امنیت در پایگاههای داده ای (سرور)

مقدمه

با گسترش استفاده از تكنولوژي وب و توسعه برنامه‌هايي كه براي كاركرد درين بستر توليد ميشوند مباحث مربوط به امنيت پايگاههاي داده اي بعد جديدتري پيدا كرده اند. هر چند از آغاز پيداش پايگاههاي داده همواره امنيت و تامين آن يک دغدغه مهم و پياده سازي مناسب و كاراي آن يک خصوصيت بنيادي در پايگاههاي داده بوده است اما بهر روي بحث امنيت (Security)همواره در سايه مقولاتي همچون عملكرد مناسب (Functionality) ، كارايي (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 كاربري sa (System Administrator) به پايگاههاي داده متصل ميشوند. از ديد امنيتي اين مطلب يک فاجعه محسوب ميشود. هيچ تغيير و يا خرابكاري اي قابل رديابي نيست، همه كاربران به همه اطلاعات دسترسي دارند و الي آخر.

آنچه ذكر شد ، در واقع تصويري از وضعيت جاري بود، كه بايد از دو منظر نگريسته شود: عدم وجود مكانيزمهاي امنيتي مناسب و نيز در صورت وجود

چنين مكانيزمهايي عدم بهره گيري صحيح ازانها يا نداشتن سياست امنيتي مطلوب.

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

اجازه دهيد يک فرض اساسي را مطرح كنيم. مديران IT يک سازمان بر دو دسته اند: مديران نوگرايي كه به صورت داوطلبانه سازمان را به سمت ارائه خدمات عمومي و گسترده هدايت ميكنند و به همين دليل تكنولوژي وب را به عنوان تنها بستر موجود براي ارائه اين خدمات ميپذيرند و مديران سنتي محافظه كاري كه قابليت اطمينان و كارايي سيستم جاري را تحت هيچ شرايطي حاضر نيستند در معرض خطر قرار دهند. وب از نظر اين گروه دوم كماكان يک تكنولوژي مشكوک غير قابل اطمينان است. در واقع دلايل فني اين گروه دوم هنوز هم چشمگير و قابل اعتناست، به خصوص گروهي كه از mainframeها صحبت ميكنند. قابليت اطمينان ۰٫۹۹۹۹۹ هنوز هم در دنياي غير Mainframe يک رويا‌ست.

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

- امنيت سرور(Server Security)

- امنیت در تصدیق اعتبار(Authentication Security)
- امنیت 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 (IIS،Apache 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 پایگاه داده در DMZ:

در صورتي که از یک معماري امن براي پیاده سازي شبکه خود استفاده کرده باشید به احتمال زیاد شبکه شما داراي یک بخش DMZ(Don’t Militarized Zone) خواهد بود. معمولا ارائه دهندگان خدمات عمومي را درین بخش از شبکه قرار میدهند. بعنوان مثال سرورهاي وب، سرورهاي میل ... که همگي جهت خدمات عمومي بکار میروند درین بخش از شبکه قرار دارند.

ایده عمومي داشتن یک بخش DMZ ساده ست: سرورهایي که خدمات عمومي بیرون سازماني ارایه میدهند نیازمند سطح کمتري از امنیت هستند. در واقع همه میتوانند به آنها دسترسي داشته باشند. این دسترسي همگاني به هیچ وجه لازم نیست در مورد تمامي منابع شبکه اعمال شود. بنابرین منابع عمومي شبکه را در بخشي از شبکه قرار میدهند که حساسیت امنیتي کمتري نسبت به آن وجود دارد. این همان بخش DMZ است. با توجه به مطالب بالا بسیار بدیهي به نظر میرسد سرور پایگاه داده را باید در همان بخش DMZ قرار دهیم زیرا که عموما این سرور نیز مسئولیت ارائه خدمات همگاني را بعهده دارد. اما قضیه در باره سرور پایگاه داده تا حدي متفاوت است. این سرور گرچه خدمات همگاني نیز عرضه میکند 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 میکند از اهمیت فوق العاده اي برخوردار است و هرگونه دسترسي به کل داده‌هاي آن میتواند فاجعه بار باشد.

بنابراین بر خلاف دید اولیه به این نتیجه میرسیم که پایگاه داده نمیتواند و نباید که در بخش DMZ قرار گیرد. اما راهکار جداسازي آن ازین بخش چیست؟

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 پایگاه 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 كه ميتوان براي جداسازي بخش امن شبكه ارائه داد استفاده از بيش از يک كارت شبكه در فايروال است (شكل ۲)

همانطور كه مشخص است درين روش توسط يک فايروال، DMZ از بخش امن شبكه جداسازي ميشود. تنها ترافيكي كه حق عبور از اينترفيس اول (eth1) به اينترفيس امن (eth۲) 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 ممكن است فايروال موجود ما عملا از چندين كارت شبكه پشتيباني نكند.

علاوه بر دو راهي كه در فوق براي جداسازي پايگاه داده از مابقي شبكه ارائه داديم راه حل سومي هم وجود دارد: اينكه اساسا پايگاه داده را از مابقي شبكه جدانكنيم! دقت كنيد كه با توجه به هزينه و نيز اندازه سازمان ممكن است جداسازي امكان پذير نباشد و حتي مجبور شويم كه اين دو سرور را برروي يک ماشين اجرا كنيم. حتي درين صورت نيز بهتر است حداقل كارهايي كه 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 كنيم. 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 پروتكل SSL است. عموم اطلاعات امن كه بر روي اينترنت منتقل ميشوند از همين پروتكل استفاده ميكنند . بعنوان مثال انتقال اطلاعات شناسايي با سرورهاي معروف ايميل، انتقال اطلاعات مربوط به كارت اعتباري و غيره.

تا بدينجا اين پروتكل كه اغلب سرورهاي وب و نيز مرورگرها ازان پشتيباني ميكنند سطحي از امنيت را تامين ميكند. اما آيا همين كافي ست؟

اغلب اين اشتباه پيش مي‌آيد كه همين سطح از رمز نگاري را در مقابل حمله Sniffing كافي ميدانند. بايد دقت كرد كه SSL به صورت عام تنها براي رمزنگاري اطلاعات مابين Client و سرور وب به كار 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 شبكه بيروني رعايت كرده باشيم، يک نفوذگر داخلي به سادگي ميتواند اطلاعات در حال انتقال مابين اين دو سرور را شنود كند. اين مطلب زماني بسيار جدي ميشود كه بدانيم بر اساس داده‌هاي موجود، بالاتر از ۶۰٪ حملات موجود حملات درون سازماني مي‌باشد.

چاره كار استفاده از يک روش رمز نگاري مابين سرور وب و سرور پايگاه داده است. اغلب سرورهاي پايگاه داده امروزه از SSL حمايت ميكنند. MS SQL Server۲۰۰۰ ، Sybase،Oracle ازين جمله اند. البته استفاده از SSL براي ارتباط

مابين اين دو سرور لازمه اش اينست كه برنامه اصلي شما (Web Application) با همين ملاحظه طراحي و پياده سازي شده باشد.

اما در صورتي كه برنامه شما از قبل موجود باشد يا از SSL پشتيباني نكند 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. يكي از قابليتهاي SSH ايجاد يک تونل امن است. به اين صورت كه ميتوان برنامه SSH را به گونه اي اجرا كرد كه بر روي يک پورت شنود كند كل اطلاعات آن را رمز كرده به كامپيوتر مقصد ارسال كند 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(شكل ۳).

مزيت استفاده ازين روش اينست كه 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 كه از Hub استفاده ميكنيم تمامي اطلاعات عبوري در هريک از سيستمهاي موجود در شبكه داخلي قابل شنود است. يک نفوذ گر معمولي با استفاده از يكي از ابزارهاي Sniffing ميتواند اينترفيس شبكه با به حالت Promiscuous برده ، تمامي اطلاعات در حال جابجايي بر روي LAN را

دريافت كند. البته استفاده از رمز نگاري خطر بالقوه بهره گيري ازين روش را كم ميكند اما هيچگاه نميتوان مطمئن بود كه كل اطلاعات رمز نگاري شده است. بنابراين بهتر است حتي المقدور امكان بهره گيري از Sniffing را بر روي شبكه كاهش دهيم. استفاده از سوپيچها به جاي‌هاب يكي از روشهاي حل اين مساله است. با استفاده از سوئيچ در واقع يک مدار مجازي (Virtual Circuit) مابين دو نود در حال مكالمه ايجاد ميشود و ديگران به اطلاعات در حال انتقال مابين آن دو دسترسي ندارند.

۶-۲. ارائه امن اطلاعات

از ديد كلي 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

۶-۲-۱. 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 كليه اطلاعات بر روي سايت و سرور اصلي قرار ميگيرد (Upload).

امنيت اين روش به سادگي تامين ميشود. كافيست كه اشخاص نام فايلهاي HTML را ندانند، درين صورت هرگز به آنها دسترسي نخواهند داشت. اينكار با استفاده از مكانيزم ساده اي صورت ميگيرد. عموم وب سرورها براي دايركتوريهاي مختلف حق دسترسي تعريف ميكنند كه يكي ازين حقوق دسترسي حق مشاهده محتويات يک دايركتوري است. در صورتي كه كاربري 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 اكيتيوي با سرور پايگاه داده وجود ندارد. اطلاعات به صورت برون خط (Offline) بر روي سرور وب بارگذاري ميشوند و پس ازان هيچ ارتباطي مابين كاربر عادي و چپايگاه داده وجود نخواهد داشت. بدين ترتيب خطر حملات به پايگاه داده كاهش چشمگيري مي‌يابد. اما از ديگر سو مديريت حجم انبوه اطلاعات با استفاده ازين روش بسيار دشوار ميباشد . ضمن اينكه قابليت انعطاف روش نيز بسيار محدود است. در واقع زماني كه ازين روش استفاده ميكنيم هدف اصلي خدمت رساني و سهولت استفاده را قرباني امنيت كرده ايم.

۶ -۲ -۲ . توليد اطلاعات به صورت ديناميک

اين روش متداول ترين شيوه ايست كه 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 دينامیک از طريق جستجوي (Query) مناسب در پايگاه داده توليد ميشود.

براي پياده سازي اين روش طيف وسيعي از تكنولوژيها وجود دارد. ISAPI،CGI،PHP،JSP،ASP... و چندين روش ديگري كه 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 نكته مهم را بايد مد نظر داشت:

- تا كنون شكافهاي جدي امنيتي در مورد هر يک ازين روشها شناخته شده إست و با وجود اين حل اغلب آنها هنوز هم هيچكدام آنها امنيت بالايي را به تنهايي تضمين نميكنند.
- با وجود نكته بالا، چون هدف اصلي ارائه خدمت ياسرويس است در بسياري موارد چاره اي بجز استفاده از يكي از اين روشها نداريم.
- هنگام انتخاب هر يک از اين روشها بايد ملاحظات امنيتي مربوط به ابزارهاي مديريت وتوسعه را نيز لحاظ كنيم.

طي بخش گذشته عموما توجه ما معطوف به اين مطلب بود كه چگونه جلوي دستيابي افراد غير مجاز به سيستم و اطلاعات گرفته شود. اما هيچ گاه به اين مطلب اشاره نكرديم كه 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 كه درين زمينه ميتوان در نظر گرفت تصديق اعتبار ساده بر حسب نام كاربري و كلمه عبور است. گرچه پياده سازي اين روش سنتي بسيار ساده است اما امنيتي هم كه تامين ميكند حداقل امنيت ممكن است. درين روش كاربر يكبار در سيستم شناسايي ميشود و پس ازان اطلاعات به صورت

عادي بر روي شبكه جريان مي‌يابد. مشكلات اين روش را ميتوان به صورت زير خلاصه كرد:

تمامي اطلاعات در بين راه قابل شنود هستند.

- بند بالا به خصوص شامل خود نام كاربري و كلمه 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 كه نام كاربري و كلمه عبور لو رود كل امنيت سيستم دچار اخلال خواهد شد.

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