**امنیت در پایگاههای داده ای (سرور)**

**Misham.ir20**

**مقدمه**

با گسترش استفاده از تکنولوژي وب و توسعه برنامه‌هايي که براي کارکرد درين بستر توليد ميشوند مباحث مربوط به امنيت پايگاههاي داده اي بعد جديدتري پيدا کرده اند. هر چند از آغاز پيداش پايگاههاي داده همواره امنيت و تامين آن يک دغدغه مهم و پياده سازي مناسب  و کاراي آن يک خصوصيت بنيادي در پايگاههاي داده بوده است اما بهر روي بحث امنيت (Security)همواره در سايه مقولاتي همچون عملکرد مناسب (Functionality) ، کارايي (Performance) و قابليت اطمينان (Reliability) قرار ميگرفت. به عبارتي هنوز هم چندان عجيب نيست اگر ببينيم يک برنامه رده سازماني (Enterprise Level) با تعداد زيادي Client بدون هيچگونه ملاحظه امنيتي توليد شده و مورد استفاده باشد. حتي ميتوان درين زمينه مثالهاي جالبتري يافت. اغلب برنامه‌هاي Client-Server با نام کاربري  sa(System Administrator) به پايگاههاي داده متصل ميشوند. از ديد امنيتي اين مطلب يک فاجعه محسوب ميشود. هيچ تغيير و يا خرابکاري اي قابل رديابي نيست، همه کاربران به همه اطلاعات دسترسي دارند و الي آخر.

آنچه ذکر شد ، در واقع تصويري از وضعيت جاري بود، که بايد از دو منظر نگريسته شود: عدم وجود مکانيزمهاي امنيتي مناسب و نيز در صورت وجود چنين مکانيزمهايي عدم بهره گيري صحيح ازانها يا نداشتن سياست امنيتي مطلوب.

اين وضعيت شايد در دنياي برنامه‌هاي مبتني بر تکنولوژي‌هاي Mainframe يا Client-Server قابل تحمل بود اما در شرايط فعلي که برنامه‌ها با سرعت زيادي به سمت بهره گيري از بستر وب ميروند ادامه اين روند فاجعه بار است. در حال حاضر ديگر کاربران يک برنامه به صورت بالقوه تنها کارمندان يک سازمان نيستند. هر فردي ميتواند به سادگي باز کردن يک مرورگر وب به پايگاه داده شما متصل شود و مطمئن باشيد اگر مکانيزمهاي امنيتي را رعايت نکرده باشيد ، حذف تمامي داده‌هاي شما حتس از عهده يک نفوذگر عادي هم بر مي‌آيد.

اجازه دهيد يک فرض اساسي را مطرح کنيم. مديران IT يک سازمان بر دو دسته اند: مديران نوگرايي که به صورت داوطلبانه سازمان را به سمت ارائه خدمات عمومي و گسترده هدايت ميکنند و به همين دليل تکنولوژي وب را به عنوان تنها بستر موجود براي ارائه اين خدمات ميپذيرند و مديران سنتي محافظه کاري که قابليت اطمينان و کارايي سيستم جاري را تحت هيچ شرايطي حاضر نيستند در معرض خطر قرار دهند. وب از نظر اين گروه دوم کماکان يک تکنولوژي مشکوک غير قابل اطمينان است. در واقع دلايل فني اين گروه دوم هنوز هم چشمگير و قابل اعتناست، به خصوص گروهي که از mainframe‌ها صحبت ميکنند. قابليت اطمينان 0.99999 هنوز هم در دنياي غير Mainframe  يک روياست.

زماني که بحث امنيت در بستر وب مطرح ميشود به صورت عمده سه جزء زير مد نظر است:

* امنيت سرور(Server Security)
* امنيت در تصديق اعتبار(Authentication Security)
* امنيت محاوره(Session Security)

در ادامه نگاهي به جزئيات هريک از اجزاي اين دسته بندي خواهيم داشت.

شايد بخش عمده امنيت سرور مربوط به مدير شبکه و نيز کارشناس امنيت اطلاعات باشد. ازين نظر DBA مسئوليت چنداني ندارد ، البته اين به شرطي ست که قبلا متخصص امنيت شبکه مکانيزمهاي امنيتي مناسب را جهت سرور پيش بيني کرده باشد. اين مکانيزمها محدوده وسيعي از ابزارها و راه حلهاي امنيتي را در بر ميگيرد: فايروالها ، تشخيصگرهاي نفوذ (Intrusion Detectors) ، ضد ويروسها ، ... از جمله ابزارها هستند . معماري امن شبکه و لحاظ کردن مسائل امنيتي درين معماري نيز ميتواند حائز اهميت باشد. تمامي اين مباحث زير مجموعه بحث امنيت شبکه مي‌باشند که در بخش آتي به صورت خيلي مختصر به آن اشاره خواهيم کرد:

**معماري امن شبکه با نگاه به پايگاه داده**

**الف. در نظر گرفتن سخت افزار جداگانه جهت سرور وب و سرور پايگاه داده**

بسياري از سرويسهاي کنوني وب و حتي  شبکه‌هاي داخلي (Intranet) به گونه اي طراحي شده‌اند که سرور اصلي پايگاه داده (Back End Server) را روي همان سروري در نظر ميگيرند که سرويس وب روي آن راه اندازي شده است. البته براي اين کار چندين توجيه وجود دارد :

* توجيه اقتصادي: در نظر گرفتن هر دو سرويس بر روي يک ماشين از جهت هزينه کل سازمان يک صرفه جويي محسوب ميشود. بايد توجه داشت که براي ارايه هر دوي اين خدمات ماشينهاي با قدرت پردازش بالا بايد در نظر گرفته شوند.
* توجيه فني: عده اي برين عقيده‌اند که ارائه اين دو خدمت بر روي يک ماشين سبب بهبود کلي کارايي ميشود. استدلال اصلي محدوديت سرعت بر روي شبکه است. اين استدلال نيز توجيه چنداني ندارد زيرا حداقل سرعت شبکه‌هاي محلي فعلي ۱۰۰Mb/s است که بسيار بالاتر از حداکثر سرعت شبکه‌هاي WAN در حال حاضر است.

بنابراين از دو توجيه بالا تنها استدلال مبتني بر صرفه جويي اقتصادي کماکان ميتواتند مطرح باشد. اما خطرات اجراي اين دو سرويس بر روي يک مکاشين به حدي ست که بهتر است سازمان به جاي پذيرش اين ريسکها، هزينه اضافي مربوطه را متحمل شود. تا کنون روشهاي متعددي براي نفوذ به سرورهاي وب طراحي و اجرا شده است. بسياري از ويروسهاي کامپيوتري و نيز کرمهاي اينترنتي (Code Redو Nimda) نيز اساسا بر پايه همين ضعفها عمل ميکنند. صرف نظر از نوع سرور وبي که در نظر ميگيريد (Apache،IIS يا هر سرور ديگر) هميشه بايد اين احتمال را بدهيد که در صورت وجود يک شکاف امنيتي در سرور مربوطه، شما در مجموع کمترين ضرر را متحمل شويد.

جدا کردن فيزيکي دو سرور وب و پايگاه داده اين امر را تا حدي (دقت کنيد که فقط تا حدي و نه به طور کامل) براي شما تضمين ميکند که حتي اگر نفوذگري توانست اختيارات مدير سيستم مربوط به سرور وب را به دست بياورد نتواند به سادگي به اطلاعات موجود روي پايگاه داده نيز دست يابد.

**ب. قرار ندادن پايگاه داده در DMZ:**

در صورتي که از يک معماري امن براي پياده سازي شبکه خود استفاده کرده باشيد به احتمال زياد شبکه شما داراي يک بخش DMZ(Don’t Militarized Zone) خواهد بود. معمولا ارائه دهندگان خدمات عمومي را درين بخش از شبکه قرار ميدهند. بعنوان مثال سرورهاي وب، سرورهاي ميل ... که همگي جهت خدمات عمومي بکار ميروند درين بخش از شبکه قرار دارند.

ايده عمومي داشتن يک بخش DMZ ساده ست: سرورهايي که خدمات عمومي بيرون سازماني ارايه ميدهند نيازمند سطح کمتري از امنيت هستند. در واقع همه ميتوانند به آنها دسترسي  داشته باشند. اين دسترسي همگاني به هيچ وجه لازم نيست در مورد تمامي منابع شبکه اعمال شود. بنابرين منابع عمومي شبکه را در بخشي از شبکه قرار ميدهند که حساسيت امنيتي کمتري نسبت به آن وجود دارد. اين همان بخش DMZ است. با توجه به مطالب بالا بسيار بديهي به نظر ميرسد سرور پايگاه داده را بايد در همان بخش DMZ قرار دهيم زيرا که عموما اين سرور نيز مسئوليت ارائه خدمات همگاني را بعهده دارد. اما قضيه در باره سرور پايگاه داده تا حدي متفاوت است. اين سرور گرچه خدمات همگاني نيز عرضه ميکند اما تنها بخشي از داده‌هاي آن ممکن است جنبه همگاني داشته باشد در حالي که عمده آن در اغلب اوقات سري ست. بعنوان مثال سروري که اطلاعات مربوط به کارت اعتباري افراد را نگهداري ميکند از اهميت فوق العاده اي برخوردار است و هرگونه دسترسي به کل داده‌هاي آن ميتواند فاجعه بار باشد.

بنابراين بر خلاف ديد اوليه به اين نتيجه ميرسيم که پايگاه داده نميتواند و نبايد که در بخش DMZ قرار گيرد. اما راهکار جداسازي آن ازين بخش چيست؟

راه حل ايده آل براي اين جداسازي به شرح زير است: به صورت عام از يک فايروال اصلي براي ايمني کل شبکه و جداسازي آن از دنياي بيرون استفاده ميشود. اين فايروال در قسمت بيروني DMZ قرار دارد و داراي قواعد خاص خود است. بدلايلي که در بخش پيش ذکر شد که کلا عبارت بود از نياز به ارائه خدمات عمومي ،اين فايروال نميتواند کل ترافيک ورودي را محدود کند و ناچار است يک سياست (Policy) حداکثري را اعمال کند.

اما در داخل خود شبکه ، مابيت LAN داخلي و DMZ از فايروال دومي استفاده ميشود. اين فايروال دوم در حالت ايده آل تمامي ترافيک ورودي را سد ميکند بجز ترافيک ورودي از وب سرور به پايگاه داده. با اين تمهيد خاص هم پچايگاه داده خدمات عمومي خود را ارائه ميدهد و هم دستيابي عموم را به آن سد کرده ايم. درين صورت يک نفوذ گر حتي پس ازينکه کنترل کامل سرور وب را در اختيار گرفت ناچار است از قواعد سختگيرانه فايروال دوم نيز عبور کند و تازه پس ازان بايد بتواند به سرور پايگاه داده نيز نفوذ کند که انجام اين هر دو کار بسيار دشوار ميباشد و ريسک چنين شبکه اي عملا پايين مي‌باشد.

اما شايد در مقابل روش ما استدلالي اينچنين ارائه شود: ميتوان تنها با استفاده از يک فايروال امنيت را تامين کرد. روش آنهم اينست که براي سرورهاي پايگاه داده از IP مجازي استفاده کنيم. در واقع اين سرورها پشت يک NAT قرار داشته باشند. درين صورت نفوذگر اساسا از وجود پايگاه داده خبر ندارد تا بخواهد به آن نفوذ کند. اين استدلال يک ابراد عمده دارد و آنهم اينست که اگر نفوذ گر بتواند کنترل سرور وب را در اختيار بگيرد عملا در همان شبکه اي قرار گرفته است که سرور پايگاه داده دران قرار دارد و داراي همان رنج IP ميشود. بنابراين پس ازينکار در واقع تمهيد قبلي ما بلااثر ميشود و نفوذ گر ميتواند بسادگي مانند يک کاربر داخلي شبکه ما عمل کند.

حال که استدلالات فوق را پذيرفته ايم ميتوانيم کمي ايده آل تر باشيم و شبکه را ايمن تر کنيم. فرض کنيد که يک نفوذگر بتواند از لايه اول امنيتي شما عبور کرده وارد DMZ شود. اگر اين نفوذ به دليل نقص قواعد امنيتي فايروال شماره يک باشد احتمال نفوذ همين شخص به لايه دوم بسيار پايين است. اما اگر اين نفوذ به دليل وجود شکاف امنيتي خاصي بر روي فايروال باشد چطور؟ فرض کنيد به عنوان مثال هردو فايروال شما Check Point است. آنوقت نفوذگر بهمان سادگي که از لايه اول عبور کرده از لايه دوم امنيتي شما نيز خواهد گذشت چون هر دو فايروال ما از يک نوع است و طبيعتا شکاف امنيتي هردو يکسان است. بنابراين ميتوان پيشنهاد داد که فرضا اگر فايروال لاه اول شما Check Point است در لايه دوم بهتر است از PIX استفاده کنيد. اين مطلب باعث امنيت بالاتر شبکه شما خواهد شد.

اين روش گرچه موثر است اما از عهده هرسازماني بر نمي آيد. نگهداري، بروزسازي و پيکربندي فايروال عموما خودش يک تخصص خاص و بالنسبه گرانقيمت است. بنابراين وقتي از دو نوع فايروال استفاده ميکنيد دو تخصص جداگانه را در سازمان خود نياز خواهيد داشت که اين مطلب باعث دو برابر شدن هزينه نيروي انساني شما خواهد شد. علاوه برينکه اصولا خود سخت افزار فايروال هم گرانقيمت است و اصولا مشخص نيست که سازمان شما حاضر باشد چنين هزينه اي را متقبل شود (حتي با فرض دانستن ريسک امنيتي بالاي آن)

راه حل ديگري که ميتوان براي جداسازي بخش امن شبکه ارائه داد استفاده از بيش از يک کارت شبکه در فايروال است (شکل ۲)

همانطور که مشخص است درين روش توسط يک فايروال، DMZ از بخش امن شبکه جداسازي ميشود. تنها ترافيکي که حق عبور از اينترفيس اول (eth1) به اينترفيس امن (eth2) را دارد ترافيک ورودي از وب سرور به سرور پايگاه داده ميباشد. اين روش بسيار ارزان تر از روش قبلي ست اما مشخصا امنيت آن در حد امنيت روش قبل نيست و علاوه برآن ممکن است فايروال موجود ما عملا از چندين کارت شبکه پشتيباني نکند.

علاوه بر دو راهي که در فوق براي جداسازي پايگاه داده از مابقي شبکه ارائه داديم راه حل سومي هم وجود دارد: اينکه اساسا پايگاه داده را از مابقي شبکه جدانکنيم! دقت کنيد که با توجه به هزينه و نيز اندازه سازمان ممکن است جداسازي امکان پذير نباشد و حتي مجبور شويم که اين دو سرور را برروي يک ماشين اجرا کنيم. حتي درين صورت نيز بهتر است حداقل کارهايي که جهت ايمني مضاعف پايگاه داده از دستمان بر مي‌آيد انجام دهيم. بعنوان مثال ميتوانيم از يک فايروال نرم افزاري ارزان قيمت جهت ايمني بيشتر استفاده کنيم. بهر حال اين راه حل توصيه نميشود مگر در شرايط اجبار.

**رمز نگاري اطلاعات مابين سرور وب و سرور پايگاه داده**

براي جلوگيري از سرقت اطلاعات در بين راه(Sniffing) عموما از روشهاي رمز نگاري استفاده ميشود. متداول ترين روش تحت وب براي انجام اين منظور استفاده از پروتکل SSL است. عموم اطلاعات امن که بر روي اينترنت منتقل ميشوند از همين پروتکل استفاده ميکنند . بعنوان مثال انتقال اطلاعات شناسايي با سرورهاي معروف ايميل، انتقال اطلاعات مربوط به کارت اعتباري و غيره.

تا بدينجا اين پروتکل که اغلب سرورهاي وب و نيز مرورگرها ازان پشتيباني ميکنند سطحي از امنيت را تامين ميکند. اما آيا همين کافي ست؟

اغلب اين اشتباه پيش مي‌آيد که همين سطح از رمز نگاري را در مقابل حمله Sniffing کافي ميدانند. بايد دقت کرد که SSL به صورت عام تنها براي رمزنگاري اطلاعات مابين Client و سرور وب به کار ميرود و به صورت عادي اطلاعات مابين وب سرور و سرور پايگاه داده به صورت عادي و بدون رمزنگاري (Plain Text) منتقل ميشوند. بنابراين حتي اگر همه جوانب را در شبکه بيروني رعايت کرده باشيم، يک نفوذگر داخلي به سادگي ميتواند اطلاعات در حال انتقال مابين اين دو سرور را شنود کند. اين مطلب زماني بسيار جدي ميشود که بدانيم بر اساس داده‌هاي موجود، بالاتر از ۶۰٪ حملات موجود حملات درون سازماني مي‌باشد.

چاره کار استفاده از يک روش رمز نگاري مابين سرور وب و سرور پايگاه داده است. اغلب سرور‌هاي پايگاه داده امروزه از SSL حمايت ميکنند. MS SQL Server2000 ، Oracle،Sybase ازين جمله اند. البته استفاده از SSL براي ارتباط مابين اين دو سرور لازمه اش اينست که برنامه اصلي شما (Web Application) با همين ملاحظه طراحي و پياده سازي شده باشد.

اما در صورتي که برنامه شما از قبل موجود باشد يا از SSL پشتيباني نکند يا به هر صورت شما مايل به ايجاد هزينه اضافي نباشيد چه؟ آيا راه حل ديگري براي رمزنگاري مابين دو سرور وجود دارد؟ خوشبختانه چنين راه حلي وجود دارد: استفاده از SSH يا يک برنامه مشابه.

اصولا SSH برنامه اي شبيه Telnet است اما نسخه امن آن. يکي از قابليتهاي SSH ايجاد يک تونل امن است. به اين صورت که ميتوان برنامه SSH را به گونه اي اجرا کرد که بر روي يک پورت شنود کند کل اطلاعات آن را رمز کرده به کامپيوتر مقصد ارسال کند و آنجا پس از تبديل به حالت عادي به پورت مقصد تحويل دهد. با استفاده از اين روش (SSH Port Forwarding) يک تونل امن به صورت شفاف مابين دو سرور ايجاد شده است(شکل ۳).

مزيت استفاده ازين روش اينست که نياز به هيچگونه تغييري در سرورها و يا برنامه‌ها ندارد و تنها توسط چند خط دستور قابل اجراست.

**د. عدم استفاده از Hub و بهره گيري از Switch**

به صورت عادي زماني که از Hub استفاده ميکنيم تمامي اطلاعات عبوري در هريک از سيستمهاي موجود در شبکه داخلي قابل شنود است. يک نفوذ گر معمولي با استفاده از يکي از ابزارهاي Sniffing ميتواند اينترفيس شبکه با به حالت Promiscuous برده ، تمامي اطلاعات در حال جابجايي بر روي LAN را دريافت کند. البته استفاده از رمز نگاري خطر بالقوه بهره گيري ازين روش را کم ميکند اما هيچگاه نميتوان مطمئن بود که کل اطلاعات رمز نگاري شده است. بنابراين بهتر است حتي المقدور امکان بهره گيري از Sniffing را بر روي شبکه کاهش دهيم. استفاده از سوپيچها به جاي‌هاب يکي از روشهاي حل اين مساله است. با استفاده از سوئيچ در واقع يک مدار مجازي (Virtual Circuit) مابين دو نود در حال مکالمه ايجاد ميشود و ديگران به اطلاعات در حال انتقال مابين آن دو دسترسي ندارند.

**۲-۶. ارائه امن اطلاعات**

از ديد کلي امنيت اطلاعات براي ارائه خدمات اطلاع رساني بر روي وب به صورت عمده دو راه وجود دارد:

* توليد اطلاعات به صورت استاتيک
* توليد اطلاعات به صورت ديناميک

# 

# ۱-۲-۶. توليد اطلاعات به صورت استاتيک و مسائل امنيتي آن

معمولترين نوع دسترسي به اطلاعات در اينترنت استفاده از صفحات HTML است. هنوز هم بسياري از متخصصين، اين روش در دسترس گذاري اطلاعات (Web Publishing) را به روشهاي ديگر ترجيح ميدهند. البته دلايل اصلي آنها بيشتر مربوط به سادگي و قابليت انعطاف اين روش است.

درين روش اطلاعات يک بار توليد ميشود. توليد اطلاعات (صفحات HTML) ميتواند به صورت دستي يا به صورت اتوماتيک توسط برنامه‌هاي معمولي Client-Server انجام شود. پس از انجام اين فاز کليه اطلاعات بر روي سايت و سرور اصلي قرار ميگيرد (Upload).

امنيت اين روش به سادگي تامين ميشود. کافيست که اشخاص نام فايلهاي HTML را ندانند، درين صورت هرگز به آنها دسترسي نخواهند داشت. اينکار با استفاده از مکانيزم ساده اي صورت ميگيرد. عموم وب سرورها براي دايرکتوريهاي مختلف حق دسترسي تعريف ميکنند که يکي ازين حقوق دسترسي حق مشاهده محتويات يک دايرکتوري است. در صورتي که کاربري اين حق را نداشته باشد از اسامي فايلها بي خبر خواهد بود و در نتيجه قادر به مشاهده آنها نيست.

استفاده ازين روش مزايا و معايب خاص خود را دارد. مزيت آن امنيت بالاست. در واقع درينجا هيچ ارتباز اکيتيوي با سرور پايگاه داده وجود ندارد. اطلاعات به صورت برون خط (Offline) بر روي سرور وب بارگذاري ميشوند و پس ازان هيچ ارتباطي مابين کاربر عادي و چپايگاه داده وجود نخواهد داشت. بدين ترتيب خطر حملات به پايگاه داده کاهش چشمگيري مي‌يابد. اما از ديگر سو مديريت حجم انبوه اطلاعات با استفاده ازين روش بسيار دشوار ميباشد . ضمن اينکه قابليت انعطاف روش نيز بسيار محدود است. در واقع زماني که ازين روش استفاده ميکنيم هدف اصلي خدمت رساني و سهولت استفاده را قرباني امنيت کرده ايم.

##### ۲-۲-۶. توليد اطلاعات به صورت ديناميک

اين روش متداول ترين شيوه ايست که امروزه جهت ارائه خدمات بر بستر وب مورد استفاده قرار ميگيرد. درين روش صفحات موجود بر روي سرور وب عملا داراي هيچ اطلاعاتي نميباشند يا داراي حداقل اطلاعات هستند. تمامي اطلاعات در پايگاه داده است. به محض دريافت هر تقاضايي توسط سرور وب ، صفحات مورد درخواست او به صورت ديناميک از طريق جستجوي (Query) مناسب در پايگاه داده توليد ميشود.

براي پياده سازي اين روش طيف وسيعي از تکنولوژيها وجود دارد. ASP،JSP،PHP،CGI،ISAPI... و چندين روش ديگري که عم٥ما حول همين توليد ديناميک اطلاعات إر محيط وب طراحي شده اند. هريک از اين زبانها و روشها خود موضوع بحث مفصل و جداگانه اي است اما از ديد بحث حاضر چند نکته مهم را بايد مد نظر داشت:

* تا کنون شکافهاي جدي امنيتي در مورد هر يک ازين روشها شناخته شده إست و با وجود اين حل اغلب آنها هنوز هم هيچکدام آنها امنيت بالايي را به تنهايي تضمين نميکنند.
* با وجود نکته بالا، چون هدف اصلي ارائه خدمت ياسرويس است در بسياري موارد چاره اي بجز استفاده از يکي از اين روشها نداريم.
* هنگام انتخإب هر يک از اين روشها بايد ملاحظات امنيتي مربوط به ابزارهاي مديريت وتوسعه را نيز لحاظ کنيم.

طي بخش گذشته عموما توجه ما معطوف به اين مطلب بود که چگونه جلوي دستيابي افراد غير مجاز به سيستم و اطلاعات گرفته شود. اما هيچ گاه به اين مطلب اشاره نکرديم که مجاز يا غير مجاز بودن افراد را چگونه تشخيص ميدهيم. در واقع روش شناسايي افراد در يک سيستم امن چگونه ميتواند باشد.

ابتدايي ترين روشي که درين زمينه ميتوان در نظر گرفت تصديق اعتبار ساده بر حسب نام کاربري و کلمه عبور است. گرچه پياده سازي اين روش سنتي بسيار ساده است اما امنيتي هم که تامين ميکند حداقل امنيت ممکن است. درين روش کاربر يکبار در سيستم شناسايي ميشود و پس ازان اطلاعات به صورت عادي بر روي شبکه جريان مي‌يابد. مشکلات اين روش را ميتوان به صورت زير خلاصه کرد:

## تمامي اطلاعات در بين راه قابل شنود هستند.

* بند بالا به خصوص شامل خود نام کاربري و کلمه عبور هم ميشود. به عبارتي اين دو هم به سادگي ميتوانند توسط شخص ثالثي در بين راه شنود شده و بعدا مورد استفاده قرار گيرند.
* در شرايطي که نام کاربري و کلمه عبور لو رود کل امنيت سيستم دچار اخلال خواهد شد.

در واقع اين روش تنها تضمين کننده حداقل غير قابل قبولي از امنيت در تصديق اعتبار افراد است. بنابراين بايد به دنبال روشهاي جايگزيني بود که معايب فوق را نداشته باشند.

رمزنگاری در پروتکل‌های انتقال

تمرکز بیشتر روش‌های امنیت انتقال فایل بر اساس رمزنگاری دیتا در طول انتقال از طریق شبکه‌های عمومی مانند اینترنت است.  دیتایی که در حال انتقال بین سازمانهاست بوضوح در معرض خطر ربوده ‌شدن در هر کدام از محلها قرار دارد. – مثلا در شبکه‌های محلی برای هر یک از طرفین یا مرزهای Internet-LAN که سرویس‌دهندگان‌اینترنت از طریق آنها مسیر دیتا را تا مقصد نهایی مشخص می‌کنند. حساسیت دیتا ممکن است بسیار متغییر باشد، زیرا دیتای انتقالی ممکن است بهر شکلی از رکوردهای مالی بسته‌بندی شده تا تراکنش‌های مستقیم باشند. در بعضی موارد، ممکن است علاوه بر محافظت دیتا روی اینترنت، نیاز به محافظت دیتا روی LAN نیز باشد. مشخصاً، محافظت از دیتا در مقابل حملات LAN مستلزم رمزنگاری دیتای انتقالی روی خود LAN است. به این ترتیب، بهرحال، نیاز به بسط امنیت تا برنامه‌هایی است که خود دیتا را تولید و مدیریت می‌کنند، و تنها اطمینان به راه‌حلهای محیطی کفایت نمی‌کند و به این ترتیب بر پیچیدگی مسأله امنیت افزوده می‌شود.

پروتکل‌ها

* اگرچه ثابت‌شده است که رمزنگاری راه‌حل بدیهی مسائل محرمانگی است، اما سردرگمی در مورد دو نوع رمزنگاری (برنامه در مقابل شبکه) همچنان وجود دارد و بدلیل وجود پروتکلهای ارتباطی گوناگون است که نیازهای تعامل بیشتر آشکار می‌شود. (مانند IPSec ، S/MIME، SSL و TLS) اگرچه این پروتکلها قول تعامل را می‌دهند، اما تعامل کامل بدلیل مستقل بودن محصولات پروتکلها در حال حاضر وجود ندارد. آزمایشهایی در حال حاضر در حال انجام هستند که به حل شدن این مسائل کمک می‌کنند، اما کاربران باید مطمئن شوند که تعامل بین محصول انتخابیشان و محصولات سایر شرکای تجاری امری تثبیت شده است. پروتکل‌های ساده‌تر (SSL/TLS، IPSec و  تا حدی پایین‌تر S/MIME ) عموماً مسائل کمتری از نظر تعامل دارند.

پروتکل‌های رمزنگاری انتقال

* با ترکیب توانایی‌ها برای تایید هویت توسط رمزنگاری متقارن و نامتقارن برای ممکن ساختن ارتباطات تاییدشده و رمزشده، این پروتکلها پایه‌های امنیت را فراهم می‌کنند. تقربیاً تمام پروتکلها نیاز‌های جامعیت را پشتیبانی می‌کنند به طوری که محتویات ارتباطات نمی‌توانند تغییر یابند، اما بیشتر آنها از Non-Repudiation پشتیبانی نمی‌کنند و به این ترتیب امکان ایجاد رکوردهای پایداری را که هویت منبع را به محتوای پیام پیوند می‌دهند، ندارند.
* به این چند پروتکل به طور مختصر اشاره می‌شود:
* SSL
* تکنولوژی SSL (Secure Socket Layer) اساس World Wide Web امن را تشکیل می‌دهد. SSL که در مرورگرهای وب کاملاً جاافتاده است، توسط بسیاری از سازمانها برای رمزنگاری تراکنش‌های وبی خود و انتقال فایل استفاده می‌شود. بعلاوه SSL بصورت روزافزون بعنوان یک مکانیسم امنیت در تلاقی با پروتکلهای پرشمار دیگر استفاده می‌شود و بهمین ترتیب ابزاری برای ارتباط سروربه‌سرور امن است. SSL ارتباطات رمزشده و بشکل آغازین خود تایید هویت سرور از طریق استفاده از گواهی را (در حالت کلاینت‌به‌سرور) پشتیبانی می‌کند. کاربران اغلب برای استفاده از برنامه‌ها از طریق کلمه عبور تایید هویت می‌شوند، و با پیشرفت SSL استاندارد (مثلا SSL V.3.0) تایید هویت کلاینت از طریق گواهی به این پروتکل اضافه شده است.
* \*برای FT (انتقال فایل): ابزار FT اغلب از SSL‌ برای انتقال فایل در یکی از دو حالت استفاده می‌کنند. اولی، مد کلاینت‌به‌سرور است که کاربر را قادر می‌سازد، در حالیکه در حال استفاده از یک مرورگر وب استاندارد است مستندات را از یک سرور دریافت یا آنها را به سرور منتقل کند. که این قابلیت نیاز به نرم‌افزار مختص انتقال در کلاینت را برطرف می‌سازد و بسیار راحت است، اما اغلب فاقد بعضی ویژگیهای پیشرفته مانند نقاط آغاز مجدد و انتقالهای زمانبندی‌شده است که سازمانها نیاز دارند. SSL همچنین می‌تواند برای اتصالات سروربه‌سرور امن – برای مثال، در اتصال با FTP و سایر پروتکلها – مورد استفاده قرار گیرد.

**TLS**

* TLS (Transport Layer Security)، جانشین SSL، برپایه SSL3.0 بنا شده است، اما به کاربران یک انتخاب کلید عمومی و الگوریتمهای Hashing می‌دهد. (الگوریتمهای Hashing فانکشن‌های یک‌طرفه‌ای برای حفظ جامعیت پیامها هستند و توسط بیشتر پروتکلها استفاده می‌شوند.) اگرچه TLS و SSL تعامل ندارند، اما چنانچه یکی از طرفین ارتباط TLS را پشتیبانی نکند، ارتباط با پروتکل SSL3.0 برقرار خواهد شد. بیشتر مزایا و معایب SSL به TLS هم منتقل می‌شود، و معمولا وجه تمایز خاصی وجود ندارد، و از همه نسخه‌ها به عنوان SSL یاد می‌شود.

**S/MIME**

* S/MIME ( Secure Multipurpose Internet Mail Extention) که اختصاصاً برای پیام‌رسانی ذخیره-و-ارسال طراحی شده است، بعنوان استاندارد امنیت ایمیل برتر شناخته شده است. مانند بیشتر پروتکل‌های رمزنگاری (مثلا SSL ، TLS و IPSec)، S/MIME با رمزنگاری تنها سروکار ندارد. بهرحال، علاوه بر تصدیق هویت کاربران و ایمن‌سازی جامعیت پیامها (برای مثال مانند آنچه SSL انجام می‌دهد)، S/MIME توسط امضای دیجیتال، رکوردهای پایداری از صحت پیامها ایجاد می‌کند (ضمانت هویت فرستنده چنانچه به محتوای پیام مشخصی مرتبط شده). این عمل باعث می‌شود فرستنده پیام نتواند ارسال آن‌را انکار کند.

**FT :**

* سیستم‌های ایمیل رمزشده (با استفاده از S/MIME) می‌توانند برای ارسال فایل‌های کوچک استفاده شوند (محدودیت حجم فایل بخاطر داشتن محدودیت حجم فایل در بیشتر سرورهای ایمیل است)، ولی S/MIME کلاً می‌تواند برای انتقال فایل‌های بزرگتر  توسط پروتکلهای انتقال فایل استفاده شود.

**SSH**

* SSH (Secure Shell) هم یک برنامه و یک پروتکل شبکه بمنظور وارد شدن و اجرای فرمانهایی در یک کامپیوتر دیگر است. به این منظور ایجاد شد تا یک جایگزین رمز‌شده امن برای دسترسی‌های ناامن به کامپیوترهای دیگر مثلا rlogin یا telnet باشد. نسخه بعدی این پروتکل تحت نام SSH2 با قابلیتهایی برای انتقال فایل رمزشده از طریق لینک‌های SSH  منتشر شد.
* \*برای FT :
* SSH‌ می تواند برای پشتیبانی انتقال فایل رمزشده (به شکل SFTP) استفاده شود اما طبیعت خط فرمان بودن آن به این معنی است که بیشتر توسط مدیران سیستمها برای ارسال درون سازمان استفاده می‌شود تا برای انتقال فایل تجاری. بعلاوه استفاده از SSH نیاز به نرم‌افزار یا سیستم عاملهای سازگار با SSH در دو طرف اتصال دارد، که به این ترتیب SSH برای سرور‌به‌سرور انجام می‌گیرد.

**آیا می توان به برنامه های رمز نگاری اعتماد کرد؟**

**عیوب رمزنگار در gnu**

امروزه از رمزنگاری در برنامه های بسیاری استفاده می شود اما از كجا بايد بدانيم كه آنچه به عنوان رمزنگاري پياده سازي شده، رمزنگاري مناسب است؟ تنها راه روشن شدن اين مطلب مهندسي معكوس مي‌باشد. همچنين روند تاريخي نرم‌افزارهاي رمزنگاري نشان مي‌دهد كه رمزنگاري با عملكرد بد، بسيار رايج‌تر از رمزنگاري با عملكرد خوب مي‌باشد. بنابراين به نظر مي‌رسد كه نرم‌افزارهاي متن باز راه‌حل مناسبي مي‌باشند. اما اين واقعيت كه كد متن خواندني است به اين معنا نيست كه توسط مجربين امنيت خوانده مي‌شود. در اين مقاله، برنامة رمزنگاري پست الكترونيكي امن بررسي مي‌گردد. GNU Privacy Guard، GPG)يا (GnuPG نسخة معروف متن باز رايگان نرم‌افزار PGP مي‌باشد و مشابه استاندارد OpenPGP است و در بيشتر توزيعهاي GNU/Linux مانند, MandrakeSoft ,Debian Red Hat و SuSE بكار مي‌رود. ما اجزاء كد متني v1.2.3 GPG را بررسي كرده و چندين عيب رمزنگاري در آن يافته‌ايم. جدي‌ترين عيب GPG به شرح ذيل مي‌باشد.

كليد خصوصي امضاكنندة پيام به روش ELGamal (توليد شده توسط مجري)، در كمتر از يك ثانيه، بر روي PC بازيابي مي‌گردد. اخيراً امضاهاي ELGamalو نشانة ELGamal + كليدهاي رمزنگاري از GPG حذف شده‌اند. خوشبختانه، ELGamal گزينة پيش فرض GPG براي كليدهاي امضا نمي‌باشد. كلمات كليدي: رمزنگاري كليد عمومي، OpenPGP, GPG, GnuPG، آناليز رمز RSA، ELGamal ، پياده‌سازي.

در دنيـــاي رمزنگاري، استانـــداردهاي متعددي چـــــون [20]RSA PKCS ،[8]NESSIE , [14]IEE P1363 [15]CRYPTREC, و … وجود دارد و با وجود چنين استانداردهايي ممكن است به نظر برسد كه رمزنگاري خوب بسيار است. اما همانگونه كه استفاده از رمزنگاري گسترده‌تر مي‌شود چگونه مي توان اطمينان داشت كه رمزنگاري پياده‌سازي شده در دنياي واقعي، رمزنگاري مناسب است. خط جداكننده بين رمزنگاري خوب و بد بسيار باريك مي‌باشد. [21,2,4] تنها راه تشخيص نحوة عملكرد نرم‌افزارهاي رمزنگاري، مهندسي معكوس است.

مثلاً نرم‌افزار رمزنگاري را در نظر بگيريد كه RSA 1024 بيتي و AES 128 بيتي را پياده‌سازي كرده است. اين ويژگيها، اطلاعات زيادي دربارة امنيت واقعي رمزنگاري بيان نمي‌كند. در اين زمينه سوالات متعددي مطرح است. از كدام RSA استفاده شده است؟ آيا RSA همان نوعي است كه در كتابها تشريح شده [5](با Zero-padding). آيا AES، 128 بيتي با نماي عمومي 3 رمزنگاري شده است؟ آيا كليدهاي خصوصي با مولدهاي عددي شبه تصادفي ضعيف مانند نسخه‌هاي قديمي Netscape توليد شده‌اند [9]؟ چه كسي مي‌داند كه آيا واقعاً RSA-OAEP [21]پياده‌سازي شده است ؟ با بررسي تاريخچه نرم‌افزارهاي رمزنگاري، متاسفانه به نظر مي‌رسد كه رمزنگاري بد بسيار رايج است. [12,28] بنابراين به نظر مي‌رسد كه نرم‌افزارهاي متن باز راه حل مناسبي مي‌باشند. اما اين واقعيت كه كد متني قابل خواندن است، بدين معنا نيست كه توسط مجربين

رمزنگاري خوانده مي‌شود. پست‌الكترونيكي امن، معروفترين تكنولوژي نرم‌افزاري استفاده شده در اينترنت مي‌باشد[1] و به كاربران امكان احراز اصالت ويا محرمانگي پست الكترونيكي را مي‌دهد. پست الكترونيكي امن، در اوايل دهة 90 با ظهور نرم‌افزارPretty Good Privacy(PGP) معروف گرديد[27]. PGP توسط Phil Zimmermann در آمريكا ايجاد شد. به دليل محدوديتهاي سخت صدور نرم‌افزارهاي رمزنگاري و ساير قوانين آمريكا در گذشته، PGP براي نواحي خارج از آمريكا بسيار نامناسب بود.[10] GNU Privacy Guard (GunPG يا GPG) در اواخر دهة 90 براي رفع سوالات مطرح در PGP ايجاد گرديد. GPG، پياده‌سازي كاملي از OpenPGP [26] است و استانداردي مي‌باشد كه PGP را گسترش داده است. GPG با گواهينامة عمومي GNU GPL))) GNU General Public License) و به صورت رايگان منتشر گرديد. كد كامل متني GPG موجود است[10] و جايگزين رايگان PGP مي‌باشد. وزارت اقتصاد و تكنولوژي فدرال آلمان پايه‌گذار گسترش بيشتر GPG بود. GPG پايه كاربري بسيار مناسبي دارد و در بيشتر توزيعات GNU/Linux مانندRedHat ، MandrakeSoft ، SuSE و Debian موجود است. اولين نسخة ايستاي GPG در 7 سپتامبر 1999 منتشر گرديد.

**مروری بر GNU- V.1.2.3**

[15]، امضاء و رمزنگاري با استفاده از ELGamal ، RSA,DSA Twofish, Blowfish, 3DES, AES, ,CASTS ,SHA-1,MD5 , RIPE-MD-160 و TIGER را پشتيباني مي‌نمايد. GPG پيامهاي PGP نسخه‌هاي 5،6،7 را رمزگشايي، ارزيابي و امضاء مي‌نمايد. PGP مطابق با استاندارد OpenGPG است ودر مرجع [26] و RFC 2440 [6] تشريح شده است.

GPG محرمانگي و/ يا احراز اصالت پست‌الكترونيكي را تأمين مي‌كند: GPG به كاربران امكان رمزنگاري و رمزگشايي، امضا و ارزيابي امضاي پست‌الكترونيكي را به كمك رمزنگاري كليد عمومي مي‌دهد و به كمــــك زيـرساخت كليد عمومي، كليد عمومي ساير كاربران را احرازاحراز اصالت مي‌نمايد.

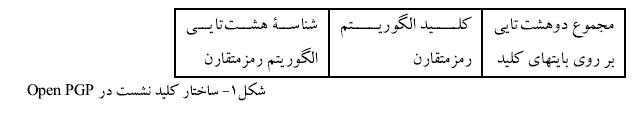
GPG v1.2.3، به كاربر امكان توليد چندين نوعكليد عمومي/خصوصي را مي‌دهد. دستور مربوط به توليد كليدgpg -- gen-key است.- در حالت استاندارد، رمزنگاري و امضا به شرح ذيل مي‌‌باشد:

• (1) DSA وELGamal : گزينه‌هاي پيش فرض مي‌باشند. كليدهاي DSA، براي امضا و كليدهاي ELGamal، براي رمزنگاري بكارمي‌روند. (نوع 16 در ترمينولوژي OpenPGP)• (2)DSA : DSA فقط براي امضا بكار مي‌رود.• (5) RSA: RSA فقط براي امضا بكار مي‌رود.

* وضعيت تخصصي رمزنگاري و امضا به شرح ذيل مي‌باشد:• (4) ELGamal براي امضا و رمزنگاري: در ترمينولوژي OpenPGP، اينها كليدهاي از نوع 20 مي‌باشند.

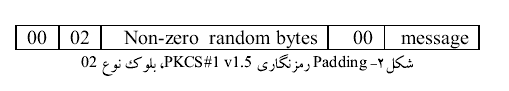
• (7)RSA هم براي امضا و هم براي رمزنگاري بكار مي‌رود.به طور خاص، كليد امضاي ELGamal، براي رمزنگاري نيز مورد استفاده قرار مي‌گيرد اما كليد رمزنگاري ELGamal محدود به رمزنگاري است. در v1.2.3 GPG، كليدهاي امضاي ELGamal فقط در وضعيت تخصصي توليد نمي‌گردند. اما نسخه‌هاي قبلي GPG اينگونه نبوده‌اند. در وضعيت استاندارد v1.0.7 GPG موارد (1)، (2)، (4)، (5) را پيشنهاد مي‌نمايد.

GPG براي رمزنگاري پست الكترونيكي از رمزنگاري تركيبي استفاده مي‌نمايد. كليد نشست (با روش رمزنگاري متقارن) با روش رمزنگاري كليد عمومي RSA و يا ELGamal رمز مي‌گردد.كليد نشست به روش OpenPGP ، شكل مي‌يابد. ( شكل1): اولاً، شناسة هشت‌تايي (one-octet) الگوريتم رمزنگاري متقارن، پيشوند كليد نشست مي‌باشد. پس از آن مجموع دو هشت‌تايي (Two-octet checksum) به كليد نشست متصل مي‌گردد كه معادل مجموع هشت‌تاييهاي قبلي مي‌باشد و شامل شناسة الگوريتم مود 65536 نيست.



مجموع دوهشت‌تايي بر روي بايتهاي كليد كليد الگوريتم رمزمتقارن شناسة هشت‌تايي الگوريتم رمزمتقارن شكل1- ساختار كليد نشست در Open PGP پس از آن مطابق با روش PKCS#1 v1.5 نوع بلوك 02 ، بايتهايي به كليد نشست افزوده مي‌شود.([17] و شكل 2): ابتدا يك بـــايت صفر به سمت چپ كليد نشست اضافه مـــي‌شود و پس از آن بايتهاي تصادفي ودر پايان بايتهاي 00 02 اضافه مي‌گردند. اگرچه PKCS#1 v1.5 فقط براي رمزنگاري RSA بكار رفته، اين ساختار هم در RSA و هم در ELGamal بكار مي‌رود. تصادفي بودن مورد نياز براي ايجاد و بايتهاي تصادفي غيرصفر با پردازه‌اي كه در اصل مندرج در [11] شرح داده شده، ايجاد مي‌شود.

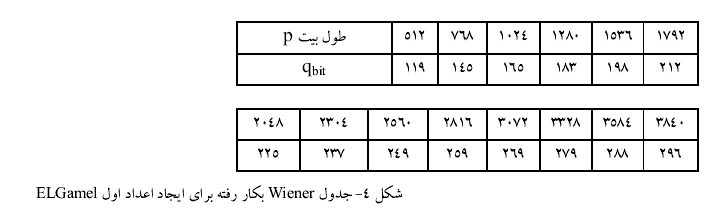
message 00 Non-zero random bytes 02 00شكل2- Padding رمزنگاري PKCS#1 v1.5، بلوك نوع02



**پیاده سازی Elgamal**

GPG ، بــــراي امضا و رمـــزنگاري، از همان متد توليد كليد، استفـــاده مي‌نمايد. ELGamal در GPG در گروه چندگانه (multiplication) با مولد g پياده‌سازي مي‌شود. كليد خصوصي با x مشخص مي‌شود و كليد عمومي مربوطه مي‌باشد. multiplication) با مولد g پياده‌سازي مي‌شود. كليد خصوصي با x مشخص مي‌شود و كليد عمومي مربوطه مي‌باشد.

عدد اول بزرگ p به طريقي انتخاب مي‌شود كه تجزيه p-1 كاملاً شناخته شده باشد و همه عوامل طول بيتي بزرگتر از آستانة qbit داشته باشند و اين آستانه وابسته به طول بيت p است. ارتباط بين سايز p و آستانة آن در جدول Wiener آمده است(شكل4): دقت كنيد كه 4qbit كمتر از طول بيت p است.



1792 1536 1280 1024 768 512 طول بيت p212 198 183 165 145 119 qbit3840 3584 3328 3072 2816 2560 2304 2048296 288 279 269 259 249 237 225شكل 4- جدول Wiener بكار رفته براي ايجاد اعداد اول ELGamel پس از انتخاب p، مولد g از با آزمايش مولدهاي بعدي پيدا مي‌گردد و اين آزمايش با عدد 3 آغاز مي‌شود: اگر 3 مولد نباشد، آنگاه عدد 4 آزمايش مي‌شود و …، توليد جفت (p,g) در روية generate-elg-prime از فايل cipher/primegen.c انجام مي‌گيرد . جفت كليد عمومي و خصوصي در رويه generate از فايل cipher/primegen.c توليد مي‌شود. اگرچه مولد g كوچك مي‌باشد اما از آنجائيكه (p-1)/2 حداقل و بيت است، و g>2 مــي‌باشد، Bleichenbachers forgery از امضاي ELGamal بكار نمي‌رود. نماي خصوصي x به عنوان عدد شبه تصادفي درهنگ p-1 انتخاب نمي‌شود، و نكتة ذيل دربارة GPG قابل ذكر است: عدد تصادفي را انتخاب كنيد كه داراي سه ويژگي است: 0<X انجام مي‌گيرد. بنابراين، x كوچكتر از p انتخاب مي‌گردد تا اعمال مخفي را تسريع نمايد. بنابراين اين امر بر امنيت نشانه‌هاي GPG- ELGamal تأثيردارد .

**امضا**

شرح: جفت(a,b) ، امضاي پيامي است كه به صورت عدد صحيح m مود p شكل يافته است. جائيكه و . عدد صحيح k، عدد تصادفي است كه نسبت به p-1 اول مي‌باشد، و با هر امضا توليد مي‌گردد. GPG امضاي (a,b) را، با بررسي اينكه آيا 0<A وجود دارد. به طور تئوريك، k عدد تصادفي امن رمزنگاري شده‌ مود p-1 است، به نحويكه k نسبت به p-1 اول مي‌باشد. حملات جديد بر روي شماهاي امضاي log گسسته [13],[2],[22])) نشان داده‌ كه هر گونه كمبود اطلاعات (يا هر ويژگي ويژه‌اي) بر روي k ممكن است باعث گردد كه حمله‌گر كليد خصوصي امضاكننده را در زمان كوتاهتري نسبت به آنچه براي حل لگاريتمهاي گسسته مورد نياز است، بازيابي مي‌نمايد. براي انجام چنين كاري، جفتهاي پيام/ امضاي بسياري در دسترس مي‌باشند. با داشتن جفت پيام/ امضا و اطلاعات جزئي بر روي k، كليد خصوصي امضاكننده افشا مي گردد، اگرچه امضا‌كننده‌ها، از k هاي مختلفي استفاده مي‌نمايند: در صورتيكه چنين جفتهايي به قدر كفايت جمع‌آوري ‌گردند، استخراج كليد خصوصي عملي مي‌باشد. نحوة توليد k در روية gen-k از فايلcipher/ElGamal.c شرح داده شده است. k با بيت شبه تصادفي انتخاب شده است(مشابه توليد نماي خصوصي x، به جز اينكه k ممكن است كمتر از بيت شبه تصادفي داشته باشد). از آنجا كه k نسبت به p-1 اول نمي‌باشد، k افزايش مي‌يابد. به طور كلي، k نهايي بسيار كوچكتر ازp مي‌باشد و بنابراين به صورت يكپارچه، در مود p-1 توزيع شده است: طول بيت k در حدود مي‌باشد، در حاليكه p حداقل است. اين امر بدين شكل تشريح مي‌گردد: IMO با k كمتر از p كفايت مي‌نمايد و كارايي رمزنگاري را به خوبي بهبود مي‌بخشد. ما از جدول Wiener استفاده مي‌كنيم و ناحية اين بزرگي را مي‌افزاييم. بايد در نظر داشت كه k به طور يكساني براي رمزنگاري و امضا بكا مي رود. به هرحال انتخاب k كوچك براي امضا نامناسب‌تر از بكارگيري k كوچك براي رمزنگاري مي‌باشد.

**آشنایی با یک برنامه رمزنگاری قدرتمند و ساده (PGP)**

 با استفاده از PGP (Pretty Good Privacy)شما می‌توانید محرمانگی پیغامها و فایلهایتان را حفظ کنید بطوریکه فقط دریافت‌کنندگان مورد نظر شما بتوانند آنها را بخوانند. بعلاوه می‌توانید پیامها و فایلهایتان را امضای دیجیتال کنید تا دریافت‌کنندگان از تعلق آنها به شما مطمئن شوید. یک پیام امضاءشده، عدم تغییر محتویات آن را نیز تایید می‌کند. البته PGP تنها نرم‌افزار ارسال و دریافت ایمیلهای امن نیست اما کاربرد آن در این زمینه نسبتا زیاد است.

PGP براساس رمزنگاری کلید عمومی عمل می‌کند که در آن از یک جفت کلید برای برقراری ارتباط امن استفاده می‌شود. برای ارسال ایمیل خصوصی به یک نفر، از کپی کلید عمومی آن شخص برای رمزنگاری اطلاعات استفاده می‌کنید و به این ترتیب تنها آن فرد می‌تواند با استفاده از کلید خصوصی خود ایمیل را رمزگشایی کند. بالعکس، چنانچه شخصی بخواهد برای شما ایمیل امن ارسال کند، از کلید عمومی شما برای رمز کردن متن نامه استفاده می‌کند و تنها شمایید که می‌توانید آن متن را با استفاده از کلید خصوصی خود رمزگشایی کنید. بنابراین شما دیگران را از کلید عمومی خودتان مطلع می‌کنید اما از کلید خصوصی خودتان، خیر!!!

همچنین از کلید خصوصی خود برای امضای ایمیلی که قصد ارسال آنرا دارید استفاده می‌کنید. دریافت‌کنندگان می‌توانند از کلید عمومی شما برای تعیین اینکه آیا واقعا خود شما آن‌را ارسال کرده‌اید و آیا متن نامه در طول ارسال تغییر نکرده است، استفاده کنند. شما هم برای تایید امضای دیگران از کلید عمومی آنها برای رمزگشایی متن دریافت‌شده استفاده می‌کنید.

در ادامه به نحوه کار با نرم‌افزار PGP اشاره می‌شود، با خواندن این مطلب به سراغ این نرم‌افزار بروید و سعی کنید از این به بعد ایمیل‌های رمزشده برای ما بفرستید.

۱- PGP را روی کامپیتور خود نصب کنید:

با مراجعه به راهنمای نصب PGP که معمولا همراه این نرم‌افزار است با نحوه نصب آن آشنا خواهید شد. در صورت نبود این راهنما، خودتان دست بکار شوید. چندان مشکل نیست.

۲- یک جفت کلید خصوصی و عمومی ایجاد کنید:

قبل از اینکه بتوانید استفاده از PGP را آغاز کنید، نیاز به تولید یک جفت کلید دارید. می‌توانید اینکار را در طول نصب PGP انجام دهید یا زمان دیگری که این نرم‌افزار را اجرا می‌کنید. شما به جفت کلید برای موارد زیر نیاز دارید:

* رمزنگاری اطلاعات
* رمزگشایی اطلاعاتی که با کلید شما رمز شده‌اند.
* امضاء کردن اطلاعات

۳- مبادله کلیدهای عمومی با دیگران:

بعد از اینکه جفت‌کلید را ایجاد کردید، می‌توانید مکاتبه با دیگر استفاده‌کنندگان PGP را آغاز کنید. شما به یک کپی از کلید عمومی دیگران نیاز دارید. کلید عمومی شما بصورت بلوکی از متن است، بنابراین تبادل کلید با شخص دیگر آسان است. می‌توانید کلید عمومی خود را در ایمیل قرار دهید، آنرا در فایل کپی کنید یا آنرا به یک سرویس‌دهنده کلید ارسال کنید تا هرکسی بتواند به کپی آن در صورت نیاز دسترسی داشته باشد. (مراقب باشید که کلید خصوصی خود را برای دیگران ارسال نکنید، در ضمن مطمئن باشید که از کلید عمومی یک نفر نمی‌توان به کلید خصوصی وی پی برد)

۴- از اعتبار کلید عمومی دیگران مطلع شوید:

هنگامی که شما یک کپی از کلید عمومی شخصی را دارید، می‌توانید آنرا به جاکلیدی خود اضافه کنید. بعد از آن می‌توانید نسبت به تعلق این کلید به شخص مورد نظر اطمینان حاصل کنید و اینکه این کلید تغییر نکرده است. اینکار با مقایسه اثرانگشت (fingerprint) یکتا که در کنار کپی کلید عمومی آن شخص دارید با اثرانگشت کلید اصلی که در اختیار صاحب اصلی کلید است، انجام می‌پذیرد. هنگامی که مطمئن شدید که کلید عمومی معتبری از آن شخص در اختیار دارید، به آن کلید نشانه معتبر بودن اضافه می‌کنید.

۵- امن‌کردن ایمیلها و فایلهایتان را آغاز کنید:

بعد از اینکه جفت کلیدهایتان را تولید کردید و کلیدهای عمومی را مبادله کردید، می‌توانید دست به کار رمزنگاری، امضاء ، رمزگشایی و تایید ایمیلها و فایلها شوید. برای انجام یک عمل PGP باید فایل یا پیامی را که می‌خواهید امن کنید انتخاب کنید و سپس عمل مورد نظر خود را «رمزنگاری (Encrypt)، امضاء (Sign) ، رمزگشایی (Decrypt) یا تایید (Verify) » از طریق منوی PGP انتخاب کنید. منوهای PGP از چند طریق در دسترس هستند؛ مثلا در Windows Explorer شما می‌توانید روی فایل مورد نظر کلیک راست کنید و سپس عمل مناسب را در قسمت PGP‌ انتخاب کنید.

۶- فایلهای مورد نظر را پاک کنید.

هنگامی که احتیاج به پاک کردن دائمی یک فایل دارید، می‌توانید با استفاده از ویژگی Wipe این عمل را انجام دهید تا مطمئن شوید که فایل قابل بازیابی نیست. فورا در محل ذخیره فایل اطلاعاتی نوشته می‌شود تا نتوان فایل را با استفاده از نرم‌افزارهای بازیابی دیسک حاصل کرد.

ضمنا نرم‌افزار PGP به شما امکان رمزکردن، رمزگشایی و سایر اعمال را روی اطلاعاتی که روی clipboard قرار دارد، می‌دهد. سپس اطلاعات تغییریافته را روی همان clipboard قرار میدهد. حتما می‌دانید که با انتخاب گزینه copy ، متن انتخاب شده به clipboard و با انتخاب گزینه paste متن موجود در clipboard به پنجره فعال شما منتقل می‌شود.

سئوالهای بودن جواب

مديريت نوين بر پايه فناوري اطلاعات طراحي شده است. مديريت تجاري و اداري به گونه‌اي تغيير خواهد يافت كه هرم تشكيلاتي كم‌ارتفاع و عريض خواهد گرديد. رياست سازماني به مدد فناوري اطلاعات به انبوهي از مديريت ‌هاي مستقل و كوچك و كارآمد متصل خواهد گرديد. سازمان‌ها در مقابل نيازهاي مشتريان و مردم چـــــابك‌تر ومسئولانه‌تـــر عمل خواهند كرد. اگر داده‌هاي مورد تبادل سازمان‌ها توسط سايرين منهدم، و يا دستكاري نشود. اگر برنامه‌هاي محرمانه در دسترس ديگران نباشد و اگر شبكه داده‌ها و شريان حيات مديريت نوين در روز مبادا از هم گسسته نشود.

1- آيا لازم نيست قبل از راه‌اندازي شبكه‌داده‌ها در مديريت سازماني به فكر استحكام آن باشيم؟

2- آيا شبكه داده‌هاي كشور براي حداكثر مقاومت در برابر بمباران وبلاياي طبيعي طراحي شده است؟

3- آيا مي‌توان داده‌هاي مورد تبادل تمامي مديريت ‌ها را در يك نقطه ازشبكه مورد شنود قرار داد؟

4- آيا كنترلي شبانه‌روزي و ابزار آلاتي قابل اعتماد براي رفع اختلالات چنين شبكه‌اي وجود دارد ؟

5- آيا قوانين مديريتي و سازماني براي تفسيرهاي تازه از ابلاغات، بخشنامه ها، لغو دستورها و جرائم سازگار است؟

6- آيا مي‌توان داده‌هاي خصوصي خود را چنان رمزنگاري كرد كه حتي پليس هم نتواند آن را بخواند؟

7- اگر كسي ادعا كند كه داده‌هاي او دزديده شده است و در نزد كسي به صورت رمز شده نگهداري مي‌شود، چه مداركي به نفع يا بر عليه مدعي است؟ و اگر پس از باز شدن رمز، ادعا ثابت نشود، خسارت افشاي داده‌ها را چگونه محاسبه مي‌كنيم و چه كسي مي‌پردازد؟

8- اگر تبعه يك كشور با قوانين آزاد در رمزنگاري وارد كشور ما بشود مي‌تواند با دستگاه خود(كه مجهز به سيستم رمزنگاري است) با خارج از كشور ما تماس بگيرد؟ مي‌تواند با همكار خود در داخل كشور تماس بگيرد؟

9- اگر تبعه يك كشور كه رمزنگاري در آن جرم است، در كشور ما(كه رمزنگاري در آن جرم نيست) از دستگاه‌هاي رمزنگاري استفاده كند و اين كار مورد اعتراض كشور متبوع او باشد، ما از اين فرد حمايت مي‌كنيم، يا آن را به كشور متبوعش پس مي‌دهيم، اگر داده‌هاي مورد تبادل را بخواهند آن را تحويل خواهيم داد؟ اساساً حق داريم اين اطلاعات را قبلاً ضبط كرده باشيم؟ چه مرجع قضائي اين حكم را مي‌دهد؟ براي ايرانيان چه كسي حكم مي‌كند؟ 10- آيا در كشور ما رمزنگاري جرم است؟ اگرنوعي خاص از آن جرم است، نويسنده نرم‌افزار خريد و فروش سهام بازار بورس چگونه مي‌تواند براي نرم‌افزار خود مجوز فروش بگيرد؟ اگر در اين نرم‌افزار براي حفظ محرمانگي، از رمزنگاري استفاده شده باشد، چه نوعي از آن مجاز است؟ نسخه صادراتي آن چطور؟

