زيرساختارهاي امنيتي مدرن براي مبادلات در شبكه اينترنت

دكتر شهرام بختياري، استاديار پژوهشكده الكترونيك دانشگاه صنعتي شريف در يك مقاله‌علمي، زيرساختارهاي امنيتي مدرن براي مبادلات در شكبه اينترنت را مورد بررسي قرار داده است.
به گزارش خبرنگار گروه فني مهندسي خبرگزاري دانشجويان ايران (ايسنا) در اين مقاله آمده است: استفاده از رايانه امروزه جزو كارهاي روزمره بسياري از افراد قرار گرفته و در كشورهاي پيشرفته، سيستمهاي رايانه‌اي جزو لاينفك زندگي افراد جامعه مي‌باشند. در كشورهاي در حال توسعه از جمله ايران، فرهنگ استفاده از رايانه با سرعت زيادي در حالت شكل‌گيري است و پيش‌بيني مي‌شود كه در آينده‌ي نه‌چندان دور، شاهد همه‌گير شدن استفاده از رايانه در ايران باشيم.
در عصر كنوني استفاده از رايانه به تنهايي قابليت زيادي را براي كاربران فراهم نمي‌كند بلكه عمدتا رايانه‌ها از طريق خطوط تلفني (dial-up) و يا شبكه‌هاي محلي (lan) به يكديگر متصل هستند. استقبال جهاني از شبكه اينترنت و وجود ابزار و استانداردهاي مختلف، زمينه‌اي را فراهم آورده تا بتوان كاربران را به راحتي با يكديگر ارتباط داد و منابع و اطلاعات الكترونيكي را درميان آنها از طريق خطوط شبكه‌اي توزيع نمود. حتي مشاهده مي‌شود كه بسياري از اطلاعات با ارزش از قبيل اطلاعات مالي (خريد و فروش) و يا اطلاعات سري نيز از طريق شكبه اينترنت بين كاربران رد و بدل مي‌شوند.
دو مساله مهم كه كاربران شبكه‌هاي كامپيوتري با آنها دست به گريبانند عبارتند از :
۱- حفظ حريم خصوصي و محرمانگي: كاربران علاقمند هستند كه كارها و ارتباطات آنها غير قابل رديابي توسط ديگران باشد و همچنين پيام‌هايي كه آنها در شبكه مي‌فرستند و يا دريافت مي‌نمايند، قابل فهم توسط مداخله‌گراني كه داده‌هاي رد و بدل شده در مسير شكبه را شنود مي كنند، نباشد.
۲- احراز هويت و عدم انكار: كاربران جهت پاره‌اي از مسائل نياز دارند كه از صحت هويت طرف مقابل، اطمينان حاصل نمايند و مطمئن شوند كه كاربري كه با آن تماس گرفته‌اند واقعا همان فردي است كه انتظارش را داشته‌اند. همچنين در بعضي از مسائل، ارسال كننده‌ي يك پيام نبايد بتواند پيامي را كه فرستاده انكار نمايد. اين ابزار همان امضاي معمولي افراد را شبيه سازي مي نمايد.
رمزنگاري به عنوان يك از روش‌هاي قابل اعتماد جهت فراهم آوردن سرويس‌هاي فوق قابل استفاده مي‌باشد. كلمه لاتين cryptography به معني علم نوشتن به رمز مي‌باشد. ولي امروز به صورت كلي‌تري جهت فراهم آوردن ابزارهايي كه مي‌توانند سرويس‌هايي را براي امنيت اطلاعات و داده‌ها ارائه نمايند، استفاده مي‌شود. امروزه رمزنگاري جزو روش‌هاي الزامي در فراهم نمودن امنيت سيستمها و شبكه‌هاي كامپيوتري مي‌باشد و مانند قديم، منحصر به سيستمهاي نظامي و بانكي نمي‌شود. در عصر شبكه‌هاي كامپيوتري، هر فرد مي‌تواند از منابع اطلاعاتي خود با استفاده از ابزارهاي امنيتي كه عمدتا توسط سيستمهاي رمزنگاري فراهم مي‌شوند، محافظت نمايند.
- سيستمهاي رمزنگاري متقارن و نامتقارن
با وجود اينكه امروزه سيستمهاي رمزنگاري براي كاربردهاي مختلفي مورد استفاده قرار مي‌گيرند ولي در ابتدا چنين سيستمهايي تنها جهت اختفا و به عنوان ابزاري براي به وجود آوردن محرمانگي پيام، طراحي شده بودند. در يك سناريوي كلي مي توان فضايي را در نظر گرفت كه در آن، كاربر A قصد ارسال پيام P به كاربر B را دارد. روش كار بدين ترتيب است كه ابتدا كاربر A ا زالگوريتم E جهت رمز نمودن پيام P

استفاده مي نمايد. الگوريتمهاي رمزنگاري، نياز به يك كليد رمزنگاري (Ke) دارند تا بتوانند از پيامي مانند P، يك خروجي مانند C توليد نمايند كه با پيچيدگي زيادي وابسته به هر دوي P و Ke باشد. كاربر B كه پيام C را دريافت مي‌كند با استفاده از الگوريتم رمزگشايي D و با استفاده از كليد رمزگشايي (Kd) اقدامه به بازنمودن پيام C مي‌نمايد و نتيجه، پيام P خواهد بود.
فرق اساسي ميان سيستمهاي رمزنگاري متقارن و نامتقارن اين است كه در سيستمهاي رمزنگاري متقارن Kd يا مساوي Ke است و يا به راحتي از آن استنتاج مي شود. در نتيجه كافي است هر دو كاربر A و B، كليد Ke را بدانند تا بتوانند پيامهايشان را توسط آن رمز نموده و سپس رمزگشايي نمايند. با توجه به اينكه Ke تنها براي A و B شناخته شده است لذا وقتي كاربر B پيام را باز مي‌كند، مطمئن مي‌شود كه پيام فوق از طرف A است (خاصيت احراز هويت) . با اين وجود A به راحتي مي‌تواند ارسال پيام فوق را انكار نمايد زيرا B نيز مي‌تواند چنان پيامي را به همان شكل، رمز نمايد.
در سيستمهاي رمزنگاري نامتقارن، كليدي‌هاي رمزگذاري و رمزگشايي متفاوت هستند. در حقيقت هر كاربر داراي يك زوج كليد مي‌باشد كه يكي كليد عمومي و ديگري كليد خصوصي مي‌باشد. فرض بر اين است كه كليد خصوصي، تنها توسط آن كاربر شناخته شده است ولي كليد عمومي براي همه افرادي كه قصد ارتباط با آن كاربر را دارند معلوم است. حال اگر A قصد ارسال پيامي محرمانه به B را داشته باشد، پيام را توسط كليد عمومي B رمز مي‌كند وآن را ارسال مي نمايد. كاربر B پيام رمز شده را توسط كليد خصوصي خود، رمزگشايي مي‌نمايد. با توجه به اينكه تنها B كليد خصوصي را داراست لذا هيچ فرد ديگري نمي‌تواند به محتواي پيام دسترسي پيدا كند. براي ايجاد خاصيت احراز هويت مي‌توان پيام را توسط كليد خصوصي رمز نمود تا هر فردي كه كليد عمومي آن كاربر را داراست بتواند رمز را باز نموده و در نتيجه هويت كاربر فوق احراز شود. البته در عمل به‌جاي اينكه متن، توسط كليد خصوصي رمز شود، توسط يك تابع در هم ساز (hash function)، يك جمع‌آزما با طول ثابت (مثلا ۱۲۸ بيت) ايجاد مي‌شود و سپس جمع‌آزما رمز مي‌شود.
- مقايسه الگوريتمهاي رمزنگاري متقارن و نامتقارن
الگوريتمهاي رمزنگاري متقارن و نامتقارن از جنبه‌هاي مختلفي قابل مقايسه هستند. با توجه به اينكه هدف ايجاد امنيت قوي در شكبه اينترنت مي‌باشد لذا امنيت، سادگي و همچنين افزايش توانايي‌هاي سيستم، داراي اهميت بيشتري مي‌باشند. از لحاظ امنيت مشكل مي توان سيستمهاي متقارن و نامتقارن را مقايسه نمود. سيستمهاي رمز نامتقارن، عمدتا بر اساس يك مساله سخت رياضي بنيان نهاده شده‌اند و تا وقتي آن مساله رياضي حل نشده، سيستم داراي امنيت لازم مي‌باشد. به عنوان مثال يكي از مسايل رياضي كه سيستمهاي رمز بر آن استوار هستند مساله تجزيه اعداد بزرگ مي‌باشد. با توجه به اينكه در سيستمهاي رمز نامتقارن، با اعداد بزرگ كار مي‌شود لذا اينگونه سيستمها در مقايسه با سيستمهاي رمز متقارن معمولا از سرعت نسبتا پاييني برخوردار هستند.
با وجود سرعت نسبتا كم الگوريتمهاي نامتقارن، سادگي كار با آنها و توانايي‌هايي كه فراهم مي‌آورند آنها را براي استفاده از يك سيستم بزرگ و همه‌گير جذب مي‌نمايند. كليدهاي استفاده شده در الگوريتمهاي نامتقارن، راحت‌تر از الگوريتمهاي متقارن قابل توزيع هستند. اگر فرض كنيم در شبكه n كاربرد وجود دارد و همه كاربران بخواهند توسط الگوريتم متقارن با يكديگر ارتباط امن داشته باشند، نياز به n (n-1)/۲ كليد مي‌باشد كه بين هر دو كاربر به اشتراك گذاشته شده است. در مقابل، اگر از الگوريتم نامتقارن استفاده شده باشد، به n زوج كليد (عمومي و خصوصي) نياز مي‌باشد. در ضمن چون در الگوريتمهاي نامتقارن، تنها كليد عمومي هر كاربر بايد در شبكه توزيع شود لذا بر خلاف الگوريتمهاي متقارن كه در آنها بايستي كليدها به طور امن (محرمانه) توزيع شوند، در الگوريتمهاي نامتقارن مشكل اساسي وجود ندارد.

- سازماندهي يك ساختار كليد عمومي
با مروري بر روند اعمال امنيت شبكه در چند دههي اخير ديده ميشود كه ديوار آتش (firewall)، جزو اولين روشهاي حفاظت در شبكه بوده است. سيستمهاي تشخيص نفوذگران (Detection Systems Intrusion) و شبكههاي خصوصي - مجازي (Virtual Private Networks) نيز پس از آن پا به عرصه وجود گذاشتند. در عصر كنوني ساختار كليد عمومي و يا اصطلاحات(PKI، Public Key Infrastructure) بهعنوان بهترين روش براي اعمال امنيت در شبكه شناخته شده است.
در اين قسمت قصد بر اين است كه ملزومات طراحي و سازماندهي يك ساختار كلي براي شبكه اينترنت بيان شود كه هر كاربر داراي يك زوج كليد مربوط به يكي از الگوريتمهاي نامتقارن باشد. با وجود اينكه امروزه ساختار كليد عمومي بسيار مطرح است ولي هنوز شاهد استفاده از روشهاي قديمي در شبكه اينترنت براي بسياري از كارهاي حساس و حتي خريد و فروش ميباشيم. البته بهدليل عدم هماهنگي در روشهاي فوق و پيروي نكردن از يك ساختار كلي و استاندارد، نياز به يك سيستم هماهنگ و كارا احساس ميشود.
- مشكلاتي كه در شبكه اينترنت وجود دارد
يكي از سادهترين مثالهايي كه نشان دهندهي ضعف شبكه اينترنت است؛ پست الكترونيكي ميباشد. سناريويي را در نظر بگيريد كه در آن كاربر A قصد ارسال پست الكترونيكي به كابر B را دارد. وقتي نامه از مبدا رها ميشود معمولا چندين گره را پشت سر ميگذارد و نهايتا به گروه مقصد يعني كاربر B ميرسد. در اين ارسال مشكلات فراواني ممكن است اتفاق بيافتند كه مهمترين آنها عبارتند از:
١) اگر ايجاد ارتباط فقط از طريق اينترنت ممكن است پس چگونه ميتوان آدرس كاربر B را به دست آورد به طوري كه مطمئن بود آدرس صحيح است؟
٢) چگونه ميتوان اطمينان حاصل نمود كه پيام ارسالي در بين راه (گرههاي عبوري) بازبيني نشدهاند و پيام محرمانه باقي مانده؟
٣) چگونه هويت فرستندهي پيام توسط گيرندهي پيام احراز ميگردد؟ بهعبارت ديگر، كاربر B از كجا بفهمد كه پيام فوق واقعا از طرف كاربر A ارسال گرديده؟
يكي ديگر از مشكلات اساسي كه هم اكنون در شبكه اينترنت وجود دارد؛ انتقال اطلاعات از طريق FTP، HTTP و حتي TELNET ميباشد. البته گونهاي از سرويسها و ابزارهاي تكميلي ساخته شدهاند كه تا حدي اينگونه مشكلات را رفع مينمايند ولي هنوز مكررا ديده ميشود كه اطلاعات رد و بدل شده در شبكه اينترنت بدون امنيت (محرمانگي و احراز هويت) ميباشد و حتي ديده ميشود كه مثلا كلمه عبور استفاده شده در پروتكلهاي FTP و يا TELNET به صورت ساده در شبكه ارسال ميشود و توسط هر فردي قابل كپي برداري ميباشد.
مهمترين مشكلي كه شبكه اينترنت با آن دست به گريبان است؛ عدم يك سيستم و ساختار كلي جهت ايجاد ارتباطات امن براي كارهاي حساس از قبيل تجارت الكترونيكي ميباشد. در حال حاضر بسياري از شركتها از طريق شبكه اينترنت اقدام به فروش كالاهاي خود نمودهاند كه عمدتا به كالاهاي ارزان قيمت محدود ميشوند، زيرا اولا هنوز اعتماد لازم بين كاربران بوجود نيامده و ثانيا بسياري از پروتكلهاي استفاده شده، از امنيت كافي برخوردار نيستند.
- راهكارهاي امنيتي
از سالها قبل، كارهاي زيادي براي ايجاد امنيت در شبكه اينترنت انجام شده است. به عنوان مثال PGP، SFTP، SHTTP، Shell Secure و Kerberos نمونههاي عملي هستند كه مورد استفاده قرار گرفتهاند، ولي هيچيك قابليتهاي لازم براي يك سيستم همهگير با تواناييهاي لازم براي نيازهاي جديد كاربران اينترنت را ندارند. يكي از معروفترين استانداردهايي كه ميتواند منجر به ساختار كلي مورد نظر شود، استاندارد X.509 ميباشد. اين استاندارد كه توسط ISO/ITU تهيه شده، جهت ايجاد يك چارچوب براي PKI ارائه شده است و مبتني بر استاندارد X.500 ميباشد.

استاندارد X.500 براي ايجاد سرويس دايركتوري (Directory service) براي شبكه‌هاي بزرگ كامپيوتري ارائه گرديده است.
استاندارد X.509 به‌عنوان يكي از قديمي‌ترين ساختارهاي مبتني بر كليد عمومي در سال ۱۹۸۸ ميلادي ظاهر شد كه متعاقب آن، نسخه‌هاي ۲ و ۳ نيز ارايه شدند. اين استاندارد هم اكنون در بعضي از سيستم‌ها و پروتكل‌ها مورد استفاده قرار گرفته و SET و SSL نيز از آن بهره مي‌برند. در اين استاندارد براي هر كاربر، يك گواهي صادر مي‌شود كه از آن طريق مي‌توان بسياري از نيازهاي امنيتي را برطرف نمود. توليد گواهي (Certification) و عمل تعيين اعتبار (Validation) دو عامل اصلي موردنياز در PKI مي‌باشند. هدف در عمل اول ايجاد ارتباط بين كاربر (يا شركت) و كليد عمومي آن بوده و در عمل دوم نيز هدف، تعيين اعتبار گواهي مي‌باشد.
- خصوصيات PKI
با توجه به مطالب ذكر شده، PKI را مي‌توان به صورت مجموعه‌ي سخت‌افزار، نرم‌افزار، كاربران، سياست‌ها و رويه‌هايي كه براي ايجاد مديريت، ذخيره، توزيع و انهدام گواهي مبتني بر رمزنگاري با كليد عمومي مورد نياز مي‌باشند تعريف نمود. خصوصياتي كه در يك سيستم PKI مورد نياز مي‌باشند عبارتند از:
۱) محرمانگي (Confidentiality): شامل محرمانگي محتواي پيام و عدم امكان شناسايي گيرنده و فرستنده پيام توسط نفر سوم.
۲) تماميت (integrity): شامل دست‌نخوردگي پيام، اطمينان از رسيدن پيام به مقصد و اطمينان از عدم دريافت بيش از يك نسخه پيام توسط گيرنده.
۳) احراز هويت (authentication): شامل اطمينان از اينكه پيام دريافت شده، از كسي ارسال شده باشد كه پيام نشان مي‌دهد و اطمينان از اينكه پيام ارسال شده را كسي دريافت مي‌كند كه فرستنده مدنظر دارد.
۴) عدم انكار (non - repudiation): شامل عدم امكان انكار دريافت پيام، توسط گيرنده پيام و عدم امكان انكار ارسال پيام، توسط فرستنده پيام.
۵) كنترل (control): شامل وجود قوانين مدون و منابع مورد اطمينان و همچنين امكان دنبال كردن و ثبت خطا در روند سيستم.
۶) در دسترس بودن (availability): اطمينان از فعال بودن سيستم در تمام اوقات.
- نحوه توزيع كليد عمومي
روش‌هاي موجود جهت توزيع كليد عمومي يك كاربر عبارتند از:
۱) ارسال مستقيم توسط كاربر.
۲) ذخيره در دفترچه تلفن.
۳) ذخيره در يك گره كه با احراز هويت، قابل دريافت باشد.
٤) استفاده از گواهي.
با يك بررسي مختصر معين مي‌شود كه روش چهارم از ديگر روش‌ها بهتر است. زيرا ضمن اينكه هويت صاحب كليد در موقع دريافت كليد عمومي قابل احراز مي‌باشد، از ايجاد ترافيك در گره‌هاي خاص (bottle - neck) نيز جلوگيري مي‌شود.
- طرح اصلي يك PKI مطلوب
براي طراحي يك سيستم PKI كامل و امن، نياز است كه ابزارهاي آن با دقت انتخاب شده و مشكلات احتمالي آن دقيقا مورد بررسي قرار گيرند. يكي از ابزارهاي اصلي در چنين سيستمي، توزيع كليد عمومي مي‌باشد كه طبق توضيحات مربوط به قسمت قبل، اين سرويس توسط گواهي قابل حل مي‌باشد.
- گواهي براي كاربران سيستم
حداقل اطلاعاتي كه در يك گواهي مورد نياز مي‌باشند عبارت است از اطلاعات شناسنامه‌اي صاحب گواهي، كليد عمومي صاحب گواهي، اطلاعات شناسه‌اي صادركننده گواهي (Authority CA:Certificate) و امضاي صادر كننده‌ي گواهي. با توجه به اينكه اين طرح يك طرح ملي بوده و قابل گسترش در سطح جهاني مي‌باشد لذا نمي‌توان انتظار داشت كه تنها يك صادركنندي گواهي براي تمام كاربران وجود داشته باشد. روش‌هاي مختلفي براي حل اين مشكل وجود دارد كه روش سلسله مراتب

بصورت cross - reference به عنوان مطلوبترين روش در نظر گرفته مي‌شود. در اين روش يك صادركننده‌ي اوليه وجود دارد كه كليه كاربران يك جامعه يا گروه به آن اطمينان دارند. دليل اينكه چنين ساختاري در نظر گرفته شده، امكان آسان و امن احراز هويت گواهي يك كاربر توسط كاربران ديگر مي‌باشد. در روش فوق نياز نيست كه هر كاربر براي تائيد هر كليد عمومي، مستقيما به صادركننده‌ي آن كليد مراجعه نمايد.

...- نحوه‌ي تعيين اعتبار گواهي كاربران
طبق ساختار سلسله مراتبي كه در قسمت قبل بيان شد، هر كاربر مي‌تواند به راحتي هويت كاربر ديگر را احراز و يا رد نمايد. با اين وجود به دليل اينكه امنيت كليدهاي استفاده شده در سيستم‌هاي رمزنگاري، تابع مقدار مصرف آن و همچنين زمان مي‌باشد، لذا لازم است كليدها پس از مدتي عوض شوند. بنابراين يكي ديگر از اقلامي كه بايد در گواهي كاربران منظور شود، تاريخ انقضاي گواهي مي‌باشد كه بر اساس متوسط زمان استفاده از كليد رمزنگاري محاسبه مي‌گردد. اين روش، مشكلاتي از اين قبيل را حل مي‌نمايد ولي اگر به دليلي، كليد خصوصي كاربري از محرمانگي خارج شود و يا كاربر تقاضاي گواهي جديد نمايد آنگاه كليد رمزنگاري قديمي آن كاربر از درجه اعتبار ساقط مي‌شود؛ در صورتي كه هنوز گواهي قديمي كابر ممكن است اعتبار داشته باشد. براي حل اين مشكل از يك ليست شامل شماره گواهي‌هاي از درجه اعتبار ساقط شده (CRL) استفاده مي‌كنيم تا گواهي‌هاي بي‌اعتبار، قابل پيشگيري باشد. بدين ترتيب اگر كار مهمي مانند انجام يك قرار داد مهم در حال انجام باشد لازم است كه كاربران پس از احراز هويت يكديگر (توسط گواهي امضا شده) اقدام به جست‌وجو در ليست فوق نيز بنمايند تا مطمئن شوند كه گواهي‌ها باطل نشده باشند.
- محتويات گواهي
جهت سازگاري با استانداردهاي جهاني، گواهي كاربران را طبق استاندارد X.509 تعريف مي نمائيم. براساس اين استاندارد، يك گواهي داراي اقلام زير مي‌باشد:
۱- شماره نسخه استاندارد: عددي صحيح كه نشان دهنده‌ي نسخه‌اي از استاندارد مي‌باشد كه در گواهي استفاده گرديده است. در حال حاضر بالاترين نسخه، ۳ مي‌باشد.
۲- شماره شناسايي: شماره شناسايي گواهي مي‌باشد و فرض مي‌شود كه يك صادركننده‌ي گواهي هيچ‌گاه دو گواهي با شماره شناسايي يكسان صادر نمي‌نمايد.
۳- شماره شناسايي الگوريتم امضا: شناسه‌اي است كه به تعيين الگوريتم صادركننده‌ي گواهي براي امضا كردن مي‌پردازد.
۴- نام صادر كننده‌ي گواهي: نام صادر كننده گواهي طبق استاندارد X.500.
۵- تاريخ اعتبار: شامل تاريخ شروع و خاتمه اعتبار گواهي.
۶- نام صاحب گواهي: نام صاحب گواهي طبق استاندارد X.500.
۷- كليد عمومي صاحب گواهي: شامل شناسه‌اي كه الگوريم نامتقارن استفاده شده و همچنين كليد عمومي متناظر با آن الگوريتم براي صاحب گواهي را معين نمايد.
اقلام ليست شده در بالا حداقل اطلاعات لازم در يك گواهي مي‌باشند. در بالا نام صادر كننده‌ي گواهي و نام صاحب گواهي، طبق استاندارد X.500 مي‌باشد كه جهت يكتا بودن نام، شامل اطلاعات سلسله مراتبي كاربر طبق فرمتي مشابه آدرس وب (URL) مي‌باشند. موارد اصلي كه در فرمت X.500 مورد استفاده قرار مي‌گيرند شامل كشور، نام كاربر، مكان، سازمان و واحد سازماني مي‌باشند.
در نسخه‌ي دوم از استاندارد X.509 به دليل اينكه ذخيره نام، طبق استاندارد X.500 ممكن است هميشه يك كاربر را به طور يكتا معين ننمايد (مثلا وقتي كاربري از شركتي اخراج شده و كاربر جديدي با همان نام استخدام شده)، لذا براي هر يك از صادر كننده‌هاي گواهي و صاحب گواهي يك شناسه يكتا در نظر گرفته شده است.
- روش محافظت از كليد خصوصي كاربران

يكي از مهمترين قسمت‌هايي كه بايد به طور جدي مورد توجه قرار گيرد؛ اطمينان از محرمانگي كليد خصوصي كاربران مي‌باشد. اگر به نحوي كليد خصوصي يك كاربر توسط كاربر ديگري مورد شناسايي قرار گيرد، كليه كارهايي كه توسط سيستم رمزنگاري نامتقارن امكان‌پذير است، توسط كاربر فوق قابل انجام خواهد بود. بنابراين محرمانگي، عدم انكار و احراز هويت براي كاربري كه كليدش كشف شده زير سوال خواهد رفت.
اولين مرحله‌اي كه در اين سيستم براي يك كاربر عملي مي‌شود؛ ايجاد گواهي است كه در اين مرحله نياز است كه كاربر يك زوج كليد رمزنگاري داشته باشد. بسته به اينكه سياست‌هاي اعمال شده در سيستم چگونه باشد، يكي از دو روش زير براي توليد كليد استفاده مي‌شوند:
۱) توليد كليد توسط كاربر: در اين روش كاربر توسط ابزارهاي مورد اطمينان، يك زوج كليد براي خود توليد نموده و سپس كليد عمومي خود را به همراه مدارك مورد تاييد صاردكننده‌ي گواهي جهت صدور گواهي ارائه مي‌دهد. حسن اين روش اين است كه كاربر از محرمانگي كليد خصوصي خود صد در صد اطمينان دارد. با اين وجود ممكن است كاربران عادي نتوانند براحتي ابزار مورد اطمينان براي توليد زوج كليد را فراهم آورند و همچنين براي انتقال كليد عمومي جهت صدور گواهي نياز است كه حتما هويت كاربر توسط صادركننده گواهي احراز گردد.
۲) توليد كليد توسط صادركننده گواهي: در اين روش صادركننده گواهي ابتدا زوج كليد كاربر را توليد مي‌نمايد و سپس با استفاده از كليد عمومي فوق، يك گواهي صادر مي‌گردد. سپس گواهي و كليد خصوصي كاربر به وي داده مي‌شوند. در اين روش كليد خصوصي بايد به صورت محرمانه به كاربر داده شود و بهترين روش حضور فيزيكي كاربر مي‌باشد. حسن اساسي اين روش، امكان قابليت كشف كليد (Key Pecovery) در سيستم مي‌باشد. با وجود اينكه امكان كشف كليد خصوصي كاربران توسط سيستم، موردعلاقه كاربران نمي‌باشد، ولي در بسياري از موارد اين خاصيت ضروري است. به‌عنوان مثال اگر كاربري اطلاعات مورد نياز يك سازمان را رمز كرده باشد و سپس از سازمان اخراج گردد، در صورت امكان كشف كليد خصوصي مي‌توان به اطلاعات فوق دسترسي پيدا كرد. مستقل از اينكه كداميك از دو روش فوق در سيستم استفاده گردند، كليد خصوصي كاربر بايد همواره به صورت محافظت شده باقي بماند.
چهار راه اصلي براي رسيدن به اين هدف عبارتند از:
۱) رمز، توسط كلمه عبور: در اين روش كه يكي از مشهورترين و پراستفاده‌ترين روش‌ها مي‌باشد، كليد خصوصي توسط يك كلمه عبور رمز مي‌شود و سپس به صورت فايل برروي ديسك و يا دستگاه‌هاي مشابه ذخيره مي‌شود.
۲) ذخيره در كارت‌هاي حافظه‌دار: در اين روش كليد خصوصي در كارت‌هاي با حافظه محافظت شده (معمولا توسط كلمه عبور) ذخيره مي‌شود و در موقع نياز، به حافظه رايانه منتقل شده و پس از استفاده دور ريخته مي‌شود.
۳) ذخيره در كارت‌هاي هوشمند: در اين روش از كارت‌هاي هوشمندي كه داراي پردازنده مي‌باشند جهت ذخيره كليد استفاده مي‌شود. با فرض اينكه قسمتي از الگوريتم رمزنگاري، داخل كارت انجام مي‌شود، كليد خصوصي هيچگاه كارت را ترك نمي‌كند.
۴) ذخيره در دستگاه‌هاي كاملا غيرقابل نفوذ (Truly attack - resitant devices): در اين روش از دستگاه‌هاي خاصي جهت ذخيره كليد استفاده مي‌شود كه بسيار امن‌تر از كارت‌هاي هوشمند (از نظر نفوذ پذيري توسط دشمن) مي‌باشند. روش اول به دليل اينكه كلمه عبور، معمولا قابل حدس زدن مي‌باشد و يا ممكن است كاربر آن را فراموش كند براي يك سيستم در سطح بزرگ PKI جالب به نظر نمي‌رسد. با مقايسه روش‌هاي ديگر، روش سوم به دليل اينكه كليد خصوصي به حافظه رايانه منتقل مي‌شود، بسياري از حملات را توسط نفوذگران فراهم مي‌سازد. روش چهارم نيز كاربر را وادار مي‌نمايد تا به توليدكننده‌ي دستگاه اطمينان دهد كه مطلوب نيست؛

زيرا مثلا دستگاه ممكن است پيام‌هاي اضافي را امضا نمايد و يا پيام‌هاي رمزشده را در خود ذخيره نمايد.
يكي از مهمترين خصوصيات كارت‌هاي هوشمند، امكان استفاده از كليد خصوصي در جاهاي مختلف مي‌باشد. در عصر ارتباطات امروزي نمي‌توان انتظار داشت كه كاربر هميشه از يك رايانه براي ارتباط با شبكه اينترنت استفاده نمايد و بنابراين كاربر با حمل كارت هوشمند خود مي‌تواند از هر نقطه‌اي كه به شبكه اينترنت متصل است (و دستگاه كارت‌خوان را داراست) ارتباط امن ايجاد نمايد.
كارت هوشمندي كه براي PKI مناسب مي‌باشد كارتي است كه در آن قسمتي از الگوريتم رمزنگاري كه نياز به كليد خصوصي كاربر دارد در كارت پياده سازي شده است و در نتيجه هيچ‌گاه نياز نيست كه كليد خصوصي از كارت خارج شود. اينگونه كارت‌ها معمولا توسط يك شماره شناسايي شخصي (PIN) محافظت مي‌شوند تا اگر كارت به دلايلي به دست فرد غيرمجاز برسد، قابل استفاده نباشد. اطلاعاتي كه در كارت ذخيره مي‌شوند، عبارتند از :
١) كليد خصوصي كاربر
٢) گواهي كاربر (امضا شده توسط صادركننده گواهي)
٣) كليدعمومي صادركننده گواهي اوليه (root)
۴) گواهي مربوط به كليه صادركننده‌هاي گواهي كه بين root و كاربر قرار مي‌گيرند
علاوه بر موارد بالا ممكن است يك شماره سريال براي هر كارت هوشمند در نظر گرفته شود و اطلاعات ديگري مروبط به الگوريتم ذخيره شده در كارت وجود داشته باشد
- مباحث تكميلي
لازم به ذكر است با وجود اينكه سيستم‌هاي PKI بسيار مفيد مي‌باشند ولي آنها نيز داراي محدوديت‌هايي مي‌باشند. به عنوان مثال كاربران بايد به يك صادركننده گواهي (جهت امضاي گواهي) اعتماد كنند. البته چنين اعتمادي دور از ذهن نيست، زيرا در سيستم‌هاي قديمي و حتي سيستم‌هاي غيرشبكه‌اي نيز همواره اعتماد، جزو ملزومات سيستم بوده است. به عنوان مثال در سيستم بانكي، دارنده حساب بايد به سيستم بانكي اعتماد داشته باشد.
يكي از نكات مهم و اساسي در ساختار طراحي شده، اعتماد به امنيت كارت هوشمند مي‌باشد. به عنوان مثال اگر كليد خصوصي كاربر و يا كليد عمومي صادركننده گواهي اوليه root، مورد دسترسي غير مجاز قرار گيرند، امنيت سيستم به خطر مي‌افتد.
در طرح ذكر شده فرض مي‌شود كه الگوريتم‌هاي رمزنگاري با شماره شناسايي، قابل تشخيص هستند و بنابراين كاربران مي‌توانند از الگوريتم‌هاي دلخواه خويش استفاده نمايند. همچنين در گواهي مي‌توان فيلدهاي متغير داشت و بنابراين بسته به نياز مي‌توان گواهي خاصي ايجاد كرد. به عنوان نمونه گواهي رانندگي، گواهي تحصيلي و غيره.
در سيستم فرض مي‌شود كه كاربر، مسوليت هر گونه امضايي كه با كليد خصوصي او انجام گرفته باشد را به عهده مي‌گيرد. حالتي را در نظر بگيريد كه كاربري متني را امضا نموده و سپس تاريخ انقضاي كليد رمزنگاري او به سر آمده، چگونه مي‌توان چنين امضايي را تاييد كرد؟ به عنوان راه اول مي‌توان همواره گواهي كاربر (و اطلاعات مربوط به صادركننده گواهي) را به همراه امضاي وي نگهداري نمود و در نتيجه امضاهاي قديمي نيز قابل پيگيري باشند. به عنوان راه دوم مي‌توان كليد عمومي كليه كاربران (حتي ابطال شده‌ها) را در يك ليست در سيستم نگهداري كرد تا در موقع بروز شكايت، قابل پيگيري باشند.
- نتيجه گيري
در اين مقاله استفاده از الگوريتم رمزنگاري نامتقارن به عنوان يك وسيله كارا براي هماهنگ كردن ساختار امنيتي شبكه در سطح بزرگ مورد بررسي قرار گرفت و يك طرح كلي براي فراهم كردن سرويس‌هاي محرمانگي، احراز هويت و عدم انكار ارائه

شـد. سـاختار ارائـه شـده بـه‌راحتـي امكـان اسـتفاده از سـرويس‌هـاي فـوق را فـراهم مي‌آورد.
برگرفته از:
خبرگزاري دانشجويان ايران - تهران
سـرويس علمي-آموزشـي

وبلاگ چيست؟

مطلب زير ترجمه مقاله آقاي هنري جنكيس – رييس گروه مطالعات تطبيقي رسانه هـا درMIT است كه در باره پديده وبلاگ نگاشته شده است . مقاله وي از منظر يك استاد ارتباطات در باره اين پديده قابل توجه است . وي اولا وب لاگ را يك رسـانه مـي دانـد و پس آن را در آينده انقـلاب ديجيتـالي بـا اهميـت ذكـر مـي كنـد . ايـن مقالـه در نشـريه Technology Reviweشماره ماه مارس ۲۰۰۲ درج شده است .

اين را بلاگ كنيد!

نويسـنده : هنري جنيكس

ترجمه با اندكي تلخيص : امير حسـين اصغري

چند ماه پيش من در كنفرانس تكنولوژي در كامدن پاپ بودم ، دوسـتي كـه در نزديكـي من نشسـته بود پيوسته مشغول تايپ كردن سخنراني ها در كامپيوتر دستي خود بـود وي لينك هاي مربوطه خود را مي يافت و با فشـار بـر دكمـه اي آن مطالـب را بـراي روز آمد كردن سايتش مي فرستاد. سريعا پس از پست مطالب در سايتش او پاسخ هايي از خوانندگانش در سراسر كشور دريافت مي كرد . او يك بلاگر بود .

بلاگرها در شكار گاه (اينترنت) مي گردند و به گرد آوري مي پردازند . بـراي مـا مطالـب را طي فعاليت خود در صفحات اينتر نت و... نمونه برداري كرده و گاه آنها را نقادي مـي كنند . ما در كنار درياي اينترنت ايم و آنها بر آن مي بارانند . بلاگرها مـردان آمـاده (رزم) انقلاب ديجيتالي هستند . كلمه « بلاگ » مختصر شده « وبلاگ » اسـت . چنـد سـال پيش يكي از كساني كه بسيار در وب مي گشت شروع به ارايـه گـزارش روزانـه كـرد . وي موجزي از اطلاعات نادر و جالب را كه در طي سـير در صـفحات وب بـه آنهـا برخـورد كرده بود را ارائـه مـي كـرد . پيشـرفت در ابـزار طراحـي «وب» ، بـراي تـازه آشـنايان بـا

اينترنت ساختن صفحات شخصي در وب را بسيار آسان كرد . تا آنجا كه بتوانند آن را بسادگي هر موقع كه خواستند روز آمد كنند – حتي هر ۵ دقيقه يكبار- بطوريكه آن دوست – در كنفرانس- انجام مي داد . بدين سان « بلاگها» داراي پويايي بيشتري نسبت به ساير استاندارد هاي وب سازي هستند . خيلي دائمي تر از پست كردن به صفحات بحث در اينترنت . آنها شخصي تر و خصوصي تر از روزنامه نگاري سنتي و عمومي تر از دفتر چه خاطرات هستند .

blogger.com يكي از چند سايتي است كه در قلب اين پديده واقع شده است . اكنون بيش از ۳۷۵۰۰۰ استفاده كننده از خدمات آن ، ثبت نام كرده اند و اين در حالي است كه روزانه بيش از ۱۳۰۰ عضو جديد بدان افزوده مي شود . صاحبان وبلاگ ها شامل افراد خيلي متفاوتي اند : از جماعت كليسايي كه وبلاگ را به عنوان پديده اي تاثير گذار براي سرپرستي روحي مخاطبان خودشان تا فعالاني كه در پي دادن آگاهي هاي سياسي هستند . همينطور از ورزش دوستاني كه مي خواهند با وبلاگ با ديگر مشتاقان داراي كنش و روابط متقابل باشند . اغلب اوقات بلاگرها تجربيا ت روزانه را تعريف مي كنند . پرچم داستانهاي جالب از انتشارات در صفحات وب تا تبادل نصايح درباره مشكلات خودماني در آنجا در اهتزاز است . سايت آنها داراي نامهاي رنگارنگي است . بعضي شان شبيه متن هاي واقعي ماجراجويي دوستان آكاردئون در قرن ۲۱ يا مهملات اروپايي هستند به حدي گاه به شما اجازه مي دهد در باره برخي از آنها تصور كنيد كه آنها داراي عقده هاي روحي جواني با زمان و فرصت زياد براي نوشتن هستند .

هنوز يك چيز خيلي مهم در جريان است . در زماني كه خيلي از نقطه . كام ها بسته مي شوند وبلاگ در حال اهتزاز و بر خاستن است . ما در آرامش بين موجهاي تجاري كردن در رسانه هاي ديجيتالي هستيم و بلاگرها تصرف كنندگان لحظه هايند كه بالقوه تنوع فرهنگي را افزايش داده و مانع انسداد مشاركت فرهنگي مي شوند .

براي دموكراسي در محيط رسانه هاي جاري چه رخ خواهد داد ؟ جايي كه قدرت در دست چند ناشر و شبكه قرار گرفته باشد . محقق رسانه ها « Robert Mc Chesney» اخطار مي دهد كه حدود رسايي صدا در بحث هاي سياسي ، تحت محدوديت و فشار در خواهد آمد . دانشكده حقوق دانشگاه شيكاگو نگران است كه متلاشي كردن وب

ممكن است موجب از بين رفتن ارزشهاي مشترك فرهنگي اي شود كه دموكراسي طالب آن است . به عنوان مصرف كنندگان ، ما اين كشاكش متقابل را تجربه مي كنيم . تلويزيون را روشن مي كنيم و اين احساس به ما دست مي دهد كه برنامه هاي كانال هاي مختلف شبيه يكديگرند . به داخل « وب » مي رويم و شلوغي نمي گذارد كه ما چيز هاي خوب را تميز دهيم . بلاگر به هر دوي اينها پاسخ مي دهد ، مناظر گوناگون را بسط مي دهد و اگر آنها باهوش باشند با ساختن دسته بندي هاي تخصصي از هرج و مرج داده ها جلو گيري مي كنند.

با ريسك خود ستايي به من اجازه دهيد اجازه دهيد تصور كنيم كه اگر بلاگر به عنوان تفسير آنلاين « رنسانس ديجيتالي» شنا خته و نگه داشته شود چه رخ خواهد داد ؟ بعضي ها ممكن است لينك هايي پست كنند و مرا الاغ پر مدعا بخوانند . ديگران ، اگر من خوشبخت باشم ، ممكن است احساس كنند كه من داراي بصيرت جالبي مي باشم . استدال من براي ريشه هاي سبزGRASS-ROOTS رسانه ها ممكن است از سوي دو گروه محافظه كار و مترقي خواه به يكسان جذب شود . اما در چارچوبهاي متفاوت ، بسته به ايدئولوژي در دستور كار صاحبان وبلاگها. در نهايت آينده مطبو عات ما ممكن است به نوعي ترك منازعه ناآرام ميان رسانه هاي تجاري واين ريشه هاي سبز GRASS-ROOTS وابسته باشد . جهاني را تصور كنيد كه در ان دو نوع قدرت رسانه اي موجود باشد يكي از ميان رسانه هاي متمركز بر آيد جايي كه هر پيام با انتشار در شبكه تلويزيون قدرت حاصل مي كند وديگري با وساطت ريشه هاي سبز مي آيد. بلاگر اين موضوع را بر خواهد گرداند به نوعي همگاني خواهد كرد كه هر كس توان در يافت و شنيدن اخبار را داشته باشد .

اين ممكن است سخت به نظر برسد كه تصور كنيم كه جامعه بلاگ به عنوان يك نيروهاي اطلاع رساني تقريبا به قدرتمندي يك رسانه داراي شخصيت حقوقي مستقل فضاي رسانه ها را تغيير خواهد داد . ما در تاريخ با كتاب هايي در باره ساموئل مورس ، مخترع تلگراف آشنا مي شويم اما نه درباره هزاران نفري كه با تلگراف كار مي كنند و پيام ها را مي فرستند و...

در نهايت شكل تكامل يافته بسياري از رسانه ها از ميان كنش متقابل ميان قدرت توزيع شده ريشه هاي سبز – نشريات مشاركتي- و نشرياتي كه شخصيت حقوقي انها متمركز است /نشريات دولتي/ متشكل مي شود .

به عنوان اينكه « انقلاب ديجيتالي» به يك دوره تحولي نزديك مي شود با وساطت وب لاگ ممكن است تا دوباره« ادراك عمومي »public perceptionبه يك رسانه تعريف شود و تاثير خود را گسترش دهد .

من وب لاگ مي نويسم / پس هستم !

ترجمه و تلخيص گزارش بي بي سي در باره پديده وب لاگ نويسي و سخنان برگزيدگان مسابقه بهترين هاي وب لاگ

بلاگرها در شكار گاه (اينترنت) مي گردند و به گرد آوري مي پردازند . براي ما مطالب را طي فعاليت خود در صفحات اينتر نت و... نمونه برداري كرده و گاه آنها را نقادي مي كنند . ما در كنار درياي اينترنت ايم و آنها بر آن مي بارانند . بلاگرها مردان آماده (رزم) انقلاب ديجيتالي هستند . كلمه « بلاگ » مختصر شده « وبلاگ » است . چند سال پيش يكي از كساني كه بسيار در وب مي گشت شروع به ارايه گزارش روزانه كرد . وي موجزي از اطلاعات نادر و جالب را كه در طي سير در صفحات وب به آنها برخورد كرده بود را ارائه مي كرد . پيشرفت در ابزار طراحي «وب» ، براي تازه آشنايان با اينترنت ساختن صفحات شخصي در وب را بسيار آسان كرد . تا آنجا كه بتوانند آن را بسادگي هر موقع كه خواستند روز آمد كنند – حتي هر ۵ دقيقه يكبار- بطوريكه آن دوست – در كنفرانس- انجام مي داد . بدين سان « بلاگها» داراي پويايي بيشتري نسبت به ساير استاندارد هاي وب سازي هستند . خيلي دائمي تر از پست كردن به صفحات بحث در اينترنت . آنها شخصي تر و خصوصي تر از روزنامه نگاري سنتي و عمومي تر از دفتر چه خاطرات هستند .

آيا تا كنون وبلاگ خوانده ايد؟ شايد شما يكي از افرادي باشيد كه وبلاگ داريد . يا ممكن است شما هنوز ندانيد كه آن چيست .

وبلاگ سايتي اينترنتي است كه توسط مردم معمولي مثل من و شما راه اندازي مي شود . آنها ، داستان ، شعر ، قطعه هاي ادبي ، عكس و يا مطالبي شبيه ساير وب سايت ها را به وبلاگ خودشان پست مي كنند.

- سريع آپ ديت مي شود .

آما نه شبيه روش home page. آنها دائماً عوض مي شوند . خيلي از وب لاگ ها يا «بلاگ ها» حد اقل هر روز روز آمد مي شوند و در بعضي موارد بارها در يك روز . بعضي از صاحبان وبلاگ مخصوصاً آنها كه براي مدتي بدين كار پرداخته اند-در صورتي كه از وبلاگ خود شهرتي به دست نياورند ، انگشت نما مي شوند. آنها ممكن است به همان اندازه در ميان همكاران خود به چهره اي قديمي باشند اما در اينترنت مشهورند .
غير از روزآمد كردن روزانه سايت ها ، نكته مهم ديگر ان است كه هر كس مي تواند يكي از آن را داشته باشد . ساختن يك وبلاگ نياز به تجربه زيادي از اينترنت ندارد و به هيچ وجه نيازي به پول نيست .

شروع ساختن وبلاگ در blogget.com ، سايتي كه پيشرفت وبلاگ ها از آنجا شروع شد – كمي بيش از دو دقيقه وقت مي گيرد – من آن را تست كرده ام – سادگي مراحل ساختن وب ، موجب افزايش سريع سازندگان وبلاگ شده است . سايت بسيار مورد توجه واقع شده است چرا كه اين ايده اكنون در جريان قرار دارد . بي بي سي نيوز آن لاين يك وبلاگ دارد كه خبرنگاران سياسي در مواقع اضطراري و سر بزنگاه اخبار را در آن به طور منظم آپ ديت مي كنند . گاردين يك وب لاگ جالب دارد كه اخبار بين المللي را در آن هم آهنگ مي كند .

وبلاگ شهرت و اعتبار خود را از حكايات و اطلاعاتي كه در خود دارد بدست مي آورد . درست مثل يك كتابخانه شخصي كه انسان مي تواند هر چيز جالبي را در آن ذخيره كند تا در روز هاي بعد به آن مراجعه كند . صاحبان وبلاگ همواره قدرت خلاقه و تجربه را در خود افزايش مي دهند .صاحب وبلاگ البته دوست دارد كه وبلاگ هاي ديگر را هم بخواند . آنها غالبا خطوط پيوسته اي ا ز يك وبلاگ به وبلاگ بعدي درست مي كنند . آنها فرا گرفته اند تا دوستاني بيابند . آنها گاه حتي با هم نرد عشق مي بازند ،

عصباني مي شوند ، بله گاهي هم از هم مي رنجند . وقتي كه هفته گذشته صاحب بهترين وبلاگ جايزه را برد شور و تهيجي در ميان وب لاگ نويسان به وجود آمد .

Tom Coates ، مرد پشت كيسه پلاستيكي ، ارگ ، جايزه بهترين وب لاگر اروپايي را برد .اجازه بدهيد جهان بداند در دفترخاطرات شما چيست ؟ او مي گويد: «من اكنون بسيار خوشحالم كه از خيلي وقت پيش تا حالا وب لاگ دارم و به همين دليل در جامعه بخوبي شناخته شده ام .» «خوب يا بد ، به نظر مي رسد كه مشتركان بسياري براي وب لاگ پيدا شده است . مردم داخل سايتي كه واقعاً براي آنها بهره اي نداشته باشد نمي آيند و به آن راي نمي دهند . بنا براين من بايد كار درستي انجام دهم » مقرر كردن جايزه ، « راهي با مزه براي ديدن سايت ها توسط افرادي است كه در صورت ديگر هرگزدر باره آنها چيزي نمي دانستند . اين همچنين تبليغي براي نوعي رسانه ي موثر است . مستقيم ، شخصي ، آنلاين و منتشر شده »

خانم Meg Pikard ديگر وب لاگ نويس انگليسي كه او هم برنده شده است ، سعي كرد تا جاذبه هاي وب لاگ نويسي را شرح دهد . « من الآن در باره وب خيلي بيشتر از چند سال پيش مي دانم كه تازه شروع به ساخت وب لاگ كردم . داشتن وب لاگي كه هر روز بايد آن را آپ ديت كرد راهي جالب براي شنا ختن سايتها ي جديد ، تكنولوژي ، خاطرات و نظرات است .من نمي خواهم يك شخصيت وبي داشته باشم ، سايت من تنها جاي پرسه زدن من است مثل زماني كه من با رفقايم به كلوپ ميروم اما در فرم ديجيتالي آن . من سايتم را براي خوشا مد و كنجكاوي خودم حفظ مي كنم .آنجا فضاي فكر كردن است .»و Dan Hon يكي از چهره هاي قديمي وب لاگ در انگلستان از زماني ياد مي كند كه تنها ۲۰ نفر وب لاگر در آنجا وجود داشت (الآن بيش از ۴۰۰ است) . او مي گويد :« اين روش ديگري براي ارتباطات است . من مي توانم از ايميل استفاده كنم اما برخي اوقات پست كردن مطالب در وب لاگم آسانتر است .»

ترجمه با اندكي تلخيص : امير حسين اصغري

موتورهاي جستجو

در ادامه بحث شيرين! روبوتها به نظر ميرسد كه اشاره اي هم بـه موتورهـاي جسـتجو يا search engines بد نباشد:

google.com, yahoo.com, Altavista.com, InfoSeek.com چنـــد نمونـــه از جستجوگرهاي معروف هستند.

موتورهـاي جسـتجو از روباتهـا (robots, spiders or crawlers) بـراي جسـتجو ميـان صفحات وب استفاده ميكنند.

بيشتر موتورهاي جستجو بانک اطاعاتي خود را بر اساس كلمات كليـدي يـا keywords تنظيم كرده اند.

Yahoo يک موتور جستجو نيست بلكه بر اساس موضـوع و كاتـالوگ بـه دسـته بنـدي اطلاعات ميپردازد.

Google.com يكي از موفق ترين موتورهاي جسـتجو در ماههـاي اخيـر ميباشـد؛ حتـي ميتوانيد در آن به جستجوي تصاوير هم بپردازيد!!

آيا ميدانستيد كه ميتوانيد كلمـات و عبـارات فارسـي را سـرچ كنيـد!؟ نتـايج جسـتجوي كلمه "خاطرات" در google جالب نيست؟!

يک راه تعيين كلمات كليدي براي صفحات وب اسـتفاده از meta tag هـا اسـت، كـافي است كه داخـل قسـمت <HEAD> از meta tag ي بـه نـام keywords اسـتفاده كنيـد:

< meta name="keywords" content=word1, word2 >

... و روبوتهـا بطـور اتوماتيـک كلمـات كليـدي نمونـه word1 و word2 را از روي متـا تـگ keywords خواهند يافـت.(سـورس ايـن صـفحه را ديـده و نگـاهي بـه keywords هـاي داخل تگ head بيندازيد. View/Source در اكسپلورر)

سايت مجـــله دنيـاي كامپيوتر هم اطلاعات جالبي در مورد موتورهاي جستجو دارد.

اگر ميخواهيد بيشتر در مورد موتورهاي جستجوگر بدانيد، سري بـه ايـن سـايت بزنيـد. اين يكي هم بد نيست.

چند لینک مفید

* در راستاي نبوي زدگي بعضيها (بر وزن بلا و مصيبت زدگي) موارد و لينكهاي ذيل جهت اچتمل كاران عزيز معرفيميگردند:

- html-color-codes.com حاوي كد هگزاي ۲۱۶ رنگ safe در اينترنت
- webmonkey سايتي كامل وخودآموز براي برنامه نويسي در اينترنت
- bignosebird.com آنچه شما خواسته ايد برنامه نويسي در اينترنت! حاوي كلي برنامه مجاني
- bootdisk.com اگر ديسک bootable لازم خواهيد داشتيد اين سايت را فراموش نكنيد.
- html_cheatsheet راهنماي سريع تگهاي HTML

* اگر بدنبال نرم افزاری برای دسته بندی و نمایش تصاویر گرافیکی هستید حتما نرم افزار irfanView (http://irfanview.tuwien.ac.at)را داون لود کرده و استفاده کنید. irfanView تحت ویندوز کار کرده بسیار کم حجم و سریع است و امکانات بسیار جالبی برای کارهای گروهی دارد مثلا میتوانید گروهی از تصاویر را به صورت اسلاید نمایش داده و یا دسته اي از تصاوير را با يک فرمان ساده resize کرده و همزمان تغيير نام دهيد و يا حتي فايل HTML براي آنها بسازيد.(برای تصاویر روز همین سایت , در چشم بهم زدنی ۴۰۰ تصویر را کوچک کرده و پس از اصلاح کیفیت از یک تا ۴۰۰ مجددا نامگذاري كرد! چيزي كه با فتوشاپ حداقل برای من ساعتها طول ميكشيد.)

http://www.khaterat.com

E – Mail: mohammad4763@yahoo.com