممکن است شامل میلیون ها دستگاه بی سیم راه دور باشد که صرفاً بر روی شبکه قابل دسترس می باشند، نمونه ای در این زمینه است. پیکربندی اتوماتیک به سازمان ها کمک خواهد کرد که هزینه نگهداری و مدیریت شبکه خود را کاهش دهند.

با این که پیکربندی اتوماتیک آدرس دهی خصوصی موسوم به APIPA (برگرفته از Automatic Private IP Addressing)، دارای خصایص مشابهی در خصوص پیکربندی است ولی ماهیت آن با پیکربندی اتوماتیک stateless کاملاً متفاوت است. APIPA از یک محدوده خاص فضای آدرس دهی IP (از محدوده IP: ۱۶۹. ۲۵۴. ۰. ۱ تا IP: ۱۶۹. ۲۵۴. ۲۵۵. ۲۵۴) در مواردی که یک سرویس دهنده DHCP در شبکه موجود نباشد و یا سرویس گیرنده قادر به برقراری ارتباط با آن نباشد، استفاده می نماید. از پروتکل ARP (برگرفته از Address Resolution Protocol) به منظور بررسی منحصربفرد بودن آدرس IP بر روی یک شبکه محلی (LAN) استفاده می گردد. زمانی که یک سرویس دهنده DHCP در دسترس قرار بگیرد، آدرس های IP سرویس گیرندگان به صورت اتوماتیک به هنگام خواهند شد.

• extension header: با این که هدر IPv۶ در مقام مقایسه با IPv۴ بسیار ساده تر شده است، ولی با ارائه extension header، امکان ارائه قابلیت های پیشرفته در سطح هدر و بسته اطلاعاتی IP پیش بینی شده است. با اضافه کردن هدر به هدر پایه IPv۶، قابلیت های چشمگیری برای قابلیت های آتی به آن اضافه شده است. بدین ترتیب، هدر پایه ثابت خواهد ماند و در صورت ضرورت می توان قابلیت های جدید را از طریق extension header به آن اضافه نمود. در آینده می توان از extension header برای پیاده سازی سرویس ها و برنامه های ارائه شده توسط یک فریمورک استاندارد و به عنوان قابلیت های جدید در IPv۶ استفاده نمود.

• امنیت اجباری: با این که در IPv۴ امکان استفاده از IPsec (برگرفته از Internet Protocol security) وجود دارد، ولی توجه داشته باشید که ویژگی فوق به عنوان یک قابلیت جدید به پروتکل فوق اضافه می گردد تا از آن در مواردی نظیر tunneling، رمزنگاری شبکه، به منظور دستیابی راه دور VPNs (برگرفته از Virtual Private Networks) و ارتباط با سایت ها استفاده گردد. تعداد زیادی از سازمان ها از پروتکل IPsec در موارد خاصی استفاده می نمایند ولی وجود موانعی نظیر NAT، می تواند زمینه بکارگیری آن را با مشکل مواجه نماید.

در IPv۶، پروتکل IPsec به عنوان بخشی الزامی در پیاده سازی مطرح شده است تا به کمک آن یک زیرساخت امنیتی مناسب به منظور ارائه سرویس های امنیتی نظیر تأیید، یکپارچگی و اعتمادپذیری فراهم گردد. ظرفیت عملیاتی IPsec به گونه ای است که سازمان ها به کمک آن می توانند وضعیت مدل امنیتی خود را بهبود و سیاست های امنیتی خود را توسعه دهند.

آدرس دهی IPv٦

تاکنون تلاش های گسترده ای به منظور استمرار حیات IPv۴ و غلبه بر محدودیت تعداد آدرس های IP انجام شده است. استفاده از سیاست های مختلف و NAT نمونه هائی در این زمینه می باشد. بر اساس آخرین گزارشات منتشرشده توسط مراکز ذیصلاح، محدودیت فضای آدرس دهی IP یک تهدید جدی است و فقط بیست و پنج درصد از فضای آدرس دهی IPv۴ باقی مانده است. با این که شاید در برخی از کشورها این موضوع نگران کننده نباشد ولی گسترش استفاده از دستگاه های گوناگون مبتنی بر IP، استفاده از IPv۶ را به یک ضرورت تبدیل کرده است.

در IPv۴، آدرس های IP سی و دو بیتی توسط چهار اکتت یا هشت بیت (از صفر تا ۲۵۵ که در مبنای ده نوشته می شوند) که توسط نقطه از هم جدا می شوند، ارائه می گردند. آدرس های IP زیر، نمونه هائی در این زمینه می باشد.

131. 107. 20. 60
192. 168. 118. 183

در IPv۶، آدرس های IP یکصد و بیست و هشت بیتی توسط هشت شانزده بیت (از صفر تا FFFF نوشته شده در مبنای شانزده) که با یک colon از یکدیگر جدا می شوند، ارائه می گردند. آدرس های IP زیر، نمونه هائی در این زمینه می باشد.

3ffe: 2900: d005: 4: 104a: 2a61: 0: 0
3ffe: ffff: 4004: 1952: 0: 7251: bc9b: a73f

در مواردی که در یک آدرس IPv۶ چندین بلاک صفر وجود داشته باشد، از «::» به منظور کوتاه تر شدن شکل نمایش آن استفاده می گردد.

fe80: 0: 0: 0: 0: 70: 77: 26 = fe80:: 70: 77: 26

با رفتن به لینک زیر می توانید از یک محاسبه گر، جهت یافتن معادل آی پی نسخه ۶ خودتان استفاده کنید و یا هر نمونه آی پی نسخه چهار را وارد و معادل نسخه ۶ را دریافت کنید:

http://www.subnetonline.com/pages/subnet-calculators/ipv4-to-ipv6-converter. php

facebook آینه ی جادوئی

(در اینترنت به مقاله ای جالب در مورد فیس بوک برخوردیم که دیدیم بد نیست آن را شما هم بخوانید. این مقاله را فلیپ ریوایر نوشته است و در دسامبر ۲۰۱۰ در ماهنامه لوموند دیپلماتیک منتشر شده است.)

چند روز پیش فیس بوک از من خواست تا تغییر نام دهم. نه به این دلیل که اسم مستعار انتخابی ام مستهجن بود، یا به نفرت نژادپرستانه دامن میزد، یا زبانم لال از نام مارک زوکربرگ قدر قدرت (مدیر، بنیان گذار و سهام دار اصلی این سایت اینترنتی) به طرز ناشایستی یاد می کرد و یا حتی به نام یک مارک شناخته شده شباهت داشت. من برای خود نامی گزیده بودم که مرکب از حروف بریل بود. مهندسین سایت کالیفرنیایی ناگهان تصمیم گرفتند که این کار از نظر تیپوگرافیک درست نیست.

هنگام نام نویسی، فیس بوک بر این امر که من وجود خارجی دارم صحه گذاشته بود و اسم رمزم را با تلفن کنترل کرده بود. آنها حتی اصرار داشتند تا من کلمه عبور ایمیل خود را نیز ارائه دهم تا بتوانند به مجموعه آدرس هایم دسترسی یابند و رد یابی تماس هایم برایشان آسان تر گردد.(در زبان رایج سایت، «دوستانم») با رعایت شرایط استفاده از سایت، که هیچ کس آن را نمی خواند، صفحه ی آبی فیس بوک که گهواره ای گرم و نرم برای اعضا می باشد و به آنها امکان می دهد تا بدون آنکه مورد تهاجم تبلیغات قرار گیرند گپ بزنند، نمایان می شود. تبلیغات نسبتاً ملایم مطرح می شوند، می توان با فراغ بال به تماشای عکس های دوستان پرداخت، از همان اطلاعاتی که آنها کسب می کنند لذت برد و یا ناراحت شد، با آنها بازی کرد، رویداد های زندگی شان، از پیش پا افتاده ترین تا فرح بخش ترین آنها را دنبال کرد. پیام هایی که رد و بدل می شوند، تمام عرصه های تفکر بشری را پوشش می دهند، از موضوع حیاتی «دوش می گیرم» تا نظرات دقیق در مورد هنر معاصر و همچنین خبر تولد نورسیده.

در فیس بوک تبادلات همیشه مثبت اند:می توان با کلیک کردن بر روی یک دکمه یک موضوع را «دوست داشت» اما نمی توان از آن بیزار شد؛ از یافتن یک دوست جدید با خبر می شویم اما از دست دادنش به اطلاع ما نمی رسد. کنترل های گوناگون کاربر را مورد محافظت قرار می دهد: به این ترتیب مسافری که از یک محل غیر متداول به شبکه وصل می شود باید به سوالات متفاوت (سرگرم کننده) همراه با عکس پاسخ گوید تا هویت خود را مسجل سازد. صفحات حساس همچون گروه حمایت از سرباز بردلی منینگ، که متهم به ارائه اطلاعات مخفی در مورد جنگ عراق در سایت ویکی لیکس می باشد گاه بدون توضیح معلق می شوند، سپس چند روز بعد مجدداً سرو کله شان پیدا می شود. برای محدود کردن برخی سوء استفاده ها، از اعضا دعوت می شود تا با کلیک کردن بر روی یک دکمه پیام های نامربوط را افشا کنند که می تواند منجر به منفصل کردن کاربر مورد ظن گردد. فیس بوک گاه خود به سانسور وسوسه می شود و ارتباط با سایت های اشتراک پرونده یا پایگاه های برجسته هنری و سیاسی مثل Seppukoo.Com را قطع می کند که به کاربران اجازه می دهند تا داده هایشان را از فیس بوک پاک کنند.

این ملغمه ی استادانه از زندگی خصوصی و میل به سرکشی در اندرونی دیگران، این نظام ملایم سرپیچی معتدل از اخلاق و این بارگاه آزادیِ تحت نظر باعث رونق روز افزون امورات آقای زوکربرگ گردید. او توانست پانصد میلیون کاربر را به سایت خود جذب کند، نیمی از آنان هر روز به شبکه وصل می شوند و جمعاً هفت صد میلیارد دقیقه در ماه در آن وقت می گذرانند. دویست میلیون نفر از طریق موبایل به فیس بوک متصل می شوند. فیس بوک از هیچ شروع کرد و یا شاید تاحدودی هیچ، چرا که اسم و رسم دانشگاه هاروارد بی شک در صعود سریع آن پس از آغاز کار در فوریه ۲۰۰۴ بی اثر نبود و با تنها ۱۷۰۰ کارمند، بزرگ ترین سایت اینترنتی کره زمین می باشد.

کاربران در آزادی کامل داده های شخصی شان را داوطلبانه وارد سایت می کنند، داده هایی که جاه طلبی هایی را بر می انگیزد. به این ترتیب به بازاریاب ها امکان می دهند تا بر اساس جنسیت، سن، تاریخ تولد، زبان، کشور، شهر، سطح تحصیلات، موضوعات مورد علاقه – بسیار دقیقتر از نظر سنجی های رسانه های سنتی– هدف گیری کنند. با کاربرانی که تعدادشان نزدیک به بینندگان تلویزیون است. روز ۲۲ نوامبر گذشته، مارک «لویی ویتان» بدون واسطه از این طریق به یک میلیون و شش صد و شصت و چهار هزار و هفت صد و هشتاد و نه کاربر دسترسی پیدا کرد. یعنی تعداد کسانی که با فشردن دکمه «دوست دارم» از دوستانشان نیز دعوت کرده بودند تا به این مارک ابراز علاقه کنند. در صفحه این فروشنده کیف و چمدان، از شو مُد تا سفر نامه بونو، خواننده معروفِ «به قلب آفریقا»، دیده می شود.

از صفحات پر خواننده می توان به صفحه استار بوکز کافی، کوکاکولا و یا بیسکویت اورئو اشاره کرد که بین ده تا بیست و پنج میلیون تماشاچی دارند. اما مارک های بزرگ در بهره وری از شبکه تنها نیستند. در مقیاسی دیگر، استاد کار محلی، نویسنده ناشناس و همچنین کارگاه کوچک نیز برای معرفی خود از این سیستم استفاده می کنند. حتی لوموند دیپلماتیک نیز از آن بی بهره نیست؛ صفحه فیس بوک آن که اواخر ۲۰۰۹ به ابتکار یک خواننده این نشریه گشوده شد امروز چهل و پنج هزار و هشت صد و شصت و یک عضو دارد.

با فراهم آوردن امکان شکل دادن به مُهر و نشانِ شخصی، برای هر فرد، فیس بوک آینه ی جادویی عصرِ خودخواه و تبلیغاتچی ماست. تجربه فیس بوک به کاربر آن اجازه می دهد تا احساس کند هر لحظه در مقابل صد و سی نفر (تعداد متوسط «دوستان» در شبکه) ظاهر می شود که می توانند برای هر حرکت و هر کلام او دست بزنند. هر اندازه انعکاس الکترونیکی وجود ما واقعیت شخصیت مان ویا آن چه می خواهیم باشیم را بیشتر نمایان سازد، بیشتر سرمست تصویر آن می شویم. این احساس هر فرد را به تغذیه هر چه بیشتر صفحه اش رهنمون می سازد که گاه از اختیار خارج میگردد. افراد در صفحه فیس بوکشان به انتشار علایق، آدرس خانه، محل های رفت و آمد خود در هر لحظه با استفاده از تکنیک های رد یابی جغرافیایی می پردازند و یا لحظه نگارِ سوز و گداز های عاشقانه شان را در ملاء عام قرار می دهند. ....

ادامه در صفحه بعد

مدیر عامل گوگل، اریک اشمیت در کنفرانس تکونومی، روز ٤ اوت ۲۰۱۰ گفت: با ١٤ عکس ما می توانیم هویت شما را شناسایی کنیم. گمان می کنید که ١٤ عکس از شما بر روی شبکه موجود نیست؟ عکس های فیس بوک یادتان نرود!

ادامه از صفحه قبل

facebook
آینه ی جادوئی

امـا فیس بوک نمی خواهد به این بسـنده کند: در نظر دارد از یک تارنمای بسـته، به گسترش در سراسر شبکه تحول یابد. دکمه «دوست دارم» که از ماه آوریل ۲۰۱۰ اضافه شده است در ظاهر کارایی ساده ای دارد، هر کاربر می تواند آن را به سایت خود اضافه کرده، شمار افرادی که به آن سر می زنند را افزایش دهد؛ با کمک این سیستم اعجاز انگیز که هم اکنون بر روی یک میلیون سـایت نصب شده، فیس بوک بر خود می بالد که امکان آن را دارد تا هر ماه سرکشی بیش از صد و پنجاه میلیون کار بر، بر روی شبکه اینترنتی را همراه با اسم و رسمشان رد یابـی کند و بـه این ترتیب گروه بندی هدفمند آنان را دقت بیشتری بخشد.

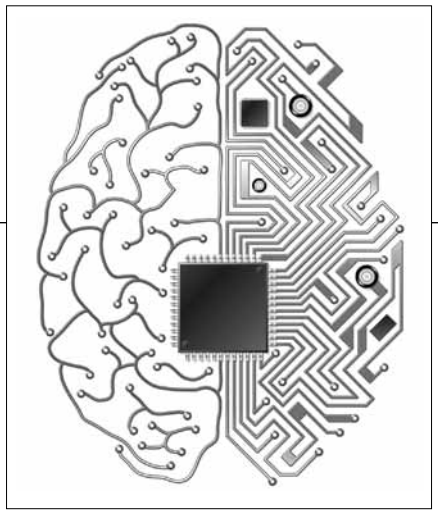
برای خدمات رسانی (و کنترل) بیشتر، فیس بوک سیستم ایمیل، اس ام اس و گفتگوی مستقیم خود را براه انداخت و با گوگل، غول دیگر کنترل اینترنتی به رقابت رو یاروی می پردازد.

فیس بوک اطمینان می دهد که تنها «دوستانمان» به این توده انبوه متون و تصاویر که به صورت مستمر در بانک داده ها واریز می شود دسترسی دارند. پس از بررسی های وال استریت جورنال که برملا کرد کـه برخی از مراکز ارائه بازی های الکترونیکی بر روی فیس بوک به هویت کاربران و دوستانشـان دسترسی داشتند، در ماه نوامبر ۲۰۱۰، شرکت فیس بوک اعلام کرد که از آن پس «مُدارا صفر» خواهد بود و هیچ داد و سـتدی بر سـر داده ها را تحمل نخواهد کرد و تضمین می کند که: «هرگز اطلاعات مربوط به کاربران را نفروخته و نخواهد فروخت».

در سـال ۱۹۹۳، یک نقاشی در نیویورک تایمز توضیح می داد که: «در اینترنت کسی نمی داند که شما یک سـگ هستید». در سال ۲۰۱۰، ناشناس ماندن در حال از بین رفتن است. مدیر عامل گوگل، اریـک اشـمیت در کنفرانس تکنونومی، روز ۴ اوت ۲۰۱۰ گفـت: «با ۱۴ عکس مـا می توانیم هویت شما را شناسـایی کنیم». «گمان می کنید که ۱۴ عکس از شما بر روی شبکه موجود نیست؟ عکس هـای فیس بوک یادتان نرود.» وضعیت عینی ای که به نظر او نه تنها نمی بایست به آن پایان بخشید بلکه وجودش ضروری است، چرا که: «در جهانی با تهدیدات گاه یک جانبه، ناشناس ماندن واقعی خطر ناک است (...) ما به یک بخش کنترل هویت دقیق نیازمندیم؛ بهترین نمونه امروزی چنین سیسـتمی فیس بوک اسـت (...) بالاخره دولت ها هم آن را طلـب خواهند کرد». اگر امـروز هنوز می توان در مورد هویت خود تقلب کرد، در آینده این کار دشوار تر خواهد شـد. معماران جهان متصل به شـبکه و رهبران سیاسـی در نظر دارند به «متمدن سازی» اینترنتی آزاد دسـت زنند که از نظر آنها منطقه ای فارغ از قوانین اسـت. اگر آنها موفق به رام سـازی آن گردند، تنها راه شـرکت تام الاختیار در شـبکه، ارائه هویت واقعی خواهد بود. تارنما تا کنون تصویر سیستمی غیر متمرکز از شبکه های به هم مرتبط را ارائـه مـی داد. هیچ کس فکر نمی کرد که یک عنکبوت چموش خود را در مرکز آن قرار دهد و به جاسوسی کاربران بنشیند.

هدف از نوشـتن این متن کاملا مشـخص است، می‌خواهـم اثبات کنـم کامپیوترها مغـز ندارند. البته بـرای اثبات این موضوع از دیدگاه فلسـفی، باید ابتدا مقدمه‌هایی را بیان کرد.

همـه چیز از چند روز پیش شـروع شـد! دورآخر مسـابقات رباتیـک لیـگ امدادگر تمام شـده بود و بالاخره فرصت اسـتراحت پیدا کرده بودیم و داشتیم گپ می‌زدیم. نمی‌دانـم چگونه بحثمان به چگونگی حمایت مسـئولان از تیم رسید، اما خوشحالم که این موضوع به میان آمد. از اتاق کوچکمان صحبت کردیم، که ابعادش حدود یک دکه روزنامه فروشی است. روبات و چهار تا شـش نفر آدم و سـه میز و چند کمد و ابزار و... را آنجـا جا داده‌اند. از مخارج تیم صحبت کردیم، از مبالـغ قابل توجهی ((۱۰ بـه توان ۷) O تومان[۱]) که اعضا از جیب خودشـان خرج کرده‌اند، درحالی که اتاق‌های ممکن قرار گرفته اسـت (کافیست که یک سر به آزمایشگاه های آزاد و روبوتیک و... بزنید!) ؛ ولی بخش‌های اداری، مانند دفاتر روسا و معاونین را معمولا در اتاق‌هایی شیک در طبقات بالای ساختمان‌ها می‌توان پیدا کرد. اگر باور ندارید چرخی در همین دانشکده برق و کامپیوتر خودمان بزنید. تصادفی نیسـت که سـالی یک بار هم یک بنر برای تبریک یک موفقیت علمی، مانند چاپ یک مقاله، کسـب رتبه‌ای در مسـابقات یا المپیاد یا کنکور روی در و دیوار دانشگاه نمی‌بینیم، اما تا دلتان بخواهد بنر و دیوار نوشـته و اعلامیه تبریک و تسـلیت در مواردی کم ارتباط یا حتی بی‌ارتباط به علم از طرف بعضی‌ها بر در و دیوار دانشـگاه زده می شـود. اگر باور ندارید چرخی در همین دانشـکده برق و کامپیوتر خودمان بزنید. تصادفی نیسـت که بیشـتر کسانی که می‌توانند بروند، دارند می روند...



کامپیوترها مغز ندارند!

مجتبی قربانعلی بیک

پرداختشـان وظیفه دانشگاه بوده اسـت. از پیشرفت مسـئولان دانشـگاه در ارائه پاسخ های غیرمسئولانه صحبت کردیـم، از پول‌هایی که بـرای فعالیت‌های پژوهشـی ندادند (همینطور خرید تجهیزات پژوهشی و آموزشـی، کارهای عمرانـی، حمایت از کانون‌های فرهنگی، و سایر موارد را نیز به فعالیت‌های پژوهشی اضافـه کنید). اما هیچ کدام از این موارد ما را عصبی نکـرد. تا اینکه صحبت به ادعاهای بعضی از مدیران درباره حمایت از فعالیت‌های پژوهشـی و نخبگان و... رسـید. یادمان آمد که بعضی‌ها، مقام سومی که ما با زحمت فراوان و بدون حمایت شایسته و بایسته‌ای از جانب مسـئولان دانشگاه بدست آورده‌ایم را در رزومه مدیریتی خودشان قرار می دهند.

واقعا عصبانی شده بودم. بلند شدم و کمی قدم زدم و فکر کردم. متوجه شـدم که ما تنها نیسـتیم، تقریبا هر کسی که در این دانشگاه کار پژوهشی می‌کند نیز در این مصیبت با ما شریک است. تصادفی نیست که بیشـتر آزمایشگاه‌های پژوهشـی و اماکن مربوط به فعالیت‌های علمی دانشگاه، در زیرزمین‌های تاریک و نمناک یا در طبقه بالای سـلف، در میان بخار قورمه سبزی و ترکیدگی لوله فاضلاب و خلاصه در بدترین

یکی از وظایفی که هر مدیر با وجدانی باید آن را انجام دهد، بررسی نتایج تصمیم‌ها و اقدام‌هایش یا به زبان مهندسـی، دریافت فیدبک است. امیدوارم روزی برسـد که کسانی مسئول شـوند که حداقل، احساس مسـئولیت کنند و حتی اگر بر فرض مثال بودجه ای هم نداشـتند، حداقل سالی یک بار از اتاق‌های شیک شـان بیرون بیایند و سر زده به زیر زمین‌های تاریک و نمناک بروند واز دانشـجو و به ویژه پژوهشـگر عذر خواهی کنند.

شـاید فکـر کنید که بحث را بـه بیراهه بردم، اما همـه این مقدمه ها لازم بود. حتمـا تا کنون عبارت "فرارمغزها" را شـنیده اید، معنـای بدون تعارف این عبارت این اسـت که شرایط به قدری نا مناسب است که هر کسی که مغز داشته باشد، ترجیح می دهد فرار کند. آنهایی که مانده اند، یا امید به بازگرداندن حقوق از دست رفته دارند یا نمی توانند از دوستان و آشنایان جدا شوند یا... یا نمی توانند ننگ فرار را تحمل کنند.

و بالاخره اثبات قضیه اصلی! کامپیوترها فرار نکرده اند و در هیچ کدام از بندهای اخیر نیز نمی گنجند. پس فرض ابتدایی دارا بودن مغز برای کامپیوتر ها اشـتباه است. کامپیوتر ها مغز ندارند.

۱ - big O: نماد پیچیدگی زمانی در طراحی الگوریتم

پرکاربردترین فرمت‌های موسیقی

محمد حسن نیرومند

تا قبل از ورود کامپیوتر به عرصه صدا، چیزی به اسم فرمت صوتی وجود نداشت. صداها، اگرچه با کیفیت های متفاوت، به روش واحدی ذخیره و خوانده می شـدند. ولـی با ورود کامپیوتر، فایل های صوتی نیز فرمت ها و قالـب های مختلفی پیدا کردند. در کامپیوتر، فرمت یک فایل به معنی نوع ذخیره سازی اطلاعات و نحوه خواندن آنها است. اجازه دهید یک مثال بزنیم. در فرمت Mid، اطلاعات صوتی بصورت نت (Note) ذخیره می شـود؛ یعنی اطلاعات مربوط به هر ساز، به همراه پرده ها، نت ها و سـایر اطلاعات، جداگانه ذخیره می شـود، ولی در فرمت Wav اطلاعات صوتی بصورت طول موج های صدا ذخیره می شـود و صدا ها قابل تفکیک نیستند. به همین دلیل، برنامه های خاصی وجود دارند که می توانند فرمت Mid را به نت های موسیقی تبدیل کنند؛ ولی در فرمت Wav چنین امکانی وجود ندارد. همچنین، چون در فرمت Wav تمام طول موج ها ذخیره می شوند، حجم فایل نسبت به فرمت Mid بسیاربیشتر است. در ابتدا هریک از برنامه های صوتی، برای خود یک فرمت جداگانه داشت؛ ولی در حال حاضر، بیشتر برنامه ها، اکثر فرمت های صوتی را پخش می کنند. تعدادی از مهم ترین فرمت های صوتی به شرح زیر هستند: mp۳, Wav, Wma, Ra, و Mid

Wav: ایـن فرمت معروف ترین و پر کاربردترین فرمت صوتی در کامپیوترهاست. Wav فرمت استاندارد ویندوز محسوب می شود. به همین دلیل، اکثر صدا های موجود در ویندوز با فرمت Wavمشاهده می شوند و کلاً این فرمت کاربرد بیشتری دارد. فرمت Wav برخلاف اکثـر فرمت های دیگر، خود انواع مختلفی دارد؛ یعنی مـی توان یک فایل Wav را به حالت های مختلفی ذخیره کرد. فرمت Wav در همه برنامه های مرتبط با صدا شناخته شده و پخش می شود.

mp3: این فرمت، محبوب ترین فرمت برای فایل های موزیک محسوب می شود. در واقع mp3 موفق ترین فرمت از خانواده Mpeg می باشد. Mpeg فرمتی بود که برای فشرده سازی صدا و تصویر، توسط گروهی از محققین ایجاد شـد. این گروه که با نام Motion Picture Experts Group فعالیت می کردند، پـس از اختـراع این فرمت، نام خـود را بر آن نهادند. (Mpeg در واقع از حروف اول همین عبارت تشکیل شـده اسـت). پس از ایجاد این فرمت که Mpg نیز خوانده می شد، فرمت های دیگری از این خانواده هم ارائه شد؛ از آن جمله : mpa, mp1,mp2,mp3 از این میان mp3 بیش از بقیه کارایی داشت و بیشتر مورد استقبال قرار گرفت. دلیل عمده موفقیت آن نیز این بود که در این فرمت، فایل های صوتی بسیار فشرده و کم حجم می شـوند، با این فرمت ما می توانیم حجم بیشـتری از موسیقی را روی CD ذخیره کنیم (حدود ۱۲ سـاعت موسـیقی روی هر CD)، همچنین زمان دریافت موسیقی از اینترنت نیز کاهش می یابد. mp3 در ویندوز ۹۵ و اولین نسخه های ویندوز ۹۸ پشتیبانی نمی شد. ولی در ویندوز های بعدی، فرمت mp3 بعنوان یکی از فرمت های پیش فرض گنجانده شده است.

CDDA: ایـن فرمت در واقع چنـدان ربطی به فایل های صوتی کامپیوتری ندارد. ولی از آنجا که در کامپیوتر اسـتفاده زیادی دارد، آن را معرفی می کنیم. CDDA در واقع فرمت CD های صوتی یا Audio cd ها اسـت که توسط ضبط ها و CD player ها قابل اجرا اسـت. این فرمت ساختار کامپیوتری ندارد و حتی نمی توان آن را روی کامپیوتر کپی کرد. در حال حاضر به دلیل حجم بالائی که این فرمت اشـغال می کند، استقبال از آن کاهش یافته است.

Mod: فرمت Mod یکی از فرمت های قدیمی کامپیوتر است که در زمان سیستم عامل داس محبوبیت زیادی داشـت؛ ولی با ورود وینـدوز، کاربرد خود را از دست داد. این فرمت تا چهار کانال صوتی را پشتیبانی می کند. البته بیشـتر برای پخش موزیک (بی کلام) مناسب است تا صدا های دیگر.

در فرمت Mid، اطلاعات صوتی بصورت نت (Note) ذخیره می شود؛ یعنی اطلاعات مربوط به هر ساز، به همراه پرده ها، نت ها و سایر اطلاعات، جداگانه ذخیره می شود

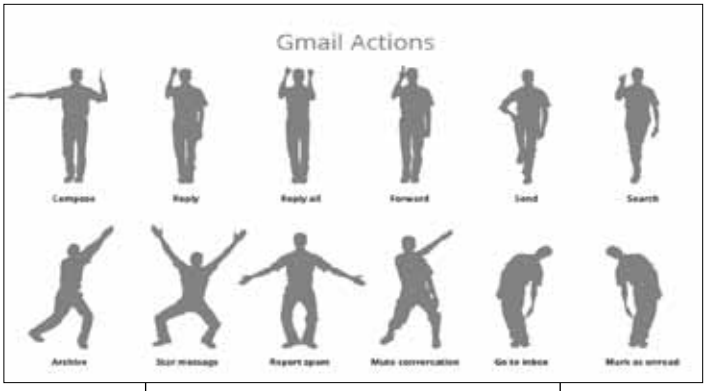
Mid: Mid یا Midi یکی از فرمت های قدیمی صداست که با وجود گذشت زمان، کهنه نشده و کاربرد خود را حفظ کرده است. Midi تشکیل شده از حروف اول این کلمات اسـت: Musical Instrument Digital Interface (بـه معنـای رابط دیجیتالی ابزارهای موسـیقی). کاربـرد اصلی فرمت Midi در موسیقی است. در واقع یک فایل Mid حاوی نت های موسیقی، اطلاعات مربوط به هر ساز، پرده ها، وقفه ها و همه اطلاعات تخصصی موسیقی می باشد. به همین دلیل با داشتن یک برنامه مناسب، می توانیم همه این اطلاعات را از فایل استخراج کنیم و این قابلیت برای موسیقی دانان بسیار مفید است. در اکثر کامپیوتر ها نیز یک درگاه Midi موجود اسـت که میتوانیم ابزارهای موسیقی را به آن متصل کرده و موسیقی نواخته شده را بـه صورت فایل Mid ضبـط کنیم. همچنین می توانیم نت ها را بنویسیم و ابزار موسیقی آن را برای ما بنوازد. فایل های Midi حجم بسیار کمی نیز اشغال می کنند و این نیز برای آنها یک مزیت محسوب می شـود. این فرمت در بسیاری از ابزارهای الکترونیک از جمله تلفن همراه نیز کاربرد دارد.

Aiff: این فرمت در اصل فرمت استاندارد کامپیوتر های آمیگا اسـت. آمیگا تا قبل از فراگیر شـدن PC حرف اول را در زمینه صدا و تصویر می زد. تا سـالها پـس از ورود pc نیز فایل هـای صوتی آمیگا کاربرد داشـت؛ ولی در حال حاضر به علت ورشکسـته شدن کمپانی Commodore این فرمت نیز توسعه نیافته و کارایی خود را از دست داده است.

Voc: این فرمت به کمپانی Creative و کارت های صوتی SoundBlaster اختصاص دارد. فرمت Voc نیز با ورود ویندوز و فراگیر شدن فرمت Wav، کم کم از گردونه خارج شد و اکنون کاربرد چدانی ندارد.

Wma: فرمت Wma یا Windows media audio یکی از جدی ترین رقیبان mp3 محسوب می شود. این فرمت حتی از بعضی جهات بر mp3 برتری دارد و با توجه به این که محصول کمپانی مایکروسافت است، آینده روشنی برای آن پیش بینی می شود. فایل های Wma حجم بسـیار کمـی دارند و کیفیت آنها نیز کاملا قابل قبول اسـت. در عرصه اینترنت نیز که حجم فایل ها اهمیت زیادی دارد، این فرمت با فرمت mp3 رقابت تنگاتنگی دارد.

Ra: فرمـت Real Audio نیـز یکی از فرمت های صداسـت که جایگاه خاصی را به خود اختصاص داده است. فایل هایRa نیز حجم کم و کیفیت قابل قبولـی دارند، ولـی چیزی که آنهـا را از دیگر فرمت هـا متمایز می کند، حجم آنها نیسـت؛ بلکه خاصیت streaming موجـود در فایل های Real اسـت. خاصیت Streaming یا جریانی، باعث می شود که فایل های صوتی از طریق اینترنت پخش شـوند، ولی کپی نشـوند. این ویژگی کمک زیادی به تولید کننده ها می کند و جلوی کپی های غیر مجاز را تا حدودی می گیرد. همچنین به کمک این قابلیت، می توان صدا را بـه صورت زنـده روی اینترنت پخش کرد. در حال حاضـر اکثر رادیو های اینترنتی برای پخش مسـتقیم برنامه های خود از فرمت Real استفاده می کنند.



Gmail Motion
دروغ سیزدهِ گوگل

محمد امینی

گوگل که یکه تاز تکنولوژی شده است نه تنها قصد ندارد سرعت خود را کم کند بلکه روز به روز آن را افزایش می دهد. گوگل تلاش می کند تکنولوژی را در کاربردی ترین شکل ممکن به مردم ارائه دهد و برای همین است که محبوب و پرکاربرد است. چندی پیش گوگل یکی دیگر از خدمات خود را در نسخه ی آزمایشی ارائه داد. Gmail Motion سرویس جدیدی است که گوگل برای راحتی کاربران ایمیل خود ارائه کرده است. با این سرویس علاوه بر موس و کیبورد، از حرکات بدن خود (در مقابل وب کم کامپیوتر خود) نیز می توانید برای کنترل جیمیل و کار کردن با آن استفاده نمایید.

روشی جدید برای برقراری ارتباط

همانطور که می‌دانید ماوس و کیبورد پیشتر از اینترنت اختراع شده اند. از آن زمان تا بحال، تکنولوژی های بسیاری در جهت استفاده ی بشر ارائه شده است. حالا چرا از کیبور و ماوس منسوخ استفاده کنیم؟! شما با استفاده از Gmail Motion می توانید با حرکات بدن خود، کارهای خود را در Gmail انجام دهید.

Gmail Motion چگونه کار می کند؟ Motion از وبکم تعبیه شده در سیستم شما برای شناسائی و ثبت جهات حرکات بدن شما، برای پیاده کردن منظور شما استفاده می کند. این حرکاتِ بسیار ساده در Gmail تعریف شده است و برایَ تمامی افراد قابل درک و راحت می باشد.

راهنمای حرکات:

شما می توانید خود را با استفاده از سند راهنمای حرکات، به استفاده ی حسی از Gmail عادت دهید. کافیست یک فایل pdf راهنما را دانلود و خوب مطالعه کنید. شما با استفاده از این، می توانید به ایمیل هایتان جواب بدهید و یا آنها را بخوانید؛ آن هم کامل، راحت و بدون صرف زمان زیاد.

شما با استفاده از این سرویس نه تنها راحت به کارتان می پردازید بلکه این کار بسیار مفید و جالب است. با استفاده از هر عمل فیزیکی، یک عمل از قبل تعریف شده را اجرا خواهید کرد. اول مطمئن باشید که اطرافتان آرام و ترو تمیز است دوم می توانید با استفاده از حرکات بدن تایپ خود را انجام دهید.

گوگل این امکان حس گر را در Gmail خلاصه نخواهد کرد. در همین سال جاری میلادی، گوگل این امکان را برای Google Doc نیز ارائه خواهد داد.

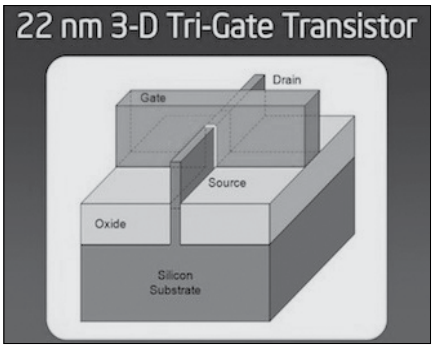
و اما اصل مطلب! آمریکایی ها هم مثل ما که دروغ سیزده داریم و توی یه روز یهو یه خبر دروغ منتشر میشه، اونا هم توی ماه آوریل همچین کاری میکنن و گوگل هم برای ادای این سنت، خبر انتشار یک تکنولوژی کاذب رو منتشر کرد! و اینچنین شد که گوگل هم مردم رو سرکار گذاشت! ولی از این گوگل بعید نیست که به زودی خبر انتشار واقعی همچین تکنولوژی ای رو منتشر کنه!

تولید انبوه ترانزیستورهای ۳بعدی توسط اینتل

محمدحسام کلانتری

برای اولین بار از زمان اختراع ترانزیستور های سیلیکونی در بیش از ۵۰ سال قبل، ترانزیستور ها توانستند که از یک ساختار سه بعدی استفاده کنند. بله اینتل ترانزیستور های سه بعدی را به تولید انبوه خواهد رساند! اینتل یک معماری انقلابی برای ساخت ترانزیستور های سه بعدی معرفی خواهد کرد که Tri-Gate (سه دروازه) نامیده می شود. البته این معماری برای اولین بار در سال ۲۰۰۲ و توسط اینتل معرفی گردید. اما اکنون می توانیم از به تولید انبوه رسیدن این ترانزیستور ها ابراز خوشحالی کنیم. این تولید انبوه با چیپ های Ivy bridge که از معماری ۲۲ نانومتری بهره می برند؛ آغاز خواهد شد.

مدیر عامل اینتل، پائول آتلینی می گوید: دانشمندان و مهندسان اینتل، یک بار دیگر ترانزیستور را اختراع کردند. اما این بار با استفاده از بعد سوم! او همچنین عنوان می کند که با استفاده از این قابلیت، دستگاه های اعجاب آورتر و دوران سازی ساخته خواهند شد. چرا که ما قانون مور را به عرصه جدیدی رساندیم. (قانون مور بیان می کند که تعداد ترانزیستور های روی یک تراشه با مساحت ثابت، هر دوسال یکبار، دو برابر خواهد شد؛ عملکرد و کارایی افزایش یافته و قیمت هم پایین خواهد آمد. این قانون بیش از چهل سال است که مدل تجاری پایه برای صنعت نیمه هادی ها محسوب می شود.)



دانشمندان مدت هاست که مزایای ساختار سه بعدی ترانزیستور ها را برای نگهداشتن سرعت قانون مور (سرعت بیشتر شدن ترانزیستور ها)، دریافته بودند. چرا که ابعاد داشت آنقدر کوچک می شد که قوانین فیزیکی سد راه پیشرفت بیشتر شده بودند. اما حالا با تولید انبوه این ترانزیستور های سه بعدی، قانون مور گسترش خواهد یافت. اکنون دری جدید به سوی نسل بعدی خلاقیت ها در طیف گسترده ای در دستگاه ها باز شده است.

ترانزیستور های ترای گیت، چیپ ها را قادر می سازند تا در ولتاژ پایین تری کار کنند و اتلاف انرژی کمتری داشته باشند. این نسل جدید، نسبت به نسل قبلی ترانزیستور ها یک ترکیب بی سابقه از افزایش کارایی و صرفه جویی انرژی را ارائه می کنند. این قابلیت به طراحان چیپ ها، این انعطاف پذیری را خواهد داد که بتوانند بسته به هدفشان، ترانزیستور ها را از نوع کم مصرف یا پرکارایی انتخاب کنند.

همچنین ترانزیستور های ۲۲ نانومتری سه بعدی جدید، توانسته اند، در برابر تارنزیستور های ۳۲ نانومتری دو بعدی؛ یک افزایش ۳۷ درصدی را در کارایی روی ولتاژ پایین تجربه کنند. این بهبود یعنی، این ترانزیستور ها برای دستگاه های قابل حمل و دستی ما نیز مناسب خواهند بود و چون در کارکرد یکسان نسبت به مدل های دو بعدی، ۵۰ درصد انرژی کمتری مصرف می کنند، می توانید به عمر باتری دستگاه های آینده خودتان خوشبین تر باشید.

در مورد چیپ های Ivy Bridge هم باید بدانید که می توانند روی لپتاپ ها، سرور ها یا کامپیوتر های رومیزی به کار روند. و خانواده بعدی Core نیز اولین پردازنده هایی خواهند بود که با ترانزیستور های ۳ بعدی به تولید انبوه خواهند رسید.

با این حساب باید باز هم منتظر کوچکتر شدن و کم مصرف تر شدن و کارا تر شدن وسایل الکترونیکی خود باشیم.

منبع :

http://newsroom.intel.com/community/intel_newsroom/blog/2011/05/04

ماجرای عجیب و غریب هک شدن SSL

افشین جمشیدی

تبریک عید از طرف سردبیر مجله، همراه بود با درخواست آماده کردن مقاله ای جدید. توی عید دنبال یه ایده ی ناب بودم که برم دنبالش، که هم خودم یه چیزی یاد بگیرم، هم اون اطلاعات رو با شما share کنم. اواخر عید شد و دیگه دنبال این بودم که بگم من نمیتونم چیزی بنویسم، تا اینکه باز یه ایرانی حادثه ساز شد و بازار ما رو از کسادی به در کرد! اول، عنوان خبر تو مایه های هک کردن gmail و yahoomail و SSL و.. بود! اصلاً منطقی به نظر نمی رسید که به راحتی یه نفر بتونه به همچین کاری بکنه. به قول یکی از نظرات، «هک کردن آر اس اِی ۲۰۴۸ چیزیه که مرغ پخته هم از شنیدنش خنده اش می‌گیره» (انتهای مقاله، توضیح مختصری از اصطلاحاتی که اینجا گفته میشه آمده است، اگر اطلاعاتتون کامل نیست، اول برید به اون قسمت)

ولی واقعا این ایرانیه ۲۱ساله چی کار کرده بود که تو خبرا گفتن گوگل هک شد یا تا هک کردن RSA پیش رفتن؟! به توانایی های خودمون شکی نیست، قبول! از اون طرف هم اگر علم در ثریا باشه مردانی از سرزمین پارس بهش دست پیدا میکنن. ولی این مورد نه تو ثریا هست که بخوایم پیداش کنیم) چون یکی از مبانی های زمینیه(، نه خیلی عملیه (چون خیلی مبانیه)! همون طور که احتمالا می‌دونید، حداقل تو تئوری نمیشه RSA و ارتباطات رمز شده رو کد گشایی کرد (هرچند که دوست هکرمون مدعی شدن که به زودی این کار رو میکنن و اوغات فراقتشون رو روی این مورد صرف میکنن!) ولی باز تا قبل از عملی شدن این ادعا، میتونیم با خیال راحت بگیم که همیشه ۲*۲=۴ میشه. البته دسترسی به ایمیل ها (بدون حساب اشتباهات کاربران) هم کار به نسبت غیر ممکنی به حساب میاد، ولی هکر ایرانی، دقیقا دست روی معضلات پیاده سازی این قوانین گذاشت و تونست به ایمیل ها نفوذ کنه.

اما دقیقا چه اتفاقی افتاده بود؟ این لینک خبر سایتیه که هک شده بود و به واسطه اون ایمیل ها قابل دسترسی شده بودن: http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

اگر اطلاعات انتهای این مقاله رو بخونید، متوجه میشید که برای تایید وجود ارتباط امن بین کامپیوتر شما و mail serverی که ازش استفاده می‌کنید، باید یه گواهینامه دیجیتال این ارتباط امن رو تایید کنه. کاری که این هکر انجام داده بود، هک کردن یکی از سایت هایی که گواهینامه دیجیتال صادر میکردن بود. به همین سادگی!!! سایت هایی که certification هاشون دزدیده شد: gmail، yahoo mail live. microsoft، mozila. البته patch امنیتی به سرعت برای ویندوز و Firefox آماده شد و گواهی نامه های جعلی تولید شده توسط هکر باطل شدند. ولی این کار به نوبه خودش نکات قابل توجه زیاد داشت. مثلا هیاهویی که به پا کرد، یا طرز متفاوت برخوردهای شخص هکر، تنها کار کردن هکر و مدعی شدن وابسته نبودنش به جای خاصی و...

نکته جذاب دیگه این بود که این سری هیچ خبری از هکرهای معروف قبلی نبود. گروه هایی از هکرهای کلاه رنگی که هر کدوم رزومه های قوی ای دارن. مثلا گروه آشیانه که طبق آمار رسمی دومین تیم هکری بزرگ دنیا هستن. یا هکرهای معروف مرتبط با مراکز دولتی. (همون طور که می‌دونید، هکرها هم طبقه بندی های خودشون رو دارن و با اهداف مختلفی حملاتشون رو انجام میدن. اطلاعات بیشتر رو میتونید از اینجا بخونید:

http://fa.wikipedia.org/wiki/رخنه-کردن

(http://zone-h.org/stats/notifierspecial

چیزی که به نظر من یه هکر رو جذاب میکنه، کارهای مرموزیه که میکنه. ولی این هکر ۲۱سالمون خیلی دنبال تشریح جزییات هست. چندین نامه عمومی منتشر کرده، با چندجا مصاحبه کرده، تقریباً جواب هر کامنتی رو در مورد این هک داده! تاکید میکنه که حرکتش نه سیاسیه، نه کاری به سیاست داره، و فقط آدم مذهبیه وطن دوستیه، ولی متاسفانه لحن صحبتای مذهبیش و وطن دوستی هاش، خیلی برای من آشنا بودن!!! هنوز ضربه ی خاصی نزده، دنبال تهدید کردن هست و حرف های پر رنگ و بو میزنه!! وقتی از روند هک شدن سایت یکی از بانک های کشورمون خبردار شدم، راه های نفوذی که هکرها داشتن تا تونستن نفوذ کنن، اعلام باگ هایی که سرورهای اون بانک داشتن و خلاصه برخورد هکراشون جذاب و متین بود ولی این هکر به سرعت، ادعای داشتن تجربه ۱۰۰۰ برنامه نویس را کرده، برای اینترنت قانون تعیین میکنه.

البته هر کاری با یه هدفی انجام میشه که ممکنه از یه زاویه دیگه اون کار بیهوده به نظر برسه. مثلاً شکستن قفل یه برنامه، با هدف استفاده ی مجانی از اون برنامه انجام میشه و نمیشه گفت اون برنامه تواناییه انجام کارهایی که قرار بوده انجام بده رو نداره، چون قفلش رو دبیرستانی ها هم تونستن بشکونن!! از طرف دیگه، هر چیزی یه مفهمی داره. دسترسی به گواهینامه های دیجیتال و جعل اونها، امنیت گوگل رو زیر سوال نمیبره و اسمش هک کردن گوگل نیست. چون هک کردن هم مراحل و مفاهیم خودش رو داره.

البته این حرف ها به این معنی نیست که کار این هکر رو به سخره بگیریم، ولی این کار دستآوردی به جز ایجاد حس ناامنی در اینترنت و بیان توانایی های شخصی نداره که اگر هدف هکر هم همین بوده، باید بگیم که موفق شده. چون به سرعت هم گواهی نامه های جعل شده انقضا شدند، هم patch امنیتی لازم ارائه شد.

می‌تونید از لینک های زیر، روند دقیق هک شدن سایت کمودور و صحبت های هکر رو از زبون خودش بخونید.

http://pastebin. com/74KXCaEZ

http://erratasec. blogspot. com/2011/03/interview-with-comodohacker. html

http://erratasec. blogspot. com/2011/03/verifying-comodo-hackers-key. html

یه راه دیگه هم برای دزدیدن اطلاعات هست. اونم این که شما یه ارتباط امن با یه جای دیگه، مثلا ISPتون برقرار کنید، و ISP به جای شما با سرور گوگل ارتباط برقرار کنه. این طوری درسته که ارتباطات رمز شده هستن، ولی یه شخص سومی وجود داره که اطلاعات از طریق اون بازخوانی و دوباره رمز نگاری میشه. البته این راه هم اما و اگر زیاد داره، که شاید در آینده در موردش بحث کردیم!!!

یه نکته ی مهمی رو یادمون نره، اونم این که ما اینجا اخبار رو از زاویه تکنولوژی بررسی می‌کنیم. بعضی چیزا اسمشون بزرگه، ولی روند کار به بزرگی اسمشون نیست. مثل ویندوز قرمز و هک کردن ایمیل ها. اسم هک همیشه جذاب بوده (و این جذابیتش باعث اشتباه غیر متخصص ها میشه که هر کاری رو که اونا نمیتونن انجام بدن رو به عنوان هک و استفاده نا متعارف از کامپوتر تلقی کنن)، مخصوصاً وقتی موردی که هک میشه، بزرگ باشه. ولی همیشه اتفاقاتی که میافته به همون بزرگی نیستن.

مثل اتفاقی که چند سال پیش افتاد و یه دانشجو، با یه حدس ساده رمز عبور ایمیل یکی از سیاستمداران آمریکایی رو به دست آورد. که میتونید اتفاقاتی که افتاد رو از لینک های زیر دنبال کنید.

http://www.huffingtonpost.com/2008/09/17/palins-email-account-hack_n_127184.html

http://en.wikipedia.org/wiki/Sarah_Palin_email_hack

ادامه در صفحه بعد

ادامه از صفحه قبل

ماجرای عجیب و غریب هک شدن SSL

اس اس ال چیست ؟

از این پروتکل برای امن کردن پروتکل های غیرامن مانندHTTP، LDAP، IMAP و ... استفاده می شود. در حقیقت SSL بر این اساس یکسری الگوریتم های رمزنگاری بر روی داده های خام قرار می دهد که قرار است از یک کانال ارتباطی غیرامن بگذرد تا محرمانه ماندن داده ها تضمین شـود. به بیان دیگر شرکتی که صلاحیـت صدور و اعطاء گوهینامه دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات بین شبکه ای را امن کنند گواهینامه صادر میکند. این مدارک باید احراز هویت کاربران را تایید کنند و از هر طرف گواهینامه تایید شـود. اگر اطلاعات حین انتقال به سرقت رفت برای رباینده قابل درک نیست که این کار را به صورت الگوریتم های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقاران انجام می دهد.

برای داشتن ارتباطات امن مبتنی بر SSL، عموماً به دو نوع گواهی دیجیتال SSL، یکی برای سرویس دهنده و دیگری برای سرویس گیرنده و هم چنین یک مرکز صـدور و اعطای گواهینامه دیجیتال (Certificate authorities) که به اختصار CA نامیده می شود، نیاز است. وظیفه CA این است که هویت طرفین ارتباط نشانی ها، حساب های بانکی و تاریخ انقضای گواهینامه را بداند و بر اساس آن ها هویت ها را تعیین نماید.

SSL چگونه کار می کند؟

SSL در واقع پروتکلی است که در آن ارتباطات به وسـیله یک کلید، رمز گذاری (Encryption) می شوند. لازم به ذکر است زمانی که قرار است یکسری اطلاعات به صورت SSL به یک سایت که سرور آن گواهینامه SSL را دارد (ابتدای آدرس سایت https باشد) ازسال شود، ابتدا باید از یک کلید به عنوان قالبی بـرای به رمز درآوردن اطلاعـات بین خدمات گیرنده (Client) و خدمات دهنده (Server) استفاده شود. برای ساخت این کلید نیاز به چند مرحله هماهنگی به شرح زیر است.

• وقتی سـرور بخواهد پروتکل SSL را فعال کند ابتدا یک کلید عمومی (Public Key) می سازد.

• سـپس کلید عمومی را همراه با یک درخواسـت گواهینامه SSL به یکی از صادرکنندگان این گواهینامه مثل وریسایین (Verisign) ارسال می کند.

• وریسایین نیز ابتدا مشخصات و میزان قابل اعتماد بودن و امنیت سرور را ارزیابی کرده و کلید عمومی را دوباره رمزگذاری می کند و برای سرور می فرستد تا در انتقال اطلاعات خود از آن استفاده کند. به این کلید جدید کلید خصوصی یا امنیتی (Private Key) می گویند.

• حال هر زمان که کاربر بخواهد از طریق پروتکل SSL به این سایت دست یابد، ابتدا کامپیوتر کاربر یک کلید عمومی برای سرور می‌فرستد (هر کامپیوتر کلید مخصوص به خود را دارد).

• سرور نیز این کلید عمومی را با کلید امنیتی خود مخلوط کرده و از آن کلید جدیدی می سازد سپس آن را به کامپیوتر کاربر می‌فرستد.

• از ایـن به بعد تمامی اطلاعاتی که رد و بدل می شوند با این کلید جدید رمزنگاری می شوند.

از اونجایی که توضیح الگوریتم RSA از حوصله این مقاله خارجه، خودتون توی لینک های زیر دنبالش برید.

http://en.wikipedia.org/wiki/RSA

http://fa.wikipedia.org/wiki/آر‌اس‌ای

اندر احوالات ارشد کامپیوتر در خواجه نصیر

محمد امینی

مهر ماه سال ۸۸ بود که گروه کامپیوتر دانشگاه صنعتی خواجه نصیرالدین طوسی، اولین ورودی کارشناسی ارشد کامپیوتر رو (در گرایش هوش مصنوعی) گرفت! خب اون موقع این خبر، باعث خوشحالی هم دانشجویان کامپیوتر و هم گروه کامپیوتر شد! اما این خوشحالی خیلی پایدار نبود. چرا که چند ماه بعد متوجه شدیم دانشجویان ارشد رضایت چندانی ندارند. ظاهرا از همون اول، گروه کامپیوتر استقبال خوبی ازشون نکرده! از مشکلات انتخاب استاد راهنما بگیرید تا عدم در اختیار گذاشـتن آزمایشـگاه و امکانات کافی و انتساب واحد ها در اول هر ترم! و بدتر از اون این تصور که بچه های ارشد کامپیوتر سطح علمی پایینی دارند! شـاید باورتون نشه! ولی یکی از دلایلی که دانشـکده به بچه های ارشد کامپیوتر آزمایشگاه و امکانات و پشـتیبانی کافی نمی‌داده این بوده که بچه های ارشد کامپیوتر خودشون رو نشون ندادن و ضعیف اند و از این حرفا! آخه یکی نیست بهشون بگه این بچه های ارشـد کامپیوتر وقتی که شما بهشون امکانات و آزمایشـگاه نمی‌دید و تحویلشون نمی‌گیرید چطوری خودشونو نشون بدن؟!

و اما دانشـکده یا گروه کامپیوتر هیچوقت نگفتند که اگر هم سطح بچه های ارشد پایینه علتش ممکنه پایین بودن سطح گروه و اساتید ارشد باشه! چند روز پیـش پای صحبت یکی از همین بچه های ارشـد نشسـته بودم. بیچاره خیلی ناراضی بود. از همه چی می نالید! اسـتاد، گروه، دانشـکده، نبودِ آزمایشگاه! (می‌گفت طبقه‌ی دوم سـاختمان اسـاتید کلی اتاق خالی داره، ولی گروه کامپیوتر گفته چون شما ضعیف اید و خودتونو نشون ندادید تا حالا، ما هم نمی‌تونیم بهتون جا و آزمایشگاه بدیم!!؟!)

و یک نکته ی جالب تر! دانشگاه پارسال با مرکز تحقیقـات مخابرات یه قـرارداد امضا می کنه با این منظور که بچه های ارشـد میتونن با پشتیبانی مالی مخابـرات پروژه هاشـون رو انجام بدند . خب چندتا از بچه های ارشـد کامپیوتر هم رفتند و طرح پروژه هاشـون رو برای مخابرات فرستادند و مخابرات هم اونا رو تأیید کرد و طبق قرار داد می بایست هزینه ی تحقیقات و پروژه ی اونا پرداخت می‌شـده. اما بعد از چند ماه هیچ خبری نشد! خود دانشجوها از هر طریق که پیگیری می کنن هیچکسی پاسخگو نیست! معلوم نیست مشـکل از مرکز تحقیقات مخابراته، مشکل از دانشگاهه و یا...! خلاصه اینکه از مصائب دانشجویان کامپیوتر هرچی بگیم کم گفتیم! عصر رایانه وظیفه‌ی خودش دونسـت که گوشه ای از مشکلات کامپیوتری های ارشد رو بگه، شاید مسئولین گروه و دانشکده این مطلب رو بخونن و دلشون به حال این بچه ها بسوزه!

و اما حرف آخر...

بـا عرض پوزش از کلام صریح بنده!! اول می‌خوام بپرسم که مسئولین گروه کامپیوتر آیا با علم به این که اسـتاد و امکانات به اندازه ی کافی ندارند، دانشـجوی کارشناسی ارشد گرفتند؟! آیا توی شرایطی که نیازهای دانشجوهای کارشناسی همچنان بی پاسخ مونده، پذیرش دانشجوی ارشد ضروری بود؟! یا حتی اگر هم پذیرش ضروری بود، آیا فراهم کردن امکانات و اساتید مناسب برای دانشجویان ارشد ضروری‌تر نیست؟! متأسفانه گروه کامپیوتر با گذشت ۵ سال از آغاز فعالیتش، با وجود تلاش خـود بچه های کامپیوتر برای ارتقاء، هنوز به اونجایی که باید و شایسـته‌ی یه دانشـگاه صنعتی توی تهران هسـت نرسیده! خوشحال می‌شویم اگر پاسخ مسئولین گروه و دانشـگاه رو در این موارد بدونیم و در شماره‌ی بعدی چاپ کنیم.

۱- تصویر قرارداد امضا شده در انجمن علمی موجود است. همچنین برای کسب اطلاعات بیشتر و جزئیات و چگونگی قرارداد و پرداخت هزینه ها به سایت مرکز تحقیقات مخابرات مراجعه کنید.
http://www.itrc.ac.ir/Itrcstudentdr.php

اگر بن لادن توییتر را چِک می کرد...

افشین جمشیدی

حـالا که بن لادن هم آفلاین شـده، اخبار مختلفی در موردش منتشر میشه. با این که آمریکایی ها تا جایی که تونسـتن، از انتشار اخبار جلوگیری کردن، ولی باز اخبار زیادی از پرخرج ترین دشمن آمریکا با هزینه ۳ تریلون دلار (به نقل از اینجا: http://mashreghnews.ir/NSite/FullStory/News/?Id=۴۵۳۶۶) منتشر میشه.

اگر پیگیر زندگی بن لادن باشید، میدونید که نه تنها تحصیل کرده بوده، بلکه آدمِ از تکنولوژی به دوری نبوده و حتی برای بچه هاش هم معلم خصوصی زبان انگلیسـی و کامپیوتـر میگرفته. از لحاظ جنبه های فردی زندگی هم با توجه به بیان همسرانش انسان خوبی بوده.

طبق اخبار منتشر شده، بن لادن با این که در محله ای اعیان نشین و در خانه ای ۱ میلیون دلاری زندگی می‌کـرده، باز هم اینترنت نداشـته، ولی القاعده را توسط ایمیل رهبری و هماهنـگ می‌کرده!! البته این بار خبری از تکنولوژی خاص و جدیدی نیست. بن لادن ایمیل ها را با فلش مموری به یکی از یاران معتمد خود می‌داده و او هم از کافی نتی ایمیل‌ها را ارسال میکرده. به همین سادگی

یکی دیگه از اتفاقات جالبی که باز به استفاده ی بن لادن از تکنولوژی برمیگرده، اینه که یه آدمی (منظور، یک هویت مجازی یا پروفایل به آدرس https://twitter.com/ReallyVirtual) بـدون اینکه در جریان حمله به بن لادن باشه، وقتی برای دوری از شهر، به کوه های همون منطقه رفته بوده، گزارش لحظه به لحظه از پرواز هلی کوپترهای آمریکایی بر فراز شهر رو در توییتر منتشر می‌کنه. بعد از انفجار یکی از هلی کوپترها، و اخباری که در مورد خبر مهمی که اوباما قرار بود اعلام کنه، حدس هایی هم می‌زنه و اون شب پر هیجان رو لحظه به لحظه توییـت می‌کنه. این جا هم اگر بن لادن اینترنت داشـت و یه سـر به توییتر می‌زد شاید مرگش به تعویق می‌افتاد...

یکـی از نتایـج اخلاقی ای که می‌شـه گرفت اینه که استفاده از تکنولوژی همیشه خوبه، به شرط این که اطلاعات کافی در موردش داشته باشی و خود تکنولوژی باعث دردسر نشه.

- http://www.msnbc.msn.com/id/43011358/ns/technology_and_science-tech_and_gadgets/t/how-bin-laden-emailed-without-being-detected/from/toolbar

Tel : 84062397

asrerayane@nasircom.com

www.NASIRCOM.com