بررسی امکانات ایمنی نرم افزار ADM
در محیطهای آموزشی

عباس خسروبیگی

آدرس :

دانشگاه آزاد اسلامی - واحد ملایر

بخش موضوعی :

آموزش و کاربرد کامپیوتر در ایران و امنیت اطلاعات

بسمه تعالی

بررسی امکانات ایمنی نرم افزار ADM در محیطهای آموزشی

چکیده

در سیستمهای عامل باز که جزئیات عملکرد سیستم را اکثر کاربران ماهر سیستم می دانند، می توان برای ایجاد امنیت در کاربردهائی که به ایمنی بالائی نیاز دارند، از نرم افزارهای آماده استفاده نمود. در این مقاله ایجاد امنیت در سیستمهایی که در محیطهای آموزشی تحت سیستم عامل DOS کار میکنند، با استفاده از نرم افزار ADM بررسی می شود و در مورد میزان امنیت ایجاد شده توسط ADM در این سیستمها بحث شده و راههای نفوذ و جلوگیری از نفوذ به سیستم مورد بررسی قرار میگیرد.

مقدمه

یکی از مهمترین کاربردهای کامپیوتر در زمینه آموزش می باشد. با توجه به پیشرفت روز افزون سخت افزارها و نرم افزارهای کامپیوتری در محیطهای کاری مختلف ، لزوم برنامه ریزی صحیح و اصولی در جهت استفاده بهینه و توسعه کاربرد کامپیوتر در امور آموزشی ، بیش از پیش احساس می شود. در این مقاله برخی از مسائل و مشکلات محیطهای آموزشی کامپیوتری بررسی گردیده و برای حل آنها روشهائی ارائه می گردد. لازم بذکر است که این مقاله به محیطهای آموزشی کامپیوترهای شخصی (PC) که سیستم عامل مورد استفاده در آنها MS - DOS باشد می پردازد . علت این انتخاب نیز گستردگی استفاده از چنین امکاناتی در کشور می باشد. بدیهی است با توجه به اینکه Windows 3.x یک نرم افزار DOS Base می باشد و ایجاد امنیت مورد بحث در این مقاله در موقع راه اندازی سیستم انجام می شود ، بنابراین امنیت ایجاد شده برای کار در محیط ویندوز نیز تعیین کننده است. همچنین ممکن است در برخی موارد برای ایجاد امنیت در کامپیوتری که سیستم عامل آن Windows 95 یا Windows 98 می باشد ، از ADM استفاده شود که این امر با توجه به اینکه هسته مرکزی سیستم عامل Windows 9x مشابه هسته مرکزی سیستم عامل DOS میباشد، در مباحث مطرح شده در این مقاله تغییری ایجاد نمی کند و موارد ذیل در چنین سیستمهائی نیز مصداق دارند.

بکارگیری ابزارهای کمکی

در سیستم عامل DOS[۲] در مقایسه با (بعنوان مثال) سیستم عامل VMS[۳] برای کامپیوترهای VAX که از درون آن چندان اطلاعی در دست نبوده و امکانات امنیتی آن کافی به نظر می رسد، ایجاد امنیت توسط ابزارهای کمکی دیگری ضرورت پیدا می کند. برای این منظور نرم افزارهای مختلفی مانند ADM[۴]، ADMPLUS[۵]، ARMOR، DISKREET[۶] و NDL توسط شرکتهای مختلف تهیه شده که هر یک امکاناتی برای حفاظت اطلاعات موجود در یک Partition، Directory و یا File را دارند. اکثر نرم افزارهای موجود از بعد ایجاد امنیت ضعیف هستند. بدین معنی که ایمنی ایجاد شده توسط آنها قابل شکست می باشد.

بررسی چگونگی ایجاد امنیت توسط نرم افزارها روی سیستم عاملهای باز موجب اطلاع از اشکالات آنها و تلاش در جهت رفع این اشکالات و افزایش ایمنی در سیستمهای کامپیوتری خواهد شد. چرا برخی نرم افزارها چنین اشکالاتی را دارند؟ شاید عدم اطلاع کاربران و محققان در زمان تهیه نرم افزار از چگونگی ایجاد امنیت و یا نفوذ به آن وجود چنین اشکالاتی را توجیه کند و نیز شاید بتوان گفت عدم توجه و دقت لازم طراحان و برنامه نویسان چنین سیستمهائی به نقاط ضعف موجود در آنها عامل وجود چنین اشکالاتی میباشد.

نیازهای ایمنی در کامپیوترهای شخصی

در سازماندهی و پیکر بندی کامپیوترهای شخصی مستقر در محیطهای آموزشی (و محیطهای مشابه) موارد ذیل بایستی رعایت شوند:

۱- **امنیت (Security)** : جلوگیری از دسترسی غیر مجاز به داده ها و برنامه ها در این مقوله میگنجد . در برخی مواقع ممکن است بخواهیم گروهی از کاربران سیستم به قسمتهائی از دیسک سخت PC دسترسی نداشته باشند.

۲- **حفاظت (Protection)** : چگونگی دسترسی مجاز به داده ها و برنامه ها را تعیین می کند. منظور این است که آیا حال که کاربری اجازه دسترسی به یک Partition از دیسک سخت را دارد اجازه عمل Write را نیز داشته باشد یا فقط بتواند عمل Read را انجام دهد؟ در برخی مواقع حفاظت می تواند حتی تبعات مهمتری از امنیت داشته باشد. زیرا اگر ما اجازه Write را به همه کاربران بدهیم عملیات PM (نگهداری نرم افزاری) برای راهبر سیستم بسیار مشکل خواهد شد. چرا که برخی کاربران عمداً یا سهواً دست به حذف و یا تغییر و دستکاری برخی داده ها و برنامه ها می کنند که این عمل چه بسا موجب عدم اجرای یک برنامه شود. اگر کاربری مبتدی در یک Session کاری ناشیانه دستور Del *.* را روی یک مسیر اجرا کند آنگاه راهبر سیستم بایستی احتمالاً وقت زیادی را صرف نصب مجدد نرم افزار روی کامپیوتر کند.

۳- **مقابله با ویروسها** : ویروسها[۱] برنامه های کامپیوتری معمولاً مخربی هستند که از طریق دیسکهای آلوده و ... به حافظه اصلی کامپیوتر نفوذ کرده و از آنجا به سیستم حمله می کنند. نقاطی که ویروسها بدانها حمله می کنند عبارتند از : Executable Files - Boot Sector - Partition Table . علت حمله

ویروسها به این نقاط ، امکان راه یابی آنها از آنجا به حافظه اصلی می باشد. برای مقابله با ویروسها تمهیدات لازم بایستی (از جمله Write Protect کردن فایلها یا درایوها) بکار گرفته شود.

۴- Partitioning : نحوه تقسیم بندی دیسک سخت سیستم بایستی کاملاً حساب شده باشد. حداقل تعداد قسمتها برای سادگی عملیات PM باید ۳ قسمت باشد (یکی برای راه اندازی سیستم ، دیگری برای نرم افزارها و سومی برای انجام تمرینات کاربران) . پیشنهاد می شود برای اکثر کاربران دسترسی به درایوهای C: و D: به صورت Read Only باشد.

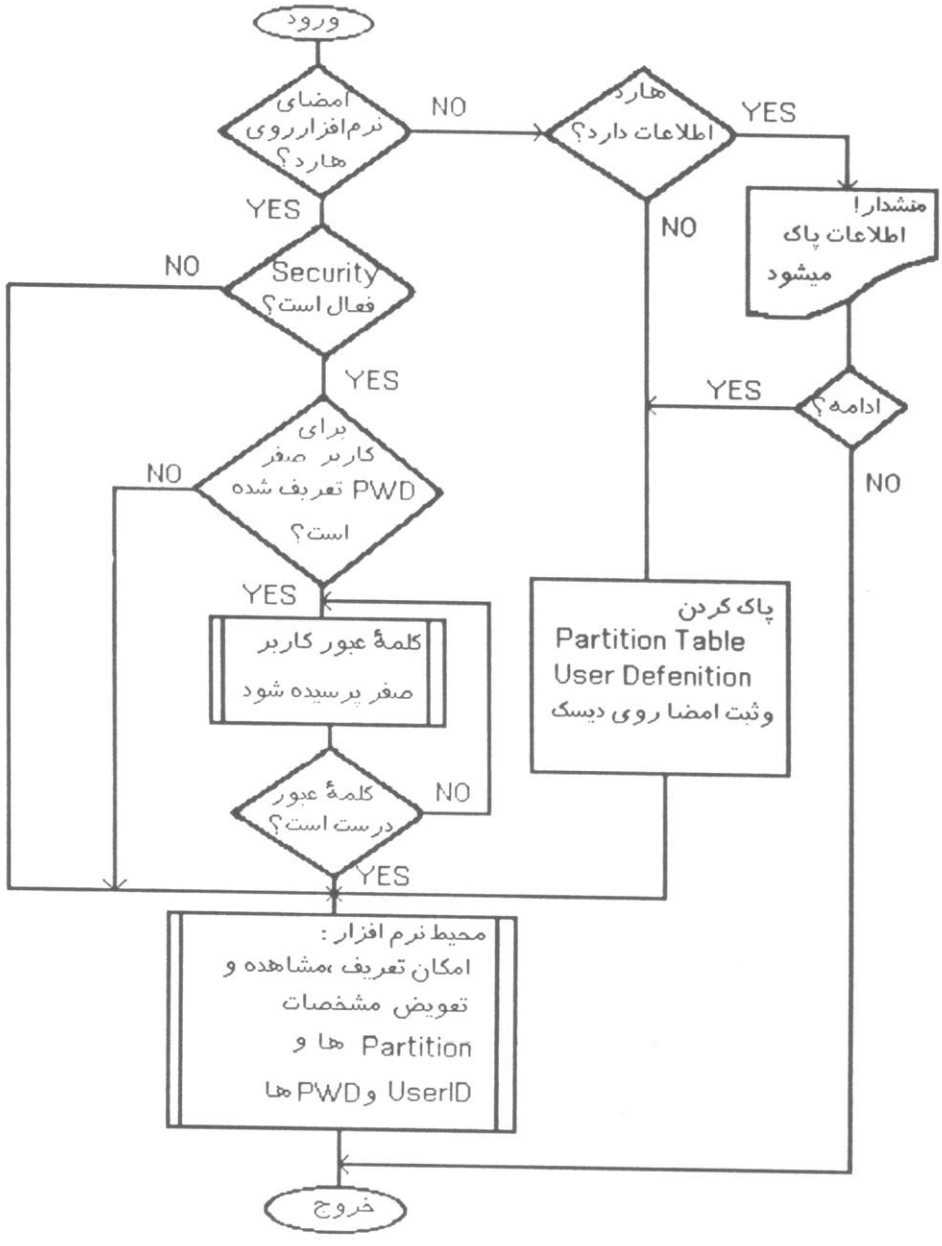
نرم افزار ADM

نرم افزار (ADM (Advanced Disk Management محصول شرکت MITAC می باشد که برای بخش بندی (Partition) دیسک سخت کامپیوترهای شخصی تحت سیستم عامل DOS و ایجاد امنیت طراحی شده است. با کمک این نرم افزار در ابتدا دیسک سخت را بخش بندی ، سپس هر قسمت را Initialize کرده و نهایتاً امکان Security را فعال و User ID و Access Right و در صورت لزوم Password تعریف میکنند. نکات حائز اهمیت در اینجا عبارتند از :

۱- نوع (Type) یکی از بخشهای ایجاد شده DOS و نوع بقیه بخشها ADM می باشد. بخشهای نوع ADM را سیستم عامل DOS به خودی خود نمی شناسد و برای اینکه کاربر بتواند به این بخشها دسترسی پیدا کند، لازم است که در موقع راه اندازی (Boot Up) سیستم و از طریق فایل Config.sys درایور Adm.sys اجرا شود.

۲- دسترسی کاربران به Partition ها در قسمت Set User's Access Right تعریف می شود که میتواند . (No Access) ، یا R (Read Only) و یا W (Read & Write) باشد. اگر برای کاربری امکان دسترسی R به قسمتی از دیسک سخت را داده باشیم در Session کاری او اجازه عمل Write نخواهد داشت.

در مورد نحوه عملکرد نرم افزار ADM باید گفت که این نرم افزار در حین اجرا ابتدا به دنبال امضای خود روی Hard Disk کامپیوتر (*MITAC-ADM*) می گردد. اگر آنرا یافت و Security ، ON بود آنگاه با احضار یک روتین Password کاربر اصلی (superuser) ، که کاربری با شماره شناسائی صفر می باشد، را می پرسد. اگر فردی که این نرم افزار را اجرا کرده اطلاعات خواسته شده را بداند مجاز به ورود به محیط نرم افزار و انجام کارهای بعدی می باشد. مراحل اجرای نرم افزار در شکل صفحه بعد نمایش داده شده است. اگر کسی وارد محیط نرم افزار شود، اطلاعات مربوط به Patitioning و User ID و PWD ها در اختیارش می باشد.


ورود
امضای نرم‌افزار روی هارد؟
NO
هارد اطلاعات دارد؟
YES
منشدار! اطلاعات پاک میشود
YES
NO
Security فعال است؟
NO
YES
ادامه؟
YES
برای کاربر صفر PWD تعریف شده است؟
NO
NO
پاک کردن Partition Table User Defenition وثبت امضا روی دیسک
YES
کلمهٔ عبور کاربر صفر پرسیده شود
کلمهٔ عبور درست است؟
NO
YES
محیط نرم افزار : امکان تعریف ،مشاهده و تعویض مشخصات Partition ها و UserID و PWD ها
خروج

راههای نفوذ در ADM و روشهای جلوگیری از آن

یکی از راههای نفوذ به ADM ، تغییر سه بایت از فایل Adm.exe به کد 90 (NOP) مـی باشـد. ایـن تغییر می تواند به کمک نرم افزار Pctools یا نرم افزارهای مشابه صورت گیرد. با ایجاد این تغییر عمل احضار روتین پرسش کلمه عبور کاربر اصلی انجام نمی شود که این مسئله باعث بهم خوردن امنیت سیستم می شود.

برای جلوگیری از چنین نفوذی می توان امضای ADM را قبل از اولین اجرا تغییر داد. برای ایـن منظـور بایستی امضای نرم افزار را در فایل Adm.exe پیدا کرده و با کمک Pctools یا نرم افزار مشابه آنرا تغییر داده و تغییرات را ذخیره کرد. در اینصورت یک اجرای غیر مجاز با شکست مواجه می شود. چرا کـه در صورتـی که ADM اجرا شود امضای خود را روی دیسک سخت پیدا نمی کند و بنا براین دیگر ادامه دادن بـی فـایده است و منجر به پاک شدن Partition Table و User Definition می شود. البته عملکرد Admplus در این مورد فرق می کند . یعنی دیگر Partition Table پاک نمی شود ، بلکه فقط User Definition پاک میشود.

یکی دیگر از نقاط نفوذ پذیر این نرم افزار حافظه اصلی می باشد. پس از راه اندازی سیستم و قرار گرفتـن درایور Adm.sys در حافظه اصلی ، نحوه دسترسی کاربر بـه Partition هـا در قسـمتی از حافظـه اصلـی نگهداری می شود. با عوض کردن محتویات این قسمت از حافظه اصلی می توان دسترسی به پارتیشـن هـا را تغییر داده و به این ترتیب به قسمتی از دیسک سخت که دسترسی وجود نداشته ، دسترسی پیدا کرد. و یا اگـر دسترسی به صورت Read بوده است آنرا به صورت Write تبدیل کـرد. ایـن ایجـاد تغیـیر در محتویـات حافظه بعنوان مثال می تواند توسط دستورات داخلی Debug انجام شود.

برای جلوگیری از چنین نفوذی نیز روتینی تهیه شده که به صورت ماندگار (Resident) در حافظـه نصـب می شود و با استفاده از سرویس وقفه صفحه کلید (Keyboard Interrupt Service Routine) مانع از تغییر Access Right می شود. این کار با تست تغییر ایجاد شده در نحوه دسترسی پـس از فشـار هـر کلیـد و در صورت تغییر ، برگرداندن نحوه دسترسی به وضعیت اولیه انجام می شود. این برنامه محافظ می تواند در موقع راه اندازی مشابه درایور Adm.sys در حافظه بارگذاری شود. لیست برنامه کامپیوتری فوق الذکر در صفحـه بعدآورده شده است:

```
PROGRAM ADM_PROTECTOR;

{ $M 1024,0,0 }
USES DOS;

VAR
  KBD    : PROCEDURE;
  FOU    : BOOLEAN;
  ADD,I  : LONGINT;
  J      : BYTE;

PROCEDURE TEST;INTERRUPT;
 BEGIN
   ASM
     PUSHF
    CALL  KBD
   END;
   IF  (MEM[0:(ADD+38)]<>$0C) THEN
        MEM[0:(ADD+38)] :=  $0C;
   IF  (MEM[0:(ADD+39)]<>$03) THEN
        MEM[0:(ADD+39)] :=  $03;
   IF  (MEM[0:(ADD+40)]<>$52) THEN
        MEM[0:(ADD+40)] :=  $52;
 END;

BEGIN
 FOU:=FALSE;
 J:=0;
 FOR I:=0 TO $FFFF DO
  IF MEM[0:I] = $41 THEN
   IF MEM[0:I+1] = $44 THEN
    IF MEM[0:I+2] = $4D THEN
     BEGIN
      J:=J+1;
      ADD:=I;
      IF J=4 THEN
       BEGIN
        FOU:=TRUE;
        BREAK;
       END;
     END;
 IF  NOT FOU THEN
   HALT(1);
 IF  MEM[0:(ADD+36)] <> $CC THEN
  MEM[0:(ADD+36)] := $CC
 ELSE
   BEGIN
    WRITELN('PROGRAM ALREADY INSTALLED.');
    HALT(1);
   END;
 GETINTVEC($9,@KBD);
 SETINTVEC($9,ADDR(TEST));
 KEEP(0);
END.
```

√

بررسی مشکلات دیگر

در موقع اجرای برخی نرم افزارها بایستی مسیر جاری DOS آزاد (قابل نوشتن) باشد و اگر Read Only باشد آن نرم افزار اجرا نمی شود. مثلاً توربو پاسکال (TP) چون موقع اجرا یک swap file ایجاد می کند، اگر مسیر جاری Protect باشد ، با یک پیغام خطا متوقف می شود. اگر با کمک ADM دیسک سخت را به ۳ بخش (قسمت) مذکور در قبل تقسیم کرده باشید و قسمتهای اول و دوم (راه انداز - نرم افزارها) را مطابق توصیه ما برای کاربران عمومی Protect (Read Only) کرده باشید و فقط قسمت سوم Writable باشد و طبیعتاً نرم افزار TP را نیز روی بخش دوم دیسک سخت گذاشته باشید ، آنگاه یک کاربر عمومی نمیتواند آنرا اجرا کند.

برای حل این مشکل می توان از Path استفاده کرد. یعنی مسیر قرار گرفتن TP را در Path برای DOS تعریف کرده و آنگاه از روی درایو E: دستور Turbo را اجرا کرد.

اما این راه حل برای برخی نرم افزارها نامناسب است . بعنوان مثال برای SPSS مشکل با ترفند فوق حل نمی شود. در مورد چنین نرم افزارهائی که کار کردن با آنها چنین مشکلاتی دارد می توان از راه حل زیر استفاده کرد:

یک Batch فایل در Path قرار دهید و در آن مجموعه ای از دستورات که کارهای زیر را انجام دهند قرار دهید:

۱- فایلهای درایو E: (Writable) را حذف نماید.

۲- یک زیر شاخه (مثلاً بنام SPSS) روی درایو E: ایجاد نماید.

۳- تعدادی از فایلها را که نرم افزار جهت اجرا بدانها نیاز دارد از محل اصلی قرار گرفتن نرم افزار در داخل زیر شاخه ایجاد شده در قسمت قبلی کپی نماید.

۴- با تعویض مسیر جاری و رفتن روی مسیر جدید قرار گرفتن نرم افزار ، آنرا اجرا نماید.

نتیجه گیری

با عنایت به اینکه در مراکز آموزشی از کامپیوترهای شخصی به معنی واقعی کلمه استفاده نمی شود (کاربرد عمومی دارند) و لذا علاوه بر امنیت فیزیکی بایستی تمهیدات دیگری در اینگونه سیستمها در نظر گرفته شوند و با توجه به ضعف های امنیتی سیستم عامل باز DOS ، گفتیم که لازم است از ابزارهای کمکی ایجاد امنیت مانند ADM استفاده شود. در بررسی اولیه مشخص کردیم که اینگونه نرم افزارهای کمکی چه نیازهای امنیتی را بایستی برآورده کنند که با توجه به بررسی امکانات ADM این نرم افزار مناسب بنظر رسیده و مورد استفاده قرار گرفته است. پس از بررسی چگونگی ایجاد امنیت توسط این نرم افزار ، راههای برهم زدن امنیت ایجاد شده توسط آن شناسائی و روشهای جلوگیری از اخلال در امنیت نیز ذکر شدند. البته با بکارگیری ترفندهای ذکر شده در مقاله ، امنیت مورد لزوم ایجاد شده توسط ADM و برنامه کمکی مطرح شده (Adm_protector) تا حدود زیادی کافی بنظر می رسد . لیکن پیشنهاد می شود که در طراحی و برنامه نویسی نرم افزارهای اینگونه در آینده دقت بیشتری صرف شده و همه امکانات لازم برای افزایش امنیت یک نرم افزار ایمن کننده از ابتدا درون نرم افزار پیش بینی شود تا دیگر نیازی به استفاده از Patch هائی شبیه Adm_protector نباشد. به امید آینده ای بلند و روشن.

مراجع

1.Jonathan L. Mayo , " Computer Viruses ",
Windcrest books ,1989

2.Microsoft , " MS-DOS version 5 , user's guide and refrence for the MS-DOS operating system " ,Goldstar Technology , 1991

3.C. Sandler , T. Badgett , L. lefkowitz , " VAX Security , protecting the system and the data " , J. Wiley & sons , 1990

4.MITAC , " Technical Refrence of ADM " , 1987

5.MITAC , " Technical Refrence of ADMPLUS " , 1991

6.Joseph Wikert , " The first book of the NORTON UTILITY 7 ",
Prentice Hall , 1991

7.Peter Norton , R. Ashley , J. Fernandez , " Advanced DOS 6 " ,
Prentice Hall , 1993

8.From the makers of Pctools , " PCTOOLS 8.0 User's Manual " ,
Central Point Software Inc. , 1983-90

۹- جابر هاشمی اصل ، راهنمای جامع توربو پاسکال ۷ برای برنامه نویسان ، کانون نشر علوم ، دی ماه ۱۳۷۳