امنیت نرم افزاری
کامپیوترهای شخصی

فهرست

آغاز

یک لامپ در دنیای فیزیکی یا روشن است یا خاموش. از روشن بودن لامپ اطلاعات دیگری را بدست می‌آوریم و آن این است که لامپ خاموش نیست پس با داشتن یک اطلاعات می‌توانیم اطلاعات دیگری را بدست آوریم.می‌دانیم که منطق انسان ها بر مبنای دهدهی است یعنی اینکه اگر به یک کودک چهار ساله گفته شود که جمع دو با دو چند می‌شود قطعاً او خواهد گفت چهار؛ زیرا در منطق فکری او مبنایی به عنوان چهار و دو وجود دارد. اما اگر به بزرگترین رایانه‌ها نیز گفته شود دو به اضافه دو چند می‌شود او در جواب خواهد گفت اول اجازه دهید من بفهمم که دو یعنی چه و بعد از آن بتوانم مقداری محاسبات انجام دهم و دو را تبدیل به مبنایی کنم که می‌شناسم و پس از انجام دادن محاسبات مربوطه جواب را تبدیل به مبنایی کنم که انسان ها آن را متوجه می‌شوند و بعد بتوانم جواب را بگویم.

پس متوجه شدیم که مبنای منطقی رایانه که دو دویی است با مبنای محاسباتی انسانها که دهدهی است اختلاف دارد و باید بین این دو پروتکل، قراردادی منعقد شود تا بتوانند زبان همدیگر را متوجه شوند.

گفته شد که یک لامپ یا روشن است و یا خاموش . در دنیای مجازی و رایانه ای نیز چنین است. یا روشن است و یا خاموش و حالت سومی وجود ندارد.به

این روشن یا خاموش بودن که کوچکترین واحد اطلاعاتی را در رایانه تشکیل می‌دهد یک بیت[1] گفته می‌شود. پس برای اینکه قرار داد بین انسان و رایانه برای فهمیدن منظور همدیگر منعقد شود باید این بیت مبنا قرار داده شود و در این قرار داد هر حالت برابر با یکی از حالات قابل فهم انسان‌ها قرار داده شود (یکی از حروف یا اعداد یا نماها و یا حرکت ها) به طور مثال :

۰۱ برابر با A

۱۱برابر با B

۱۰ برابر با C

۰۰ برابر با D

مشکل انسان ها با رایانهاز اینجا به بعد شروع می‌شود زیرا دیگر نمی‌توان هیچ ترکیبی از صفر و یک را متصور شد که بتواند دیگر کاراکترها را برابری کند و اگر قرار داد به این منوال پیش رود با مشکل روبرو خواهد شد. یعنی قابل ادامه دادن نخواهد بود.هر کدام از این برابری ها یعنی یک حرف یا عدد یا نماد یا حرکت را یک بایت[2]می گویند.

پس در این قرار داد صرفا چهار بایت قابل پوشش خواهد بود و برای دیگر بایت ها به طور مثال در زبان‌هایی که دارای ۶۸۰ یا ۷۲۰ حرف هستند، چکار باید کرد.

پس چون نمی‌توان از ستون این نماد ها را افزایش داد می‌بایست از سطور آنها را افزایش داد تا بتوان از ستون نیز گسترش داد. پس باید با استفاده از شکل‌دهی خاصی که آن را فرمت[3]می‌نامند اینکار را انجام داد.یعنی :

---

[1] Bit

[2] Byte

[3] Format

۰۰۰۱۱

۱۱۰۱

۱۰۱۰

پس یک بایت عبارت است از تعدادی از بیت ها که به شکل هدفمند در کنار یکدیگر قرار گرفته و در این قرارداد معرف یک کاراکتر هستند و با توجه به نوع فرمت که می‌تواند به شکلهای مختلف باشدمی‌تواند گسترش پیدا کند.

FAT۱۲,FAT۱۶,FAT۳۲,NTFS

چون انسان ها در کاربرد رایانه عملاً استفاده از بیت و بایت را مبنای کار قرار نمی‌دهند و استفاده کاربردی ندارد پس مجبورند تعدادی از بایت ها یا کاراکترها را به صورت هدفمند در کنار یکدیگر قرار دهند و از آنها یک کلمه بسازند تا بتوانند استفاده کنند.

این کلمات را می‌توان در رایانه تعبیر به فیلد های اطلاعاتی نمود که اگر در کنار یکدیگر به صورت هدفمند قرار گیرند می‌توانند تشکیل یک رکورد اطلاعاتی را بدهند و از در کنار همدیگر قرار گرفتن این رکوردها فایل رایانه‌ای تشکیل می‌شود که برای انسانها کاربرد پیدا می کند و می‌توان گفت که من فلان فایل را نیاز دارم و آن را به من بدهید.

فایل‌ها مانند اوراق یک دفتر است که اگر به یکدیگر دوخته نشوند ممکن است باد آنها را به هر طرف اندازد. پس اگر فایل ها در کنار یکدیگر قرار گیرند می‌توان آنها را در داخل یک فولدر و یا دایرکتوری قرار داد تا نظم بین آنها برقرار شود. فولدر ها نیز در داخل پارتیشن رایانه که همان درایو های :C:,D:,E و ... هستند قرار می‌گیرد و درایوها نیز معمولا در داخل هارد رایانه که به عنوان اصلی ترین ابزار ذخیره ساز اطلاعات است قرار می‌گیرد.

هر فایل دارای خصوصیات و ویژگی‌های خاصی است که در امر امنیت رایانه نقش ایفا می‌کند.

ویژگی های یک فایل رایانه‌ای

چند مورد از ویژگی های یک فایل رایانه‌ای عبارتند از:

- نام فایل

نام فایل درگذشته محدودیت‌هایی داشتهاست ولی در سیستم عامل‌های جدید این محدودیت‌ها برداشته شده است و می‌تواند حروف و اعداد و علایم باشد و معمولا معرف اطلاعاتی است که به صورت سلیقه ای و توسط تولید کننده اطلاعات نوشته می‌شود.

- پسوند فایل[1]

پسوند فایل عبارت است از یک عبارت سه یا چهار حرفی که بعد از نام فایل قرار گرفته و با یک نقطه از آن جدا شده است و معمولاً دارای استاندارد خاصی بوده و از قرارداد بین المللی تبعیت می‌کند. نوع پسوند به صورت استاندارد و قراردادی توسط نرم‌افزاری که اطلاعات به وسیله آن تولید شده است انتخاب می‌شود. پسوندها قراردادی بوده و معمولاً نشان‌دهنده نوع اطلاعات موجود در فایل هستند.

- تاریخ و ساعت فایل

این تاریخ و ساعت نشان دهنده تاریخ و ساعتی است که فایل رایانه‌ای تولید شده و یا اینکه آخرین تغییرات بر روی آن انجام پذیرفته است.در

---

[1] Extension

حالت عادی این تاریخ و ساعت به صورت خودکار ازرایانه‌ایکه اطلاعات بوسیله آن تولید شده است دریافت و بر روی فایل قرار داده می‌شود.

بسیاری از کاربران عادی گمان می‌برند که اگر اتفاقی برای فایل رایانه‌ای آنها بیفتد می توان با بررسی ساعت و تاریخ پی به این برد که در چه ساعتی این اتفاق افتاده است و با بررسی آن ساعت و افرادی که احیاناً دسترسی به رایانه را داشته اند مسبب را پیدا نمود.لیکن امروزه شما می‌دانید که اگر ساعت و تاریخ یک دستگاه رایانه قبل از تغییر در فایل دستکاری شده و تغییر پیدا کند و سپس فایل رایانه‌ای تغییر نماید ساعت و تاریخ درج شده بر روی آن واقعی نخواهد بود زیرا تغییر دهنده پس از اعمال تغییرات مجددا آن را به حالت اولیه برگردانده است.علاوه بر آن امروز نرم افزار هایی در اینترنت می‌توان پیدا کرد که وظیفه آنها تغییر در خصوصیات یک فایل (از جمله ساعت و تاریخ) است.پس نمی‌توان با بررسی تاریخ و ساعت یک رایانه پی به زمان واقعی اعمال تغییرات در فایل رایانه‌ای برد.

- حجم فایل

حجم یک فایل نشان‌دهنده میزان کاراکترهای استفاده شده در فایل و به تعبیری میزان حافظه استفاده شده از رایانهاست.

همانگونه که در فضای فیزیکی یک هزار گرم برابر با یک کیلوگرم است در فضای مجازی نیز به صورت عرفی به شکل زیر محاسبه می‌شود:

۱۰۰۰ بایت = یک کیلو بایت

۱۰۰۰ کیلو بایت = یک مگا بایت

۱۰۰۰ مگا بایت = یک گیگا بایت

۱۰۰۰ گیگا بایت = یک ترابایت

و ...

آخرین میزانی که امروز انسان ها با آن کار می‌کنند برابر است با یک اگزا بایت که معادل یک همراه با ۱۸ صفر است.

در حالت واقعی دررایانه هر ۱۰۲۴ بایت برابر با یک کیلو بایت است و اگر به محاسبه فوق دقت فرمایید در یک رایانه۵۰۰ گیگا بایتی تعداد ۲۴*۱۰۰۰*۱۰۰۰*۵۰۰= ۱۲۰۰۰۰۰۰۰۰۰ بایت (۱۲ گیگا بایت) فضای نادیده وجود دارد که می‌تواند مورد استفاده افرادی که به نوعی امنیت رایانه را به خطر می اندازند قرار گیرد.

ویژگی های یک فایل

یک فایل دارای ویژگی های مختلفی است که برای هر کدام از آنها علایم اختصاری قرار داده شده است:

A= آرشیو (خصوصیت عام فایل هایرایانه‌ای)

H= پنهان[1]: به مفهوم این است که این فایل از دیده ها پنهان است. (در سیستم‌عامل‌های قدیمی این ویژگی مفهوم داشته است لیکن در سیستم‌عامل‌های نسل جدید معمولاً فایل‌هایی که دارای این ویژگی باشند یا به صورت کامل دیده می‌شوند و یا اینکه حداکثر کم رنگ تر دیده می‌شوند. در هر حالت از دیده ها پنهان نمی‌شوند!)

[1] Hidden

R= فقط قابل خواندن[1]: این ویژگی باعث می‌شود که فایل‌ها قابل تغییرات نبوده و استفاده‌کننده می‌تواند فقط اطلاعات درون آنها را مشاهده کند و نتواند تغییر دهد.

W= قابل نوشتن[2]: این ویژگی باعث می‌شود که بتوان اطلاعات فایل را علاوه بر مشاهده تغییر نیز داد.

S= قابلیت مشاهده فایل در زمان اسکن کردن فایل.این ویژگی فایل‌ها، بر روی نام فایل قرار داده شده و کاربران می‌توانند بر اساس نوع ویژگی هر فایل نسبت به استفاده از آن فایل بهره برداری کنند.

انواع نرم افزار

نرم افزارهایمورد استفاده در رایانه‌ها انواع و اقسام مختلفی دارند که با توجه به ویژگی آنها و میزان استفاده در بین کاربران عادی، مهمترین آنها نرم‌افزارهای سیستم عامل ونرم افزارهای کاربردیهستند.

نرم افزار های سیستم عامل

این نرم افزارها از ابتدایی ترین و اصلی ترین نرم افزارهای مورد نیاز کاربران برای راه اندازی یک رایانهاست و بدون داشتن این نرم افزار عملاً استفاده از یک دستگاه رایانه امکان پذیر نیست. سیستم عامل انواع و اقسام کارها را برای یک رایانه انجام می‌دهد ولی مهمترین وظیفه آن عبارت است از مدیریت بر منابع

---

[1] Read only

[2] Writeable

نرم افزاری و سخت افزاریرایانه. بدون ایـن نـرم افـزار، مـدیریت بـر منـابع (اجـزا) سخت افزاری و نرم افزاری رایانه عملا امکان پذیر نخواهد بود.

به علت خاص بودن این نرم‌افزار خطـرات آن نیـز خـاص بـوده و نفـوذگران تلاش بر این دارند تا بتوانند از طریق این نرم افزار مدیریت یـک رایانـه را بدسـت گرفته و بر آن غلبه کنند.

انواع سیستم های عامل رایج در کشورمان و بسـیاری از نقـاط دیگـر دنیـا بـه شرح ذیل هستند:

- سیستم های عامل OPEN SOURCE
- سیستم عامل DOS

این سیستم عامل از قدیمی ترین سیستم‌های عامل است که توسط شرکت میکروسافت تهیه و توزیع شده است و در نسخه های مختلف طی سالیان متمادی مورد استفاده کاربران بوده است. هرچند که استفاده از این سیستم عامل امروزه در بسیاری از نقاط دنیا منسوخ شده‌است لیکن هنوز در برخی از نقاط دنیا و همچنین در برخی از سازمانهای دولتی و عمومی کشورمان و بعضا در سیستم خصوصی مورد استفاده قرار می گیرد.

با مطالعه در کتب چاپ شده توسط شرکت میکروسافت ملاحظه می‌شود که مقوله‌ای تحت عنوان امنیت در این سیستم‌عامل دیده نشده است و این به مفهوم آن است که هر ساختاری که از این سیستم‌عامل استفاده نماید اهمیتی به مقوله امنیت اطلاعات خود نداده و در حقیقت دسترسی دیگران به اطلاعات اهمیتی ندارد و اطلاعات را پس از تولید در محلی قرار داده است که هر شخصی که دسترسی فیزیکی به رایانه دارای

این سیستم عامل پیدا نماید می‌تواند به راحتی به اطلاعات این رایانه با کمترین دانش رایانه‌ای دسترسی پیدا کند.

بعضی از کاربران برای ایمن نمودن رایانه‌های خود در گذشته اقداماتی را انجام می‌دادند. به طور مثال در هنگام فرمت کردن رایانه خود از نرم افزارهایی (مانند ADM)[1] استفاده کرده و هارد رایانه را به پارتیشن‌های کوچکتری تقسیم بندی نموده و برای هر پارتیشن نامگذاری عددی که با صفر (بالاترین سطح دسترسی)شروع و همینطور افزایش می‌یافت قرار می‌دادند. برای هر پارتیشن کاربر می‌توانست رمز دلخواهی را قرار داده و پارتیشن خود را محفوظ نگاه دارد.(از محدودیتهای این سیستم این بود که معمولا پارتیشن‌های کم حجم (۲۰ مگا بایتی) را تحت پوشش قرار می‌داد.)

همگام با این اقدام کاربران، نفوذ گران نیز نرم افزاری نوشته و اسم آن را ADMPASS گذاشته و به مجرد boot شدنرایانه با سیستم عامل dos و اجرای این نرم افزار از طریق فلاپی و یا هر مدیای دیگر دو اقدام قابل انجام بوده است:

- نشان دادن رمز مربوط به کاربران (مخصوصا کاربر صفر)
- از بین بردن رمز مربوط به کاربران (مخصوصا کاربر صفر)

در هر دو حالت نفوذ گر قادر به دسترسی به اطلاعات سیستم بوده و می‌توانست از آن کپی تهیه کرده و از سیستم خارج نماید. در حالت اول رد پایی از خود به جای نمی گذاشت و در حالت دوم نفوذگر رمز پاک

[1] Advanced disk manager

شده را با رمز دیگری جایگزین می‌کرد و کاربر در ورود به سیستم با اشکال مواجه شده و در برخی مواقع فکر می‌کرد کهرایانه خراب شده است و یا او رمز را فراموش کرده است!

از مهمترین دلایل عدم امنیت سیستم عامل DOS امکان دسترسی فرد نفوذ گر به سیستم از طریق فلاپی BOOT بوده است. به همین دلیل میکروسافت تصمیم گرفت با توجه به رشد نیازهای کاربران به استفاده از رایانه در امور مختلف ضمن طراحی سیستم عاملهای جدید در ارتقای امنیت سیستم عامل نیز تلاش داشته باشد.

پس از این مسئله شرکت میکروسافت وارد مرحله جدیدی از سیستم عامل شد که به آن سیستم عامل ویندوز گفته شد.

- سیستم عامل ویندوز

سیستم‌های ویندوز انواع و اقسام مختلفی دارند. قبل از پرداختن به انواع سیستم عامل ویندوز به این مطلب می‌پردازیم که در زمان نصب این سیستم عامل بر روی یک رایانه چه اتفاقی رخ می‌دهد و به چه شکلی سیستم عامل ویندوز، باعشرقت اطلاعات دارنده رایانه می‌شود.

پس از نصب سیستم عامل ویندوز بر روی یک رایانه فضای ذخیره ساز رایانه به صورت مجازی به دو قسمت مجزا از یکدیگر تقسیم می‌شود:

۱. محیط عمومی [۱]
۲. محیط اختصاصی [۲]

محیط عمومی محیطی است که سیستم‌عامل در آن قسمت نصب می‌شود و عملا غیر از سیستم عامل اطلاعات دیگری در آن قسمت وجود ندارد و دسترسی به آن صرفا باعث دسترسی به سیستم عامل (و نه اطلاعات تولید شده به وسیله کاربران) می‌شود.

زمانی که در سیستم عامل ویندوز توسط مدیر سیستم (مالک رایانه) کاربر تعریف می‌شودسیستم برای هر کاربر یک محیط اختصاصی جداگانه ایجاد نموده و اطلاعات اختصاصی و تولید شده توسط هر کاربر در آن محیط به صورت جداگانه نگهداری می‌شود.تمام کاربران به محیط عمومی دسترسی داشته لیکن هر کاربر فقط به محیط اختصاصی خودش دسترسی دارد.

برای اینکه کاربران به محیطهای اختصاصی دیگران دسترسی نداشته باشند برای هر کاربر امکان تعریف رمز ورود[۳]وجود دارد و در صورت فعال سازی آن در صورتی که به خوبی تعریف شده[۱]باشد امکان دسترسی به محیطهای اختصاصی برای افراد غیر مجاز وجود نخواهد داشت.

کلیه سیستم‌های ویندوز از هر نوعی که باشند به صورت کلی به این روش اطلاعات را حیطه بندی نموده و از دسترس افراد غیر مجاز دور نگه می‌دارند.

---

[۱] Public

[۲] rivate

[۳] Password

انواع سیستم‌های‌عامل ویندوز به لحاظ امنیتی(نه به لحاظ کاربردی) را می‌توان به دو گروه عمده تعریف نمود:

۱. سیستم های عامل گروه ۹X

این گروه در بر گیرنده سیستم های عامل ذیل است:

- سیستم عامل ویندوز ۹۵
- سیستم عامل ویندوز ۹۷
- سیستم عامل ویندوز ۹۸
- سیستم عامل ویندوز میلینیوم

۲. سیستم های عامل ویندوز گروه NT [۱]

این گروه شامل سیستم های عامل زیر است:

- انواع سیستم عامل XP
- انواع سیستم عامل NT

- اشکالات امنیتی سیستم عامل ویندوز گروه ۹X

یکی از اشکالات اصلی این سیستم عامل که مشابه با سیستم عامل داس است این است که به مجرد اینکه فردی تلاش کند با

[۱] New technology

لوحBootable میلینیوم و از طریق لوح درایو این سیستم را بوت نماید امکان دسترسی به اطلاعات این رایانه مهیا می‌شود.

معمولاًبرای امن نمودن رایانه در مقابل این نوع دسترسی تلاش می‌کنند که لوح‌درایو و یا فلاپی درایو در رایانه نداشته باشند(رایانه بدون این دو وسیلهدیگر چه کاربردیدارد؟)و یا اینکه تلاش می‌کنند تا به روشنرم‌افزاری از طریق Setupسیستم ابزار بوت کننده سیستم را غیر فعال نموده و برای آنها رمزی فعال نمایند و برای استفاده از آنها باید فرد رمز را بداند و در صورت ندانستن رمز عملاً امکان استفاده از آنها امکان پذیر نخواهد بود.

حال فرض کنیم یک رایانه داریم که به لحاظ امنیتی تمام موارد فیزیکی مبنی بر عدم امکان دسترسی فیزیکی به سیستم‌عامل بسته شده است می‌خواهیم بررسی نماییم در این صورت آیا این رایانه ها دارای امنیت هستند؟

- اشکالات اساسی سیستم عامل ویندوز گروه ۹X

در صورتی که فردی رمز مربوط به کاربری خود را فراموش کرده باشد و یا اینکه اصلا رمز را نداند(فرد غیر مجاز نفوذگر) در صورت انجام هر کدام از اقدامات ذیل رمز سیستم عاملرا نیاز نداشته و وارد قسمت عمومی سیستم عامل خواهد شد.

۱. اگر فرد در قسمت ورود به سیستم از روی صفحه کیبرد دگمه ESC را فشار دهد.
۲. در قسمت ورود به سیستم به جای اینکه رمز را زده و سپس دگمه OK را کلیک نماید دگمه Cancelرا کلیک نماید.

در هر کدام از حالات فوق فرد غیر مجاز یا فرد مجازی که رمز را فراموش کرده باشد وارد قسمت عمومی رایانه خواهد شد و اگر مدیر رایانه، رایانه را به خوبی پیکربندی نکرده باشد فرد می‌تواند ازطریق My Computer به قسمت های دیگر رایانه دسترسی داشته و وارد محیط های اختصاصی کاربران شده و به اطلاعات آنها دسترسی پیدا کند.

فرض را بر این می‌گیریم که مدیر سیستم این کار را انجام داده باشد و ورود کننده به این قسمت از رایانه دیگر دسترسی به محیطهای اختصاصی پیدا نمی کند! شما چه فکر می‌کنید.

در زمانی که مدیر سیستم برای هر کاربر رمز ورود جداگانه‌ای را تعریف می کند به صورت خودکار و توسط سیستم عامل ویندوز **۹X** یک فایل به نام کاربر ایجاد می‌شود(نام کاربر هر چه باشد این فایل نیز به همان نام ایجاد می‌شود – به طور مثال اگر نام کاربر علی باشد نام این فایل نیز علی خواهد بود یا اگر ۱۲۳ باشد نام آن فایل نیز ۱۲۳ خواهد بود).پسوند این فایل توسط سیستم به نام **PWL**[۱]خواهد بود. این فایل در قسمتی و فولدری که سیستم عامل در آنجا نصب شده باشد ایجاد می‌شود.پس پیدا کردن آن وقت زیادی نخواهد خواست و با یک جستجوی ساده فایلهای با پسوند PWL می‌توان آنها را پیدا کرد.اگر فرد تلاش نماید تا با باز کردن این فایلها به روش عادی مانند استفاده از یک واژه پرداز به محتویات این فایلها که همان

[۱] Password list

تنظیمات امنیتی و رمز کاربری است دسترسی پیدا کند عملا نه اینکه به هیچ چیز دسترسی پیدا نمی کند بلکه باعث خراب شدن این فایل خواهد شد.اما اگر این فایل را از محل اصلی خود جابجا کرده (با دستور CUT و PASTE) و رایانه را یک بار خاموش و روشن نماید همان اتفاقی که نباید بیفتد خواهد افتاد و اینبار دیگر از نفوذگر رمز عبور را درخواست نخواهد کرد و نفوذگر می‌تواند اطلاعات مورد نظر را کپی کرده و از رایانه خارج نماید.(ممکن است این سوال به ذهن خواننده رسوخ کند که کاربر اصلی پس از دسترسی به رایانه متوجه خواهد شد که در رایانه‌اش اتفاقی افتاده است و دیگر از او رمز نمی‌خواهد)

حال اگر نفوذگر پس از اتمام کار فایلی را که جابجا کرده است را به جای اولیه برگرداند و رایانه خاموش و روش شود انگار که هیچ اتفاقی نیفتاده است و دلیلی بر این وجود ندارد که کاربر اصلی متوجه شود در زمانی که دور از رایانه بوده است برای رایانه اتفاقی افتاده است!!

به همین راحتی ممکن است فرد نفوذگر بدون دانستن یک رمز خوب (ولو رمزی که تمام شرایط یک رمز خوب را داشته باشد) می‌تواند در این سیستم عامل به اطلاعات به شکل غیر مجاز دسترسی پیدا نماید بدون اینکه ردپایی از خودش به جای گذارد.

شرکت میکروسافت پس از اطلاع از اینکه این نقاط ضعف سیستم‌عامل ویندوز گروه **۹X** باعث افت بازار اقتصادی شرکت در این رابطه شده است با کمک کارشناسان و متخصصین ۵۱ کشور دنیا سیستم عامل جدید خود را نوشته و شروع به تبلیغات

وجود امنیت در این سیستم عامل کرد و حدودا مبلغ سه میلیون دلار در رابطه با تبلیغات وجود امنیت در سیستم عامل جدید هزینه کرد.

- امنیت در سیستم عامل ویندوز گروه NT

شرکت میکروسافت پس از ارایه سیستم عامل جدید خود اولین اقدامی را که انجام داد این بود که به کاربران نشان داد که نه تنها سیستم عامل جدید مشکلات امنیتی سیستم عامل قبلی را ندارد بلکه علاوه بر اضافه کردن نکات کاربردی در این سیستم عامل امنیت را نیز بالا برده است. در این سیستم عامل کاربران دیگر نمی توانستند با زدن دگمه ESC از رمز عبور، عبور نموده و وارد محیط عمومی سیستم عامل گردند. دیگر در صفحه ورود کاربران دگمه Cancel وجود نداشت تا کاربران بتوانند بر روی آن کلیک کرده و از رمز عبور گذر کنند. در این سیستم عامل جدید از فایلهایی با نام کاربر و پسوند PWL خبری نبود تا کاربران بتوانند با حذف آنها وارد صفحات اختصاصی کاربران گردند و ...

در سیستم عامل جدید اطلاعات امنیتی مربوط به کاربران در فایلهایی با پسوند SAM بوده است لیکن با بالا آمدن سیستم عامل این فایلها به علت امنیتی از دسترسی کاربران خارج می‌شده و امکان دخل و تصرف و تغییرات در آنها وجود نداشته است.

در سیستم عامل جدید امکانات امنیتی دیگری نیز به آن اضافه شده بود و یکی از آنها اضافه کردن رمز دیگری به سیستم

عامل و امکان انتقال رمز بر روی یک فلاپی و قرار دادن آن در محیط امنی بود تا دیگران نتوانند بدون داشتن آن به رایانه دسترسی داشته باشند.

حال تصور کنید که یک دستگاه رایانه دارای سیستم عامل جدیدرا خریداری و یا در سیستم اداری و یا خصوصی تحویل گرفته اید ودر نظر دارید:

- اطلاعات مربوط به خودتان را با این رایانه مدیریت کنید.
- در منزل از این رایانه برای مدیریت اطلاعات خصوصی و خانوادگی استفاده کنید .
- از این رایانه در محیط اداری برای ثبت اطلاعات طبقه بندی شده اداری استفاده کنید.
- از این رایانه در محیط شرکت خصوصی برای ثبت اطلاعات محرمانه و اقتصادی شرکت خودتان استفاده کنید.
- رایانه نوت بوک خودتان را در سفرهای زیارتی و تجاری همراه خودتان به کشورها و شهرهای دیگر ببرید تا بتوانید در طول سفر علاوه بر انجام امور کاری خود گزارشات روزانه خودتان را در آن درج فرمایید.
- و بسیاری از استفاده های دیگر که می‌توانید از رایانه به عنوان یک رایانه مستقل بهره برداری کنید.

اولین دغدغه خاطر تمام کاربران این است که به چه شکلی رایانهرا امن گرداند تا دیگران نتوانند به اطلاعات خصوصی دسترسی داشته باشند و نتوانند اطلاعاتی را که شما بهعنوان یک پژوهشگر در طی سالیان متمادی جمع‌آوری کرده‌اید تا به عنوان یک کتاب چاپ کنید قبل از شما چاپ کنند.در این مرحله می خواهیم امنیت را در یک دستگاه رایانه دارای سیستم عامل XP برقرار کرده و نقاط ضعف امنیتی آن را بررسی کنیم.

اولین و بدیهی‌ترین اقدام برای تامین امنیت در این سیستم عامل شناسایی و تامین امنیت کاربران سیستم عامل است.شیوه تامین اولیه امنیت در سیستم عامل از طریق کاربران است پس باید کاربران را شناخت و شیوه امن کردن آنها را یاد گرفت. نکته مهم این است که باید تکلیف تمام کاربران را به لحاظ امنیتی مشخص کرد زیرا در فضای مجازی این سیستم عامل، فردی مالک اطلاعات رایانه است که بتواند از سیستم عامل عبور نموده و مدیریت بر سخت افزار و نرم افزار رایانه را بدست بگیرد.

انواع کاربران سیستم‌عامل ویندوزXp عبارتند از:

۱. مدیر سیستمیا هم طراز مدیر سیستم[۱]

مدیر سیستم در سیستم همه کاره بوده و به کل اطلاعات سیستم و کاربران دسترسی داشته و هر کاری که مد نظر داشته باشد می‌تواند انجام دهد. به همین خاطر بالاترین سطح دسترسی را در

[۱] Administrator

سیستم دارد و هر فرد مجاز و یا غیر مجاز که بتواند این کاربر را بدست بگیرد در سیستم همه کاره خواهد بود. این کاربر جزء کاربران پیش فرضسیستم بوده و با نصب سیستم عامل بر روی یک دستگاه رایانه به صورت پیش فرض بر روی سیستم ایجاد می‌شود. برخی از نکاتی که در رابطه با این کاربر مهم استعبارتند از:

- این کاربر پیش فرض سیستم عامل است.
- این کاربر را نمی توان از روی سیستم حذف کرد.

در هنگام نصب سیستم عامل از نصب کننده سوال می‌شود که آیا مایل به این هستید که بر روی آن رمز عبور بگذارید یا خیر و در صورت عدم اقدام نصب کننده، این کاربر فاقد رمز خواهد بود.

این کاربر بر روی صفحه دسکتاپ بسیاری از کاربران دیده نمی‌شود و بسیاری از کاربران حتی متوجه نمی‌شوند که چنین کاربری برروی سیستم‌شان وجود دارد و به همین علت بسیاری از نفوذگران از این ناآگاهی کاربران سوءاستفاده می کنند.

با گرفتن همزمان دکمه‌های ALT+CTRL+DELET و دو بار پشت سرهم فشار دادن آن صفحه‌ای در دسکتاپ ظاهر می‌شود که می‌توان در قسمت کاربر آن نام ADMINISTRATOR را نوشت و اگر فاقد رمز عبور باشد قسمت رمز عبور را خالی گذاشت و با دسترسی مدیر سیستم وارد سیستم‌عامل شد(با بالاترین سطح اختیارات). بسیاری از کاربران

متأسفانه بر اثر این خطا اطلاعات خود را در معرض خطر قرار داده اند.

برای امن نمودن این کاربر باید اطمینان حاصل کرد که رمز ورود مربوط به آن را فقط مالک رایانه در اختیار دارد.پس اگر فاقد رمز عبور بود بر روی آن رمز عبور مناسب گذاشته و اگر دارای رمز عبور بود آن را با رمز عبور مناسب تعویض می کنیم.

یکی از اشتباهات رایج کاربران این است که می گویند این کاربر دارای رمز عبور است ولی ما آن را نمی‌دانیم. روزی که برای خرید رایانه و یا تحویل گرفتن رایانه رفته بودیم بر روی این کاربر رمز عبور گذاشتند ولی الان چند سال گذشته است و دیگر رمز عبور آن را نمی‌دانیم(توجه داشته باشید که دیگر شما مالک اطلاعات این رایانه نیستید بلکه آن فرد یا افرادی که این رمز عبور را می‌دانند مالک اصلی اطلاعات هستند.)

۲. میهمان یا هم طراز میهمان[۱]

این کاربر نیز جزء کاربران پیش فرض سیستم بوده و قابل حذف از سیستم‌ها است. سطح دسترسی این کاربر صرفا دسترسی به اطلاعات محیط عمومی سیستم است (جایی که ویندوز نصب شده است) برای امن نگه داشتن سیستم ابتدابابد برای این کاربر رمز دسترسی تعریف کرد و سپس آن را غیر فعال کرد.

۳. کاربران مجاز تعریف شده توسط مدیر سیستم[۱]

---

[۱] Guest

این کاربران توسط مدیر سیستم تعریف شده و میزان دسترسی آنها به اندازه‌ای است که مدیر سیستم تعریف می‌کند. برای ایمن کردن این کاربران ابتدا می‌بایست نسبت به حذف کاربرانی که نیاز نداریم اقدام و سپس کاربرانی که فاقد رمز هستند را برایشان رمز عبور مناسب تعریف و کاربرانی را که رمز دارند را تعویض رمز کنیم.

یکی از اشتباهات رایج کاربران در این مرحله این است که کاربرانی را که نیاز ندارند همچنان نگه می‌دارند و به تجربه دیده شده است اینگونه کاربران در دراز مدت برای سیستم مشکل آفرین شده اند.

۴. کاربران میهمان ناخوانده

این گونه کاربران توسط مدیر سیستم ایجاد نشده و جزء کاربران پیش فرض نیز نیستند و به مجرد اینکه برخی از سرویس های ویندوز فعال می‌شوند این کاربران به صورت اتوماتیک ایجاد می‌شوند. کاربرانی مانند ASP.NET و Helpassistant و Support_**۳۸۸۹۴۵**a۰ از این نوع کاربران هستند و معمولاً برای دسترسی به رایانه از راه دور مورد استفاده سیستم واقع می‌شوند. در استفاده از رایانه به صورت مستقل و برای کارهای عادی و عمومی معمولا به این کاربران نیازی پیدا نمی‌شود و برای ایجاد امنیت بیشتر می‌توان تمام آنها را حذف نمود.

---

[۱] Users

۵. کاربران میهمان ناخوانده پنهان

اینگونه کاربران نه پیش فرض سیستم هستند و نه اینکه توسط مدیر سیستم ایجاد شده است و به طور مثال در زمانی که در سیستم برای مدیریت بر بانکهای اطلاعاتی از SQL استفاده شود کاربری به نام sa ایجاد می‌شود که اگر دقت نشود و در امتداد امنیت دیگر قسمتهای سیستم قرار داده شود می‌تواند امنیت سیستم را به خطر بیندازد. توضیح اینکه این کاربر برای کاربرانی که از سیستم به صورت مستقل استفاده می‌کنند معمولا خطر ساز نیست و اگر قرار باشد در شبکه ای از این رایانه ها استفاده شود می‌تواند برای رایانه خطر ساز باشد(تاکنون شبکه های مختلفی در اینترانت ها و یا اینترنت از این طریق مورد حمله قرار گرفته و هک شده اند)

این کاربر از طریق سیستم‌ها، برنامه‌ها و سرویس‌های داخلی ویندوز قابل شناسایی نبوده و نمی توان بر روی آن اقدامی را انجام داد.

کاربران گروه اول تا سوم معمولا از طریق User Accounts قابل اقدام است ولی در برخی مواقع مانند رمز گذاری بر روی کاربر میهمان به مشکل بر می‌خورد. کاربران گروه چهارم را نیز نمی‌توان از این طریق مشاهده و اقدام نمود. پس باید با استفاده از روشی این کارها را انجام داد و تکلیف امنیتی کاربران را روشن نمود.

یکی از راحت‌ترین و بهترین راهها برای این کار استفاده از دستورNETUSER به شکل زیر است:

۱-all programs

۲- run

۳- cmd

۴-ok

در این حالت صفحه مشکی مربوط به DOS معروف نمایان است. در این قسمت اگر با دسترسی مدیر سیستم و یا همطراز مدیر سیستم، سیستم را روشن کرده باشیم می‌توانیم کار را ادامه دهیم و نیازی به این نداریم که نوشته‌های بر روی خط فرمان را بلد بوده و ترجمه کنیم. فقط باید این را بدانیم که اگر پس از هر دستور و زدن اینتر پاسخ زیر را دریافت کردیم سیستم دستور ما را پذیرفته است.(The command completed successfully)

شیوه استفاده از این دستور به شکل زیر است:

۱. اگر از دستور NET USERبه صورت خالی استفاده شده و پس از آن اینتر زده شود نتیجه مشاهده کلیه کاربران چهار گروه اول سیستم خواهد بود.
۲. اگر پس از NET USER نام کاربر مورد نظر و پس از آن رمز مورد نظر و سپس اینتر زده شود نتیجه ایجاد رمز جدید برای کاربر و یا تعویض رمز قبلی خواهد بود(در این روش نیاز به دانستن رمز قبلی نیست)
۳. اگر پس از NET USER نام کاربر مورد نظر موجود و سپس delete/ زده شود کاربر مربوطه از سیستم حذف می‌شود.

۴. اگر پس از NET USER نام کاربر جدید مدنظر و سپس رمز مورد نظر و سپس ADD/ زده شود کاربر جدیدی با نام زده شده و با رمز داده شده ایجاد خواهدشد.(توضیح اینکه این دستور بدون ارایه رمز نیز امکان‌پذیر خواهد بود اما موکدا تاکید می‌شود حتما رمز را وارد نمایید تا کاربر بدون رمز بر روی سیستم شما ایجاد نشود)

پس با استفاده از این دستورات می‌توان مشکل رمز گذاری برای کاربر میهمان و همینطور حذف کاربران میهمان ناخوانده را حل کرده و بدین صورت مشکل ایمن کردن کاربران را به صورت کامل (البته فقط برای رایانه مستقل)حل کرد.

***

دلایل و روش های نرم افزاری دسترسی به اطلاعات

در هنگام کار با سیستم عامل احتمالاً پیامهای مختلف سیستم عامل را مبنی بر اینکه اگر رمز خود را فراموش نمایید دیگر نمی‌توانید به اطلاعات خودتان دسترسی داشته باشید را ملاحظه نموده اید.

احتمالا در سایت میکروسافت و سایتهای مختلف و وبلاگ ها و کتب مختلف آموزشی و دوره های آموزشی ICDL این مطلب به شما گوشزد شده است که اگر رمز خود و مدیر سیستم را فراموش کنید دیگر قادر به دسترسی به اطلاعات خودتان نمی باشید و مجبورید یک نسخه جدید ویندوز را نصب نمایید و با این عمل اطلاعات قبلی قابل دسترسی نخواهد بود!

بسیاری از کاربران از این خبر خوشحال شده و امیدوار می‌شوند که اگر این اقدامات امنیتی را رعایت کنند اطلاعات آنها توسط افراد غیر مجاز قابل دستیابی

نخواهد بود.این قبیل کاربران در زمانی که رایانه آنها با مشکل سخت افزاری و یا نرم‌افزاری روبرو می‌شود پس از انجام اقدامات امنیتی آن را به راحتی در اختیار افراد مجاز و غیر مجاز برای تعمیر قرار می‌دهند.این قبیل کاربران در مسافرتهای خارج از کشور خود به راحتی نوت بوک خود را امن ساخته و همراه خود به سفر برده و با آن اطلاعات خود را مدیریت می‌کنند.این قبیل کاربران رایانه های خود را امن کرده و آن را برای دقایقی همراه با افراد مجاز و غیر مجاز به تنهایی رها می‌سازند.و بسیاری موارد دیگر که باعث دسترسی فیزیکی افراد به رایانهمی‌شود.

در این مرحله فرض می‌کنیم ما دارای یک رایانه هستیم که تمام کاربران آن ایمن شده و با استفاده از دستورSYSKEY دارای یک رمز شده و رمز آن به داخل یک فلاپی منتقل شده و همیشه همراه ما است.می‌خواهیم بررسی کنیم اگر یک فرد غیر مجاز در نظر داشته باشد به اطلاعات این رایانه دسترسی داشته باشد:

چه میزان اطلاعات فنی مورد نیاز دارد؟

چه میزان سرمایه گذاری مادی برای این کار نیاز دارد؟

چه میزان زمان برای این کار نیاز دارد؟

چه ابزاری برای این کار نیاز دارد؟

چه رد پایی از خودش به جای می‌گذارد تا پس از به دست گرفتن رایانه خود مشکوک به دسترسی افراد غیر مجاز به رایانه خود شویم و در نظر داشته باشیم موضوع را پیگیری نماییم.

جواب کلی به تمام سوالات فوق "یک نفر با تحصیلات ابتدایی رایانه و با داشتن حداکثر پانصد تومان و در زمان دو دقیقه و بدون گذاشتن هیچ رد پایی موفق به این کار خواهد شد". در ادامه روش های دسترسی به فایل های محرمانه شما را مرور می کنیم.

- استفاده از LIVE CD ویندوز یا لینوکس

در این روش با توجه به اینکه فرد مهاجم از یک سیستم عامل دیگری برای ورود به رایانه استفاده می‌کند و سیستم عامل اولیه به هیچ عنوان فعال نمی‌شود تا بتواند نرم افزارهای امنیتی و گذر واژه ای را فعال نماید به همین خاطر پس از BOOT شدن رایانه با این سیستم عامل و دسترسی به کلیه اطلاعات رایانه و انجام هرگونه اقدام مد نظر از قبیل کپی گیری از اطلاعات و یا فعال کردن نرم افزار مخرب و .... و سپس خاموش کردن رایانه و خارج کردن سیستم عامل ثانویه هیچگونه اثری بر روی رایانه باقی نخواهد ماند و در صورت مراجعه کاربر عادی به رایانه، به حالت عادی می‌تواند با رمزهای تعریف شده و به شکل قبلی کار را ادامه دهد.

- استفاده از نرم افزارهای حمله کننده به رمز:

اینگونه نرم افزارها که امروزه با نازل‌ترین قیمت و در برخی از اوقات به صورت مجانی در اینترنت و مغازه‌ها یافت می‌شود می‌توانند در مدت زمان حدود ۱۵ الی ۴۵ ثانیه کلیه رمزهای تعریف شده را غیر فعال ساخته و باعث دسترسی بدون نیاز به رمز به اطلاعات رایانهشود. در برخی مواقع دیده شده این نفوذ گران برای اینکه ذهن کاربران عادی را از دغدغه خاطر داشتن دسترسی افراد غیر مجاز به رایانه دور کنند پس از اتمام کار یک رمز دیگری را برای رایانه تعریف کرده و سپس رایانه را خاموش می‌کنند و کاربر عادی در مراجعه به رایانه خود نمی‌تواند با رمز قبلی وارد رایانه شود و برخی از کاربران آماتور احساس می‌کنند یا رمز را فراموش کرده اند و یا اینکه رایانه خراب شده و به هم ریخته‌است.(ولی کاربران

حرفه‌ای می‌دانند که تنها اتفاقی که افتاده است این است که اطلاعات به دست افراد غیر مجاز رسیده است)

پس:

- اگر در مراجعه به رایانه خود متوجه شدیم که هیچ اتفاقی نیفتاده است و رایانه ما با همان رمزهای قبلی به خوبی کار می‌کند قسم نخوریم که کسی به اطلاعات ما دسترسی پیدا نکرده است زیرا ممکن است طرح LIVE CD اجرا شده باشد!
- اگر در مراجعه به رایانه خود متوجه شدیم رایانه ما فاقد رمز شده است مطمئن باشیم که حتما کسی به رایانه ما دسترسی غیر مجاز پیدا کرده است.
- اگر در مراجعه ما به رایانه خود مواجه با تغییر رمز ها و عدم قبول رمز خودمان روبرو شدیم مطمئن باشیم که حتما کسی به رایانه ما نفوذ کرده است.

پس راه حل چیست؟ اطمینان از عدم دسترسی افراد غیر مجاز به صورت فیزیکی به رایانه ما ولو برای ۱۵ ثانیه!!

با توجه به مطالب فوق کاربرانی که به دنبال راههای امن سازی نرم‌افزاری رایانه‌ای هستند برای امن سازی اطلاعات به دنبال نرم افزارهای کاربردی هستند.

- امن سازی نرم افزارهای کاربردی

بسیاری از نرم افزارهای کاربردی که امروزه در نقاط مختلف دنیا توسط کاربران به کار گرفته می‌شوند (رایجترین آنها به طور مثال نرم افزار

Office) این قابلیت را برای کاربر ایجاد کرده است تا کاربر بتواند به سلیقه خود دو رمز را برای ایمن سازی فعال کند:

- رمز اول – برای اجازه باز کردن اطلاعات و رویت آن
- رمز دوم – برای اجازه اعمال تغییرات در اطلاعات

این رمزها را می‌توان در مراحل تولید اطلاعات فعال نموده و به گفته تولیدکننده‌های این نوع نرم افزارها، در صورتی که فردی رمزهای مربوطه را نداشته باشد نمی‌تواند به اطلاعات دسترسی پیدا کند هر چند به فایل مربوطه دسترسی داشته باشد و بتواند آن را کپی کرده و از رایانه خارج و در رایانه خود اجرا نماید(رمزها همچنان معتبر خواهند بود)

اما کار بران حرفه ای می‌دانند که امروز حداقل ۳ روش برای حمله به رمز وجود دارد که افراد غیر مجاز می‌توانند با به کارگیری آن موفق به دستیابی به رمز شده و هر کسی که رمز را بداند عملا مالک اطلاعات خواهد بود.

۱. روش حمله Bruth force

در این روش، حمله کننده نمی‌داند که رمز مربوطه از چه حروفی و با چه ترکیبی استفاده شده است پس سیستم حمله کننده مجبور است تمام حالتهای ممکن را مورد بررسی قرار دهد.امروزه این حمله با سرعت حدود ۱۵۰۰۰۰ مورد در ثانیه انجام می‌شود.(در برخی از کتابها نوشته شده است حالات مختلف این حمله حدود ۲۲۰۰۰۰۰۰۰۰۰ حالت است و حمله کامل بین ۶۰ الی ۷۰ سال طول میکشد!!) ولی کاربران حرفه ای می‌دانند امروزه این کار، برای یک کلید واژه ۴ حرفی حداکثر ۲ ساعت طول می‌کشد.

۲. روش حمله Dictionary

این روش حمله ای در زمانی صورت می‌گیرد که رمز استفاده شده، در یکی از لغت نامه های زبانهای دنیا پیدا شود(هرچند لغت بسیار بزرگی باشد) امروزه با نرم افزارهای رایج این حمله حداکثر ۳ ثانیه طول می‌کشد.

۳. روش حمله مستقیم

در نرم‌افزارهایی که الگوریتم رمز آنها و محل قرار گرفتن رمز در اطلاعات فاش شده است معمولاً از این روش استفاده می‌شود.