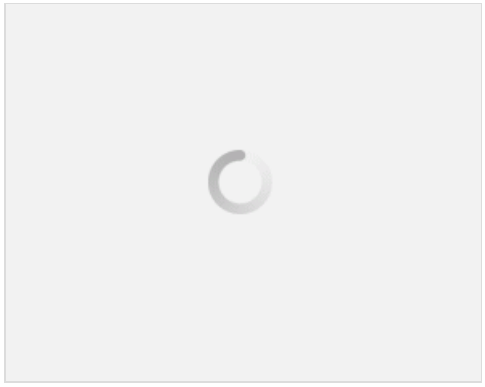
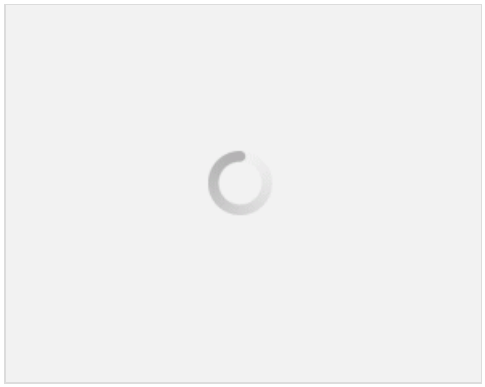
۴ مفهوم در سرویس RDP مایکروسافت (نسخه PDF)

با سـلام خـدمت همه دوسـتان،در این مقاله سـعی کردیم تا در مورد نحوه برقراری کلاینت با ریموت سـرور بصورت جزئی تر بحث نمائیم. وظیفه برقراری و نگه داری ارتبـاط در این سـرویس از طرف کلاینت توسط یک برنامه بسـیار کوچک است(Remote Desktop Connection) این برنامه اطلاعات کاربر از قبیل ضـربات کلیـد و حرکات موس را به سـرور و بالعکس اطلاعات برنامه ها و پردازش ها را به کلاینت منتقل می کند.



از طریق پورت TCP به شماره ۳۳۸۹ یک کلاینت آغازگر ارتباط با ریموت سـرور می باشد.در سـمت سـرور Listener ای که وجـود دارد این درخواست ارتبـاط را تشـخیص داده و یک Instance(نمـونه) جهت مـدیریت این درخواست RDP کلاینت ایجاد میکنـد. برنامه Listener همچنان به این پورت گوش می دهد تا چنانچه درخواست دیگری از سـمت کلاینت های دیگر صادر شد برای هر کدام یک Instance مجزا ایجاد کند.



ابتدا باید یک سطح رمزگذاری ایجاد شود .ریموت سرور از چهار لایه رمزگذاری پشتیبانی می کند:

low, client compatible, high and FIPS compatible

۱. **Low** :تنهـا اطلاعات ارسالی از طرف کلاینت به سـرور را رمزنگاری می نمایـد و برای محافظت از دیتای حساس ماننـد رمز کاربر می باشد.
۲. **Client compatible** :در این روش اطلاعات ارسالی بین کلاینت و سـرور با توجه به حـداکثر طول کلیـدی که کلاینت پشتیبانی می کند رمز گذاری می شود.
۳. **High** :ماننـد روش قبل در این حالت نیز تمام اطلاعات ارسالی رمز نگاری می گردد با این تفاوت که حـداکثر طول کلیدی که سـرور پشتیبـانی می کنـد اساس این رمزنگاری بوده و کلاینت هایی که قادر به پشتیبانی این سـطح نیسـتند نمی تواننـد ارتباط را برقرار نمایند.
۴. **FIPS compatible** :در این سـطح از استاندارد FIPS ۱۴۰-۱ جهت رمز گـذاری اسـتفاده می شود.(جهت کسب اطلاعات بیشتر در مورد این استاندارد می توانید به آدرس http://csrc.nist.gov//publications//fips//fips۱۴۰۱.htm مراجعه نمائید.)

در این لحظه پیش از نمایش صـفحه logon به کاربر باید جزئیات لایسـنس بین کلاینت و سـرور بررسـی و مذاکره شود و در صورت تائید توسط سـروری که کنترل لاینسـس را بر عهده دارد (این سرور می تواند خود ریموت سرور باشد) مرحله بعد آغاز می شود که ریموت سرور Instance ایجاد شـده برای این ارتباط را پس از آنکه کاربر، نام کاربری و رمز را وارد نمود و تائیـد شد با یک Id به آن اختصاص می دهد.از

طریق همین Id است که چنانچه ارتباط قطع شـد کاربر مجددا می تواند به همان Instance متصل شـده و کار خود را ادامه دهد.کنترل نام کـاربری و رمز(احراز هویت) بـا توجه به تنظیماتی که در قسـمت Security layer وجـود دارد به سه روش صـورت می پـذیرد که امن ترین حالت روش SSL میباشد.

نویسنده : محمد رفیعی

منبع : مایکروسافت

مطلب اصلی